Cavirin CyberPosture Intelligence for the Hybrid Cloud

Cavirin User Guide – Winter, 2019

February 12, 2019

Table of Contents

Introduction

The *Cavirin User Guide* describes regular use of the Cavirin system. At a high level, regular use includes:

- Specifying the credentials that the Cavirin system must present to computing resources in a data center or to cloud environments.
- Discovering assets in computing environments that exist in an on-prem data center, a cloud, or both.
- Assessing the discovered assets in a cloud or on-prem for the security posture (in the form of a score).
- Analyzing the assessment results.
- Remediating security risks.

The regular users for whom this *Guide* is intended will have a role of Group Admin, Devops, or Analyst, and to a lesser extent, a user logged in as Super Admin.

The *Guide* and the uses begin after the Cavirin system has been set up and is ready to use, and the Super Admin has provided a password for your role. (One of the tasks you can do after first-time login is change your password and other details in your profile.)

This *Guide* is intended primarily for individuals with the role of Group Admin, DevOps, or Analyst, and to a lesser degree, a user in the Super Admin role. These roles are part of Cavirin's use of a security enhancement, role-based access control (RBAC). RBAC enforces a scheme of confining capabilities to different roles. The Super Admin assigns new users to one of the default roles.

Many variations exist in the computing environments and use cases, so the workflow descriptions refer you as needed to document sections that apply to your organization.

> **NOTE**: Users in a non-admin role should have the knowledge and operational parameters for the cloud and on-prem environments of your organization. Also, for cloud accounts, you should be experienced with navigating the cloud provider's portal and configuring the cloud services.

The core documents for the Cavirin system are an admin guide and a user guide:

- The *Cavirin Administrator Guide* focuses on pre-operational setup, initial system setup, and maintenance tasks. These tasks can involve activities in the CLI, in the Cavirin UI, and in the management portal of a cloud. The *Administrator Guide* is first directs the Cavirin Super Admin to set up the system and the desired services on the back end. A user who is logged into the Super Admin role has capabilities that only the Super Admin role supports. In its later tasks, the *Administrator Guide*

directs a user—possibly the same person as the Super Admin—logged in the role of Group Admin for tasks the Super Admin cannot perform.

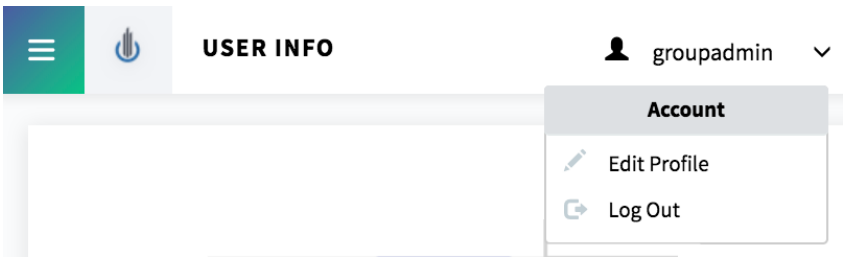
- This *Cavirin User Guide* contains detailed descriptions for regular operation. In general, the focus is on discovery and assessment of on-prem resources or cloud resources (operating systems or cloud services); reporting on the assessment; analyzing the results; and manually or automatically remediating the issues. Nearly all tasks in this *Guide* are for roles other than Super Admin.

How to Change Your User Profile, Including Password

As a Group Admin, Devops engineer, or Analyst, your account has been set up by the system administrator. You can change your profile and, for items not accessible in the profile, discuss them with the Super Admin. The place to access your profile is under your login name, which appears in the upper-right corner of the UI.

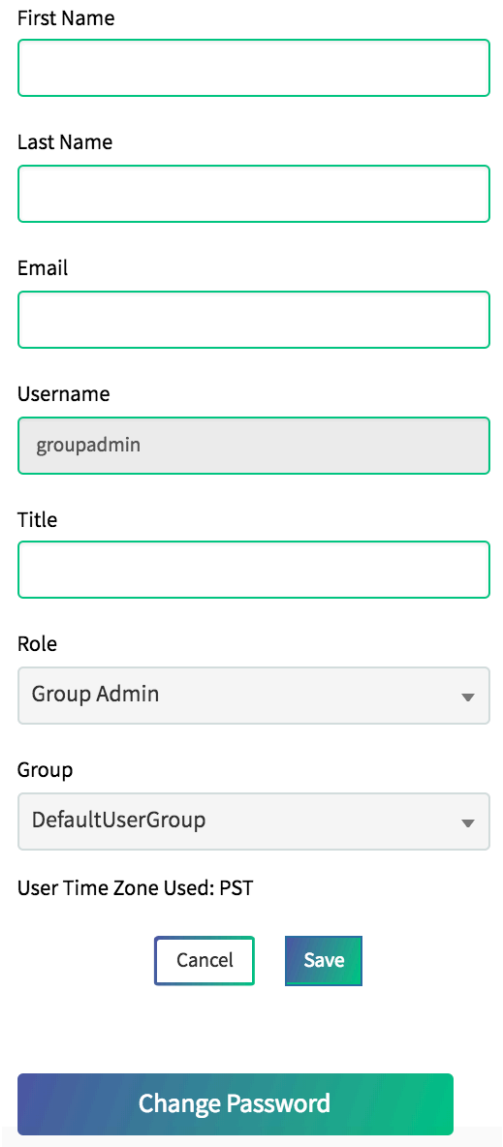
To change your profile:

1. Click **Edit Profile** in the dropdown next to your current login name in the upper-right corner of the UI (next figure).

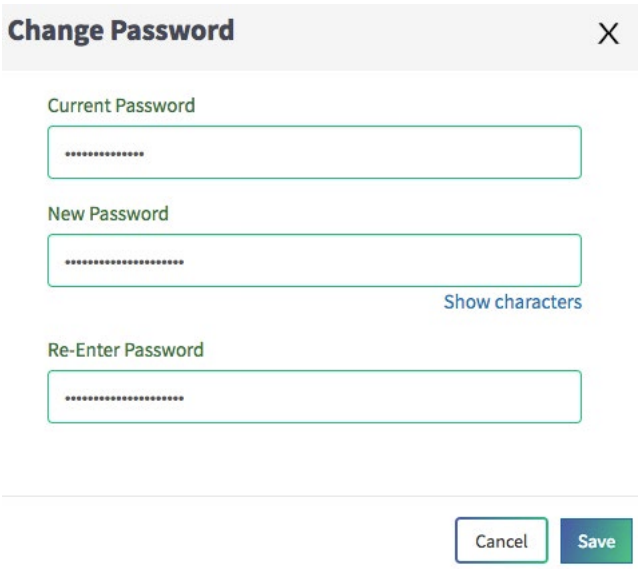


The popup with your profile appears in the subsequent figure. The values you can change are in white and the fields you cannot change, in gray.

2. Modify as needed the fields and click **Save** if not changing the password (step 3).



3. To change the password, click **Change Password** at the bottom of the popup. Another popup opens, as the next figure illustrates.
4. Type the current password, type the new password, and re-type it.
5. Click **Save**.


Change Password
Current Password
New Password
Show characters
Re-Enter Password
Cancel
Save

Add Credentials for Clouds and On-prem Hosts

Before the Cavirin system can communicate with your organization's computing assets or cloud environment, the assets or cloud can authenticate Cavirin by checking the user-configured credentials that Cavirin offers to those computing resources or cloud accounts. In any default role other than Super Admin, you can specify multiple sets of credentials for any environment, as needed:

- The Cavirin system offers *cloud credentials* so it can get access to a cloud environment.
- The Cavirin system Cavirin offers *host credentials* to resources that have an OS and are on-prem in Docker (in Docker Image or AWS in the current release).
- To specify IAM credentials for an AWS account, go to Configuring IAM Role Credentials for an AWS Cloud.
- To specify ARN credentials for an AWS account, go to Configuring ARN Credentials for AWS.
- To specify Access Key/Secret Key credentials for an AWS account, go to Configuring Access Key and Secret Key Credentials.

  Optional configurations for AWS are:

  - Setting Up Auto-remediation with Lambda (see Lambda Remediation for additional details).
  - Monitoring an AWS Cloud.
- To create credentials for Azure, go to Adding Credentials for Microsoft Azure.
- To create credentials for Google, go to Adding Credentials for Google Cloud.
- To create on-prem credentials, go to Creating Host Credentials.

You configure AWS cloud credentials in the AWS cloud and then copy them to the Cavirin system. Choices for AWS credentials are:

- IAM Role.
- An Amazon Resource Name (ARN) uniquely identifies an AWS resource. (AWS needs an ARN if a resource is to be specified unambiguously across all of the AWS environment.) An ARN can apply to IAM policies, Amazon Relational Database Service (Amazon RDS) tags, and API calls, for example.
- Access Key and Secret Key (AKSK).

NOTE: One of the credential parameters is *Usage*—global or restricted. When feasible, use a restricted credential because it is more specific to the targeted resources and efficient. The global credentials are offered to all assets.

Adding IAM Role Credentials for an AWS Cloud

The screen for adding an AWS cloud account with IAM Role is divided as follows:

- At left, the steps performed on the Cavirin system.
- At right, a description of steps performed in the cloud itself.
- Some values you enter in the cloud are also added to the Cavirin configuration.

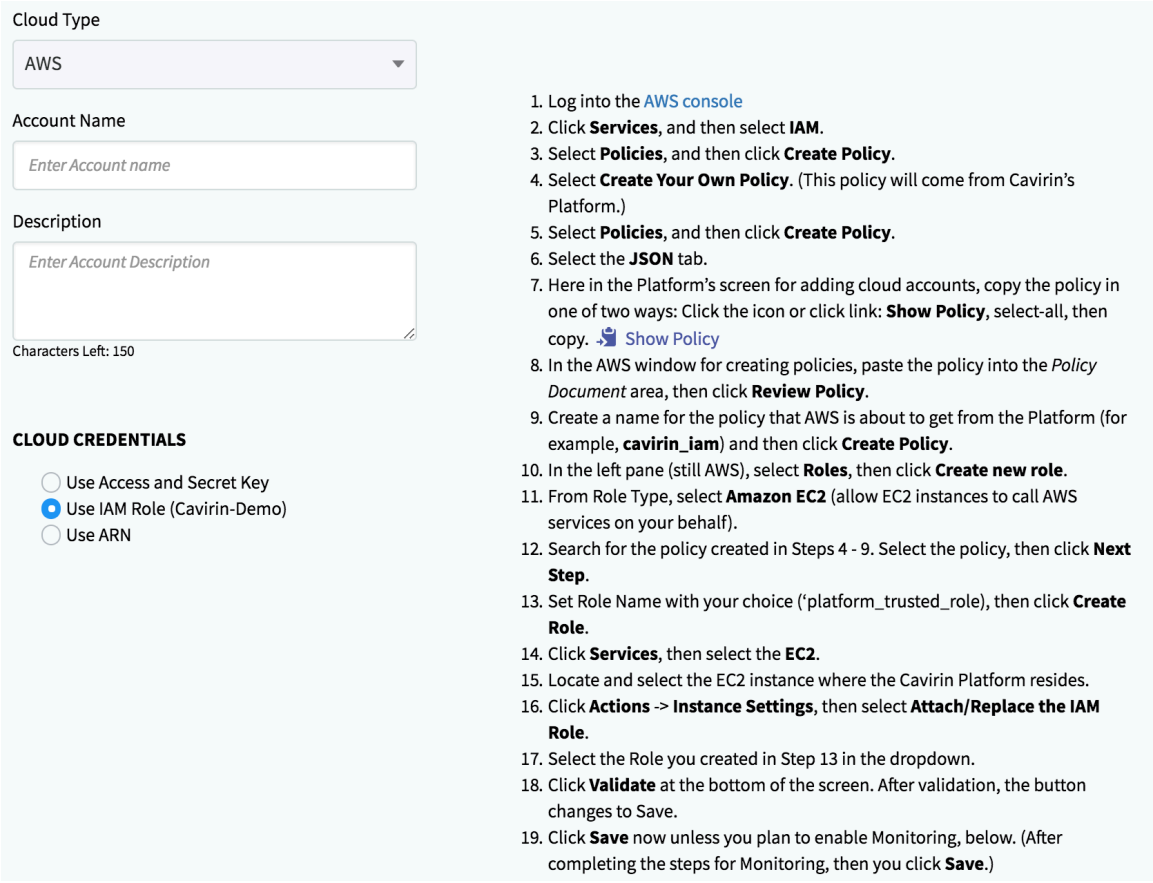
NOTE: The following steps are current. Use these steps if the UI appears different.

1. Log into the AWS Console.
2. Click **Services** at upper-left in the banner; a page with services opens: under *Security, Identity, and Compliance,* click **IAM** to open *Identity and Access Management*.
3. Click **Policies** in the navigation pane. The policies creation page opens; click **Create Policy** at upper-left.
4. Click **Create Your Own Policy**. (This policy will come from Cavirin.)
5. Click the **JSON** tab. A text-entry area for *Create Policy* opens.
6. In the Cavirin screen, copy Cavirin's policy in one of two ways: You can click the blue icon (see figure) or click **Show policy**, select-all, and then **copy** the policy.
7. In the AWS window for creating policies, paste the policy into the text-entry area (overwrite any default text); click **Review policy** in the lower-right corner to open the *Review Policy* page.
8. Type a name in the *Name* box for the policy you pasted and click **Create policy**.
9. In the left pane (still AWS), click **Roles** in the navigation pane; click **Create role**.
10. With the *AWS service* box highlighted, click **EC2** (notice the subtext "allow EC2 instances to call AWS services on your behalf").
11. Click the **Next: Permission** button at lower-right corner of the screen.
12. Search for the policy created in Steps 4 – 8. You can type the name in the search box. Mark its check box, and then click **Next: Review**. The *Review* page opens.
13. Type a role name in the *Role name* box; *description* is optional. Click **Create Role**. The Review page closes, and the new role now appears in the list of roles.

14. Click **Services** in upper-left corner, then click **EC2** (under *Compute*).
15. In the nav pane, click **Instances**; locate and select the Cavirin EC2 instance.
16. Click Actions > Instance Settings > Attach/Replace the IAM Role.
17. Select the role in the IAM role* dropdown (from Step 13). Click **Apply** then **Close**.
18. Back in the Cavirin UI, click **Validate** at bottom-right. After validation, the button changes to *Save*.
19. Click **Save** now unless you plan to enable Monitoring or Lambda remediation, below. (After completing any subsequent steps, then you click **Save**.)

Adding a cloud account ends with **Validate** and then **Save** (unless you plan for monitoring or auto-remediation with AWS Lambda). As needed, see How to Set Up Monitoring of AWS Clouds before you proceed because of the alternate sequence. With monitoring, the final sequence is:

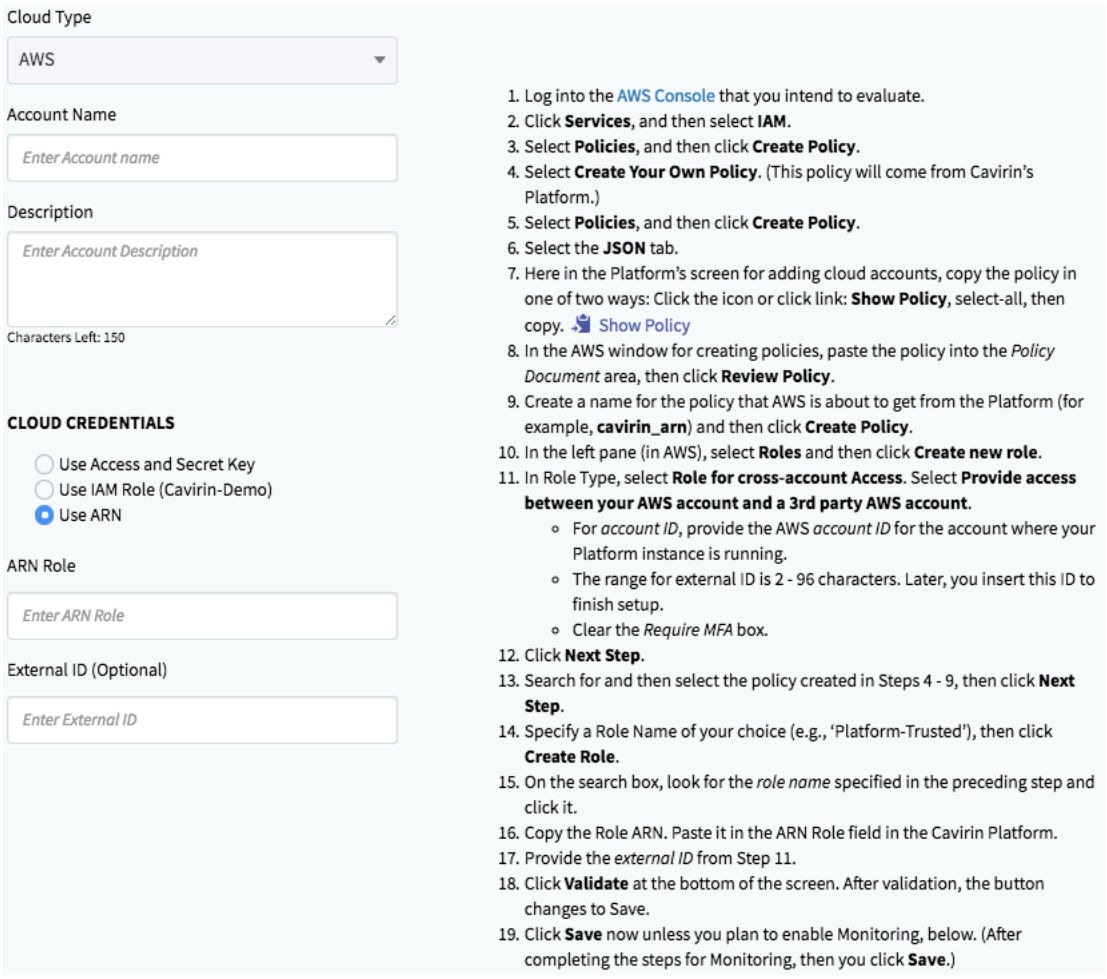
1. Click **Validate**. After validation finishes, the button changes to *Save*.
2. Complete the steps described in How to Set Up Monitoring of AWS Clouds.
3. Click **Save.**



Adding ARN Credentials for AWS

1. Log into the AWS account that you intend to evaluate (here: AWS Console).
2. Click **Services**, and then select **IAM**.
3. Select **Policies**, and then click **Create Policy**.
4. Select **Create Your Own Policy**. (This policy will come from the Cavirin's system.)
5. Click the **JSON** tab.
6. In the Cavirin Add Cloud Account screen, copy the policy in one of two ways: (1) Click the icon or (2) click **Show Policy**, select-all, and then copy it.
7. Paste the policy (copied from Cavirin in Step 6) into the text area in the AWS policy window; click **Create Policy**.
8. Type the name for the policy from the Cavirin system you pasted at Step 7.
9. In the nav pane at left (still in AWS), select **Roles** and then click **Create new role**.
10. In *Role Type*, select **Role for cross-account Access**. Select **Provide access** between your AWS account and a 3rd party AWS account.
    - For *account ID*, provide the AWS *account ID* for the account where your Cavirin instance is running.
    - The range for *external ID* is 2 - 96 characters. Later, insert this ID to finish setup.
    - Clear the *Require MFA* box.
11. Click **Next Step**.
12. Search for and then select the policy created in Steps 4 - 8, then click **Next Step**.
13. Specify a *Role Name* for your choice, then click **Create Role**.
14. On the search box, find the *role name* typed in the preceding step and click it.
15. Copy the Role ARN value. Paste it in the ARN Role field in the Cavirin UI.
16. Provide the *external ID* from Step 10.
17. Click **Validate** at the bottom of the Cavirin screen. After validation, the button changes to *Save*.

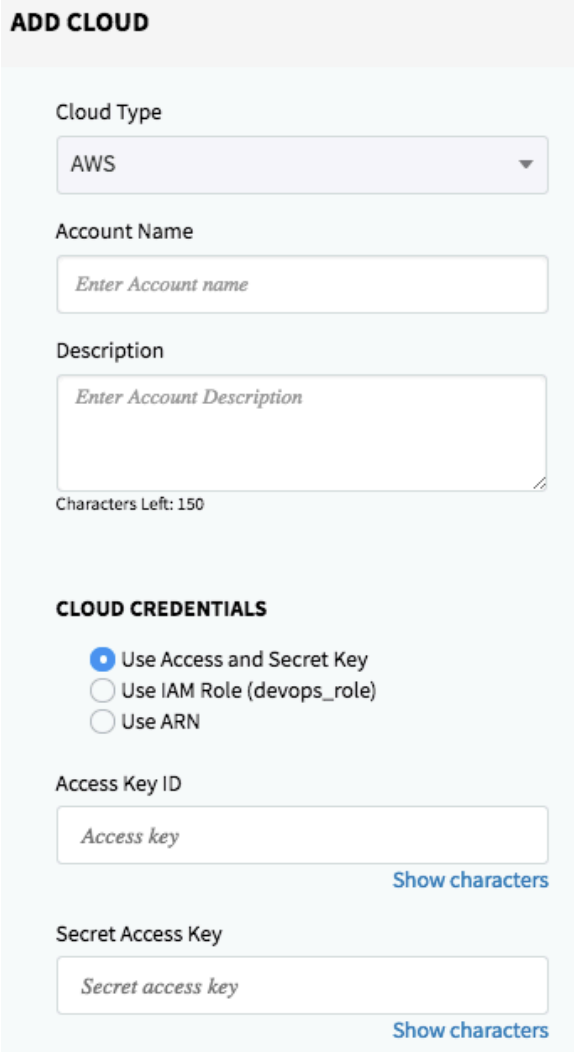
18. Click **Save** now unless you enable Monitoring (see How to Set Up Monitoring of AWS Clouds). (Then, after completing the steps for Monitoring, click **Save**.)



Adding Access Key and Secret Key Credentials

It is assumed that you have the Access Key ID and the Secret Access Key for AKSK credentials. Any default RBAC role other than Super Admin lets you add these credentials and otherwise configure the AWS cloud accounts on the Cavirin system.

Addition of a cloud account ends with **Validate** and then **Save** (unless monitoring of Lambda auto-remediation is planned). If your organization plans to enable monitoring, see How to Set Up Monitoring of AWS Clouds before proceeding because of the additional steps that monitoring and auto-remediation involve.



Enabling AWS Lambda Auto-remediation

Lambda auto-remediation is enabled on a per-account basis. The full process for configuring Lambda remediation on an AWS account has three locations:

- The AWS console
- The Cavirin CLI
- Cavirin's Add Cloud Account page—the subject of this section

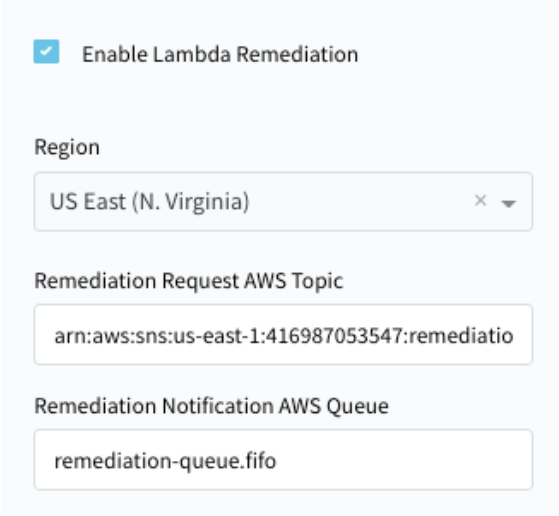
For a description of the steps in the CLI and the AWS console, refer to the *Cavirin Administrator Guide*. The steps on the CLI determine the region in Step 2, below, and provide the *AWS Topic* and *AWS Queue* for Steps 3 and 4.

IMPORTANT: Before you enable the AWS Monitoring or Lambda remediation feature when you add the AWS account to Cavirin, the Super Admin must have already set them up in the Cavirin back end, as described the *Cavirin Administrator Guide*.

NOTE: AWS Monitoring can monitor environments in in any region. However, the monitoring program runs in only certain regions. Currently, Monitoring and Lambda remediation can run in at least six regions: US East (N. Virginia), US East (Ohio), US West (Oregon), EU (Ireland), and more.

To enable auto-remediation through Lambda for an AWS account:

1. Mark the Lambda check box (next figure).
2. Select the region where this Lambda remediation applies.
3. Type or paste the Remediation Request AWS Topic. (The Group Admin or Super Admin can provide the value of *Topic*.)
4. Type or paste the name of the queue for *Remediation Notification AWS Queue*. (The Group Admin or Super Admin can provide the value of the *Queue*.)
5. Click **Validate** in the lower-right corner of the page. After validation completes, the *Validate* button changes to *Save*.
6. Click **Save** (not shown in the next figure).



For the description of how to trigger Lambda remediation in the Dashboard, see Using Lambda Auto-remediation in the Dashboard.

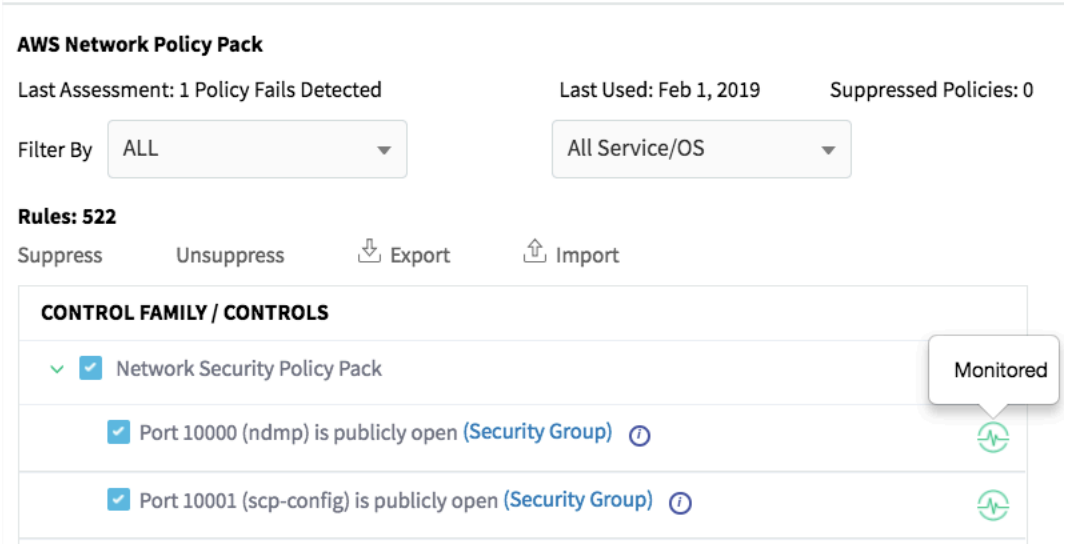
WARNING: Remediation is irreversible, so Cavirin prompts you to confirm remediation.

Monitoring an AWS Cloud

In addition to assessing resources and AWS services, Cavirin can *monitor* for events in a cloud. The purpose of cloud monitoring is to identify suspicious activities and possible intrusion attempts. The types of events that Cavirin monitors are a subset of all AWS event types. Cavirin selected these event types as the most relevant to monitor for security. For example, *security group* is a type of event.

Furthermore, in policy packs with rules that pertain to cloud monitoring, a green graphic shows the rules that can be monitored in the environment if you enable monitoring in the *Add Cloud Account* page. At lower-right, the next figure illustrates how green indicates the rule's potential for monitoring in the *Browse & Tailor Policy Packs* screen for the *AWS Network Policy Pack*. Near the upper-left corner of the figure, the number of rules in this policy pack is shown.

If Lambda remediation is enabled and a rule violation is corrected, and the correction status appears in the *Monitor* > *Alerts* display. See Viewing Alerts for an example of the Alerts page.



> **NOTE**: *In the current release*, event monitoring is enabled in all AWS cloud accounts by default. The monitoring variables that can be configured are specified by the system administrator (Super Admin or GroupAdmin role), as described in the *Cavirin Administrator Guide*. Because monitoring is enabled by default, the regions of all asset groups in the cloud are monitored. However, the response to monitored events is where things become specific—specific to regions and specific to asset groups.

The tasks for configuring the Monitoring feature on an AWS account has three locations:

- The AWS console (described in the *Cavirin Administrator Guide*)
- The Cavirin CLI (described in the *Cavirin Administrator Guide*)

- Cavirin's Add Cloud Account page, the subject of this section—but not *in the current release* because monitoring is enabled in all cloud accounts by default.

The steps on the CLI (*Cavirin Administrator Guide*) determine the *region* and Monitoring *queue* you specify in How to Enable Monitoring of AWS Clouds, below. In that section, step 1-a is for specifying the region, and step 1-b is for providing the *Monitoring queue*.

- **IMPORTANT**: If you want to create cloud credentials (add an AWS cloud account) without enabling Monitoring or Lambda, go to Add Credentials for Clouds and On-prem Hosts.

The monitored events are defined in AWS policy packs. For example, an asset group applied to a cloud account is monitored for all the rules in the following policy pack:

- AWS Network Policy Pack

When a monitored event is detected, the information goes into the *Monitor > Alerts* screen. If the threshold of events is crossed during a 10 to 15-minute window in the cloud, an assessment automatically is initiated. After the auto-assessment begins, the event count is reset. However, if an assessment on the asset group has been initiated, the auto-assessment does not run.

The system administrator can adjust the threshold if you are flooded with excessive events. Such a situation also could cause excessive reporting activity.

> **NOTE**: In the current release, no automatic notification is transmitted when an event threshold is crossed, you should periodically check the Reports screen to see if an unexpected assessment has run. You can also check the *Monitor > Alerts* page to see alerts for the period specified in the upper-right corner of the page. See Viewing Alerts for an example of the Alerts page.

