Cavirin CyberPosture Intelligence for the Hybrid Cloud

Cavirin Administrator Guide – Winter 2019

February 25 2019

Table of Contents

Introduction

The primary audience for this *Cavirin Administrator Guide* is system administrators who are skilled with the environment(s) of your organization (on-prem environment or cloud).

The tasks In this *Guide* are set-up procedures you perform on the CLI and in the Cavirin system's user interface (UI). After you set up the necessities and create the accounts for regular users, you can direct users to the *Cavirin User Guide* for regular operation.

When you create a user account and assign an email address, the user receives a system-generated password, which he or she must change to a strong password. Users can later change their password within their profile.

For the CLI, you need the privileges to run commands at the level described in this *Guide*.

For activities in the UI, Cavirin supports role-based access control (RBAC). Of the four default RBAC roles, you use all of them at least once in this *Guide*.

The SuperAdmin 's Access in the UI

In the current release, the areas to which only a SuperAdmin has access are:

- Licenses
- Application Settings
- Users & Roles
- Integrations

Although not used with this Guide, other areas where the SuperAdmin shares some permissions with other roles are:

- Browse & Tailor Policy Packs
- Alerts (issues in a cloud environment, found by the cloud monitoring feature)
- Plan for Target CyberPosture (a plan to achieve a certain CyberPosture score)
- Reports

Outline of Tasks in the UI

Although many of the tasks in this Guide entail a mix of CLI commands and UI steps, this section lists the tasks by role and in the sequence as they appear in this *Guide*. In general, nearly all tasks belong to the SuperAdmin role. The Group Admin role has limited application here, and the DevOps and Analyst roles are used only once.

SuperAdmin

- First-time login after you install the Cavirin system

- Upload of the product license (unless the Cavirin system is in AWS)
- Configure SMTP
- Integrate your organization's third-party applications with the Cavirin system
- Create user accounts

How Cavirin Manages Credentials and Sensitive Information

Cavirin uses third-party software, Hashi-Corp's Vault™, to store credentials and sensitive information. The Vault service is installed along with the Cavirin software to aid in protecting credentials.

Vault encrypts the credentials and other sensitive information prior to writing them to its storage. Vault uses AES256 to encrypt and decrypt data, so if unauthorized users gain access to the raw storage, that access is not enough for them to gain access to data.

Subsequently, the system uses a secure token in an API call to get credentials from Vault.

For more information about Vault, visit https://www.hashicorp.com.

Tasks Performed on the CLI

Some tasks in this *Guide* are performed on the CLI (RBAC roles are not involved):

- Pre-requisite, network-related tasks that enable the Cavirin system to communicate with your organization's computing environment and assets.
- Installing the Cavirin system in the environment.
- Upgrading a Cavirin system from Summer Release to Winter Release, as needed. See the Upgrading a System from Summer to Winter Release section.
- Migrating the Cavirin database from Spring Release to Winter Release, as needed. See the Migrating the Data from Spring to Summer 2018 SP2 section.

  Modifying the threshold of monitored events that trigger an auto-assessment.

Required Network Parameters

This section lists the networking configurations that Cavirin needs for communicating with and assessing an environment. The TCP ports and OS-dependent services are listed below but are not configured on the Cavirin system; they must be configured before you start the tasks listed in the

Initial Tasks on the Cavirin System section.

DNS

The Cavirin system must be connected to the appropriate DNS system.

Internet Connectivity

Although an on-prem system can be installed by way of an OVA, the upgrade of any system necessitates Internet connectivity.

Windows

- Windows Remote Management (WinRM) should be enabled and running. By default, WinRM is installed but not running.
- The WinRM version should be 2.0 or higher. To check the release number, users can run the **winrm id** command on the CLI.
- WinRM over HTTP is on TCP port 5985. WinRM over HTTPS is on TCP port 5986. WMI uses port 135. Windows uses port 135 for remote management and ICMP for pings in on-prem assessments.
- Cavirin users should have WMI privileges. To initiate an assessment, a user must have at least a local administrator permission and be a member of a local admin group or domain admin group.