Enabling the Monitoring Feature in an AWS Region

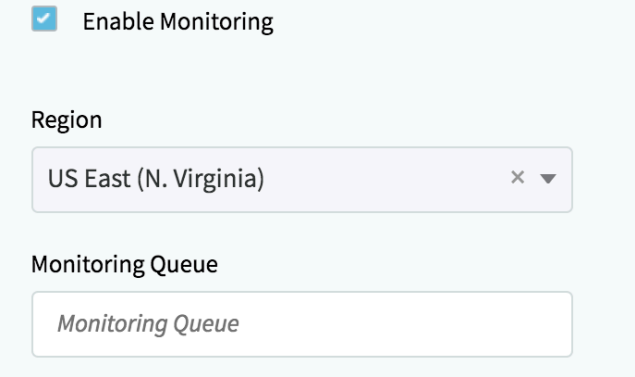
> **NOTE**: In the current release, monitoring is on by default. Before you specify the details for monitoring in a cloud account, the system administrator can tell you the region where the monitoring program runs and the name of the monitoring queue, values you specify when adding the cloud account. Subsequently, when you identify the cloud account and an asset group in the *Identify > Discover & Assess Resources* screen, that is the point where you name the regions *where the assets exist* (rather the region where monitoring runs).
>
> Also, although you cannot affect the threshold at which monitored events automatically trigger an assessment, the sysadmin can adjust the threshold and, therefore, how often auto-assessments run.

Monitoring and Lambda auto-remediation are configured for the Cavirin system at the back-end. A system administrator must have set up the monitoring or Lambda auto-remediation before you can enable it in the *Add Cloud Account* page.

The monitoring and Lambda remediation programs run in a limited set of regions but can monitor events and remediate issues in any region. The regions where monitoring and Lambda run have already been specified by the system administrator. For your tasks, the regions you specify in the *Discover & Assess Resources* wizard are the regions where resources to be assessed reside. (In the current release of this *Guide*, AWS supports monitoring and Lambda programs in the following regions: US East (N. Virginia), US East (Ohio), US West (Oregon), EU (Ireland), Asia Pacific (Sydney), and Asia Pacific (Tokyo).

To enable monitoring of the environment of the selected AWS account:

1. Mark the *Enable Monitoring* checkbox. The screen subsequently displays two parameters for you to specify.
    a. Select a region in the dropdown.
    b. Type or paste from AWS the name a monitoring queue (for example, **example-monitoring-queue.fifo**).
2. Click Validate.
3. Click **Save** after validation completes.



Adding Credentials for Microsoft Azure

This section describes how to add the credentials and specify a Microsoft Azure account to the Cavirin system. Any default RBAC role other than Super Admin enables you to access this function. The site of the configuration steps alternates between Cavirin's Add Cloud Account screen and the Azure Management Portal. You should understand your organization's Azure presence before executing these steps. As the description in this procedure indicates, Cavirin supports *RM type* cloud credentials for Azure.

The steps for specifying the credentials and adding or editing the account begin after you navigate to **Protect** > **Cloud Credentials**. You click **Add Cloud Account** for a new Azure account or select an existing Azure account and then click **Edit**.

NOTE: To complete the steps in Azure, you must have the role of *owner* in Azure.

IMPORTANT: The steps that follow are current. The steps in this section and the steps included in the UI (for convenience) are the same. However, if a change to the procedure occurs, for example, if a component changes in the Cavirin UI or the CSP's UI, the most up-to-date steps are in this *User Guide*.

1. Type a name for new the Azure account that the Cavirin system uses locally. (For editing, you have already selected it for editing by this time.) The name does not need to match the account name entered in the Azure UI.
2. Type a description as needed.
3. Log into the Azure Management Portal.
4. Go to Azure Active Directory. (A frequent Azure user easily finds this in the blade at left, but a new Azure user will have to search for it.) Click **Properties**.
5. Copy the directory ID.
6. In Cavirin, paste the *directory ID* value into the **Tenant ID.**

NOTE: For the first-time use of the next step, you locate *App registration* by clicking **More Services** at the bottom of the navigation pane. Thereafter, *App registration* appears as a favorite, outside *More Services*.

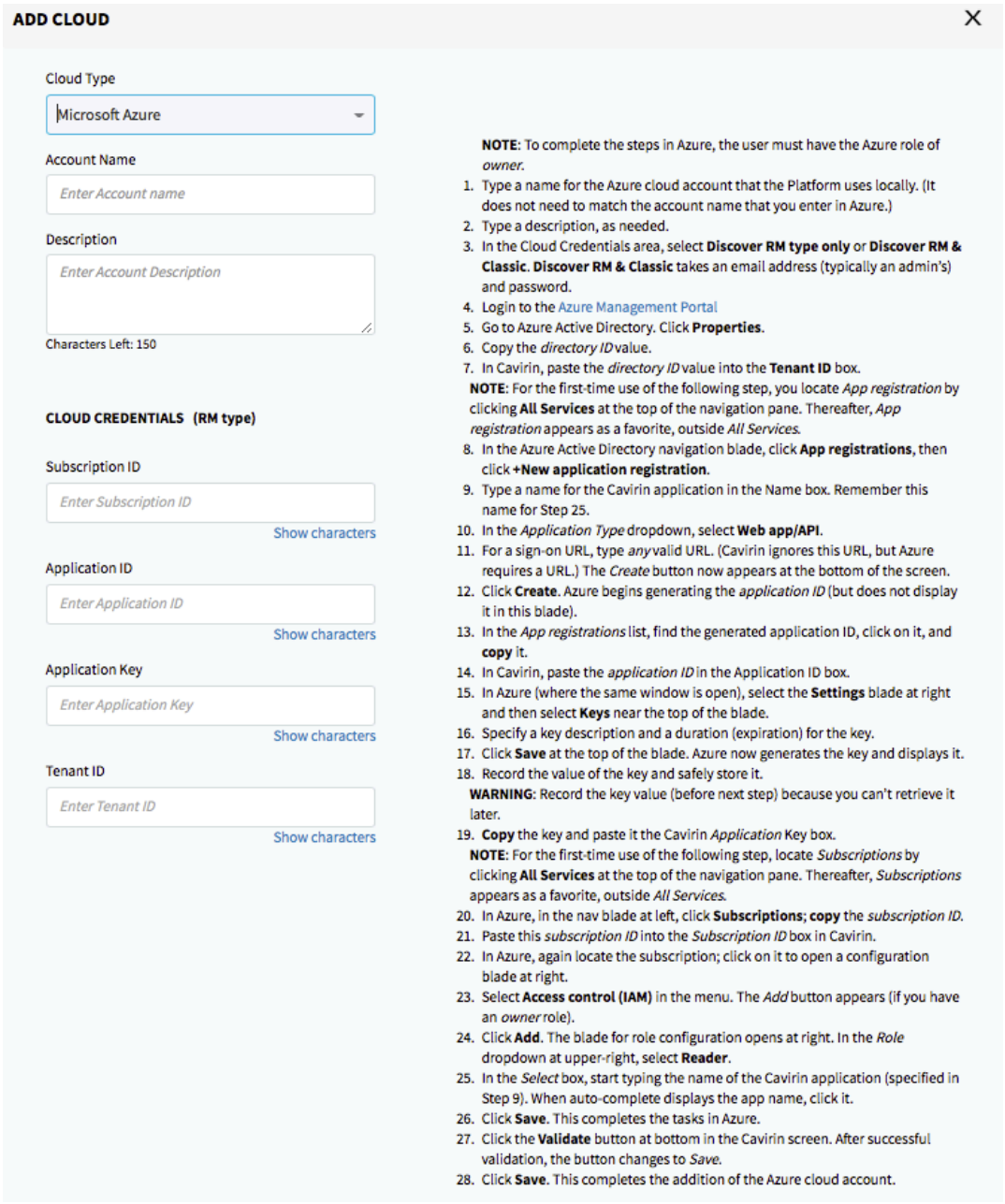
7. In the Azure Active Directory navigation blade, click **App registrations**, then click **+New application registration**.
8. Type a name for the Cavirin application in the Name box. Remember this name.
9. In the *Application Type* dropdown, select **Web app/API**.
10. For a sign-on URL, type *any* valid URL. (Cavirin ignores this URL, but Azure requires a URL.) The *Create* button now appears at the bottom of the screen.
11. Click **Create**. Azure begins generating the *application ID* (but does not display it in this blade).
12. In the *App registrations* list, find, select, and copy the generated application ID.
13. In Cavirin, paste the *application ID* in the Application ID box.
14. In Azure (where the same window is open), select the **Settings** blade at right and then select *Keys* near the top of the blade.
15. Specify a key description and a duration (expiration) for the key.
16. Click **Save** at the top of the blade. Azure now generates the key and displays it.
17. Record the value of the key and safely store it.

WARNING: Record the key (before next step) because you can't retrieve it later.

18. **Copy** the key and paste it the Cavirin *Application Key*.

NOTE: For the first-time use of the following step, locate *Subscriptions* by clicking **More Services** at the bottom of the navigation pane. Thereafter, *Subscriptions* appears as a favorite, outside *More Services*.

19. In Azure, in the blade at left, click **Subscriptions**; **copy** the *subscription ID*.
20. Paste this *subscription ID* into the Cavirin UI's *Subscription ID* box.
21. In Azure, again locate the subscription; click on it to open a configuration blade at right.
22. Select **Access control (IAM)** in the menu. The *Add* button appears—if you have an *owner* role.
23. Click **Add**. The blade for role configuration opens at right. In the *Role* dropdown at upper-right, select **Reader**.
24. In the *Select* box, start typing the name of the Cavirin application (from Step 8). When auto-complete displays the app name, click it.
25. Click **Save**. This completes the tasks in the Azure management portal.
26. Click the **Validate** button at the bottom of the screen (not shown in next figure). After successful validation, the button changes to *Save* (also not shown).
27. Click **Save**. This completes the addition of the Azure cloud account.



Adding Credentials and Other Options for Google Cloud

This section describes the steps for adding a Google Cloud (GCP) account so that Cavirin can assess its resources and services. The DevOps or GroupAdmin users that executes these steps should understand your organization's GCP presence.

This section also has descriptions for how to enable Cavirin's optional monitoring and remediation in the Google Cloud. Before enabling these capabilities, monitoring or remediation (or both) at the organization level or project level must have been set up on

the Cavirin system's back end, as described in the *Cavirin Administrator Guide*. If in doubt, confirm with your system administrator that these capabilities are available.

Adding or Modifying Google Cloud Credentials

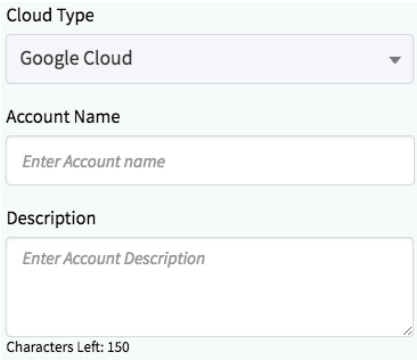
The sites for adding a cloud account alternate between the Cavirin *Add Cloud Account* screen and the Google Cloud Console.

> **NOTE**: If a change to the procedure occurs, for example, if a component changes in either the Cavirin UI or the CSP's UI, the most up-to-date steps are documented in this *User Guide*. Therefore, use the steps described below if the UI appears different.`````

The credential that Cavirin needs for accessing a GCP account is a key in JSON format.

1. Type a name for the Google Cloud account for the system to use locally. (It does not need to match the account name entered in GCP.)
2. Type a description, as needed.
3. In the *Cloud Credentials* area, select **JSON**.
4. Log into the organization's Google Cloud Console. https://cloud.google.com
5. Select the name of a project at the top of the screen; click **Open**.
6. In the upper-left corner, click the list icon (for *Products and Services*) to open a navigation pane.
7. Click **APIs and services** and select Dashboard (default). (You can bypass the dashboard by selecting).
8. Click **Enable APIs and Services**. You will use a search box to locate and enable two APIs (they might already be enabled).
9. In the *Enable APIs and Service* search box, type **Google Compute Engine API** to start searching for it. After finding it, click on the API.
10. Click **Enable** if this button is visible (otherwise, the API is already enabled).
11. In the same search box, type **Google Cloud Resource Manager API**. After finding it, click on this API. Click **Enable** if visible (otherwise, it is already enabled).
12. Again, in **APIs and Services**, locate and click **Credentials** (in the menu at left).
13. Click Create Credentials, and then select Service account key.
14. In the *Service account* dropdown, choose **New service account** (near the bottom of the list).
15. Type a name for the service account (for example, "Cavirin").

16. Access the *Role* dropdown and select the **Viewer** role.
17. For *Key type*, select **JSON**.
18. Click **Create**. GCP creates and downloads a key to your local system.
19. (This and the remaining steps are in the Cavirin system.) In the *Select JSON* box, **Browse** to and select the JSON file (downloaded in preceding step); click **Open**.
20. At the bottom of the screen for a new account, click **Validate** (not visible in the next figure). The *Save* button is already visible if this is an existing that account you are editing. After validation succeeds, the button changes to *Save*.
21. Click **Save** (not visible in the next figure) unless you also plan to enable monitoring or remediation. For these features, proceed to Enabling Remediation or Monitoring in a Google Cloud before you click **Save**.



1. Type a name for the Google cloud account that the Platform uses locally. (It does not need to match the account name that you enter in GCP.)
2. Type a description, as needed.
3. In the *Cloud Credentials* area, select **JSON**.
4. Log into the organization's Google Cloud Console.
5. Select the name of a project at the top of the screen; click **Open**.
6. In the upper-left corner, click the list icon (for *Products and Services*) to open a navigation pane.
7. Click **APIs and services** and select Dashboard (default). (You can bypass the dashboard by selecting **Libraries**.)
8. Click **Enable APIs and Services**. You will use a search box to locate and enable two APIs (they might already be enabled).
9. In the *Enable APIs and Service* search box, type **Google Compute Engine API** to start searching for it. After finding it, click on the API.
10. Click **Enable** if this button is visible (otherwise, the API is already enabled).
11. In the same search box, type **Google Cloud Resource Manager API**. After finding it, click on this API. Click **Enable** if this button is visible (otherwise, it is already enabled).
12. Again, in **APIs and Services**, locate and click **Credentials** (in the menu at left).
13. Click **Create Credentials**, and then select **Service account key**.
14. In the *Service account* dropdown, choose **New service account** (near bottom of the list).
15. Type a name for the service account (for example, "Cavirin").
16. Access the *Role* dropdown and select the **Viewer** role.
17. For *Key type*, select **JSON**.
18. Click **Create**. GCP creates and downloads the key in JSON format to your local system.
19. (This and the remaining steps are in the Cavirin system.) In the *Select JSON* box, **Browse** to and select the JSON file (downloaded with preceding step); click **Open**.
20. At the bottom of the screen for a new cloud account, click **Validate** (or **Save** if present). After validation succeeds, the button changes to *Save*.
21. Click **Save**.

Enabling Remediation or Monitoring in a Google Cloud

Enabling the monitoring feature or the remediation feature takes values that the administrator obtained during the back-end setup for these features, as described in the *Cavirin Administrator Guide*. The information you should get from the administrator is:

For Cloud Function Remediation

- Project ID
- Remediation request topic
- Subscription name

For Monitoring

- Project ID
- Subscription name

In Cavirin's current release, the following Google Cloud services are monitored:

- Cloud IAM
- Virtual Private Cloud
- Sub-network
- Compute Engine
- Cloud Storage (Object Store)
- BigQuery
- Cloud KMS
- Cloud SQL
- Spanner

The event types are configuration changes for the GCP Network or CIS GCP policies.

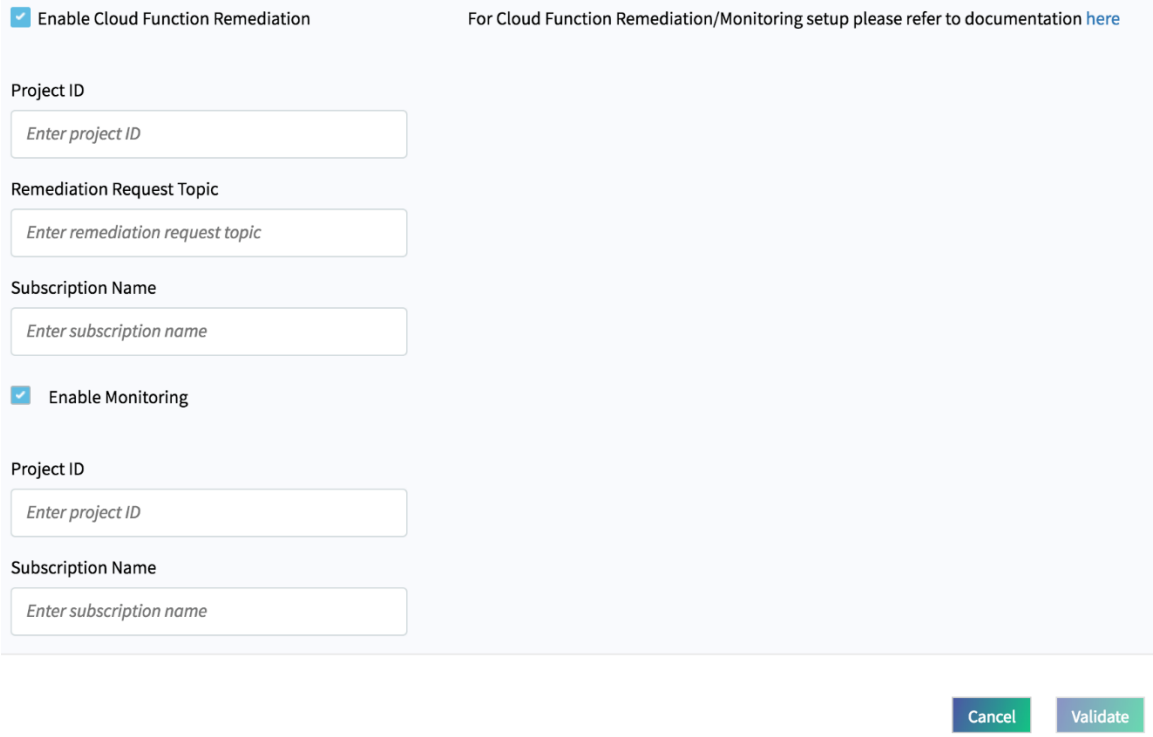
NOTE: In the steps that follow, the task ends when you save. However, if you have not yet validated the configuration of the other details of the cloud account, first you should *validate* the configuration. After validation, the *Validate* button changes to *Save*.

To enable remediation:

1. Mark the Enable Cloud Function Remediation checkbox; populate the fields.
2. Click **Save**.

To enable monitoring:

1. Mark the Enable Monitoring checkbox and populate the fields that appear.
2. Click **Save**.

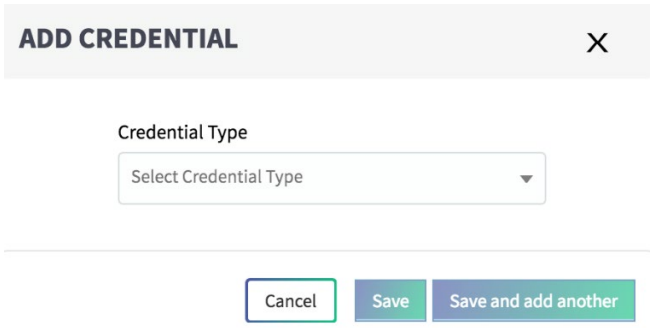


Creating Host Credentials

A resource with an operating system requests a host credential from the Cavirin system. The available host credential types are Windows Administrator, Linux – SSH, and Docker Host. The example for this section is Linux – SSH and a PEM key file for authentication.

To specify Linux – SSH host credentials (in any default role except SuperAdmin):

1. Navigate: **Protect** > **Host Credentials**.
2. Click **Add** in the upper-left corner of *Host Credentials*. The *Add Credential* popup opens. The popup is for selecting the credential type

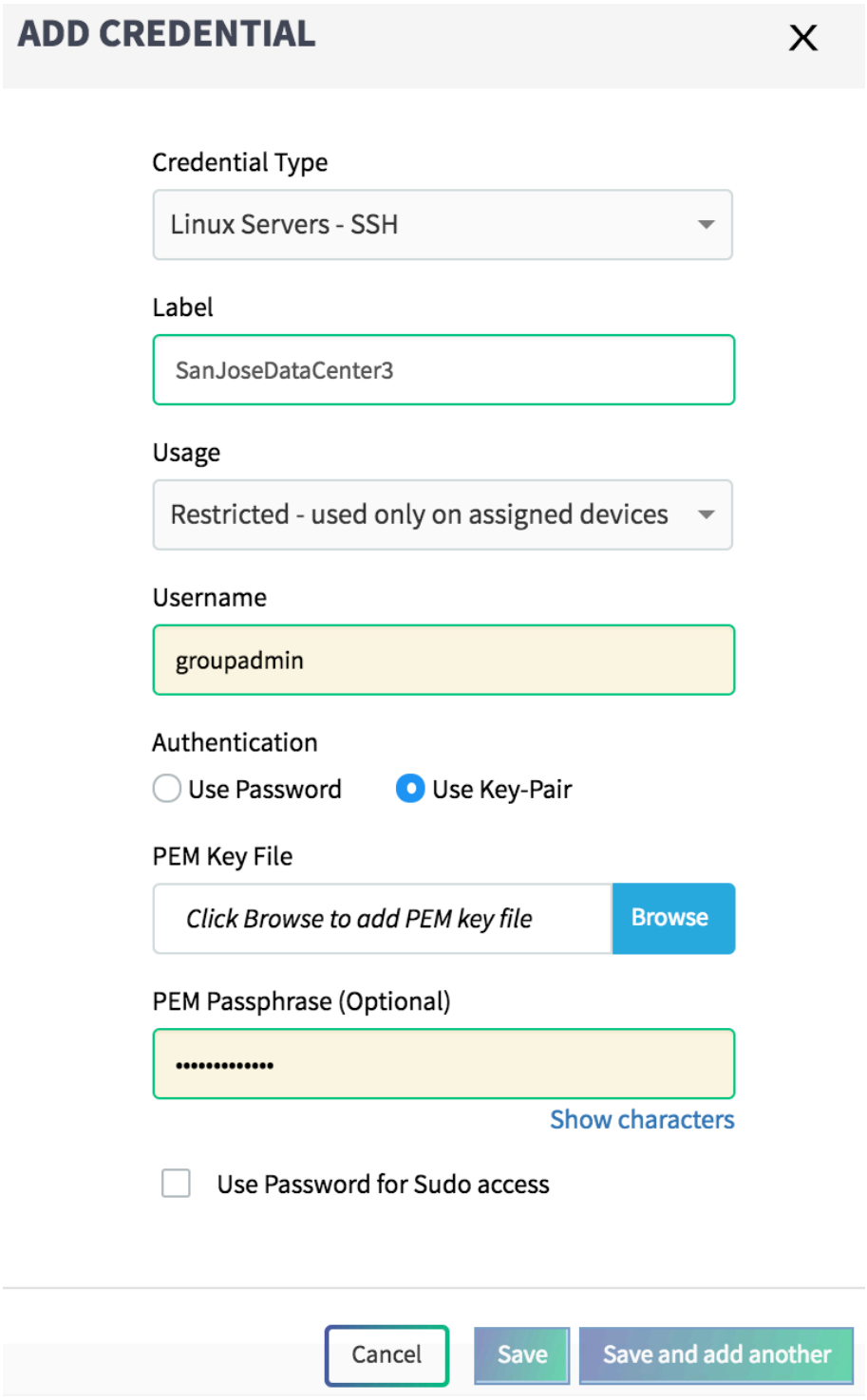


3. In the *Credential Type* dropdown, select **Docker Image** (which can be for an AWS or Docker Image), **Linux Servers - SSH**, or **Windows Administrator**. See next figure. The *label* in the figure is the name of this credential set. Subsequently, you identify the credential set by its label while editing or deleting the credential set or setting up a discovery and assessment in the Discovery wizard.

   The next step is for the Linux credentials. It is slightly more complicated than the Windows or Docker credential; this example can apply to Windows and Cloud host credentials.

4. Select **Linux Servers** for the credential type. The next figure shows the configuration popup and the default authentication method as PEM-key.

5. Type a meaningful name for this credential set in the Label box.



6. Choose a usage of *Global* or *Restricted*. Global means the Cavirin offers this credential to all hosts in the on-prem environment. Restricted means this credential is offered to hosts in a specific group of computing resources. Restricted is the more efficient of the two types of usage.

7. For Authentication, choose one of the following:
    - If you select **Use Key-Pair**, as in the next figure, click **Browse** to locate and select a PEM key file. Optional specifications are a passphrase for the key file and a password that must be provided by any user that wants to use **sudo**.
    - If you selected **Use Password**, type a password.
8. Select **Save** if done or **Save and add another** for another Linux credential set.

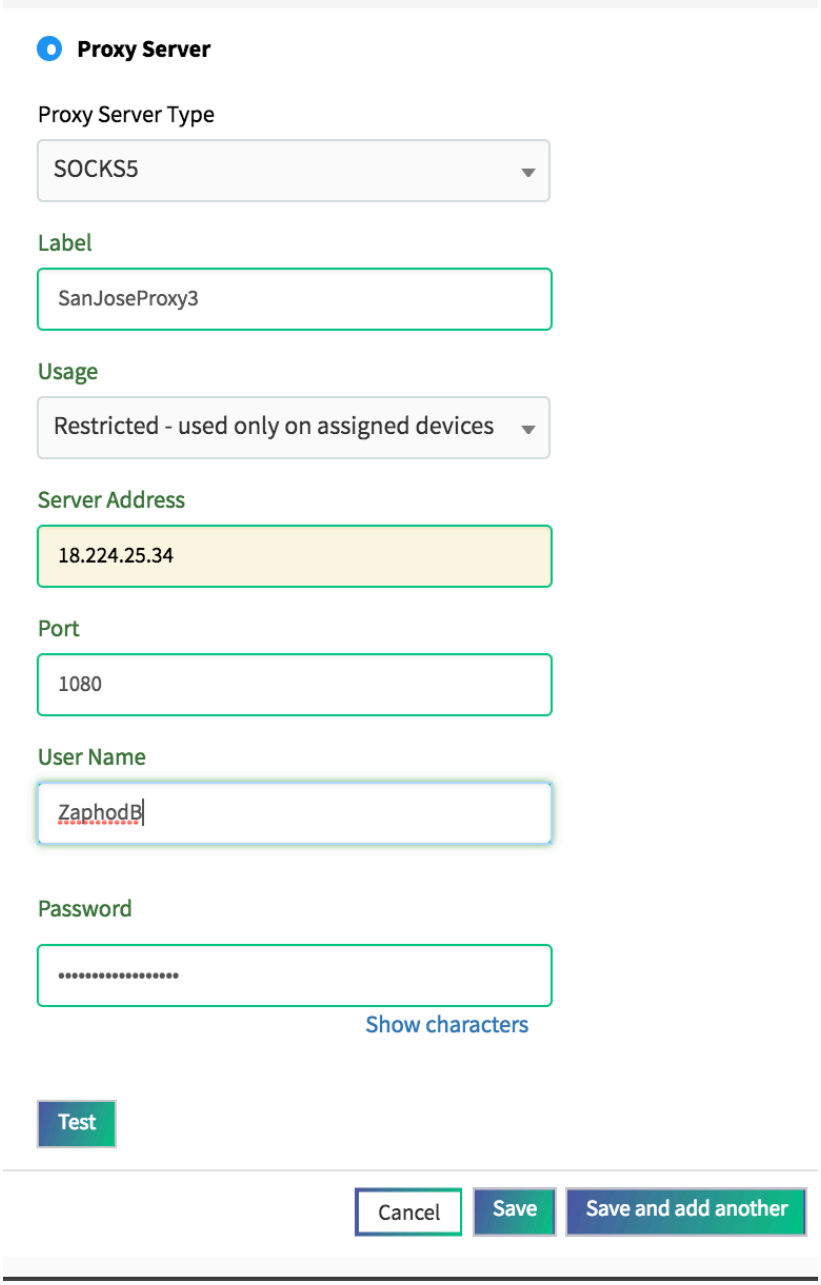
Specifying a Proxy Server

With the Group Admin or Devops rights, you can specify one or more proxy servers if your organization is using them. Their configuration resembles the specification of cloud or host credentials. Your organization (the system administrator) must provide the values for the configuration. For example, you need to know the:

- Type of proxy server, as shown by its protocol (HTTP, HTTPS, SOCKS4, or SOCKS5)
- IP address
- Port number of the proxy server: 80, 443, or 1080 (for either SOCKS protocol)
- Credentials the Cavirin system offers to the proxy (username and password)

To specify a proxy server:

1. Navigate: **Protect** > **Proxy Servers**.
2. Provide the details shown in the next figure.
3. Click **Test**. If you get an error message, check your information and consult the system administrator if a repeat test fails.
4. Click **Save** or **Save and add another**.

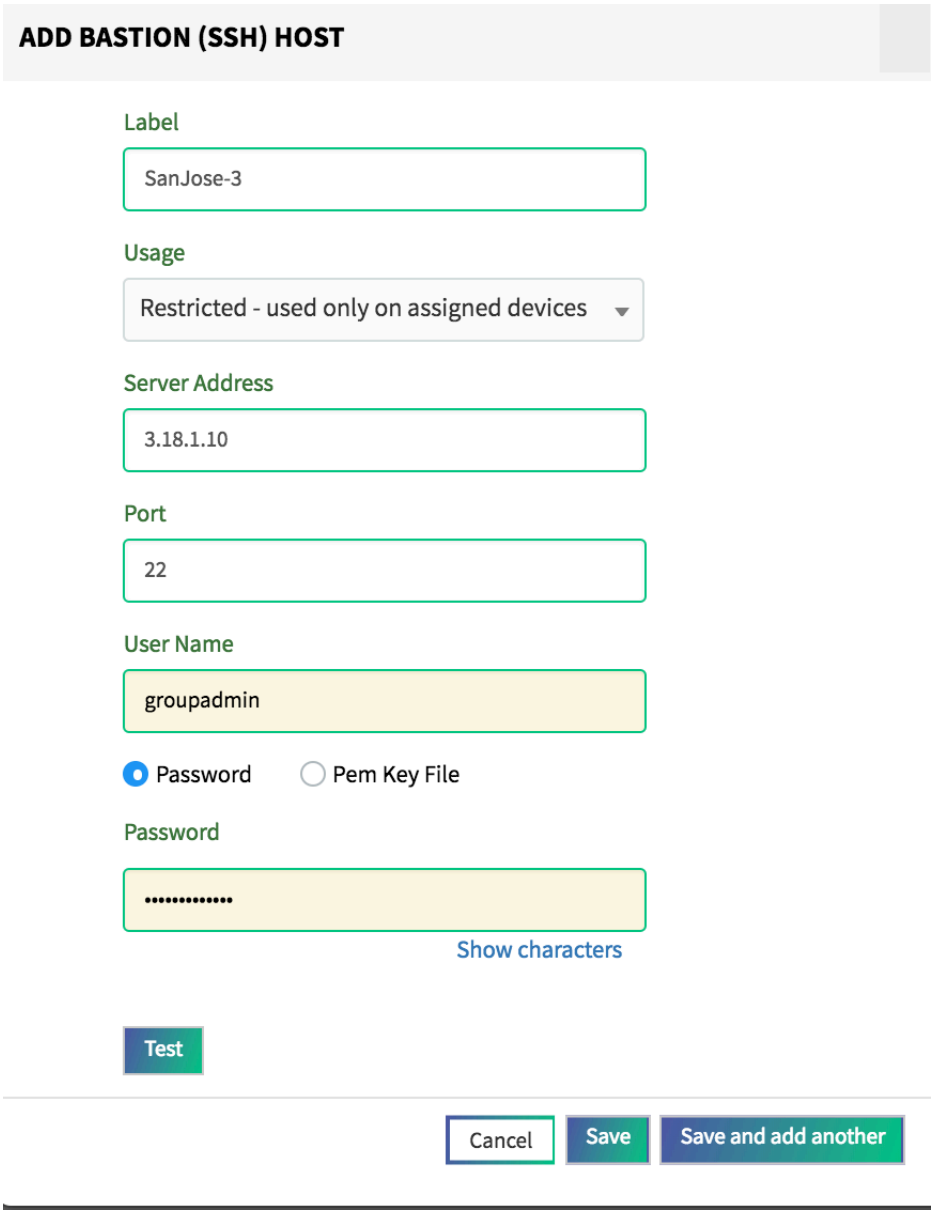


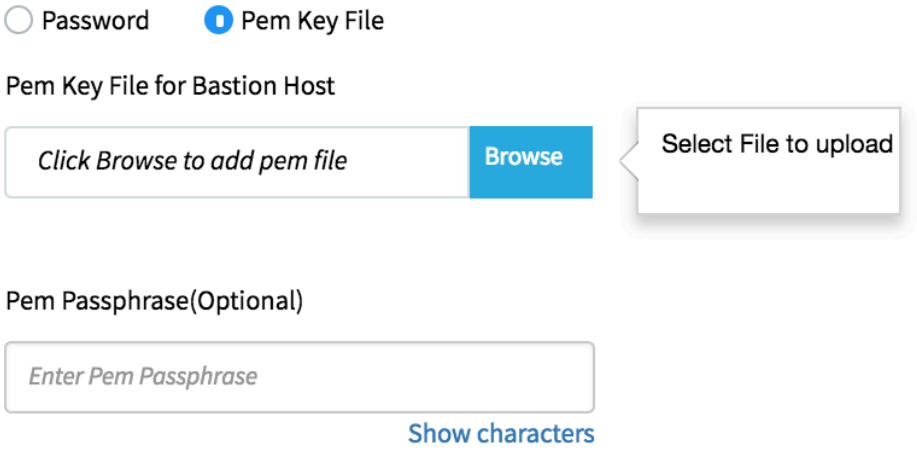
Specifying a Bastion Host

This section describes how to specify a bastion host in your environment to the Cavirin system. With the Group Admin or Devops rights, you can specify one or more bastion hosts if your organization has them. After a bastion host is configured, you can add it to an assessment you are configuring (see Discovering and Assessing Resources in AWS for an example use case).

No back-end setup by a system administrator is necessary before you specify a bastion host. However, the organization or system administrator must provide the details of the configuration to you. For example:

- Usage of the credentials that the Cavirin system offers, global or restricted
- IP address of the bastion host (server address)
- Port 22 because only SSH is used
- Username and password (next figure) or username and PEM key and passphrase if desired (as subsequent figure illustrates)




Password
Pem Key File
Pem Key File for Bastion Host
Click Browse to add pem file
Browse
Select File to upload
Pem Passphrase(Optional)
Enter Pem Passphrase
Show characters

Discovering and Assessing Resources in AWS

This section describes how to use the wizard to discover the AWS resources in an asset group; choose a policy pack to assess the groups assets; schedule an assessment or immediately assess; and then start the assessment based on your specifications. For the description of assets and asset groups, see Resource Groups and Asset Groups.

NOTE: Although you can run multiple assessments simultaneously across different environments, multiple assessments in one environment run sequentially.

NOTE: A subset of AWS policy packs supports Level 1 and Level 2 profiles for security stringency (Level 2 profile *extends* the Level 1 profile). In the current release, the policy packs that support profiles are CIS AWS Cloud and Cavirin Web Application. In general, the effect of policy profiles at Level 1 and Level 2 have the following general traits:

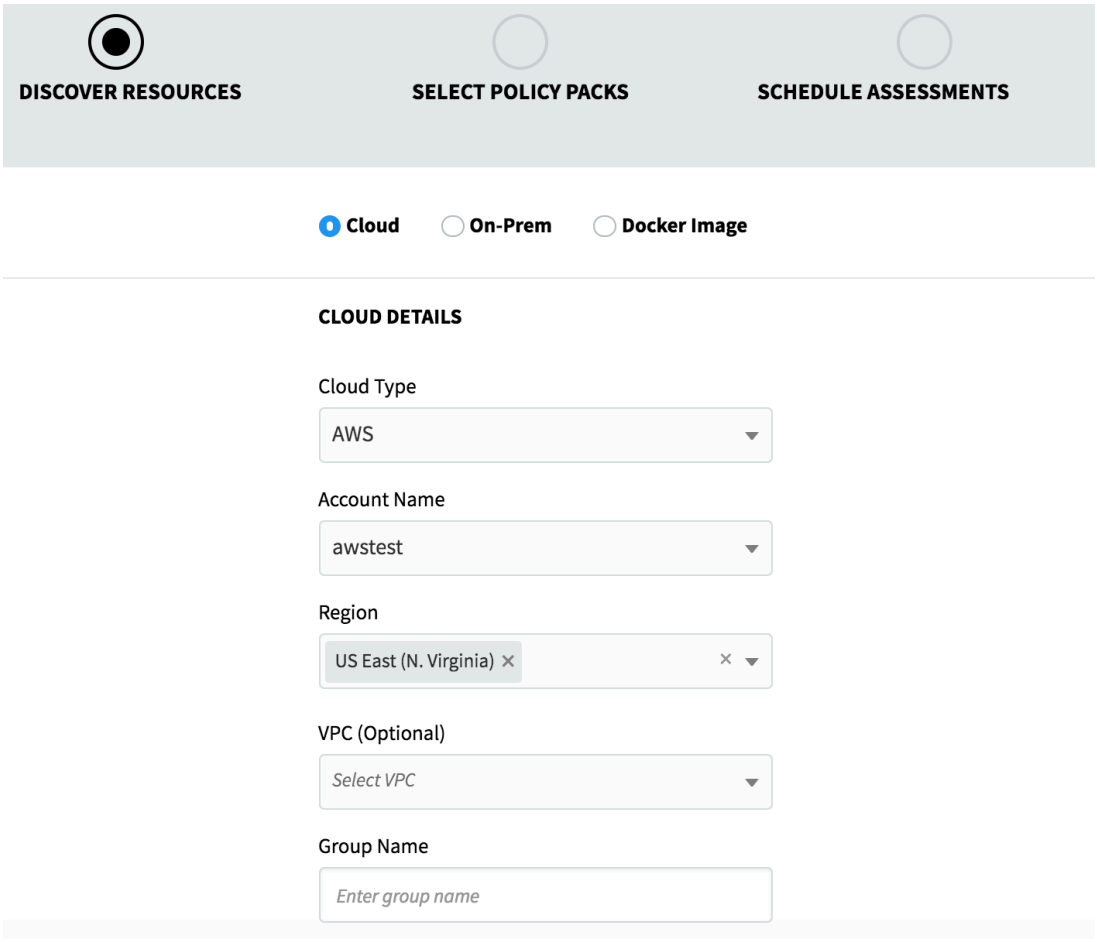
- Policies in a Level 1 profile exhibit one or more of the following characteristics:
  - Are practical and prudent
  - Provide a clear security benefit
  - Do not inhibit the utility of the technology beyond acceptable means
- Policies in a Level 2 profile exhibit one or more of the following characteristics:
  - Intended for environments or use cases where security is extremely important
  - Act as a defense-in-depth measure
  - Can lower the utility or performance of the technology

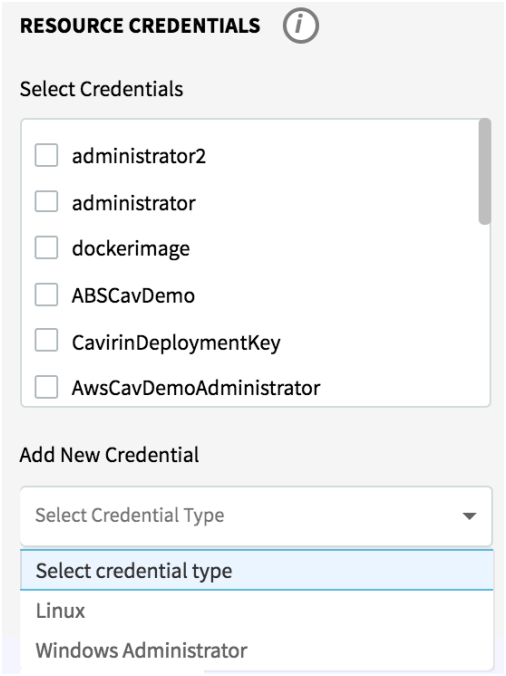
NOTE: For existing groups, go to **Identify** > **Asset Groups**. Select a group and click **Assess**.

To create a new asset group, discover its resources, and then either exit or select policies packs and assess those resources:

1. Navigate: **Protect** > **Discover & Assess Resources**.
2. Keep the default environment (Cloud). The portion of the first wizard popup in the next figure is for the cloud details.
3. Select an account name. Account Name refers to the AWS account nsmed in the *Cloud Credentials* page.
4. Pick one or more AWS regions.
5. Select a VPC. If you do not specify a VPC, all VPCs are assessed.

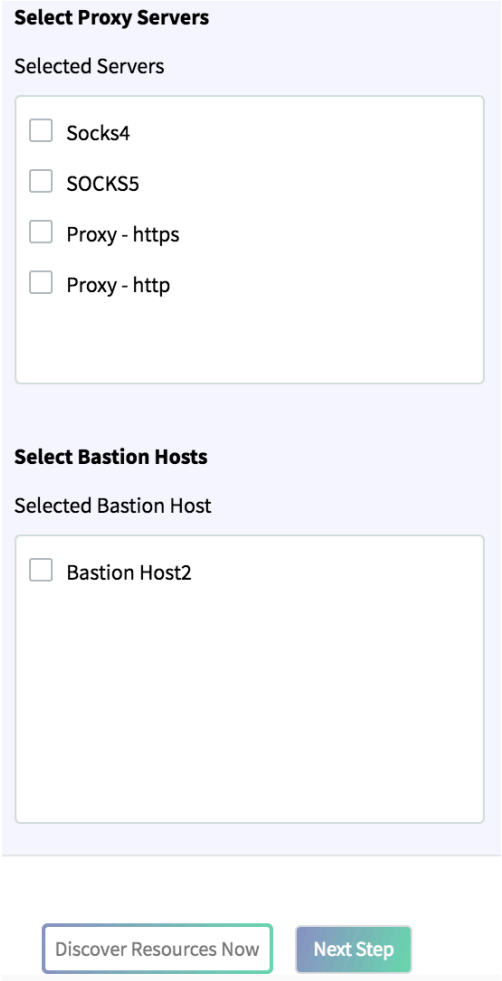
6. Type a name for the asset group you are creating in this wizard.





7. Select a resource credential to apply to the new asset group (preceding figure). If you have not specified the resource credentials in *Protect > Host Credentials*, you can create credentials now in the *Add New Credential* dropdown. If not selecting optional proxy servers or bastion hosts, you can click **Next Step** or **Discover Resources Now** at the bottom of the screen.

8. (Optional) Select proxy servers or bastion hosts if these have been added in *Protect > Proxy Servers* or *Protect > Bastion Hosts*. (As described in Specifying a Proxy Server and Specifying a Bastion Host, a user with GroupAdmin or Devops rights can set up these facilities after receiving the configuration values from a system administrator.)



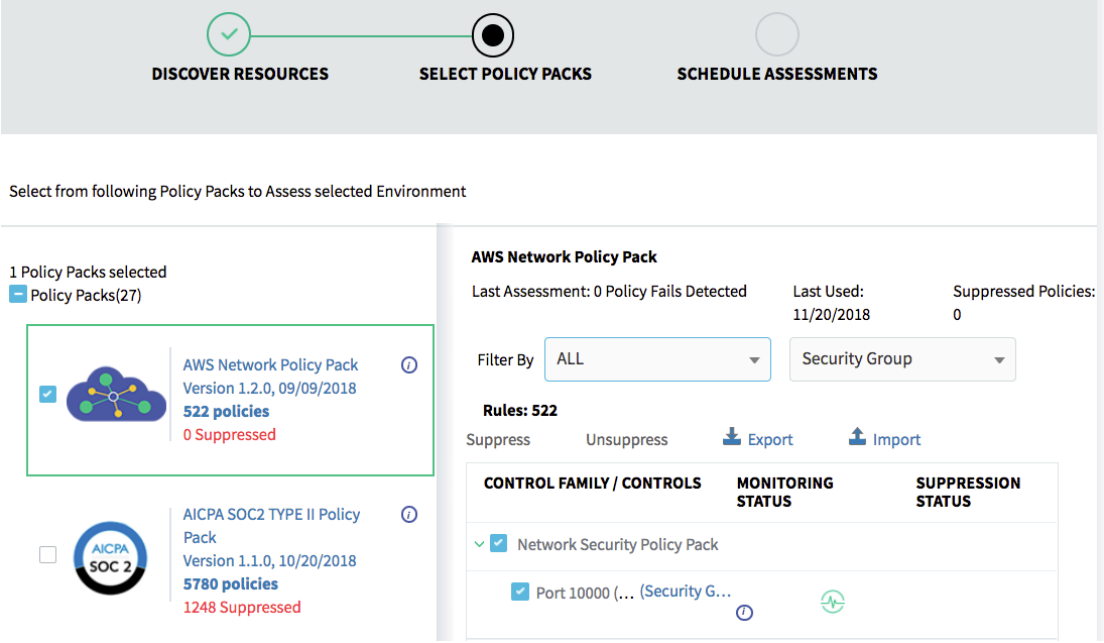
9. At this point, you can click **Discover Resources Now** to discover the resources but not assess their compliance, or you can click **Next Step** to select policy packs.

10. Click **Next Step** to open the wizard for specifying one or more policy packs for assessing the resource group. The system activates the checkboxes for the related policy packs.

11. Select **AWS Network Policy Pack**.

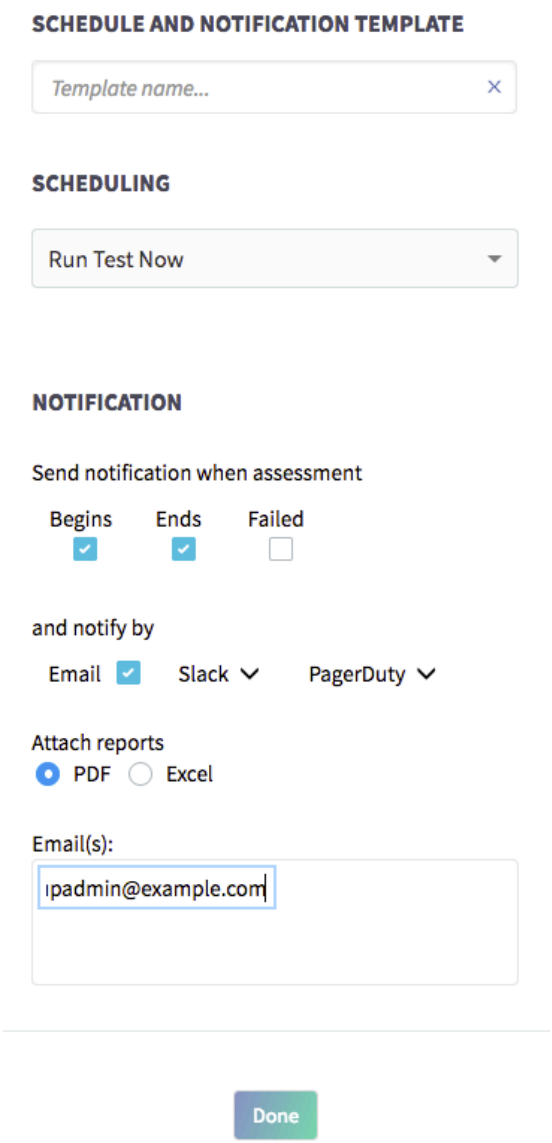
12. Click **Next Step** at the bottom of the screen (not shown in next figure). The wizard opens for scheduling an assessment time or immediately initiating the assessment opens (see subsequent figure).

NOTE: For a description of Cavirin's support for Compensating Controls (by suppressing rules), see Compensating Controls: Suppressing Rules.



13. Keep the default of *Run Test Now* so the assessment can start immediately. The next choices are the notification options:
    - Notification triggers can be the assessment start, end, and a failure.
    - Notifications can come by email—one email for each selected trigger—and Slack and PagerDuty if these notification services are integrated.
    - For email, type one or more email addresses (SMTP configuration must exist, but no integration is necessary).
14. Click once *outside* the email box after you finish typing email addresses.
15. Click **Done** when you are ready to start the assessment.
16. Click the Cavirin logo in the upper-left corner of the screen to go to the CISO Dashboard to see the high-level view of the scores when the assessment finishes.

NOTE: The available scores in the Dashboard apply to the asset groups to which you have access. Among the default roles, only a user with a Super Admin role can see the totality of CyberPosture scores.



To view the CyberPosture score at a high level, start some investigation, or initiate some remediation, refer to the Examining CyberPosture Score and Specific Scores section.

Compensating Controls: Suppressing Rules

For valid reasons (valid according to auditors and industry standards), an organization can use the *Compensating Controls* feature to suppress specific rules in a policy pack. Valid reasons are that the organization has alternative controls that *compensate* for rules in a policy pack. Suppressing at the level of a policy pack is global; its rules are not applied in an assessment—unless you unsuppress the rules at a later time. The override is local to the asset group; suppressed rules at the policy pack level stay suppressed. To re-activate controls, click the empty checkbox of a suppressed rule.

In addition to suppressing rules in a policy pack, you can save the set of suppressed rules *for a specific OS* or non-compute service as a template in JSON format for use on the same OS in another policy pack. The purpose is to save time. The save operation for the template is *Export*, and the application of the template is *Import*.

NOTE: The option to export a set of suppressed rules becomes active only when you select a specific OS or service. The import option becomes active if a template exists that matches the current OS.

NOTE: The Super Admin role does not have permission to suppress or unsuppress rules. Also, a user in this role can import (use) a template of suppressed rules but cannot export (create) a template.

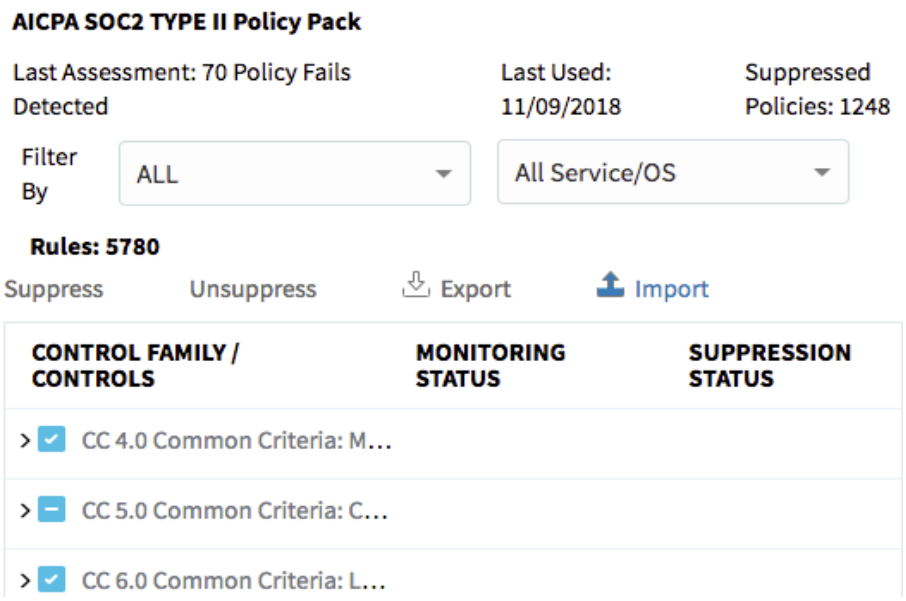
You can override the suppression of policies when you select:

- The second wizard that appears after you click **Protect** > **Discover & Assess Resource**. The second wizard is for selecting policies packs for the assessment.
- The policy pack list after navigating to **Identify** > **Asset Groups** > [*asset group name*] > **Assess.**

For a detailed example of the effect of rule suppression, see Appendix D – Effect of Rule Suppression on Scores.

To suppress rules in the AICPA SOC2 Policy Pack (refer to next figure):

1. Select the policy pack (AICPA SOC2 Type II in the current example).
2. Select an OS for these resources (not selected in this example).
3. Expand the control family called CC3.0 Common Criteria Related to Risk.
4. Expand the Risk Mitigation control family.
5. Click the ❶ icon to display the full Disable Automounting description to determine if this rule actually applies.
6. Clear the checkbox for Disable Automounting.
7. Click **Suppress** (located just above "Control Families/Controls"). A popup opens and requires a reason for the suppression.
8. Type a reason and click **Suppress**.

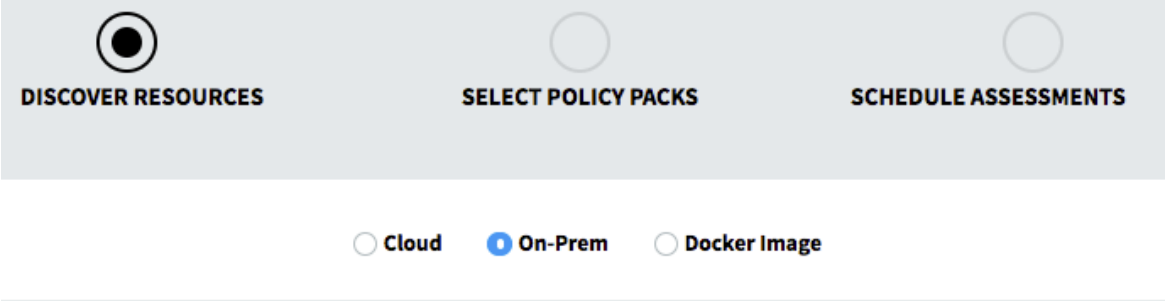

AICPA SOC2 TYPE II Policy Pack
Last Assessment: 70 Policy Fails Detected
Last Used: 11/09/2018
Suppressed Policies: 1248
Filter By
ALL
All Service/OS
Rules: 5780
Suppress
Unsuppress
Export
Import
CONTROL FAMILY / CONTROLS
MONITORING STATUS
SUPPRESSION STATUS
CC 4.0 Common Criteria: M...
CC 5.0 Common Criteria: C...
CC 6.0 Common Criteria: L...

Discovering and Assessing the On-prem Resources

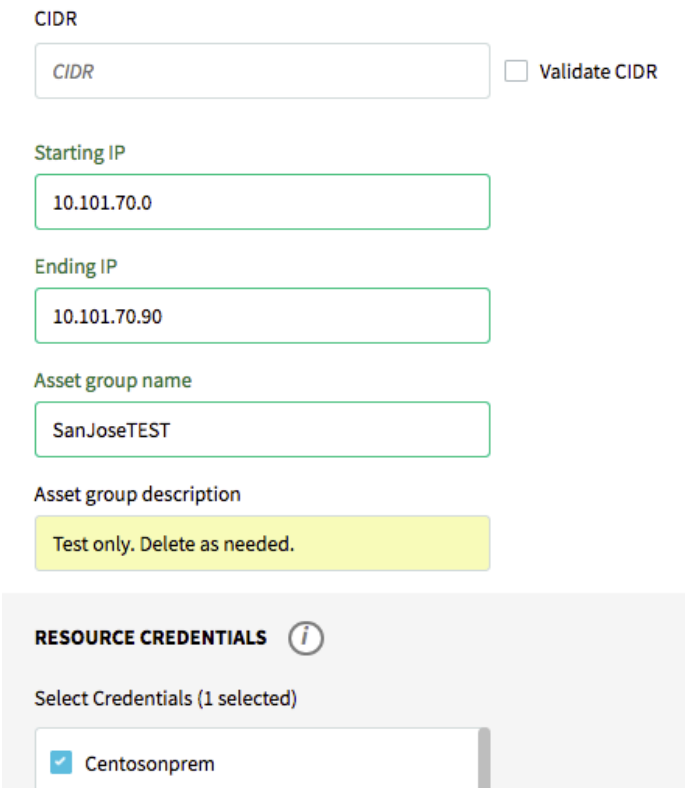
This section describes how to configure and initiate assessment of hosts in an on-prem environment. It relies on the Discover & Assess Resources wizard.

NOTE: Although you can run multiple assessments simultaneously across different environments, multiple assessments in one environment run sequentially.

1. Navigate to **Protect** > **Discover & Assess Resources**. The first wizard is *Discover Resources*. The next figure shows the top of the wizard.
2. Click the **On-prem** radio button (see figure).

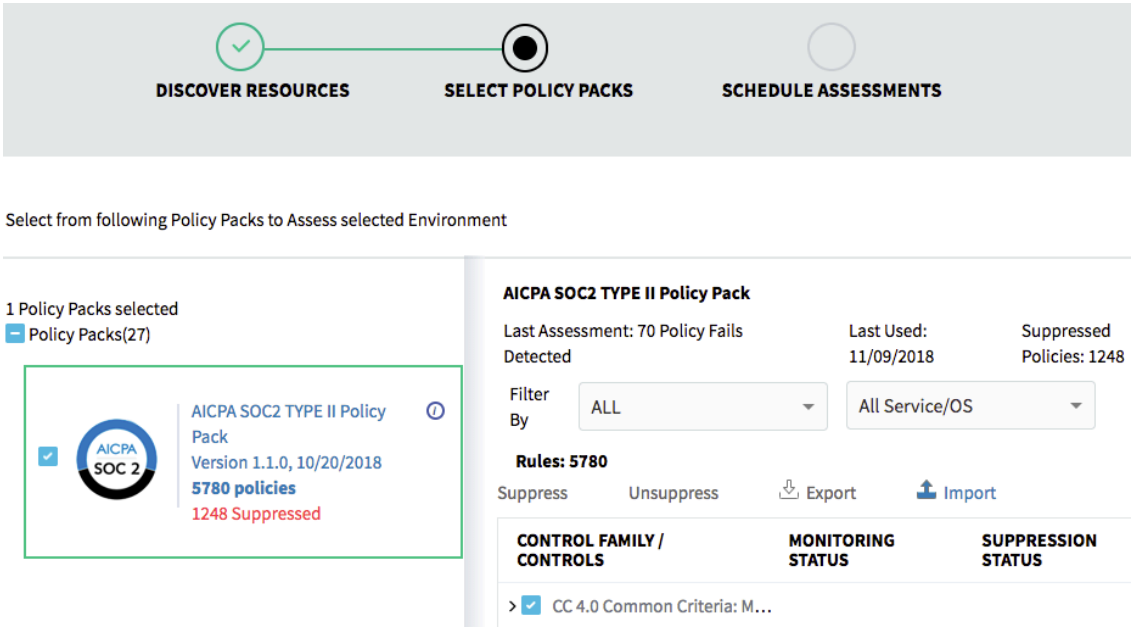


3. Type the IP address range of the on-prem environment in CIDR format or as a starting and ending IP address.
4. Type a name for the new asset group.
5. (Optional) Type a description of the asset group.
6. Select the resource credentials that Cavirin offers to hosts during an assessment.
7. Do either of the following:
   - Click **Next Step** to continue to selecting policy packs. The second wizard (subsequent figure) opens with relevant policy packs highlighted.
   - Click **Discover Resources Now** to exit the wizard and start resource discovery.



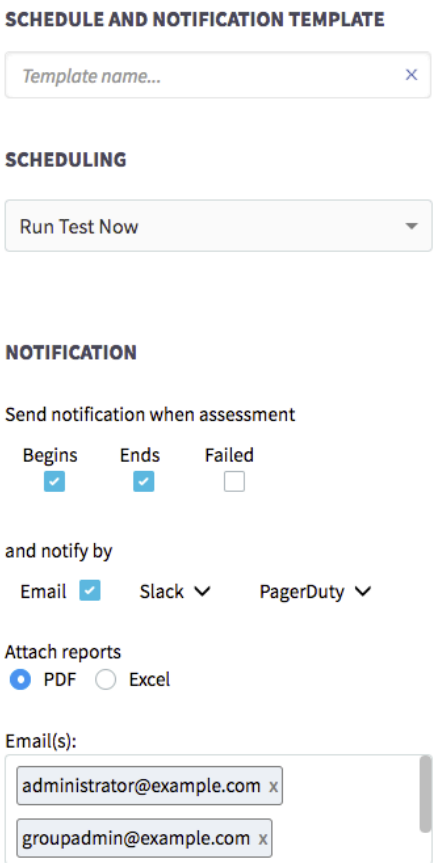
8. Select one or more policy packs. (For AWS, some policy packs give the option to suppress control families or individual polices.)