Linux

- Linux uses SSH and must have access through port 22 and also must support ICMP for pings in on-prem assessments. (An option for changing the SSH TCP port exists in the Administer area of the UI and is documented in this *User Guide*. See the Application Settings section for details.)
- Users must have access to passwordless **sudo** before they can use it.

Ports for APIs

- For API calls to a Javascript server, port 443 must be open.

Installing a New Cavirin System

This installation procedure applies to all environments that host a new Winter release of the Cavirin system.

1. Copy the tar file to /tmp directory or the directory of your choice.

   mkdir -p /tmp/PulsarBuild

   mv $TARFILE /tmp/PulsarBuild

2. Untar the file.

   cd /tmp/PulsarBuild

   tar -xvf $TARFILE

3. Run the installer script with the **clean** option.

   ./Pulsar-SingleVM-Installer.sh clean

After installing the Cavirin system, you can log into it at the IP address of the system and follow the steps for a first-time login. See First-time Login to a New Cavirin System.

Upgrading a System from Summer to Winter Release

1. Copy the tar file to /tmp directory or the directory of your choice.

   mkdir -p /tmp/PulsarBuild

   mv $TARFILE /tmp/PulsarBuild

2. Untar the file.

   cd /tmp/PulsarBuild

   tar -xzf $TARFILE

3. Run the installer script with the **upgrade** option.

   ./Pulsar-SingleVM-Installer.sh upgrade

Upgrading a Cavirin System from Spring to Winter 2018

Cavirin does not support a direct upgrade path from a Spring release to a Winter release. The system first must be upgraded from the Spring release to a Summer SP2 release, as described in Installing a Summer SP2 System. This intermediate upgrade also necessitates a process of migrating the Spring release database to Summer SP2, as described in Migrating the Data from Spring to Summer 2018 SP2.

The steps for upgrading a Cavirin system depend on whether the down-rev system is a version of Summer 2018 or a release before Summer 2018 (Spring SP1 or Spring SP2):

- For *upgrading* Summer 2018 SP1 to Summer 2018 SP2, see
- .
- For *migrating* Spring 2018 SP1 or Spring 2018 SP2 to Summer 2018 SP2, see **Error! Not a valid bookmark self-reference.**. (The first step for this process is to install a new Summer 2018 system, as described in

- Introduction
- The primary audience for this *Cavirin Administrator Guide* is system administrators who are skilled with the environment(s) of your organization (on-prem environment or cloud).

The tasks In this *Guide* are set-up procedures you perform on the CLI and in the Cavirin system's user interface (UI). After you set up the necessities and create the accounts for regular users, you can direct users to the *Cavirin User Guide* for regular operation.

When you create a user account and assign an email address, the user receives a system-generated password, which he or she must change to a strong password. Users can later change their password within their profile.

For the CLI, you need the privileges to run commands at the level described in this *Guide*.

For activities in the UI, Cavirin supports role-based access control (RBAC). Of the four default RBAC roles, you use all of them at least once in this *Guide*.

The SuperAdmin 's Access in the UI

In the current release, the areas to which only a SuperAdmin has access are:

- Licenses
- Application Settings
- Users & Roles
- Integrations

Although not used with this Guide, other areas where the SuperAdmin shares some permissions with other roles are:

- Browse & Tailor Policy Packs
- Alerts (issues in a cloud environment, found by the cloud monitoring feature)
- Plan for Target CyberPosture (a plan to achieve a certain CyberPosture score)
- Reports

Outline of Tasks in the UI

Although many of the tasks in this Guide entail a mix of CLI commands and UI steps, this section lists the tasks by role and in the sequence as they appear in this *Guide*. In general, nearly all tasks belong to the SuperAdmin role. The Group Admin role has limited application here, and the DevOps and Analyst roles are used only once.

SuperAdmin

- First-time login after you install the Cavirin system
- Upload of the product license (unless the Cavirin system is in AWS)
- Configure SMTP
- Integrate your organization's third-party applications with the Cavirin system
- Create user accounts

How Cavirin Manages Credentials and Sensitive Information

Cavirin uses third-party software, Hashi-Corp's Vault™, to store credentials and sensitive information. The Vault service is installed along with the Cavirin software to aid in protecting credentials.

Vault encrypts the credentials and other sensitive information prior to writing them to its storage. Vault uses AES256 to encrypt and decrypt data, so if unauthorized users gain access to the raw storage, that access is not enough for them to gain access to data.

Subsequently, the system uses a secure token in an API call to get credentials from Vault.

For more information about Vault, visit https://www.hashicorp.com.

Tasks Performed on the CLI

Some tasks in this *Guide* are performed on the CLI (RBAC roles are not involved):

- Pre-requisite, network-related tasks that enable the Cavirin system to communicate with your organization's computing environment and assets.
- Installing the Cavirin system in the environment.
- Upgrading a Cavirin system from Summer Release to Winter Release, as needed. See the Upgrading a System from Summer to Winter Release section.
- Migrating the Cavirin database from Spring Release to Winter Release, as needed. See the Migrating the Data from Spring to Summer 2018 SP2 section.

  Modifying the threshold of monitored events that trigger an auto-assessment.

Required Network Parameters

This section lists the networking configurations that Cavirin needs for communicating with and assessing an environment. The TCP ports and OS-dependent services are listed below but are not configured on the Cavirin system; they must be configured before you start the tasks listed in the

Initial Tasks on the Cavirin System section.

DNS

The Cavirin system must be connected to the appropriate DNS system.

Internet Connectivity

Although an on-prem system can be installed by way of an OVA, the upgrade of any system necessitates Internet connectivity.

Windows

- Windows Remote Management (WinRM) should be enabled and running. By default, WinRM is installed but not running.
- The WinRM version should be 2.0 or higher. To check the release number, users can run the **winrm id** command on the CLI.
- WinRM over HTTP is on TCP port 5985. WinRM over HTTPS is on TCP port 5986. WMI uses port 135. Windows uses port 135 for remote management and ICMP for pings in on-prem assessments.
- Cavirin users should have WMI privileges. To initiate an assessment, a user must have at least a local administrator permission and be a member of a local admin group or domain admin group.

Linux

- Linux uses SSH and must have access through port 22 and also must support ICMP for pings in on-prem assessments. (An option for changing the SSH TCP port exists in the Administer area of the UI and is documented in this *User Guide*. See the Application Settings section for details.)
- Users must have access to passwordless **sudo** before they can use it.

Ports for APIs

- For API calls to a Javascript server, port 443 must be open.

- Installing a New .)

Installing a Summer SP2 System

This installation procedure applies to all environments that host a Summer release.

1. Copy the tar file to /tmp directory or the directory of your choice.

   mkdir -p /tmp/PulsarBuild

   mv $TARFILE /tmp/PulsarBuild

2. Untar the file.

   cd /tmp/PulsarBuild

   tar -xzf $TARFILE

3. Run the installer script with the **clean** option.

   ./Pulsar-SingleVM-Installer.sh clean

Migrating the Data from Spring to Summer 2018 SP2

This section describes how to migrate the data from a Spring 2018 SP1 or SP2 system to a Summer 2018 SP2 system as a stage of upgrading from Spring to Winter release. Data migration consists of two core processes:

1. Converting specific data sets in the Spring system
2. Moving the converted data to the Summer 2018 system

This description:

- Lists the data sets that will be transferred
- Lists pre-requisite tasks and information
- Walks you through the tasks on the new system and the CLI of the Spring system
- Takes you through a verification process after the migration finishes
- Points out how things vary for a Cavirin system in AWS and on-prem
- Describes how to create a PEM key for an on-prem system that has no PEM key

The volume of data determines how long the transfer lasts, usually one to five minutes. Thereafter, you confirm that the data transferred correctly by examining it in the Summer system. No rollback is supported! Subsequently, you delete the old Cavirin system.