9. Click **Next Step** of the wizard (not shown at the bottom of next figure).



The third wizard, Schedule and Notifications, appears in the next figure.

10. Select any of the following courses of action:
    - Select an existing schedule and notification template.
    - Continue with *Run Test Now*.
    - Schedule Test Later (and use its configuration fields to set up a schedule).
11. Select optional notifications of when the assessment:
    - Begins
    - Ends
    - Fails



12. Select one or more notifications (3rd- party notifications must have be integrated):
    - Email
    - Slack (a list of available Slack channels is displayed)
    - PagerDuty

13. Click **Done** (not shown in preceding figure). The assessment begins according to the time you specify—now or later. When the assessment ends, whether it completes or fails, some form of report becomes available in the *Reports* area. A report for an assessment of many assets takes longer to generate after the assessment finishes.

Examining CyberPosture Score and Specific Scores

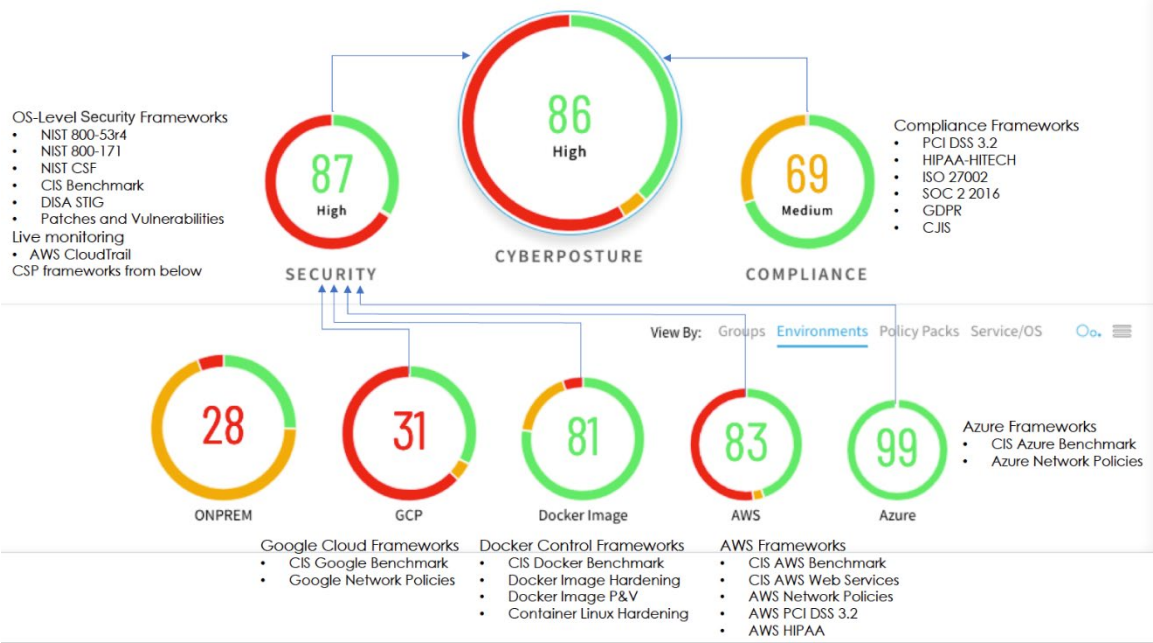
This section describes how to explore and address the assessment results. The topics are:

- Comprehensive CyberPosture score, security score, and compliance score
- Filtering scores for groups, environments, policy packs, OSs, and cloud services
- Prioritizing the issues, remediation reports, and Lambda auto-remediation
- Notifications (requires integration) through Jira, Slack, ServiceNow, or PagerDuty
- Trendline of the day-to-day scores
- Dashboard display template

The CISO Dashboard and CyberPosture Score

Start exploring the CISO Dashboard by reading the annotations next to the scores in the next figure. The figure illustrates the security and compliance frameworks that were applied in different environments:

- At upper-left, the figure shows the policy frameworks for assessing security.
- At upper-right, it shows the policy frameworks for assessing compliance.
- The *View By* option at center-right, between two rows of scores, lets you select the view to be for *asset groups*, *environments*, *policy packs*, or *services/OSs*.
- In the lower half, it shows the five different *environments* (on-prem, GCP, and so on); the policy frameworks that applied; and the score that each environment contributed specifically to the security score.



The CyberPosture Score in the CISO Dashboard varies with the role of the current user:

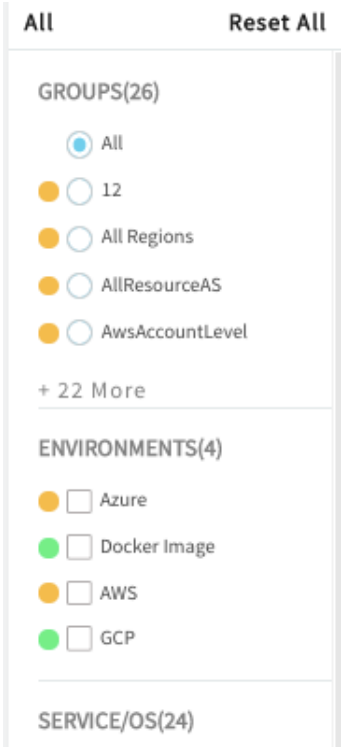
- In the Super Admin role, you can see the comprehensive CyberPosture score. This score represents a summation of all the latest scores for all assessments in all user-roles, all asset groups, all applied policy packs, and so on.
- In other roles, you can see the latest scores that apply just to that role.

NOTE: The meaning of *latest* score varies with the selected time frame of the display. You can modify the time frame in *CyberPosture Trend* (located below the Scores area of the Dashboard). For details, see Trendline of the Periodic Scores.

How the User's Role Affects the Displayed Scores

This section illustrates how different CyberPosture scores in the CISO Dashboard depend on Cavirin's Role-Based Access Control (RBAC).

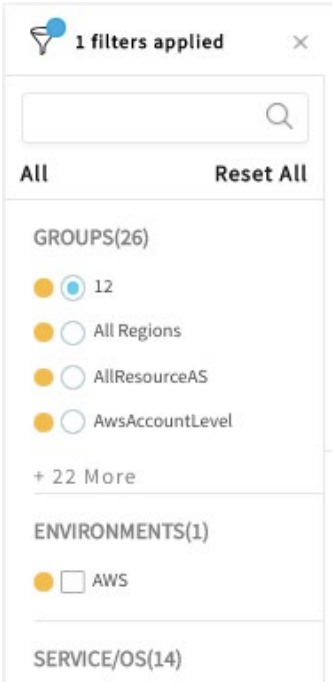
Super Admin: A user with the Super Admin role can see the summed scores for all asset groups but cannot initiate assessments. In the filter panel on the left side of the Dashboard (see next figure), the top of the panel shows the Groups filter has the default option *All*. This *All* option appears for only the Super Admin role. The Super Admin user can also filter for one asset group. The figure is a partial view of the filter panel and shows 26 groups, 4 environments, and 24 services or OSs.



Devops or **Group Admin**: With a Devops or Group Admin role, you can initiate an assessment and see the scores for one asset group at a time. The subsequent figure is a partial view of filters for Devops and Group Admin. This view of the filter panel shows 26 groups, 1 environment, and 15 services or OSs. If you select a different group, numbers for environments, services/OSs, and so on can change.

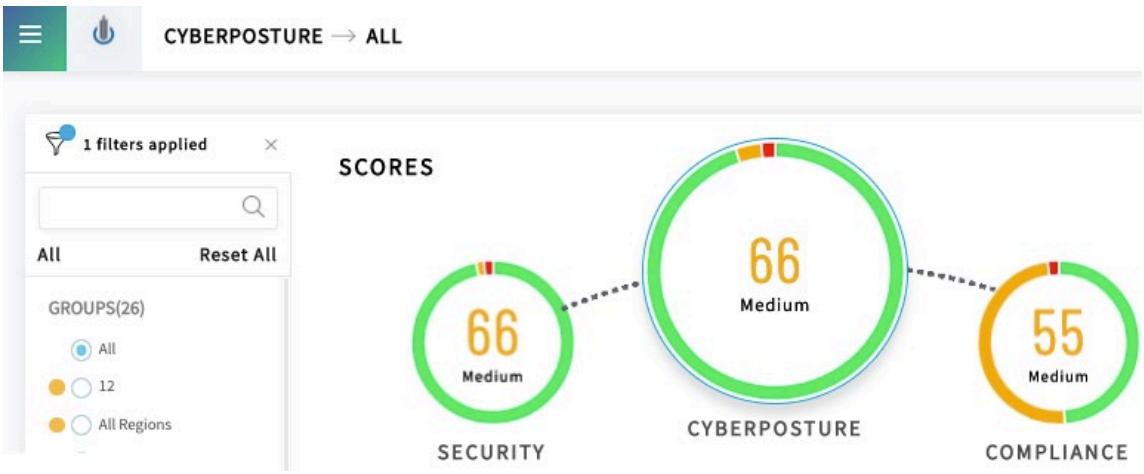
NOTE: After selecting the filters, click the **Apply** button at the bottom of the panel.

NOTE: For the table of all roles and permissions, see Role-Based Access Control.



The next two figures show Dashboards for the Super Admin role and the Group Admin role. The Super Admin role defaults to All groups (with a score of 66). Notice the descriptive *CyberPosture -> All* at the top of the figure.

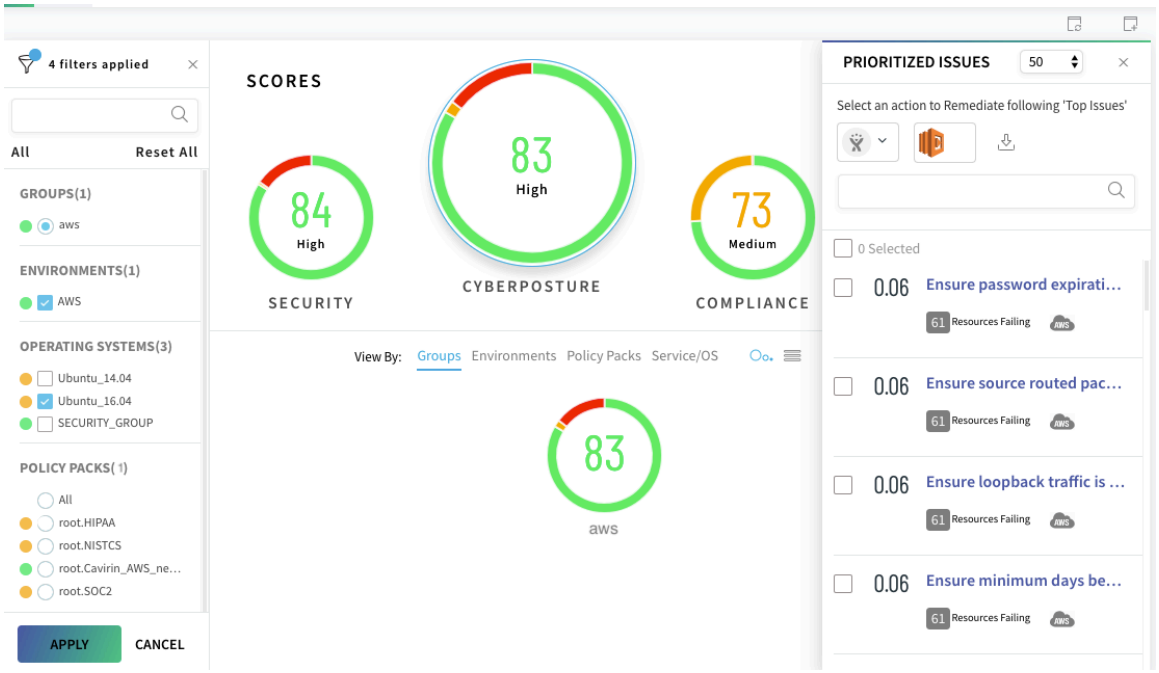
The subsequent figure is for the Group Admin role. Notice the descriptive *CyberPosture -> All Regions* at the top of the figure. For the Group Admin role, the All Regions group has a score of 61 (contrast with 66 visible to the Super Admin).



Exploring the CISO Dashboard

To begin:

1. Click the Cavirin icon in the upper-left corner of the window if you are not in the Dashboard. From left to right in the following figure are:



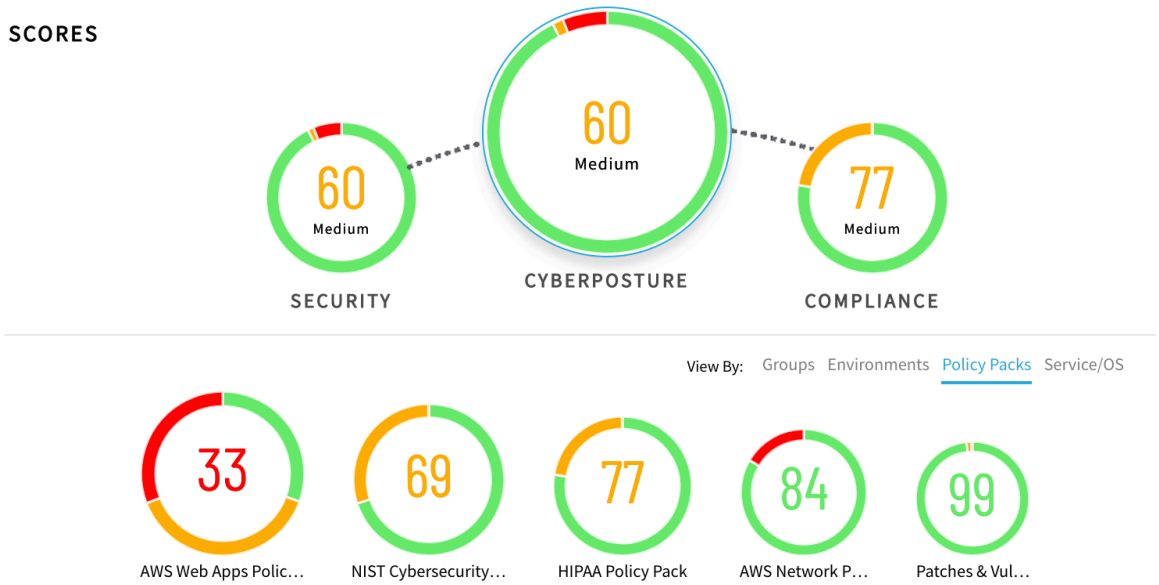
NOTE: A matrix of influences can shape the display in the Scores area:

- In the Scores area (and below the CyberPosture score), you can see the *View By* row, which specifies that scores are shown by asset groups, policy packs, environments and so on. The default is *Groups*.
- With the panel of filters at left, you can select one policy pack, environment, operating system, and so on; these filters determine what is available for the

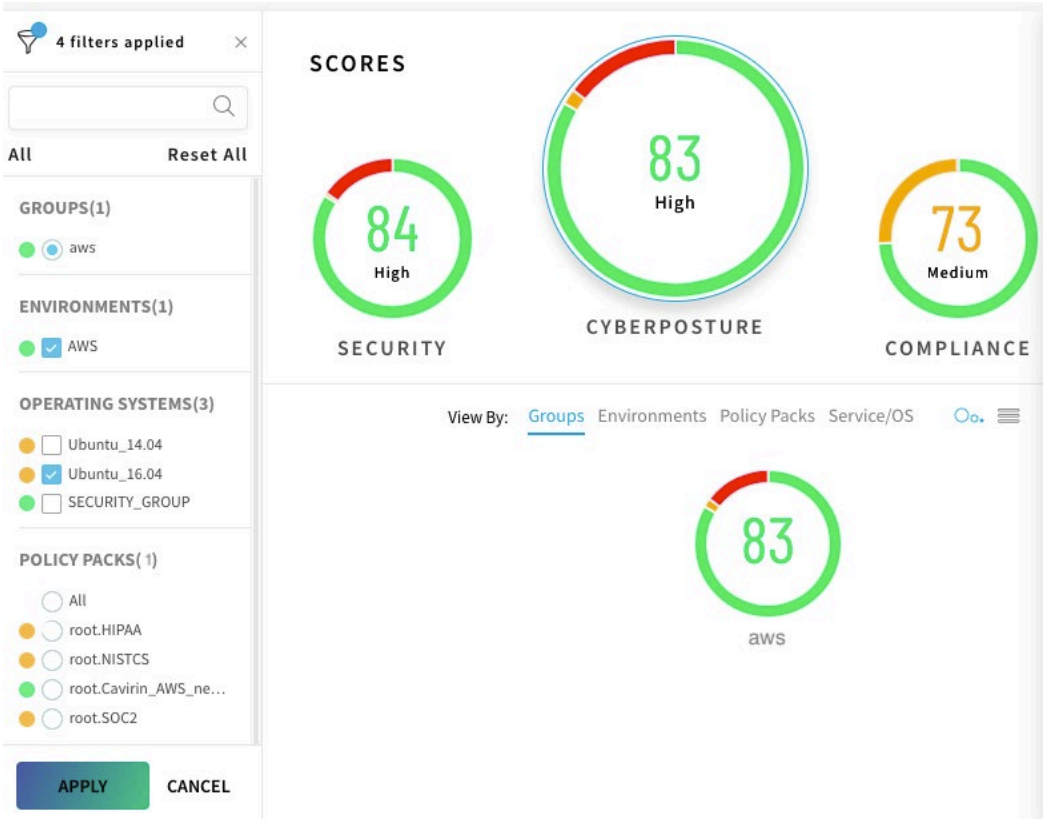
Scores and *View By* areas to display. For example, if *View By* is for Services/OS and there are four OSs reflected in the score, if you select an OS in the Filters panel at left, the *Scores* area changes to show the score for just that OS.

2. Click **Policy Packs** in *View By*. As the next figure shows, all policy packs are shown.

3. Click on a policy pack and see the scores change to reflect just that policy pack.



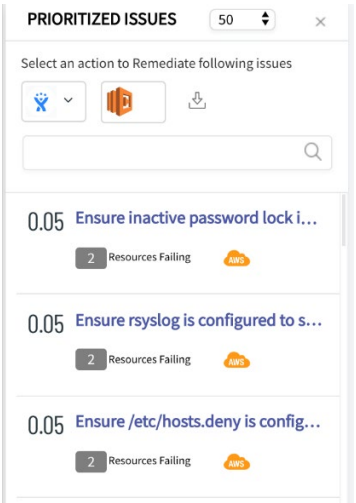
4. In the Filters panel, select **aws** for the group, **AWS** for the environment, and **Ubuntu 16.04** for the OS, and then click **Apply**.



Prioritized Issues

To send a notification through a third-party service, start Lambda remediation (AWS only) or Google Cloud remediation, or download a report of how to remediate the top 50, 25, or 10 issues:

1. Click the Cavirin logo at upper-left to open the CISO Dashboard from any screen. The next figure shows the *Prioritized Issues* on the right side of the Dashboard.

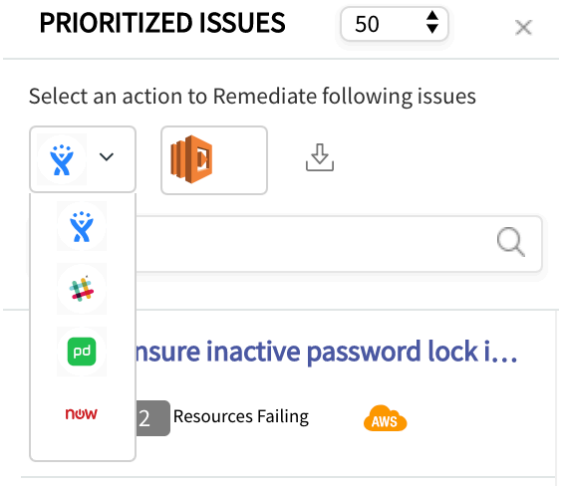


2. Choose one of the following courses of action:

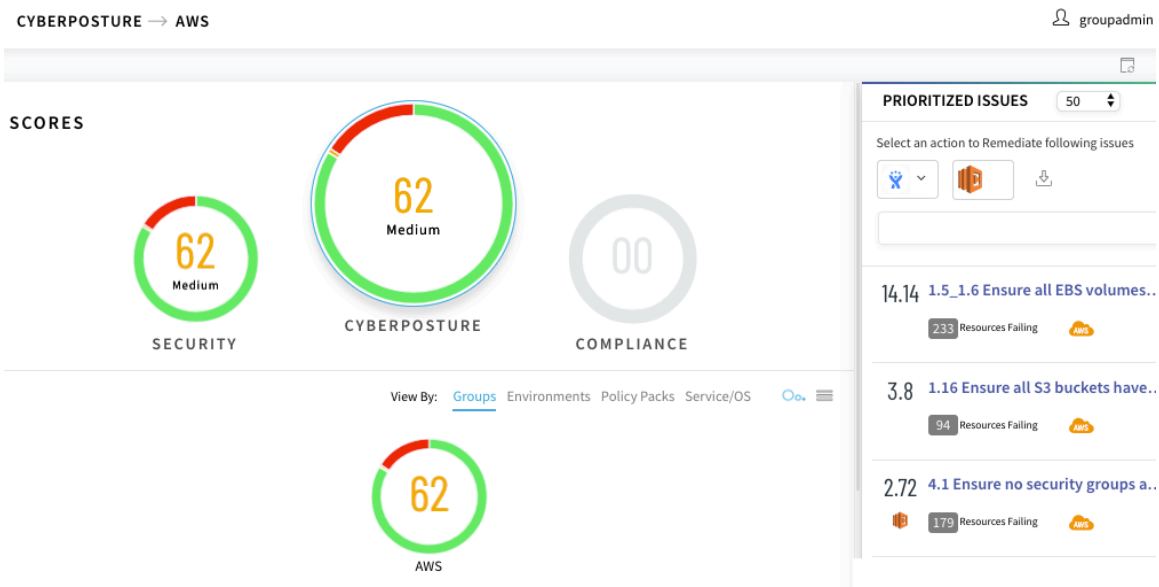
   - Click one of the colored icons in the dropdown list of notifications to activate the corresponding ticket or message. The four colored icons shows that Jira, Slack, PagerDuty, and ServiceNow have been integrated. (For a service you have not integrated, the icon is gray.) Examples of PagerDuty and ServiceNow usage follow.

   - Click the AWS Lambda icon in the middle. The Lambda pane opens at left in the Dashboard. (The prerequisite for Lambda remediation is that Lambda has been set up in the Cloud Credentials for this specific AWS account.) See Setting Up Auto-remediation with Lambda.

   - Click the download icon at right to export a report for steps to remediate the top issues. A popup asks for a name for the report. The report will appear by name and type ("Remediation") in the Reports page.



The next view has been redrawn for a Group Admin role (see upper-right corner). The focus will first be on downloading a remediation report and later on activating auto-remediation with Lambda in an AWS environment.



To get a remediation report for the contents of the top 50, 25, or 10 issues:

1. Click the download icon near the top of Prioritized Issues to *export* the report.
2. Type a name for the report in the popup that appears and click **Save**. A message confirms the report is being generated and will be available in the Reports page. For the details on a prioritized issues report, see Remediating the Prioritized Issues.

Remediating with Lambda from the Dashboard

If a Lambda remediation has been set up, you can apply it to all issues in the *Prioritized Issues* list that show the Lambda icon next to the issue (next figure).

The places where Lambda remediation has first been *set up* on the Cavirin back end and subsequently *enabled* in the AWS cloud account are as follows:

- Back-end configuration requires the CLI, AWS management portal, and Cavirin UI. These tasks were performed while the Cavirin system was being set up for regular use, as described in the *Cavirin Administrator Guide*.
- Enabled in the *Add Cloud Account* page accessed through the Cloud Credentials menu item. See Enabling AWS Lambda Auto-remediation.

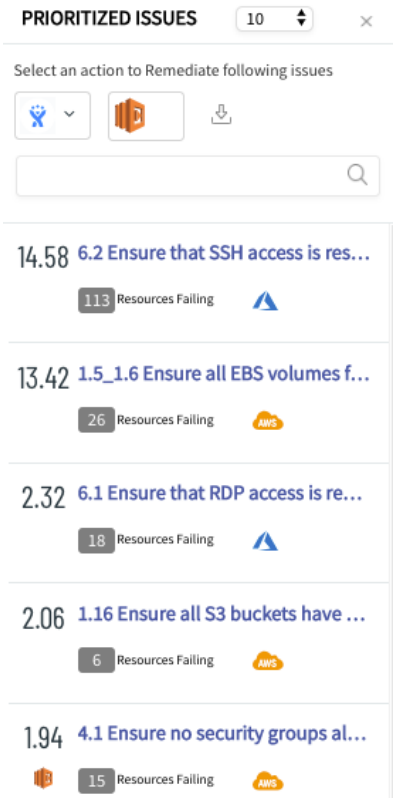
The next figure shows the Lambda icon below the value of potential score improvement. (You mark the checkbox and click the Lambda icon to begin remediation steps).

> **NOTE:** Issues that can receive Lambda remediation might not be of a high enough priority to fit in the top 10, 25, or 50, so you would not see these issues. However, if you click the Lambda icon at the top of the Prioritized Issues panel, these issues appear in the full list of resources that are Lambda-ready.

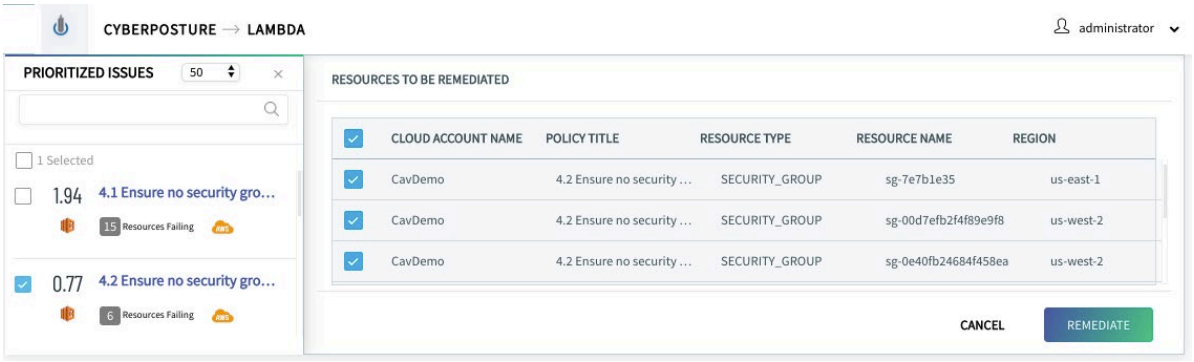
The next figure shows one rule valuation and the remediation ("Ensure no security group has open port 22 on IP address 0.0.0.0"). Remediation will apply to all resources with this issue. This example shows that only one resource has the issue.

1. Click the Lambda icon near the top of *Prioritized Issues*. (Near the bottom of the following figure, one issue with a Lambda exists on 15 resources.)

2. Click the Lambda icon near the top of panel (next figure) to begin the steps for Lambda remediation. After you click the icon, the UI changes; the subsequent figure shows a Lambda remediation panel on the left side of the Dashboard and an area that shows the remediation for resources with this issue.



3. Mark the checkbox next to the issue whose remediation on 6 devices will raise the score by .077. The resources appear under *Resources to be Remediated*, at right.



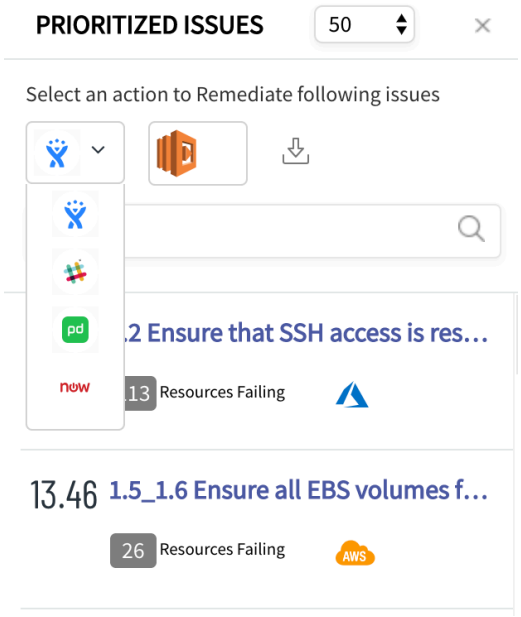
4. Click the **Remediate** button in the lower-right corner. If remediation has been set up in the cloud account, the problem is corrected on all devices with this issue.

NOTE: An administrator must have set up Cavirin's ability to use Lambda remediation on the system back end, as described in the *Cavirin Administrator Guide*.

WARNING: Remediation is irreversible, so Cavirin prompts you to confirm remediation.