The data sets this procedure transfers are:

1. Credentials – host and cloud (if applicable)
2. Assessment schedules
3. Asset groups but not the assets themselves (you will have to rediscover assets)
4. User accounts
5. Integrations (Slack, Jira, and so on)
6. Application settings – SMTP, custom port configurations, SSO configuration (for Summer SP1 in the current release of this migration utility)
7. Reports (the largest data set)

Pre-requisites

This section describes pre-requisite steps to take before the data migration and the pre-requisite information you should know before beginning the data transfer.

1. A clean VM with a Summer 2018 SP2 system (the destination VM) must be installed in the same environment as the Spring system (the source VM). Complete the new installation as described in

2. Introduction

3. The primary audience for this Cavirin Administrator Guide is system administrators who are skilled with the environment(s) of your organization (on-prem environment or cloud).

The tasks In this *Guide* are set-up procedures you perform on the CLI and in the Cavirin system's user interface (UI). After you set up the necessities and create the accounts for regular users, you can direct users to the *Cavirin User Guide* for regular operation.

When you create a user account and assign an email address, the user receives a system-generated password, which he or she must change to a strong password. Users can later change their password within their profile.

For the CLI, you need the privileges to run commands at the level described in this *Guide*.

For activities in the UI, Cavirin supports role-based access control (RBAC). Of the four default RBAC roles, you use all of them at least once in this *Guide*.

The SuperAdmin 's Access in the UI

In the current release, the areas to which only a SuperAdmin has access are:

- Licenses
- Application Settings
- Users & Roles
- Integrations

Although not used with this Guide, other areas where the SuperAdmin shares some permissions with other roles are:

- Browse & Tailor Policy Packs
- Alerts (issues in a cloud environment, found by the cloud monitoring feature)
- Plan for Target CyberPosture (a plan to achieve a certain CyberPosture score)
- Reports

Outline of Tasks in the UI

Although many of the tasks in this Guide entail a mix of CLI commands and UI steps, this section lists the tasks by role and in the sequence as they appear in this *Guide*. In general, nearly all tasks belong to the SuperAdmin role. The Group Admin role has limited application here, and the DevOps and Analyst roles are used only once.

SuperAdmin

- First-time login after you install the Cavirin system
- Upload of the product license (unless the Cavirin system is in AWS)
- Configure SMTP
- Integrate your organization's third-party applications with the Cavirin system
- Create user accounts

How Cavirin Manages Credentials and Sensitive Information

Cavirin uses third-party software, Hashi-Corp's Vault™, to store credentials and sensitive information. The Vault service is installed along with the Cavirin software to aid in protecting credentials.

Vault encrypts the credentials and other sensitive information prior to writing them to its storage. Vault uses AES256 to encrypt and decrypt data, so if unauthorized users gain access to the raw storage, that access is not enough for them to gain access to data.

Subsequently, the system uses a secure token in an API call to get credentials from Vault.

For more information about Vault, visit https://www.hashicorp.com.

Tasks Performed on the CLI

Some tasks in this *Guide* are performed on the CLI (RBAC roles are not involved):

- Pre-requisite, network-related tasks that enable the Cavirin system to communicate with your organization's computing environment and assets.
- Installing the Cavirin system in the environment.
- Upgrading a Cavirin system from Summer Release to Winter Release, as needed. See the Upgrading a System from Summer to Winter Release section.
- Migrating the Cavirin database from Spring Release to Winter Release, as needed. See the Migrating the Data from Spring to Summer 2018 SP2 section.

  Modifying the threshold of monitored events that trigger an auto-assessment.

Required Network Parameters

This section lists the networking configurations that Cavirin needs for communicating with and assessing an environment. The TCP ports and OS-dependent services are listed below but are not configured on the Cavirin system; they must be configured before you start the tasks listed in the

Initial Tasks on the Cavirin System section.

DNS

The Cavirin system must be connected to the appropriate DNS system.