Using Integrated Notification Services in the Dashboard

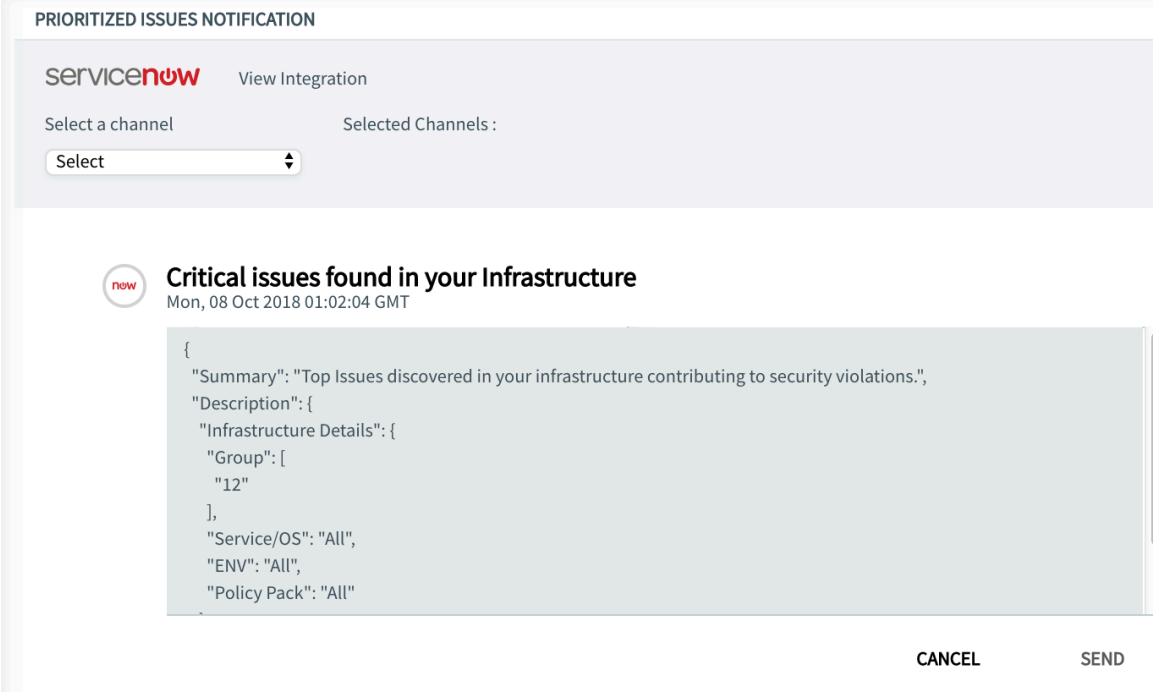
In the Prioritized Issues area of the Dashboard, you can activate any third-party notification service that has been integrated by the system administrator. In the next figure, the colored icons show that all the notification services are integrated with this Cavirin system. A workflow for generating a trouble ticket in ServiceNow follow, in the Requesting a ServiceNow Trouble Ticket in the Dashboard section.



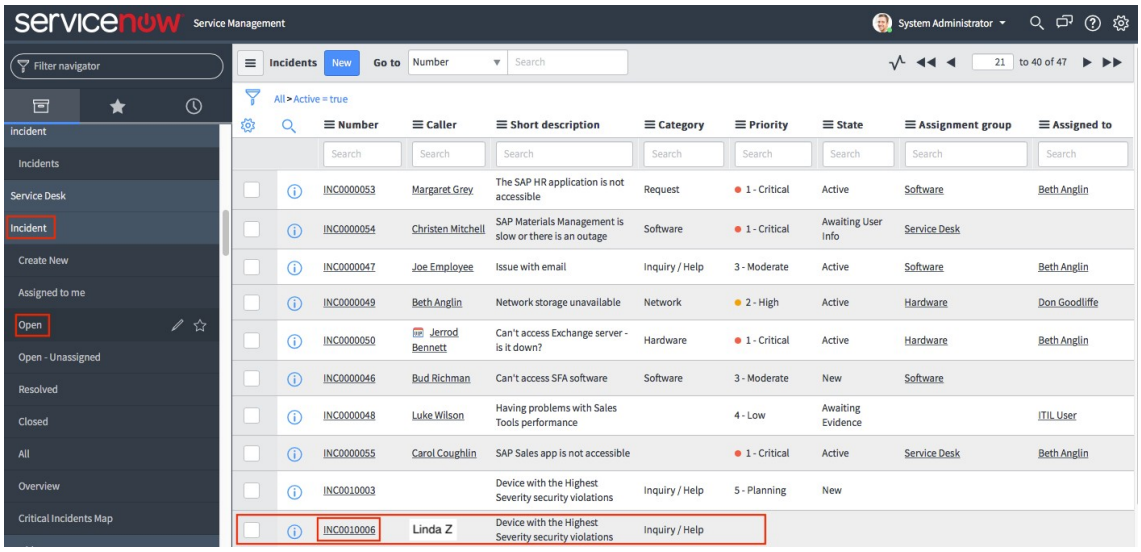
Requesting a ServiceNow Trouble Ticket in the Dashboard

After an assessment finishes, you can see the option to open the list of top issues in the Prioritized Issues area, as follows:

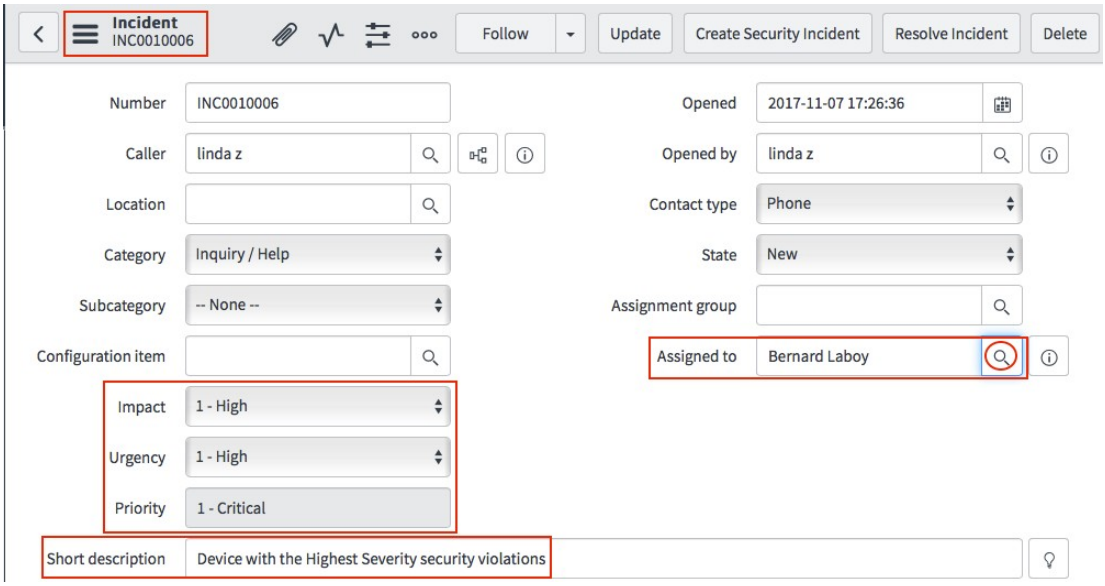
1. Click **now** (ServiceNow) in the dropdown of notification services in the Dashboard Prioritized Issues area. The form for describing the issue opens (next figure).
2. Fill in the details of the form. For this example, make the assignee Linda Z.
3. Click **Send**.



1. Log into ServiceNow. Navigate to **Incident** > **Open** > **INC0010006**. (Next figure.)



2. Click on **INC0010006**. The page in the next figure opens and reflects the choices that have been made. For example, some priorities have been set, and an assignee for this incident has been selected to initiate this ticket. The 'Short description' at the bottom reflects information from Cavirin.



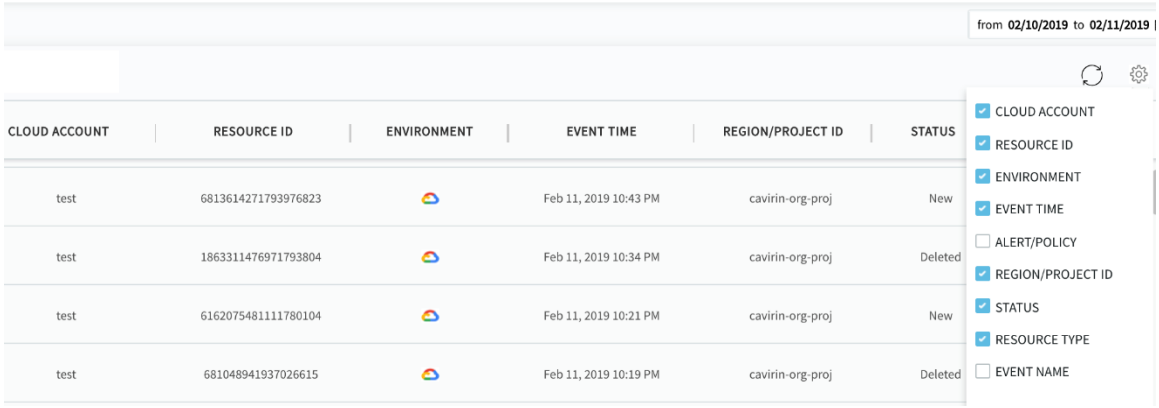
3. Scroll down the screen shown in the preceding figure. An area appears as shown in the next figure, with details provided by a user in the Super Admin role (who sent the notification to Linda Z).

Viewing Alerts

If monitoring or Lambda have been enabled, the nature, source, status, and other details of alerts appear in *Monitor > Alerts*. The next figure illustrates alerts for a Google Cloud. The figure also shows the gear icon for selecting the column to display. For space reasons, the choice of columns to display depends on what you are trying to find.

> **NOTE**: If your environment has a Lambda configuration, the alert shows that the cause has been remediated by actions from the cloud provider.

> **NOTE**: When you select an alert and mark it as read, it from the alert table.



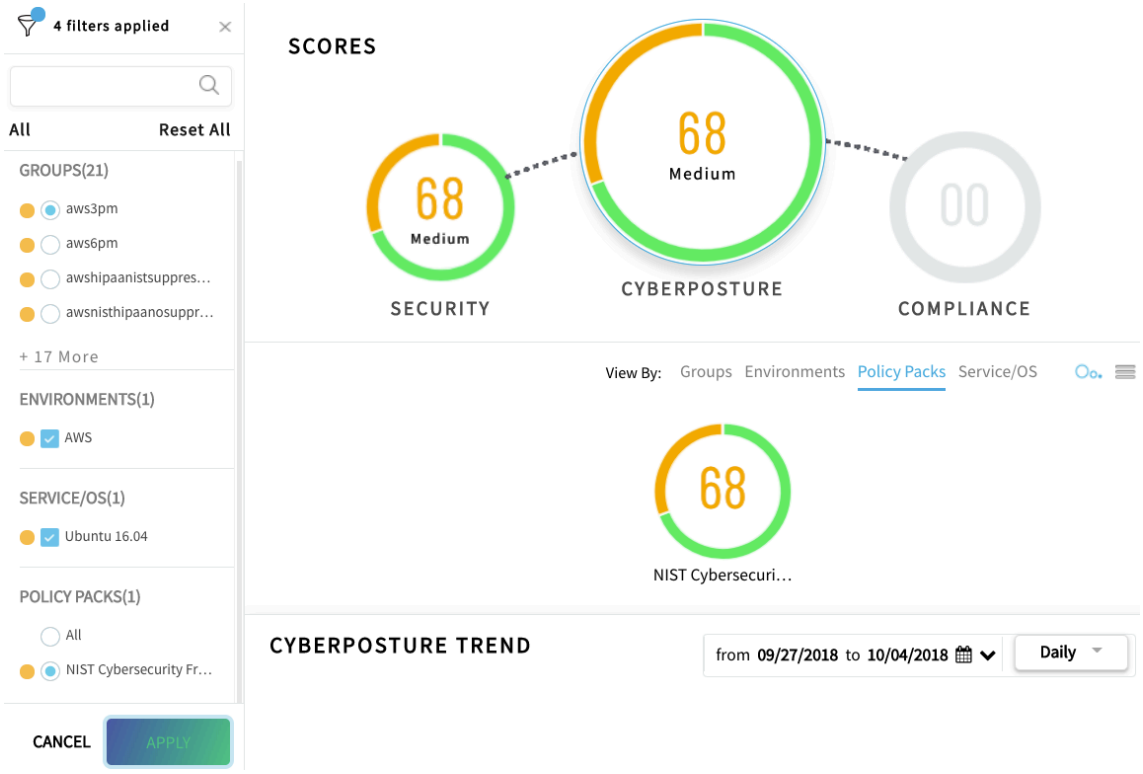
Dashboard Display Templates

A Dashboard display template is a shortcut. Instead of repeating the steps of selecting groups, services, policy packs, and so on, you can select a template that displays your selections. The purpose of a display template is to save you time when filtering the display. You can create one *default* template and multiple, other templates. The other templates you select by name to redraw the Dashboard, as described in this section.

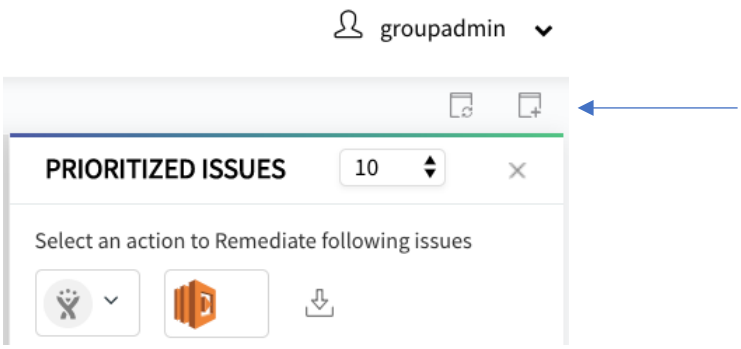
Creating and Loading a Display Template

To create a template from the current display:

1. Use Dashboard filters at left and a *View By* choice to create the view you want to be a template. Note the applied filters (also reflected up top) and the *View By*.



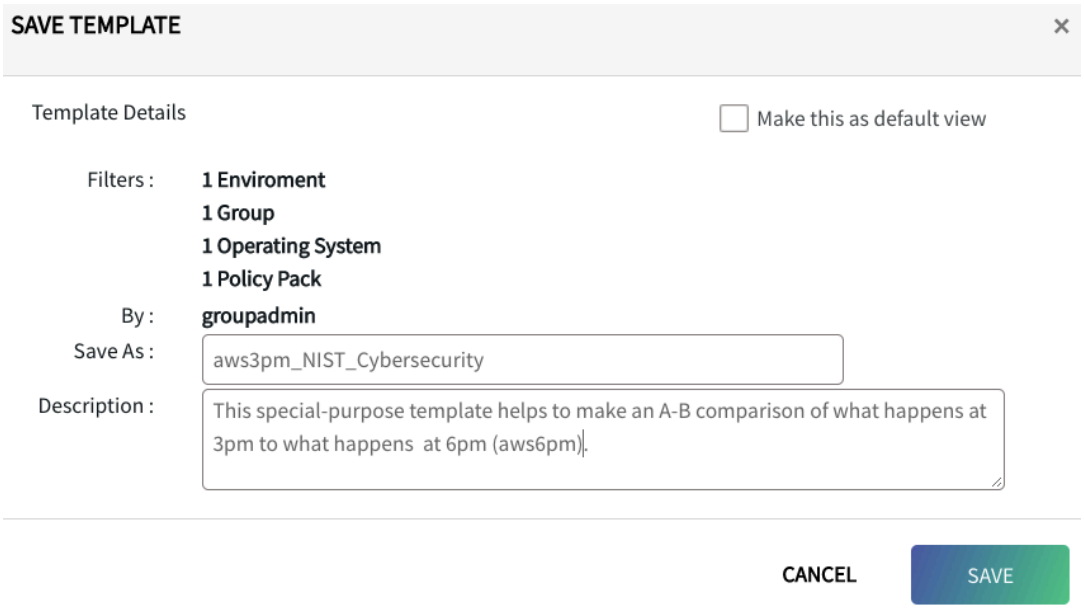
2. Click the plus sign (+) icon at upper-right, below your user name (next figure).



The *Save Template* popup shows filter-metadata about the current display.

3. Type a name and description for the template.
4. Mark the checkbox as needed to make this the default view.

5. Click **Save** when ready. You can create more templates as needed.

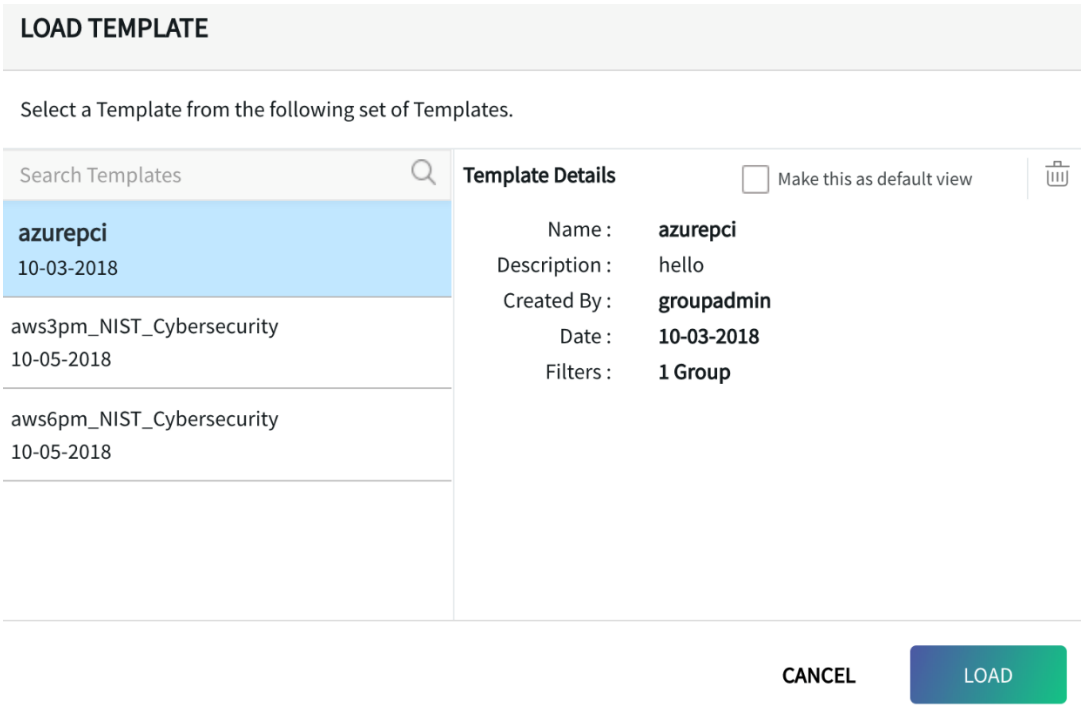


To switch the Dashboard display settings to a template:

1. Click the icon with a circle to open the Load Template popup when you want the display to switch to that configured display in the template's configuration—unless the template is the default view whenever you or someone in the current role logs in. The next figure shows three templates exit.
2. Select the template to load.
3. Click **Load**. The Dashboard is redrawn to match the filter set and *View By* choice when the template was created.

To delete a display template:

1. Select the template in the *Load Template* popup.
2. Click the trash icon. A confirmation message says the template was deleted.

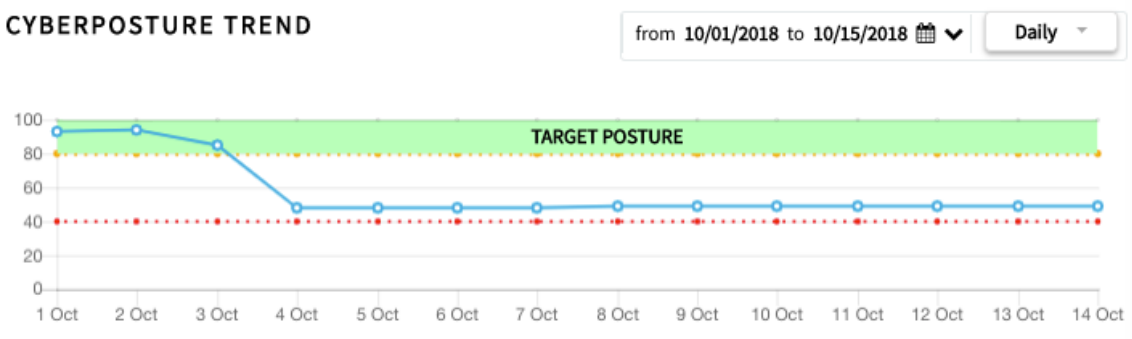


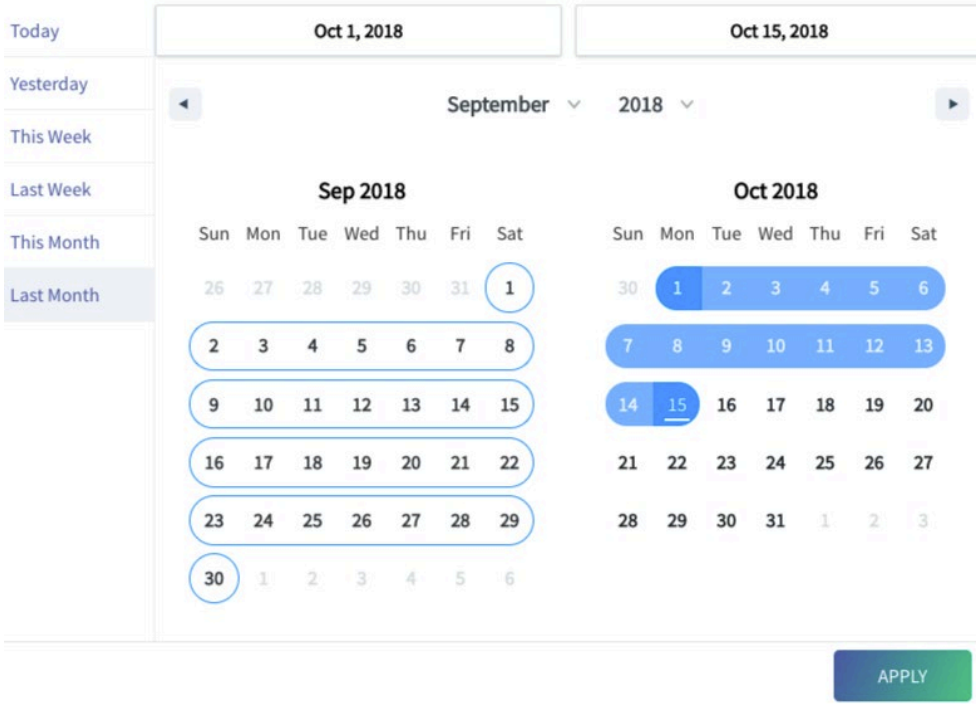
Trendline of the Periodic Scores

Below the Scores area of the Dashboard, you see a graph that shows a trend in scores (if more than one day of scores are available, otherwise, there is no trend). The trend adjusts to any filtering you specify in the Dashboard.

The next two figures illustrate:

- The date vs score graph and zoom points (Daily, Weekly, etc) on the time line.
- Clicking the calendar icon to the right of the date range opens the popup in the subsequent figure for setting the score's date range (see Oct 2018).
- The left side of the subsequent figure shows another capability: You can select a past time frame instead of the current time to display—*Last Month,* (September) in this example. Click **Apply** when ready.




Today
Yesterday
This Week
Last Week
This Month
Last Month
Oct 1, 2018
Oct 15, 2018
September
2018
Sep 2018
Sun Mon Tue Wed Thu Fri Sat
26 27 28 29 30 31 1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 1 2 3 4 5 6
Oct 2018
Sun Mon Tue Wed Thu Fri Sat
30 1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31 1 2 3
APPLY

The Reports

For this section, note the following characteristics related to Cavirin Reports:

- An *assessment* is performed on one asset group and by using all the policy packs you select for that asset group's assessment.
- A *report* shows the findings of the assessment and distinguishes between . For example, if an assessment uses five policy packs, Cavirin produces five reports.
- The Reports feature provides different types of reports, based on the assessments, your filter selections in the Dashboard, and your on-demand requests. Any report can be downloaded as a PDF or spreadsheet. Report types are:
    - *System-Generated* For each assessment, Cavirin automatically generates a comprehensive report for all the components of the assessment. System-generated reports automatically appear in the Reports page. From the comprehensive report, you can select a variation, such as a Delta report.
    - *Resource* reports simply show the state of all resources in the assessed resource group. Details consist of resource, criticality of the resource, score, and so on.
    - *Remediation* reports show how to remediate each rule failure for all resources with the failure and for each service, OS, and so on. (See example spreadsheet, below.)
    - *Delta* - This report describes the differences between the current report and the preceding report.
    - *Prioritized Issues* One part of the CISCO Dashboard is *Prioritized Issues*. These are the most serious issues. It shows the top 10, 25, or 50 issues whose remediation brings the greatest improvement to the CyberPosture score.
    - *Remediate to Target* This report shows the changes you must make to reach a CyberPosture score that you specify.
- Some report types are requested from outside the Reports screen, after which you can locate the report in the Reports screen and download. In the current release, for example, you request a *Prioritized Issues* report in the CISO Dashboard or request a *Remediate to Target* report in the *Respond > Plan for Target CyberPosture*. Subsequently, you find the reports in the Reports screen, as the next figure illustrates.
- Subdivisions for each downloaded report type are format (PDF or spreadsheet) and focus on remediation or resource information.

- A *Resource Report* shows data for resources, the score for each rule applied to a resource, and the state of the assessment result for that one rule (pass, fail, not applicable, and so on. (For the definition of the states, see Appendix B – Definitions of the Assessment State).

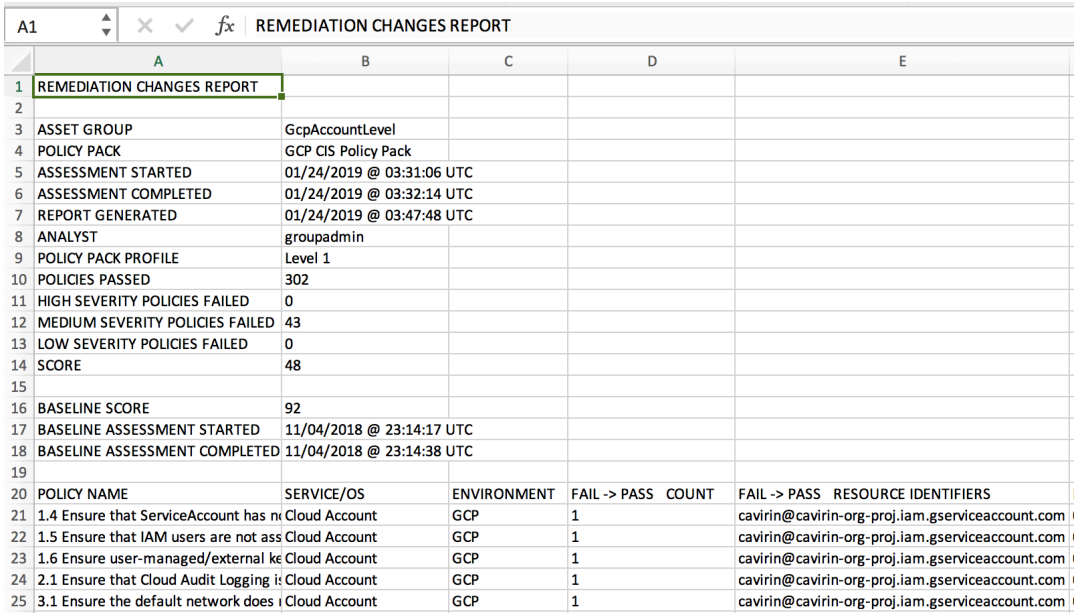
- A *Remediation Report* lists the remediation tasks for failures on compute resources and cloud services, where applicable.

To access a report, start with the comprehensive Reports page:

1. Navigate: **Analyze** > **Reports**.

   In the next figure, notice the report types in the left column, the Download column for selecting the file type as PDF or XLS, and the drop-down in the lower-right corner for selecting a report that focuses on resources, remediation, or changes in the resources or remediation state between this group's current assessment and the preceding assessment.

2. Click on your choice of report target, filetype, and focus to download column to download it. The next figure is an example of a remediation report as an XLS file.



A1 | REMEDIATION CHANGES REPORT

	A	B	C	D	E
1	REMEDIATION CHANGES REPORT				
2					
3	ASSET GROUP	GcpAccountLevel			
4	POLICY PACK	GCP CIS Policy Pack			
5	ASSESSMENT STARTED	01/24/2019 @ 03:31:06 UTC			
6	ASSESSMENT COMPLETED	01/24/2019 @ 03:32:14 UTC			
7	REPORT GENERATED	01/24/2019 @ 03:47:48 UTC			
8	ANALYST	groupadmin			
9	POLICY PACK PROFILE	Level 1			
10	POLICIES PASSED	302			
11	HIGH SEVERITY POLICIES FAILED	0			
12	MEDIUM SEVERITY POLICIES FAILED	43			
13	LOW SEVERITY POLICIES FAILED	0			
14	SCORE	48			
15					
16	BASELINE SCORE	92			
17	BASELINE ASSESSMENT STARTED	11/04/2018 @ 23:14:17 UTC			
18	BASELINE ASSESSMENT COMPLETED	11/04/2018 @ 23:14:38 UTC			
19					
20	POLICY NAME	SERVICE/OS	ENVIRONMENT	FAIL -> PASS COUNT	FAIL -> PASS RESOURCE IDENTIFIERS
21	1.4 Ensure that ServiceAccount has n	Cloud Account	GCP	1	cavirin@cavirin-org-proj.iam.gserviceaccount.com
22	1.5 Ensure that IAM users are not ass	Cloud Account	GCP	1	cavirin@cavirin-org-proj.iam.gserviceaccount.com
23	1.6 Ensure user-managed/external ke	Cloud Account	GCP	1	cavirin@cavirin-org-proj.iam.gserviceaccount.com
24	2.1 Ensure that Cloud Audit Logging i	Cloud Account	GCP	1	cavirin@cavirin-org-proj.iam.gserviceaccount.com
25	3.1 Ensure the default network does	Cloud Account	GCP	1	cavirin@cavirin-org-proj.iam.gserviceaccount.com

Remediation Report

For this example:

1. Navigate: **Analyze** > **Reports**. Decide on a report. For this example, we use the asset group named *GcpAccountLevel*.

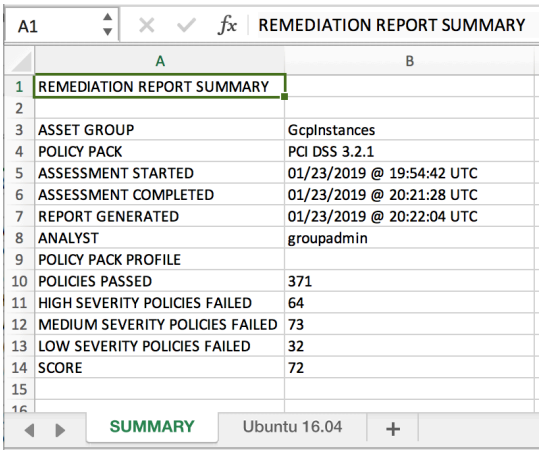
2. In the Download column for the *GcpAccountLevel* report:

   a. Open the **Select XLS report** dropdown.

   b. Click **Remediation**.

   A status popup states that the report is being downloaded.

3. Click the file XLS file in your download folder. The name of the XLS file reflects the name of the asset group, environment, power pack, and report type (remediation). The next figure illustrates the summary tab of the report, and the subsequent figure illustrates the recommended remediation for the issues under the Ubuntu 16.04 OS.

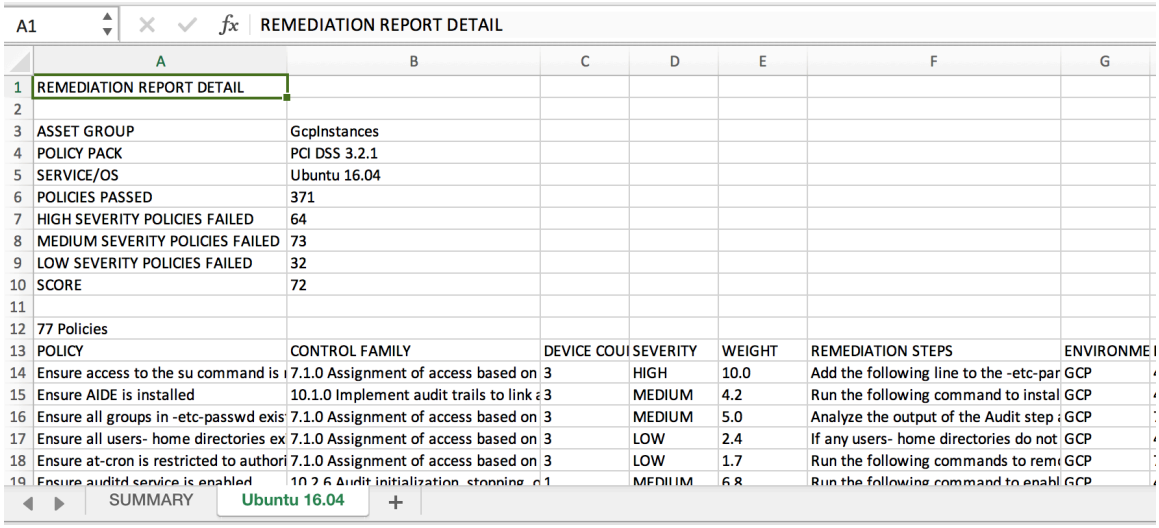


A1 REMEDIATION REPORT SUMMARY

	A	B
1	REMEDIATION REPORT SUMMARY	
2		
3	ASSET GROUP	GcpInstances
4	POLICY PACK	PCI DSS 3.2.1
5	ASSESSMENT STARTED	01/23/2019 @ 19:54:42 UTC
6	ASSESSMENT COMPLETED	01/23/2019 @ 20:21:28 UTC
7	REPORT GENERATED	01/23/2019 @ 20:22:04 UTC
8	ANALYST	groupadmin
9	POLICY PACK PROFILE	
10	POLICIES PASSED	371
11	HIGH SEVERITY POLICIES FAILED	64
12	MEDIUM SEVERITY POLICIES FAILED	73
13	LOW SEVERITY POLICIES FAILED	32
14	SCORE	72
15		

SUMMARY | Ubuntu 16.04 | +

4. Click the **Cloud Account** tab. For each unique failed policy, the spreadsheet displays the policy, Cavirin-computed severity, weight, remediation, and so on.



A1 REMEDIATION REPORT DETAIL

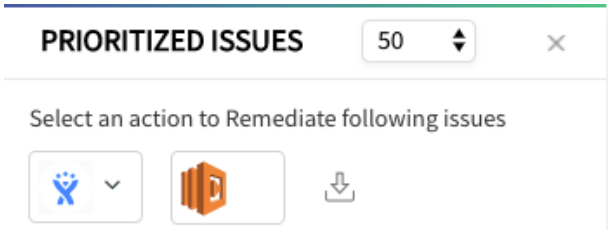
	A	B	C	D	E	F	G
1	REMEDIATION REPORT DETAIL						
2							
3	ASSET GROUP	GcpInstances					
4	POLICY PACK	PCI DSS 3.2.1					
5	SERVICE/OS	Ubuntu 16.04					
6	POLICIES PASSED	371					
7	HIGH SEVERITY POLICIES FAILED	64					
8	MEDIUM SEVERITY POLICIES FAILED	73					
9	LOW SEVERITY POLICIES FAILED	32					
10	SCORE	72					
11							
12	77 Policies						
13	POLICY	CONTROL FAMILY	DEVICE COU	SEVERITY	WEIGHT	REMEDIATION STEPS	ENVIRONME
14	Ensure access to the su command is r	7.1.0 Assignment of access based on	3	HIGH	10.0	Add the following line to the -etc-par	GCP
15	Ensure AIDE is installed	10.1.0 Implement audit trails to link a	3	MEDIUM	4.2	Run the following command to instal	GCP
16	Ensure all groups in -etc-passwd exis	7.1.0 Assignment of access based on	3	MEDIUM	5.0	Analyze the output of the Audit step a	GCP
17	Ensure all users- home directories ex	7.1.0 Assignment of access based on	3	LOW	2.4	If any users- home directories do not	GCP
18	Ensure at-cron is restricted to authori	7.1.0 Assignment of access based on	3	LOW	1.7	Run the following commands to rem	GCP
19	Ensure auditd service is enabled	10.2.6 Audit initialization, stopping, o	1	MEDIUM	6.8	Run the following command to enabl	GCP

SUMMARY | Ubuntu 16.04 | +

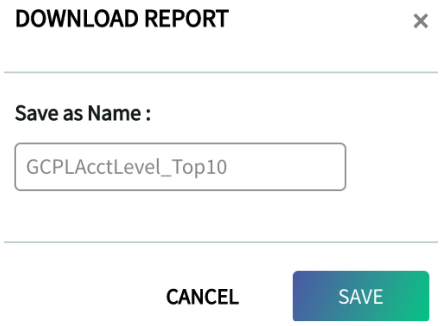
Remediating the Prioritized Issues

To generate a remediation report from the upper-right corner of the Dashboard:

1. Choose 25 or 10 top issues or keep the default issue count of 50.
2. Click the download icon in the upper part of the CISO Dashboard to export a report. A popup requests a name for the report.



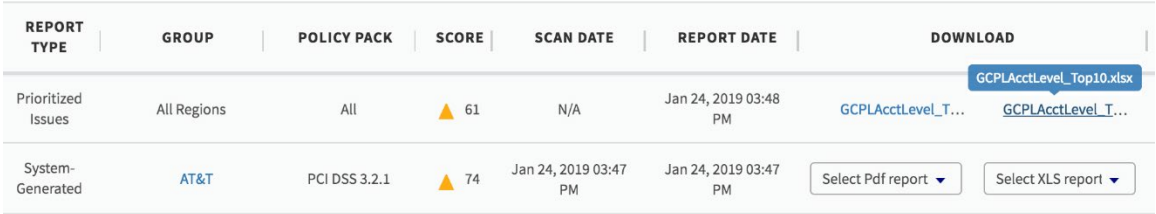
3. Type a meaningful name for the report and click **Save**. The Reports page will have the report but show "Generating" until the report is actually available.



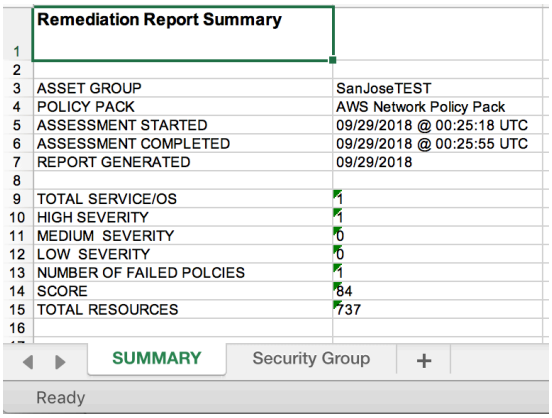
In the Reports screen, the type of report you just requested is "Prioritized Issues."

Notice in the next figure the Download column shows the name of the report rather than the label for PDF or XLS. The tool tip indicates the spreadsheet version is at right.

4. Click the report name at right to download it as the detailed spreadsheet.



The next figure shows the Summary sheet of the report.



	Remediation Report Summary	
1		
2		
3	ASSET GROUP	SanJoseTEST
4	POLICY PACK	AWS Network Policy Pack
5	ASSESSMENT STARTED	09/29/2018 @ 00:25:18 UTC
6	ASSESSMENT COMPLETED	09/29/2018 @ 00:25:55 UTC
7	REPORT GENERATED	09/29/2018
8		
9	TOTAL SERVICE/OS	1
10	HIGH SEVERITY	1
11	MEDIUM SEVERITY	0
12	LOW SEVERITY	0
13	NUMBER OF FAILED POLCIES	1
14	SCORE	84
15	TOTAL RESOURCES	737
16		

SUMMARY | Security Group | +

Ready

5. Click the **Security Group** tab at the bottom of the page. The next figure shows one rule that failed on hundreds of security groups, and the remediation step for this failure. The remediation of this failure propagates to all affected services groups. The see the change in CyberPosture score, run the assessment again.

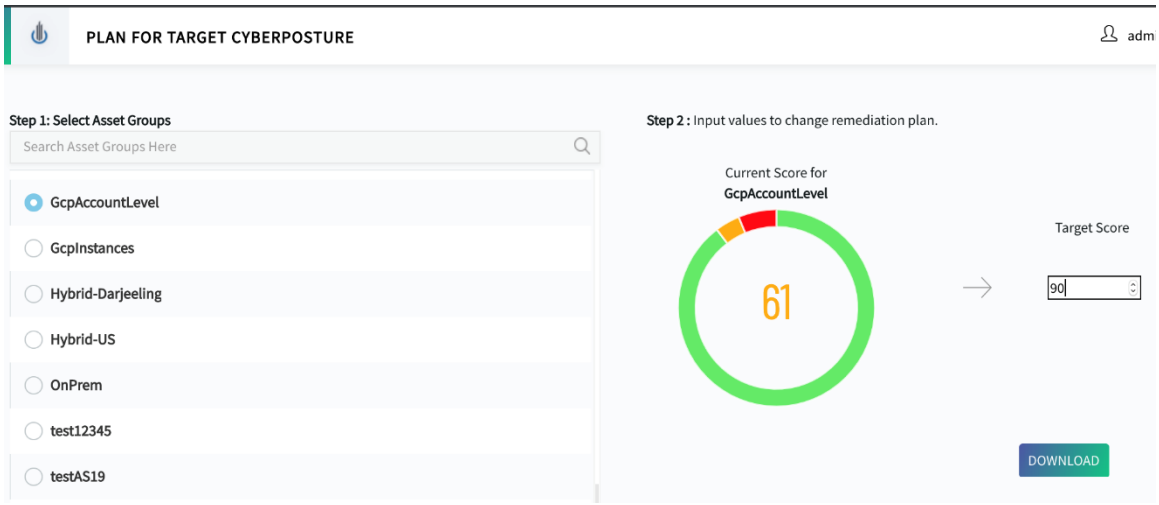
	A	B	C	D
	Remediation Report Detail			
1				
2				
3	ASSET GROUP:	SanJoseTEST		
4	POLICY PACK:	AWS Network Policy Pack		
5	HIGH SEVERITY:	1		
6	MEDIUM SEVERITY:	0		
7	LOW SEVERITY:	0		
8	SERVICE/OS:	Security Group		
9	TOTAL RESOURCES:	737		
10				
11	**POLICY**	**SEVERITY**	**WEIGHT**	**REMEDIATION**
12	Port 10000 (ndmp) is publicly open	HIGH	10.0	Perform the following to implement the prescribed state: * Login to the AWS Management Console at https://console.aws.amazon.com/vpc/home [https://console.aws.amazon.com/vpc/home] * In the left pane, click Security Groups * For each security group, perform the following: * Select the security group * Click the Inbound Rules tab * Identify the rules to be removed * Click the x in the Remove column * Click Save

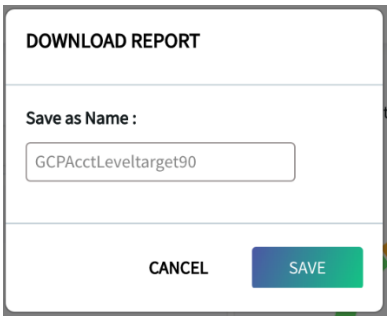
Remediating to a Target Score

This feature lets you create an asset group report that shows how to go from the current CyberPosture score to a score you specify. Any role except DevOps can create a report.

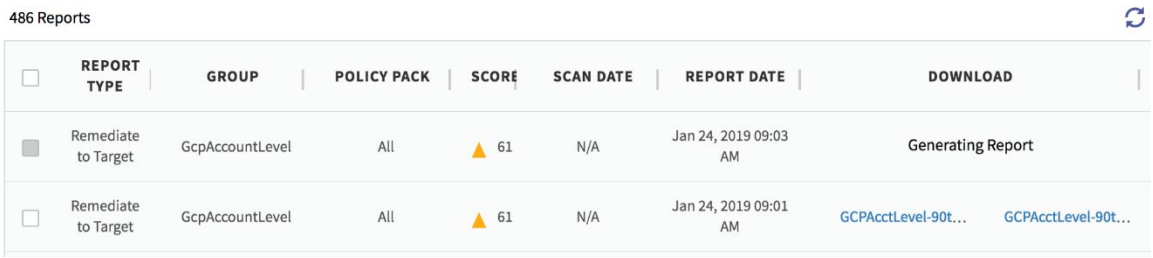
To specify and achieve a CyberPosture score:

1. Navigate: **Respond** > **Plan for Target CyberPosture**. See next figure.
2. Select the name of the asset group whose score you want to improve.
3. In the Target Score box on the right side of the window, select a score.
4. Click **Download**. A popup prompts you to name the report. then states that the guidance for achieving the desired score is in the Reports screen. Click **OK**.





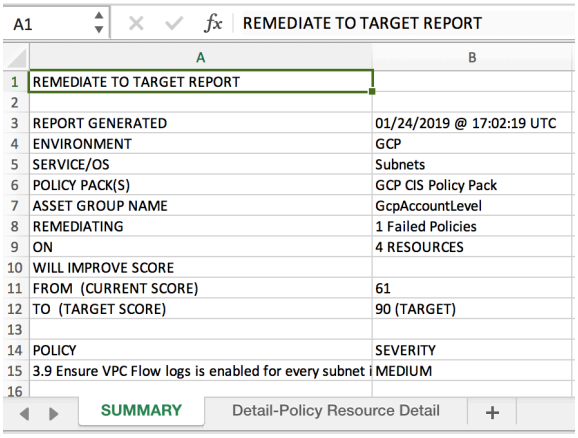
5. Navigate to **Analyze** > **Reports** (available to any role except Devops). The next figure is the report list. The top two rows show the type you want—*Plan to Target*.
6. In the Download column, click the report name at right to download the **XLS** spreadsheet. The spreadsheet is more specific than the report in PDF.



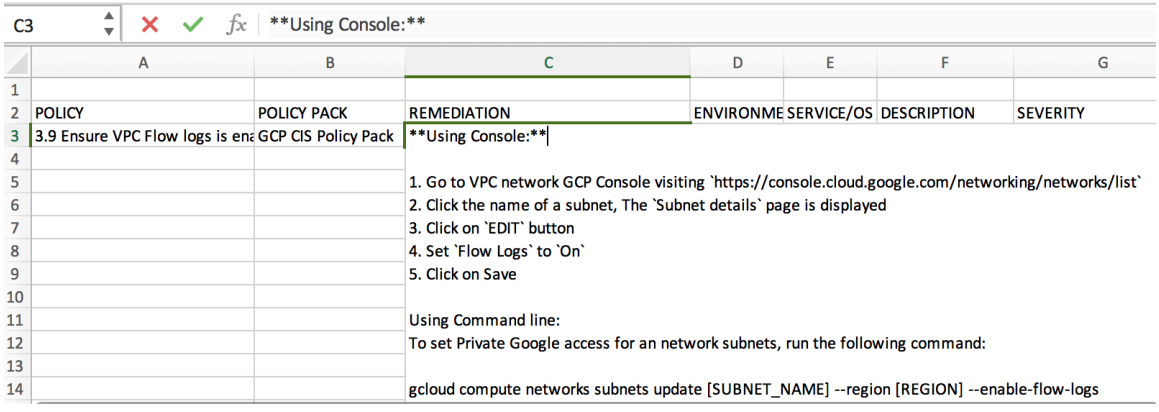
The next figure shows the summary of a target plan. The current score is on the row labeled "From (Current Score);" the target score is on the "To (Target Score)" row.

Notice that the row labeled *Remediating* shows the number of failed policies, and the row labeled *On* shows the number of resources with a specific problem.

7. Click the **Detail-Policy Resource Detail** tab at the bottom of the *Summary* sheet.



8. Expand the contents of Remediation cell for the policy to be corrected. Notice that the remediation is implemented on the CLI.



Resources and Asset Groups

The main mission of the Cavirin solution—discovering vulnerabilities by assessing security and compliance—is configured, scheduled, and launched from either of two areas:

- In *Protect > Discover & Assess Resources*, a new logical asset group is created; its resources are discovered; and its assessment is scheduled for later or now.
- Under *Identify* heading in the nav pane:
    - In the *Asset Groups* screen, *existing* groups can be edited, deleted, re-discovered (if assets are added, subtracted, turned off/on), and their assessment begun.
    - In the *Resources* screen, you can examine assets that are either *compute* (possessing an OS) or *non-compute* (cloud services); assign a *criticality* to each asset; or individually discover a resource or add it to a new asset group. You can initiate discovery and assessment of a resource by adding it to an asset group. For a description of criticality, see Specifying the Criticality of Assets.

NOTE: Cavirin uses the words "asset" and "resource" interchangeably.

The subsections that follow describe how to discover and view the resources, create an asset group by naming and adding resources to it, assess a group, and create and assess a hybrid group.

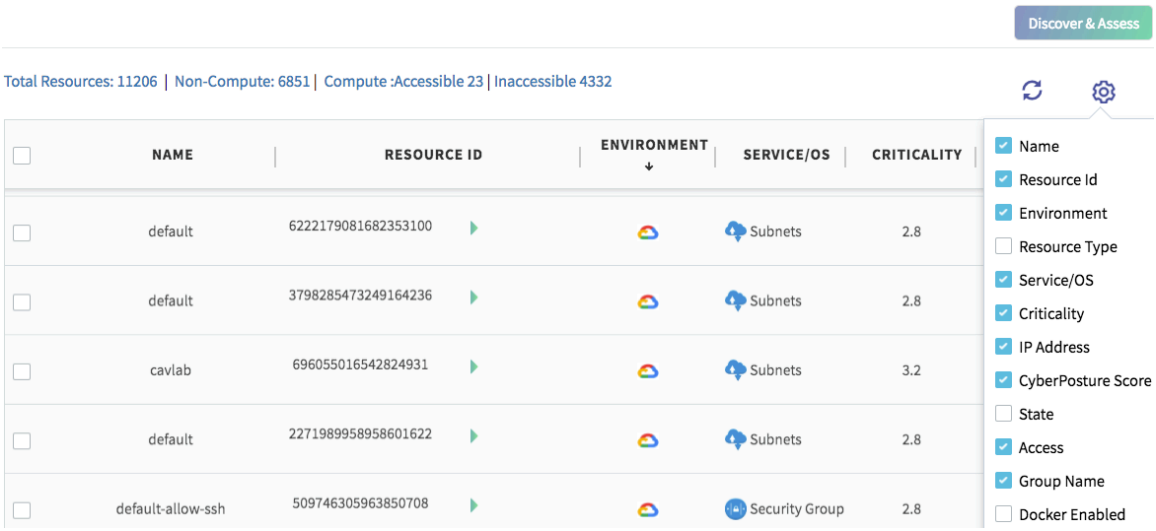
NOTE: The Super Admin can view the *Identify* pages but cannot discover or assess resources or asset groups (the *Discover & Assess* button is inactive). Roles other than Super Admin can discover and assess resources.

Understanding the Resources Area

After you have discovered all the resources—the *compute* resources (with operating systems) and the *non-compute* resources (cloud services)—the resources are visible in the highly filterable Resources screen. The next figure is a comprehensive (unfiltered) view of the Resources page. It shows:

- The top row shows the numbers of *total* assets, *non-compute* resources, *compute* resources, and *inaccessible* resources. These labels also are active links for filtering the display. Filtering can help with your objective. For example, you can create a hybrid group with only the assets that are *compute* and *accessible*.

- To the right of the actions described in the preceding list item are the screen refresh icon, *Discover & Assess* button (not active for a Super Admin), and a gear icon for displaying the columns you can hide or display (shown in the next figure).
- The name column shows the host name that the organization has assigned. The resource ID is generated by the resource itself. The comprehensive list of resources in the next figure is showing only Google Cloud resources and the services for each asset in the Cloud. Each environment or service has its own icon. For example, the Environment column shows the Google Cloud icon, and the visible services are *Subnets* and one *Security Group*. Each cloud provider has its own set of icons for its services. To the right of each *resource ID*, a green arrow head (when applicable) is for opening a popup at right with details about the resource. The next two sections illustrate these details.
- You can add a resource to an asset group after clicking *Discover & Assess* while in any role that has permission to assess the resources.

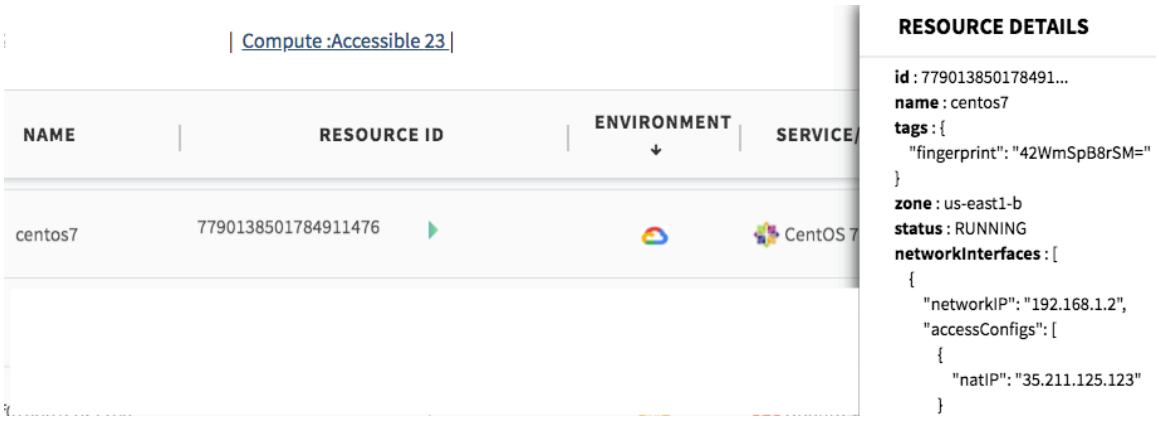


The next figure illustrates compute resources (note the OSs under Service/OS).

NAME	RESOURCE ID	ENVIRONMENT	SERVICE/OS
bgtarget2	3973341730300940213		CentOS 7
bgtest	612550497153499073		Debian 9
centos7	7790138501784911476		CentOS 7
centos7	859e37bb-e484-40d4-829d-d...		CentOS 7
i-01e82c0e64b150991	i-01e82c0e64b150991		Ubuntu 14.04

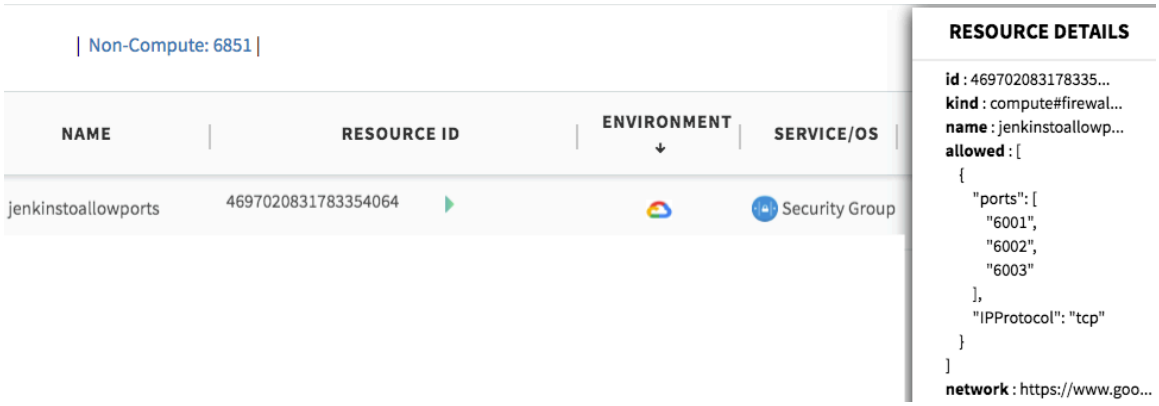
Compute Resources

In the following figure, the focus is on a CentOS 7compute resource. Clicking the green arrowhead next to the resource ID opened a pane of this asset's details. It shows some details in the resource table but also many more details. The details list can be long.



Non-compute Resources

In the following figure, the focus is on a non-compute resource with a *Security Group* service in Google Cloud. Clicking the green arrowhead next to the resource ID opened a pane of resource details. It shows some details that are visible in the resource table but also many more that are not visible, such as the type of service (firewall), allowed TCP ports, and many other details that are not visible in this figure.



First-time Asset Discovery and Adding to an Asset Group

With a new Cavirin installation, the organization needs to discover all the resources it wants Cavirin to assess and monitor. Subsequently, you create asset groups simply by selecting the resources and placing them in asset groups that you name. These asset groups are logical entities on the system that map to the needs of the organization.

Specifying the Criticality of Assets

Cavirin supports your assigning criticality values to each asset. Criticality has three *categories—confidentiality*, *integrity*, and *availability* (CIA)—and 5 levels for any of these categories and a default level of 2:

1. Negligible
2. Low
3. Moderate
4. High
5. Very High

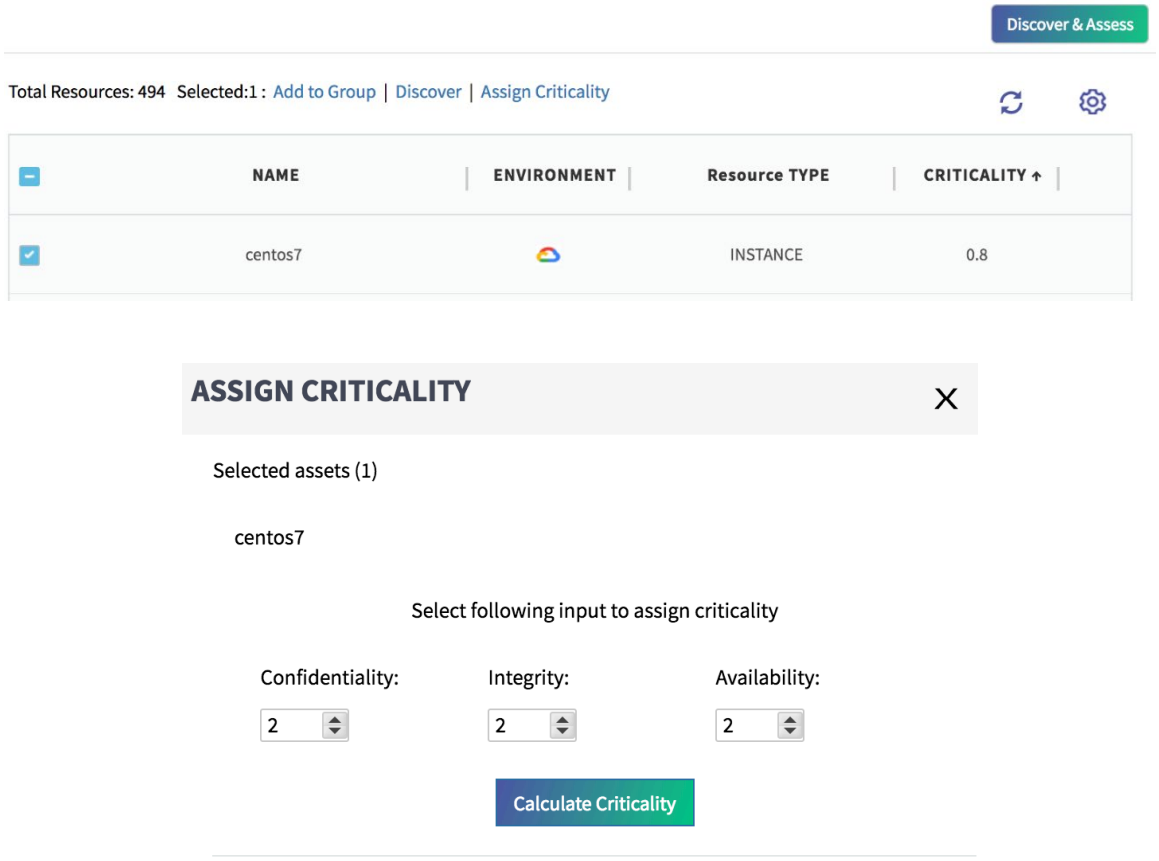
Be aware that the higher the criticality, the lower will be the assessed score because a higher score sets a higher goal for compliance or security.

IMPORTANT: If you change any value and compute the new criticality, the configuration popup displays the new criticality value. However, assigning the new value does not affect the CyberPosture score until you reassess the group.

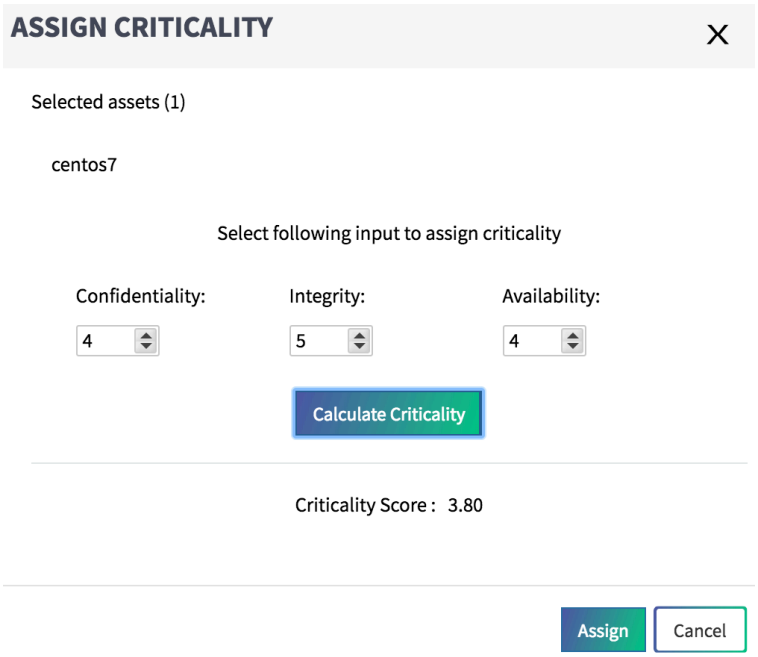
To specify an asset's criticality:

1. Navigate to **Identify** > **Resources** (next figure).
2. Select a resource. A row of functions appears, including **Assign Criticality**.

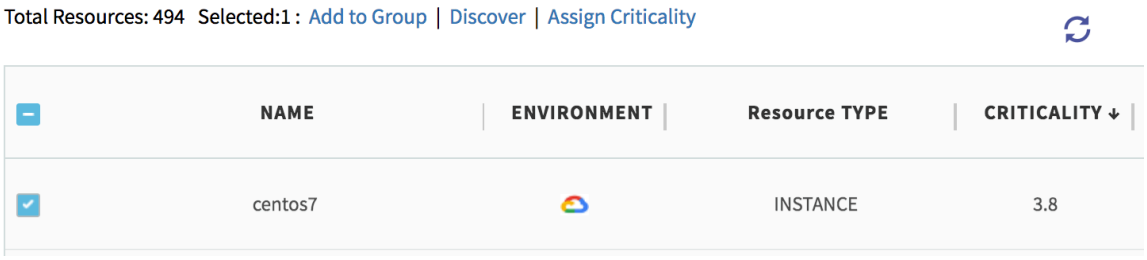
3. Click **Assign Criticality**. Regardless of the *current* settings for criticality, the configuration popup displays the default settings (2 for each category of CIA).



4. For this example, select CIA values of **4-5-4**.
5. Click **Calculate Criticality**. The next figures shows the aggregated criticality ("Criticality Score") below the *Calculate Criticality* button.
6. Click **Assign**.
7. Observe the new criticality for this asset in the resource table.



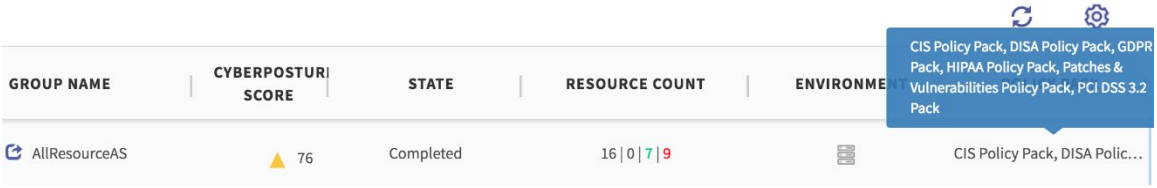
The criticality for this asset now is the value just calculated, as the next figure shows.



Understanding the Asset Groups Area

An asset group is a logical collection of resources. When Cavirin performs an assessment, it is assessing an asset (resource) group. In the Asset Groups area:

- You can view details about each resource in an asset group.
- In the next figure, the Environment column shows a hybrid asset group. (The icon for a hybrid group is a gray data center.) Note the export icon, left of the group name. Clicking this icon opens a list of assets in the group.



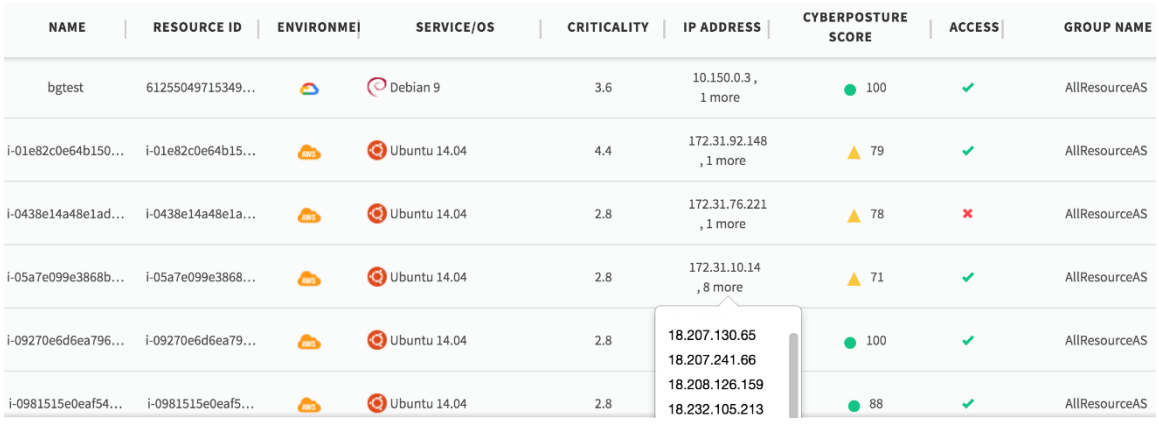
The CyberPosture score is the latest score for every type of assessment of the group. (The list of policy packs applied in an assessment, whether all packs or a subset, is your choice at the time of setting up an assessment.)

The Resource Count column shows the group's total count of resources, non-compute resources, compute resources, and the inaccessible resources.

The *state* of the assessment can be:

- An empty cell: Cavirin has not completed any action on the group.
- *Prescan* means Cavirin is finding the resources by sending pings to on-prem resources or making API calls to clouds.
- *Prescan complete* means the prescan has finished.
- *Discovery* (or *deep discovery*) means Cavirin is gathering details about the compute resources or, in the case of a cloud instances, metadata.
- *Discovery complete* means deep discovery has finished. You can see the discovered data in the Resource table.
- *Scanning* means Cavirin is assessing the assets with selected policy packs.
- *Complete* means the assessment finished. (If no score is visible, it is possible that no resources were accessible. Click the export symbol next to the group name to open the resources table and see whether the asset are accessible.)

To the left of the group name (see preceding figure), the export icon is for opening a browser window of the assets in the group. The next figure illustrates the list of assets in the group (note at bottom the IP address list you can see).



Provisioning and Assessing a Hybrid Asset Group

Cavirin can assess the resources in diverse environments by way of *hybrid asset groups*.

> **NOTE**: For the current release, assessments of a hybrid group apply to operating systems ("compute resources") only, not cloud services.

> **NOTE**: For the current release, the *Usage* setting for host credentials must be *global*. If you specify the credential usage as restricted, the report on the assets shows "N/A." For a description of host credentials, see Creating Host Credentials.

You create a hybrid asset group in the Resource table by placing *compute* assets (assets that have an OS) in a *new* group. Hybrid group assets can be in AWS, Azure, Google Cloud, and on-prem environments.

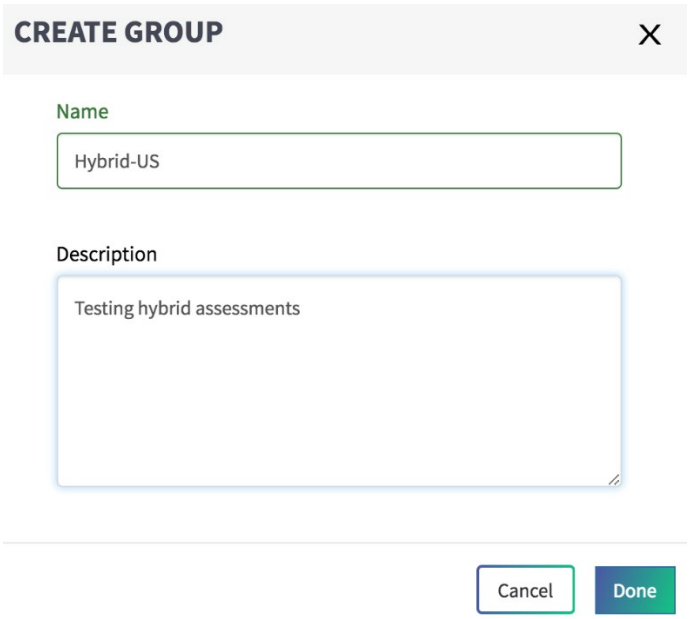
> **IMPORTANT**: Before you create a hybrid asset group, the resources must have been *discovered* and be *accessible*. As needed, set the criticality of each resource if the default is not correct for the resource in any of the categories of confidentiality, integrity, and accessibility. (See Specifying the Criticality of Assets.)

To create a hybrid asset group while in any role except *Super Admin*:

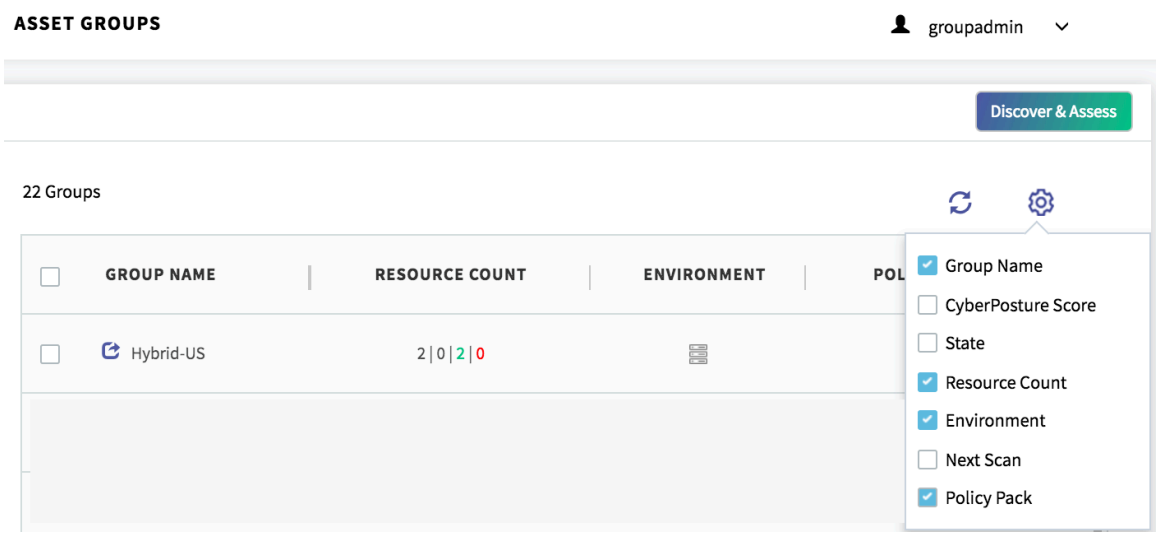
1. Navigate to **Identify** > **Resources**.
2. Click the **Compute: Accessible** option near the top of the page so it shows only the resources that can go into the hybrid group (the next figure has been filtered for accessible compute resources).
3. Select the resources that are running on CentOS7. The **Add to Group** option appears at the top of the resource table (not shown in next figure). Also, note the two selected compute resources have a criticality of 5.0. The popup for naming and describing the new asset group appears as in the subsequent figure.

NAME	RESOURCE ID	ENVIRONMENT	Resource TYPE	CRITICALITY
centos7	779013850178491147 6		INSTANCE	5.0
jenkins-1-vm	522091268332962191 3		INSTANCE	3.6
bgtarget2	397334173030094021 3		INSTANCE	3.6
centos7	859e37bb-e484-40d4-829d-d...		INSTANCE	5.0

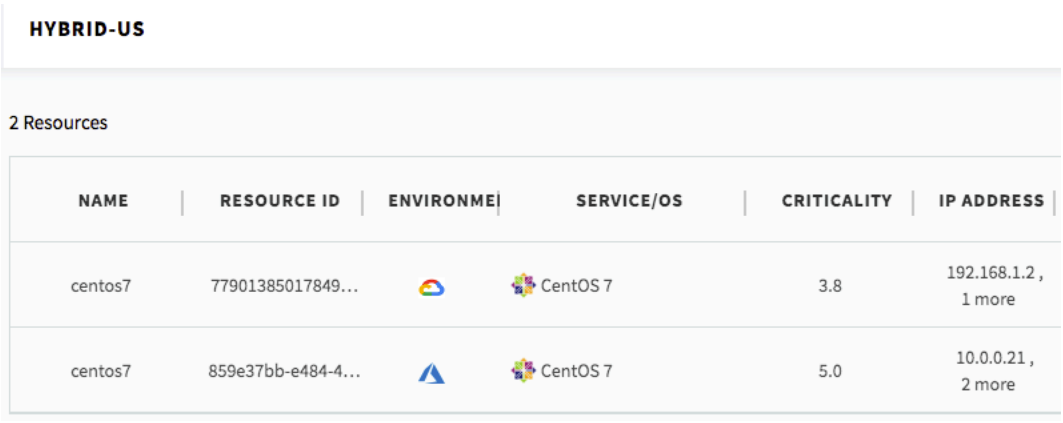
4. Name the hybrid asset group "Hybrid-US" in the *Create Group* popup.
5. Click **Done** when satisfied with the contents.



Hybrid-US now appears in the *Asset Groups* page. The *Environment* column shows the gray data center icon for a hybrid group. This display has been simplified by column selections under the gear icon.



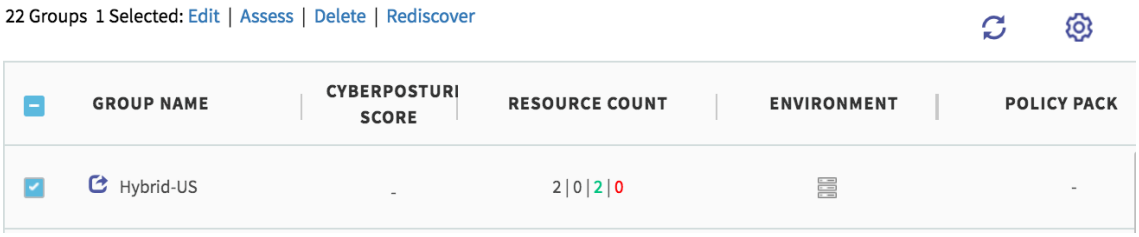
8. Click the export icon to the left of the Hybrid-US name to open a browser window listing Hybrid-US resources. Along with the expected details in the columns, each asset has a score because it was assessed before going into the new group.



9. Specify host credentials for the hybrid group.

   For resource credentials, you can choose among existing credentials after creating the hybrid group. To do so, select the group in the Asset Groups window and then click the **Edit** link that appears at the top of the *Group Name* list. For the credential *Usage*, we usually recommend *restricted*. However, in the current release, only the global usage is supported for a hybrid group. To see the configuration of available credentials or to create credentials for a hybrid group, navigate to **Protect** > **Host Credentials** (see Creating Host Credentials).

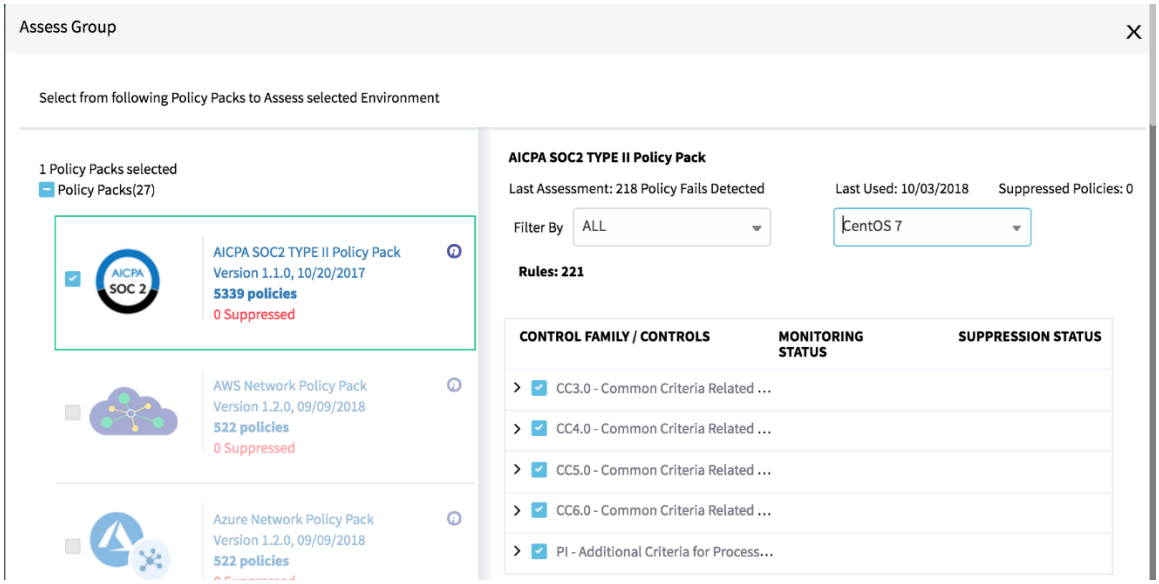
10. Select **Hybrid-US** in the Asset Groups window. *Assess* and other options appear.



11. Click **Assess** to begin the steps for an assessment. The page for selecting policy packs opens.

12. Use the default policy pack, AICPA SOC2, and in the Service/OS dropdown at right, select **CentOS 7**.

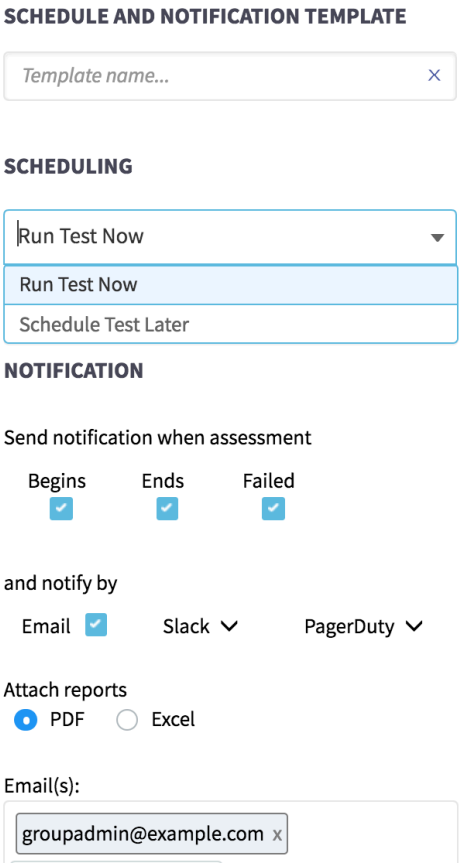
13. Scroll down the policy pack list and **Next** at the bottom of the screen (not shown). The next step is scheduling the assessment and configuring notifications. The subsequent screen the *Schedule and Notifications*.



In the first dropdown of the next popup (Schedule and Notification Template), you could select an existing schedule. In the second dropdown, you can create a new template by choosing **Schedule Test Later**.

1. Keep the default, **Run Test Now** for this workflow.
2. Select the events that can trigger a notification—when the assessment begins, ends, or fails.
3. Select one or more types of notification. The third-party notification options are active only if they have been integrated.

   If you mark the email box, type one or more email addresses. After typing email addresses, click once outside the *Emails(s)* area before continuing to other steps.
4. For email, choose the file format of the report to attach to the email.
5. Click **Done** at lower-right (not shown in next figure) to start the assessment. The next step is for reports.



6. Navigate to **Reports**. And download the resource and remediation reports.

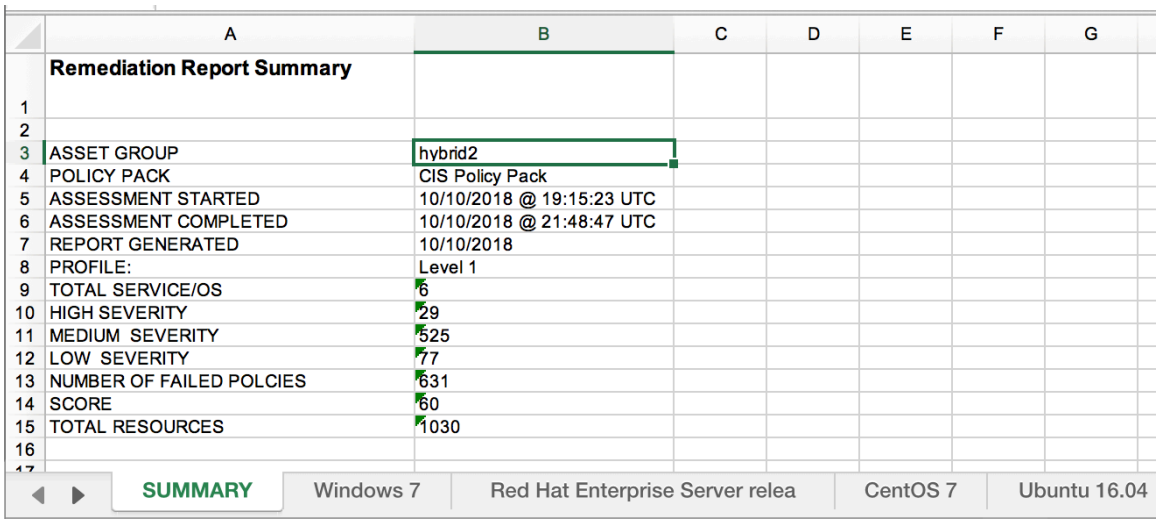
The next two figures show a resource report and a remediation report for the assessment of group *hybrid2* (because of its abundance of data).

The resource report has a row for each resource (1030 resources, as row 15 shows).

	A	B	C	D	
	RESOURCE REPORT SUMMARY				
1					
2	ASSET GROUP	hybrid2			
3	POLICY PACK	**CIS Policy Pack**			
4	ASSESSMENT STARTED	10/10/2018 @ 19:15:23 UTC			
5	ASSESSMENT COMPLETED	10/10/2018 @ 21:48:47 UTC			
6	REPORT GENERATED	10/10/2018			
7	PROFILE:	Level 1			
8	ANALYST	groupadmin			
9	SEVERITY	ALL			
10	HIGH SEVERITY FAIL COUNT	2064			
11	MEDIUM SEVERITY FAIL COUNT	54987			
12	LOW SEVERITY FAIL COUNT	12178			
13	Score	60			
14					
15	1030 RESOURCES				
16					
17	**Resource Name**	**Resource Identifier**	**OS Name**	**Criticality**	**OS/Service**
18	DL7040U14-02	4202931B-B1E5-DF06-7EBC-18DAA99E2F2E	Ubuntu 14.04	0.8	Ubuntu 14.04
19	ubuntu	4235C22D-FCE9-FF2B-5FA3-631A934B55F4	Ubuntu 14.04	0.8	Ubuntu 14.04
20	ubuntu	564DD245-ABF4-E237-A451-DF54A09E8A5C	Ubuntu 14.04	0.8	Ubuntu 14.04
21	DL7047U14-173	422163F0-C022-EF3A-5ACB-ACCCBD92AD70	Ubuntu 14.04	0.8	Ubuntu 14.04
22	DL7056U14-203	4221D473-A5B7-45E4-C17C-7018EB2C7A1E	Ubuntu 14.04	0.8	Ubuntu 14.04
23	DL7041N2U14-198	4202391C-A0F2-6D0F-B068-7AD456F094C7	Ubuntu 14.04	0.8	Ubuntu 14.04
24	DL7040U14-139	4202FB3F-E26E-BAF3-C8D5-6465B96DB663	Ubuntu 14.04	0.8	Ubuntu 14.04
25	DL7047U14-172	42212ADB-1877-1314-D2FE-8CF0ADEB2DD4	Ubuntu 14.04	0.8	Ubuntu 14.04

SUMMARY | CISPP-5836 | CISPP-6158 | CISPP-5603 | CISPP-6355 | CISPP-6201 | CISPP-5842 | CISPP-5788

The remediation report lists the remediation for each resource failure under each operating system in the assessment. With 1030 resources (row 15), this means 1030 times the number of operating systems, some of which appear in the next figure. The figure shows the summary and a sheet for each OS (see tabs at the bottom of the figure).



	A	B	C	D	E	F	G
1	**Remediation Report Summary**						
2							
3	ASSET GROUP	hybrid2					
4	POLICY PACK	CIS Policy Pack					
5	ASSESSMENT STARTED	10/10/2018 @ 19:15:23 UTC					
6	ASSESSMENT COMPLETED	10/10/2018 @ 21:48:47 UTC					
7	REPORT GENERATED	10/10/2018					
8	PROFILE:	Level 1					
9	TOTAL SERVICE/OS	6					
10	HIGH SEVERITY	29					
11	MEDIUM SEVERITY	525					
12	LOW SEVERITY	77					
13	NUMBER OF FAILED POLCIES	631					
14	SCORE	60					
15	TOTAL RESOURCES	1030					
16							

SUMMARY | Windows 7 | Red Hat Enterprise Server relea | CentOS 7 | Ubuntu 16.04

Appendix A – Cavirin Solution Glossary

This appendix defines Cavirin's common terminology:

- *Resource* (synonymous with "asset") is a virtual machine, application, cloud instance, Docker/container, or cloud service.
- *Host* is a resource (or asset) that has an operating system (OS).
- *Resource group (asset group*) is a user-specified, logical collection of assets (or resources) that you create and target for assessment.
- *Workload* is an instance of an OS, container, or virtual machine.
- *Policy framework* is a generic term that refers to all the benchmarks, the policies in all the policy packs, and the other mechanisms that support Cavirin's mission.
- *Control, policy*, and *rule* are synonymous terms that refer to a single best practice, such as not giving a high-risk privilege to all users.
- *Policy packs* are collections of individual security policies (grouped into control families) established by a wide range of standards organizations, such as the National Institute of Standards and Technology (NIST). A policy pack provides a security baseline. Multiple policy packs can be applied in an assessment of a group of assets. Furthermore, the policy pack can be applied in an assessment for all operating systems or a specific operation system.
- *Control family* is a policy grouping based on logical similarities. A control family is a logical association of individual controls (or rules or policies). Example control families are Access Control (AC) and Configuration Management (CM).
- *Hybrid* refers to a group that has resources in different environments and targeted for assessment as one group. A hybrid group can contain assets in different cloud types (from different cloud service providers) or reside in a cloud and on-prem. Placing resources from different environments in one logical group is key to how Cavirin has a unified view of hybrid cloud environments.
- *Security benchmarks* applied by Cavirin are from the Center for Internet Security (CIS) and the Defense Information Systems Agency (DISA). Cavirin uses current best practices to create new benchmarks where they do not yet exist. Cavirin Engineering has contributed to multiple benchmarks from CIS and continues to author new benchmarks for OSs, clouds, and frameworks.
- *Resource discovery* examines an organization's entire on-prem or cloud network and the individual resources (servers, containers, operating systems, and so on). In

addition, for a cloud environment, the choices of applied policy packs determines how deep into the cloud the Cavirin system discovery reaches.

- *Deep discovery* returns system information, release information applicable to the resource (OS and version, for example), the host name and machine ID, or meta data about the resource if a cloud instance.
- *Severity* is the seriousness or danger of a security issue. Severity is computed by Cavirin and can be high, medium, and low. Severity indicates the priority of remediation for the security analyst, response team, devops engineer, and so on.
- *CyberPosture score* represents the current risk, security, or compliance posture. This score is the result of an assessment and has a range of 0 – 100.
- *Agentless* means that Cavirin does not use agents for discovery or analysis. The agentless architecture means lighter overhead and less attack surface.

Appendix B – Definitions of the Assessment State

This section describes the meaning of the *pass* or *fail* state of an assessment. This state refers to the result of one policy applied to one resource. State is a major factor in the assessment scoring—Cavirin uses *pass* or *fail* when computing the score. However, an assessment can return more than *pass* or *fail*, and Cavirin interprets (or maps) those other states to *pass* or *fail*. The table in this appendix defines how Cavirin maps all states to pass or fail. The description begins by showing you how to locate the state of policy result.

Locating a Resource's Per-Policy Assessment State

The path to a resource's assessment state begins in the *Reports* area:

1. Navigate to **Analyze** > **Reports**.

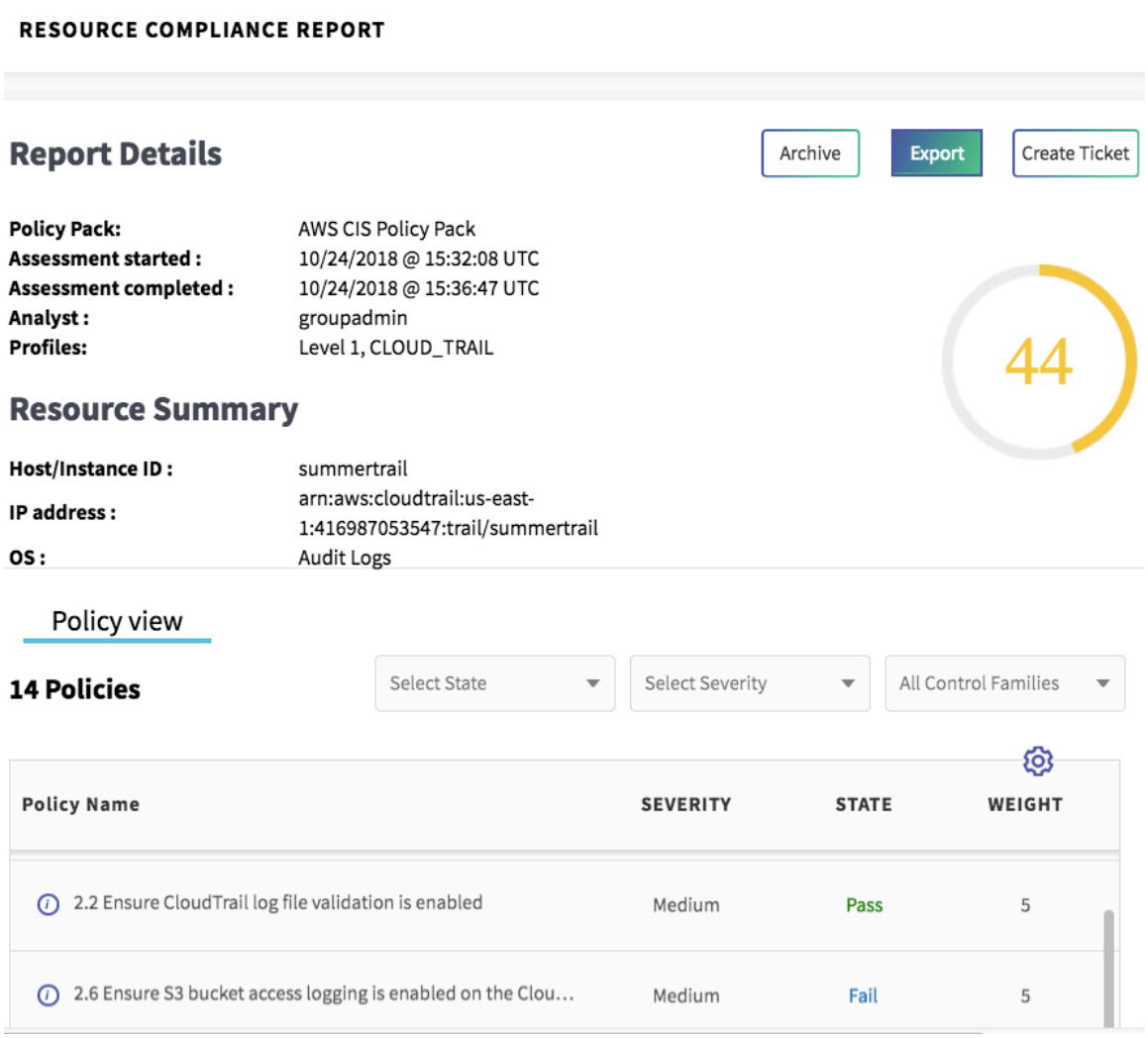
2. Click on the name of the asset group in the Group column for the scan date or report date you want (many reports can exist for a group over time). The report for the group must have a score. The report type can be remediation of device. The type of report that opens is Group Assessment Report.

   Mid-page on the left is the choice for *Device view* or *Remediation view*.

3. Click **Device view** to open a table with assessment results for all the devices (resources) in the group.

4. Click the name of a resource. The *Resource Compliance Report* opens. In the Resource Summary area, the Host/Instance ID field shows 'summertail' for this example. The *Policy view* part of the page identifies each policy applied to this resource, the Cavirin-defined severity of the score, the pass or fail state as described in this appendix, and the weight of policy.

   The State column for this 'summertrail' example has one row for pass and one row for fail.



Mapping the Status of Assessments to Pass or Fail

In a *device report*—whether "device" refers to a compute resource or to a cloud service—the result can have one of different types of status. However, for scoring purposes, the status of each rule's outcome is mapped to *pass* or *fail*. This section defines the mapping of a status to pass or fail. In the following table, "not used" means that Cavirin received the status but did not use it for calculating the CyberPosture score.

Assessment Status	Cavirin's Use in Scoring	Meaning
Pass	pass	The target system or a system component satisfied all conditions of the *<xccdf:Rule>*.

Fixed	pass	The <*xccdf:Rule*> had failed but was then fixed (by a tool that can automatically apply remediation or a human auditor).
Fail	fail	The target system or a system component did not satisfy all conditions of the <*xccdf:Rule*>.
Error	fail	The system could not complete the assessment, so the target's compliance status with the <*xccdf:Rule*> is not certain. This could happen, for example, if the system ran with insufficient privileges and could not gather necessary information.
Unknown	fail	The system encountered a problem, so the result is unknown. For example, this status might mean the system was unable to interpret the output of the test (the output had no meaning to the system).
Not Selected	not used	The <*xccdf:Rule*> was not selected in the benchmark.
Not Applicable	not used	The <*xccdf:Rule*> was not applicable to the target of the test. For example, the <*xccdf:Rule*> might be specific to a different version of the target OS, or it might have been a test against a platform feature that was not installed.
Informational	not used	The <*xccdf:Rule*> was checked, but the output from the system is simply for informing auditors or administrators; it is not a compliance category. This status value is designed for <*xccdf:Rule*> elements whose main purpose is to extract information from the target instead of testing the target.
Not Checked	not used	The <*xccdf:Rule*> was not evaluated by the checking engine. This status is designed for <*xccdf:Rule*> elements that have no <*xccdf:check*> elements or that correspond to an unsupported checking system. It might also correspond to a status returned by a checking engine if the checking engine does not support the indicated check code.

Appendix C – Computing a CyberPosture Score

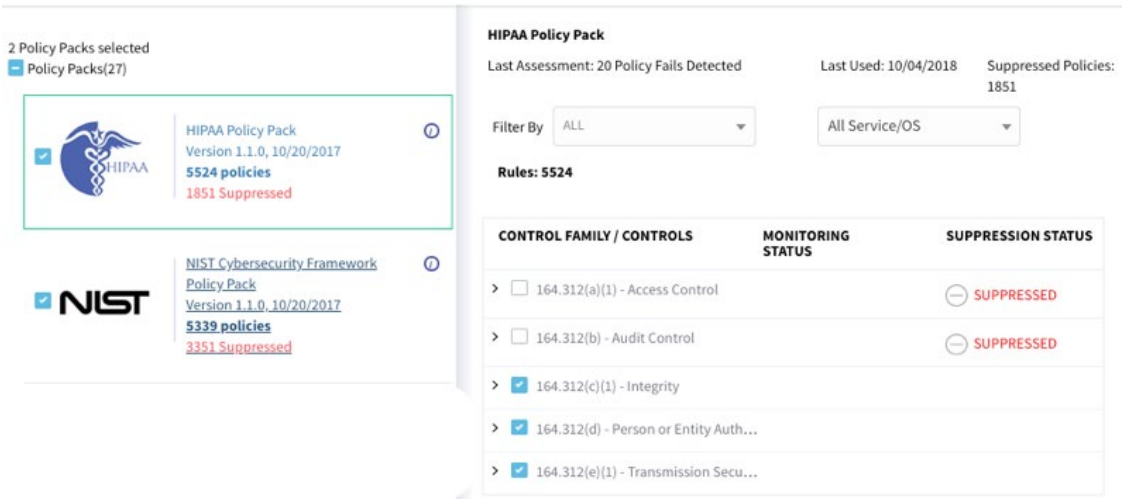
The CyberPosture score in the Dashboard ranges from 0-100. It is the amalgamation of the Security and Compliance scores (also displayed at the Dashboard). The higher the score is, the more secure the environment is. Some policy packs (such as HIPAA) are for compliance, and others are for security (such as CIS).

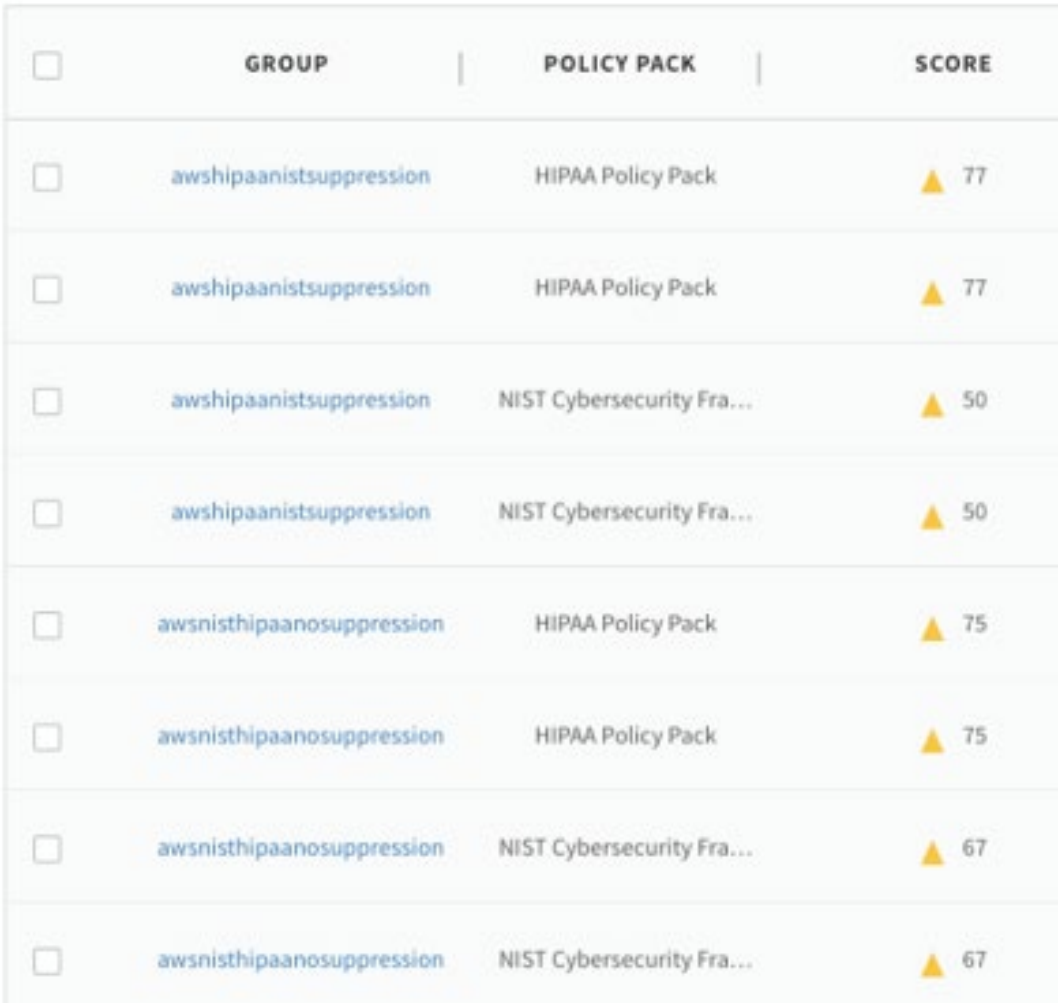
Cavirin's proprietary scoring methodology combines the net results of the latest policy assessments on each resource and the weight of each policy. The score factors together the *most recent* assessments. This means that if some but not all policy packs were applied in an assessment today, the most recent results for the policies *not applied today* still affect the score. The CyberPosture score can also reflect a user-assigned *criticality* for any resource.

Appendix D – Effect of Rule Suppression on Scores

This section illustrates the effect of using the *Compensating Controls* feature—identified in the interface as *rule suppression*. The reason for suppressing rules is that the organization has *compensating controls* that accomplish the security or compliance purpose of the rules to be suppressed. (Auditors are interested in knowing what the valid reasons are.)

Two asset groups are shown: *awshipaanistsuppression* and *awsnisthipaanosuppression*. These groups consist of identical resources in AWS and are evaluated for the same two policy packs except for the suppressed rules: The *awshipaanistsuppression* group has suppressed rules in the first three control families in NIST and the first two families in HIPAA.





GROUP	POLICY PACK	SCORE
awshipaanistsuppression	HIPAA Policy Pack	77
awshipaanistsuppression	HIPAA Policy Pack	77
awshipaanistsuppression	NIST Cybersecurity Fra…	50
awshipaanistsuppression	NIST Cybersecurity Fra…	50
awsnisthipaanosuppression	HIPAA Policy Pack	75
awsnisthipaanosuppression	HIPAA Policy Pack	75
awsnisthipaanosuppression	NIST Cybersecurity Fra…	67
awsnisthipaanosuppression	NIST Cybersecurity Fra…	67

For completeness, the overall CyberPosture score for the asset group is 60 because the table inherits the score from the latest assessment—*awsnoon* in this case.

awshipaanistsuppres…	60	Completed	1548 | 1400 | 66 | 82
awsnisthipaanosupp…	60	Completed	1546 | 1399 | 65 | 82
awsnoon	60	Completed	1542 | 1396 | 64 | 82

Focusing on the NIST results, you see the score when suppressed is once again 50 across all assessed resources. A look at one Ubuntu 16.04 resource reveals 51 with 145 out of the 220 polices suppressed and a calculation based on state and weight. Other resources, with different scores, result in the weighted score of 50.

Policy Name	Severity	State	Weight
Ensure successful file system mounts a	Medium	FAIL	10
Ensure use of privileged commands is c	Medium	FAIL	10
Ensure system is disabled when audit k	Medium	FAIL	10
Ensure unsuccessful unauthorized file a	Medium	FAIL	4
Ensure discretionary access control per	Medium	FAIL	7.5
Ensure session initiation information is c	Medium	FAIL	8.3
Ensure events that modify the system's	Medium	FAIL	10
Ensure events that modify the system's	Medium	FAIL	7.6
Ensure events that modify user/group i	Medium	FAIL	10
Ensure events that modify date and tim	Medium	FAIL	10
Ensure kernel module loading and unlo	Medium	FAIL	10
Ensure file deletion events by users are	Medium	FAIL	6.8
Ensure all AppArmor Profiles are enforci	Low	FAIL	4.3
Ensure default user umask is 027 or mo	Medium	FAIL	5
Ensure all users' home directories exist	Medium	FAIL	4.3
Ensure all groups in /etc/passwd exist i	Medium	FAIL	6.8
Ensure root PATH Integrity	Medium	FAIL	3.3
Ensure core dumps are restricted	Medium	FAIL	4.3
Ensure bootloader password is set	Medium	FAIL	6.8
Ensure separate partition exists for /var/	Low	FAIL	6.8
Ensure separate partition exists for /var	Low	FAIL	4.3
Ensure separate partition exists for /tmp	Low	FAIL	5
Ensure noexec option set on /dev/shm p	Medium	FAIL	4.3
Ensure separate partition exists for /hom	Low	FAIL	4.3
Ensure separate partition exists for /var/	Low	FAIL	4.3
Ensure separate partition exists for /var/	Low	FAIL	7.2
Ensure auditing for processes that start	Medium	FAIL	10
Ensure filesystem integrity is regularly c	Medium	FAIL	10
Ensure AIDE is installed	Medium	FAIL	7.5
Ensure chrony is configured	Medium	PASS	4
Ensure ntp is configured	Medium	PASS	7.5
Ensure login and logout events are coll	Medium	PASS	2.1
Ensure changes to system administratio	Medium	PASS	2.1
Ensure system administrator actions (su	Medium	PASS	6.8
Ensure no legacy "+" entries exist in /et	Medium	PASS	5.3
Ensure SSH LoginGraceTime is set to o	Low	PASS	7.6
Ensure address space layout randomiz	Low	PASS	5.3
Ensure nodev option set on /home parti	Medium	PASS	5.3
Ensure nosuid option set on /var/tmp pa	Medium	PASS	4.4
Ensure shadow group is empty	Medium	PASS	6.5
Ensure prelink is disabled	Low	PASS	0.8
Ensure no unconfined daemons exist	Low	PASS	1.7
Ensure no legacy "+" entries exist in /et	Medium	PASS	5.3
Ensure password hashing algorithm is S	Medium	PASS	6.8
Ensure nosuid option set on /dev/shm p	Medium	PASS	5
Ensure the SELinux state is enforcing	Low	PASS	4.3
Ensure no users have .rhosts files	High	PASS	10
Ensure no users have .netrc files	Medium	PASS	9.3
Ensure no users have .forward files	Medium	PASS	6.8
Ensure cron daemon is enabled	Medium	PASS	10
Ensure noexec option set on /var/tmp p	Medium	PASS	6.8
Ensure nodev option set on /var/tmp pa	Medium	PASS	7.6
Ensure nodev option set on /tmp partiti	Medium	PASS	7.5
Ensure SELinux is not disabled in bootl	Low	PASS	5
Disable Automounting	Low	PASS	6.8
Ensure AppArmor is not disabled in boo	Medium	PASS	6.8
Ensure nodev option set on /dev/shm p	Medium	PASS	4.3
Ensure no legacy "+" entries exist in /et	Medium	PASS	7.5
Ensure nosuid option set on /tmp partiti	Medium	PASS	6.8
Ensure SELinux policy is configured	Low	PASS	9.3
Ensure rsyslog Service is enabled	Medium	PASS	10
Ensure auditd service is enabled	Medium	PASS	10
Ensure rsyslog or syslog-ng is installed	Medium	PASS	3.3
Ensure syslog-ng service is enabled	Medium	PASS	4.3
		pass	212
		fail	202
			49%

Now look at the same resource, this time with non-suppressed rules. Of the 220 policies, some are *non-scored* or *informational*, and these do not appear in the table as pass or fail. Of the rules that appear, 30% fail, yielding a score of 70. Other resources have different scores and result in the weighted score of 67.

Policy Name	Severity	State	Weight
Ensure permissions on all logfiles are c	Medium	FAIL	9.3
Ensure rsyslog is configured to send lo	Medium	FAIL	10
Ensure the audit configuration is immut	Medium	FAIL	6.8
Ensure no ungrouped files or directories	Medium	FAIL	7.5
Ensure no unowned files or directories e	Medium	FAIL	8.5
Ensure no world writable files exist	Medium	FAIL	5
Ensure access to the su command is re	Medium	FAIL	4.3
Ensure at/cron is restricted to authorize	Medium	FAIL	7.5
Ensure permissions on bootloader conf	Medium	FAIL	4.3
Ensure sticky bit is set on all world-writat	Low	FAIL	9.3
Ensure /etc/hosts.deny is configured	Medium	FAIL	4.3
Ensure firewall rules exist for all open p	Medium	FAIL	4.7
Ensure loopback traffic is configured	Medium	FAIL	6.8
Ensure source routed packets are not a	Medium	FAIL	7.5
Ensure IP forwarding is disabled	Medium	FAIL	6.1
Ensure default deny firewall policy	Medium	FAIL	6.1
Ensure system accounts are non-login	Medium	FAIL	6.8
Ensure inactive password lock is 30 da	Medium	FAIL	7.2
Ensure minimum days between passwo	Medium	FAIL	5
Ensure password expiration is 90 days	Medium	FAIL	7.6
Ensure password creation requirements	Medium	FAIL	6.8
Ensure mounting of FAT filesystems is c	Low	FAIL	6.8
Ensure mounting of squashfs filesystem	Low	FAIL	4.9
Ensure successful file system mounts a	Medium	FAIL	10
Ensure use of privileged commands is c	Medium	FAIL	10
Ensure system is disabled when audit lo	Medium	FAIL	10
Ensure unsuccessful unauthorized file a	Medium	FAIL	4
Ensure discretionary access control per	Medium	FAIL	7.5
Ensure session initiation information is c	Medium	FAIL	8.3
Ensure events that modify the system's	Medium	FAIL	10
Ensure events that modify the system's	Medium	FAIL	7.6
Ensure events that modify user/group in	Medium	FAIL	10
Ensure events that modify date and tim	Medium	FAIL	10
Ensure kernel module loading and unlo	Medium	FAIL	10
Ensure file deletion events by users are	Medium	FAIL	6.8
Ensure all AppArmor Profiles are enforci	Low	FAIL	4.3
Ensure default user umask is 027 or mo	Medium	FAIL	5
Ensure all users' home directories exist	Medium	FAIL	4.3
Ensure all groups in /etc/passwd exist in	Medium	FAIL	6.8
Ensure root PATH Integrity	Medium	FAIL	3.3
Ensure core dumps are restricted	Medium	FAIL	4.3
Ensure bootloader password is set	Medium	FAIL	6.8
Ensure separate partition exists for /var/l	Low	FAIL	6.8
Ensure separate partition exists for /var	Low	FAIL	4.3
Ensure separate partition exists for /tmp	Low	FAIL	5
Ensure noexec option set on /dev/shm p	Medium	FAIL	4.3
Ensure separate partition exists for /hon	Low	FAIL	4.3
Ensure separate partition exists for /var/l	Low	FAIL	4.3
Ensure separate partition exists for /var/l	Low	FAIL	7.2
Ensure auditing for processes that start	Medium	FAIL	10
Ensure filesystem integrity is regularly cl	Medium	FAIL	10
Ensure AIDE is installed	Medium	FAIL	7.5
Ensure only approved MAC algorithms a	Medium	PASS	7.6
Ensure rsyslog default file permissions c	Medium	PASS	4.9
Ensure syslog-ng default file permission	Medium	PASS	4.3
Ensure audit logs are not automatically	Medium	PASS	10
Ensure permissions on /etc/cron.daily a	Medium	PASS	5
Ensure permissions on /etc/cron.d are c	Medium	PASS	10
Ensure permissions on /etc/ssh/sshd_co	Medium	PASS	10
Ensure permissions on /etc/shadow- ar	Medium	PASS	3.6
Ensure permissions on /etc/hosts.allow	Medium	PASS	4.3
Ensure permissions on /etc/group are c	Medium	PASS	7.5
Ensure permissions on /etc/gshadow- a	Medium	PASS	4.3
Ensure permissions on /etc/shadow are	Medium	PASS	6.8
Ensure permissions on /etc/group- are c	Medium	PASS	4.9
Ensure SSH access is limited	Medium	PASS	5
Ensure permissions on /etc/cron.monthl	Medium	PASS	5
Ensure permissions on /etc/passwd- are	Medium	PASS	10
Ensure permissions on /etc/cron.hourly	Medium	PASS	7.5
Ensure permissions on /etc/crontab are	Medium	PASS	4.3
Ensure permissions on /etc/gshadow ar	Medium	PASS	10
Ensure permissions on /etc/cron.weekly	Medium	PASS	10
Ensure permissions on /etc/hosts.deny a	Medium	PASS	10
Ensure permissions on /etc/issue are c	Medium	PASS	7.5
Ensure users own their home directories	Medium	PASS	10
Ensure users' home directories permissi	Medium	PASS	9.3
Ensure users' .netrc Files are not group	Medium	PASS	4.3
Ensure users' dot files are not group or	Medium	PASS	2.6
Ensure permissions on /etc/passwd are	Medium	PASS	10
Ensure /etc/hosts.allow is configured	Medium	PASS	6.1
Ensure TCP SYN Cookies is enabled	Medium	PASS	5
Ensure Reverse Path Filtering is enable	Medium	PASS	2.1
Ensure bogus ICMP responses are ignc	Medium	PASS	4.3
Ensure broadcast ICMP requests are ig	Medium	PASS	9.3
Ensure suspicious packets are logged	Medium	PASS	2.1
Ensure secure ICMP redirects are not a	Medium	PASS	4.3
Ensure ICMP redirects are not accepte	Medium	PASS	5
Ensure packet redirect sending is disab	Medium	PASS	10
Ensure TCP Wrappers is installed	Medium	PASS	5
Ensure SSH MaxAuthTries is set to 4 or	Medium	PASS	7.6
Ensure SSH Idle Timeout Interval is cont	Medium	PASS	4.3
Ensure iptables is installed	Medium	PASS	3.5
Ensure no duplicate user names exist	High	PASS	7.6
Ensure no duplicate GIDs exist	High	PASS	4.3
Ensure no duplicate UIDs exist	High	PASS	9.3
Ensure password fields are not empty	High	PASS	5
Ensure no duplicate group names exist	High	PASS	4.3
Ensure password reuse is limited	Medium	PASS	2.1
Ensure password expiration warning da	Medium	PASS	6.8
Ensure SSH PermitEmptyPasswords is	High	PASS	7.5
Ensure root is the only UID 0 account	High	PASS	10
Ensure default group for the root accou	Medium	PASS	4.3
Ensure mounting of freevxfs filesystems	Low	PASS	10
Ensure SSH HostbasedAuthentication	Medium	PASS	9.3
Ensure DNS Server is not enabled	Medium	PASS	10
Ensure HTTP server is not enabled	Medium	PASS	10
Ensure xinetd is not enabled	Medium	PASS	7.6
Ensure mounting of udf filesystems is d	Low	PASS	7.8
Ensure mounting of hfsplus filesystems	Low	PASS	0.8
Ensure FTP Server is not enabled	Medium	PASS	5
Ensure NIS Client is not installed	Low	PASS	6.8
Ensure telnet server is not enabled	High	PASS	10
Ensure talk server is not enabled	High	PASS	2.1
Ensure rsync service is not enabled	Medium	PASS	9.3
Ensure DHCP Server is not enabled	Medium	PASS	5.8
Ensure discard services are not enable	Medium	PASS	6.8
Ensure daytime services are not enable	Medium	PASS	10
Ensure chargen services are not enabl	Medium	PASS	6.8
Ensure GDM login banner is configured	Medium	PASS	10
Ensure rsh server is not enabled	High	PASS	10
Ensure time services are not enabled	Medium	PASS	2.1
Ensure SSH IgnoreRhosts is enabled	Medium	PASS	2.1
Ensure mounting of cramfs filesystems i	Low	PASS	7.5
Ensure NIS Server is not enabled	Medium	PASS	2.1
Ensure mounting of hfs filesystems is di	Low	PASS	5
Ensure mounting of jffs2 filesystems is c	Low	PASS	7.2
Ensure message of the day is configur	Medium	PASS	5
Ensure CUPS is not enabled	Medium	PASS	10
Ensure X Window System is not installe	Medium	PASS	3.5
Ensure SSH root login is disabled	Medium	PASS	10
Ensure SSH Protocol is set to 2	High	PASS	4.3
Ensure SSH LogLevel is set to INFO	Medium	PASS	5
Ensure SSH warning banner is configur	Medium	PASS	2.1
Ensure SSH X11 forwarding is disabled	Medium	PASS	6.8
Ensure LDAP client is not installed	Medium	PASS	0.8
Ensure telnet client is not installed	Low	PASS	4.3
Ensure talk client is not installed	Low	PASS	2.1
Ensure rsh client is not installed	Low	PASS	5
Ensure NFS and RPC are not enabled	Medium	PASS	4.3
Ensure mail transfer agent is configure	Medium	PASS	10
Ensure SNMP Server is not enabled	Medium	PASS	9.3
Ensure HTTP Proxy Server is not enabl	Medium	PASS	9.3
Ensure tftp server is not enabled	High	PASS	7.6
Ensure SSH PermitUserEnvironment is c	Medium	PASS	9.3
Ensure Avahi Server is not enabled	Medium	PASS	7.8
Ensure LDAP server is not enabled	Medium	PASS	10
Ensure IMAP and POP3 server is not e	Medium	PASS	4.3
Ensure echo services are not enabled	Medium	PASS	6.8
Ensure Samba is not enabled	Medium	PASS	6.8
Ensure chrony is configured	Medium	PASS	4
Ensure ntp is configured	Medium	PASS	7.5
Ensure login and logout events are coll	Medium	PASS	2.1
Ensure changes to system administrati	Medium	PASS	2.1
Ensure system administrator actions (su	Medium	PASS	6.8
Ensure no legacy "+" entries exist in /et	Medium	PASS	5.3
Ensure SSH LoginGraceTime is set to o	Low	PASS	7.6
Ensure address space layout randomiz	Low	PASS	5.3
Ensure nodev option set on /home parti	Medium	PASS	5.3
Ensure nosuid option set on /var/tmp pa	Medium	PASS	4.4
Ensure shadow group is empty	Medium	PASS	6.5
Ensure prelink is disabled	Low	PASS	0.8
Ensure no unconfined daemons exist	Low	PASS	1.7
Ensure no legacy "+" entries exist in /et	Medium	PASS	5.3
Ensure password hashing algorithm is S	Medium	PASS	6.8
Ensure nosuid option set on /dev/shm p	Medium	PASS	5
Ensure the SELinux state is enforcing	Low	PASS	4.3
Ensure no users have .rhosts files	High	PASS	10
Ensure no users have .netrc files	Medium	PASS	9.3
Ensure no users have .forward files	Medium	PASS	6.8
Ensure cron daemon is enabled	Medium	PASS	10
Ensure noexec option set on /var/tmp p	Medium	PASS	6.8
Ensure nodev option set on /var/tmp pa	Medium	PASS	7.6
Ensure nodev option set on /tmp partiti	Medium	PASS	7.5
Ensure SELinux is not disabled in boot	Low	PASS	5
Disable Automounting	Low	PASS	6.8
Ensure AppArmor is not disabled in boo	Medium	PASS	6.8
Ensure nodev option set on /dev/shm p	Medium	PASS	4.3
Ensure no legacy "+" entries exist in /et	Medium	PASS	7.5
Ensure nosuid option set on /tmp partiti	Medium	PASS	6.8
Ensure SELinux policy is configured	Low	PASS	9.3
Ensure rsyslog Service is enabled	Medium	PASS	10
Ensure auditd service is enabled	Medium	PASS	10
Ensure rsyslog or syslog-ng is installed	Medium	PASS	3.3
Ensure syslog-ng service is enabled	Medium	PASS	4.3

fail	355
pass	839
	30%

This is the end of the *Cavirin User Guide*.