Internet Connectivity

Although an on-prem system can be installed by way of an OVA, the upgrade of any system necessitates Internet connectivity.

Windows

- Windows Remote Management (WinRM) should be enabled and running. By default, WinRM is installed but not running.
- The WinRM version should be 2.0 or higher. To check the release number, users can run the **winrm id** command on the CLI.
- WinRM over HTTP is on TCP port 5985. WinRM over HTTPS is on TCP port 5986. WMI uses port 135. Windows uses port 135 for remote management and ICMP for pings in on-prem assessments.
- Cavirin users should have WMI privileges. To initiate an assessment, a user must have at least a local administrator permission and be a member of a local admin group or domain admin group.

Linux

- Linux uses SSH and must have access through port 22 and also must support ICMP for pings in on-prem assessments. (An option for changing the SSH TCP port exists in the Administer area of the UI and is documented in this *User Guide*. See the Application Settings section for details.)
- Users must have access to passwordless **sudo** before they can use it.

Ports for APIs

- For API calls to a Javascript server, port 443 must be open.

4. Installing a New before you begin the steps described in Cavirin License and User Credentials on the Summer Release System.

    - You should know the IP address of the source (Spring) system and the destination (Summer) system.

5. On the new Summer SP2 system, you will create two passwords (for two of the user roles in Summer release). Later, you provide these passwords on the Spring system in the migration process. These roles are part of Cavirin's role-based access control (RBAC) in Summer release. The roles are SuperAdmin (username *administrator*) and Group Admin (username *groupadmin*).

- You also specify host credentials as a *username* and a PEM key on the Spring system. (The *username* is **ubuntu** in AWS, **cavirin** on-prem.) This PEM key is the Summer release's key, but you place a copy on the old Spring system. Even if an on-prem system normally does not use a PEM key file, data migration necessitates a PEM key file. A description of PEM key generation and upload to the on-prem Spring system is in
- Creating a PEM Key File.

6. Ports 22, 443, and 5432 must be open between the two systems. The two Cavirin instances must be able to communicate over port 22.

- Download *migration.zip* from the Cavirin website, copy it to the Spring system.

NOTE: You will be running commands in a *migration* directory you create. For commands in the *migrate* directory, you must be the owner of the directory to run them.

7. At the conclusion of the data transfer instructions, the text points out that all old user accounts are in the Summer *default user group* (part of Cavirin's RBAC).

The following is a high-level view of the migration workflow:

8. Run the export script on the Spring release system: **./export-master.sh**
9. Run the import script on the Spring release system:
    - **./import-master.sh** (a series of prompts will follow)
    - Enter a username: **ubuntu** (for AWS) or **cavirin** (for on-prem).
    - Enter the full path *on the* Spring *system* of the PEM key file.
    - Enter password for *administrator*.
    - Enter password for *groupadmin*.

Overview of the Migration Sequence

After reading and acting as needed on the items in the pre-requisites list:

1. From your local host, go to the following location (requires registration):

   https://cavirin.zendesk.com/hc/en-us/articles/360017693411-Migration-from-Spring-2018-Summer-2018-

   Notice the Amazon link to the zipped migration file at the bottom. This link applies to AWS and on-prem.

2. Download *migration.zip* to your local host.

3. Transfer the file to the Cavirin Spring instance (with a tool such as WinSCP).

4. Unpack the file; confirm two scripts are present: *export-master.sh* and *import-master.sh*.

NOTE: Obstacles to data migration can be incorrect permissions, the wrong PEM key, or network problems.

Cavirin License and User Credentials on the Summer Release System

The next steps are necessary on the Summer system. You will upload a product license and specify user login credentials for *administrator* (SuperAdmin role) and *groupadmin* (Group Admin role).

1. Go to the IP address of the Summer instance.

2. **Upload** a license key. It can be the same license as the Spring build uses. If you do not have the license, contact support@cavirin.com.

3. Log into the Summer system with default username **administrator** and password **cavirin123**.

4. Change the password when prompted. Securely record the new password.

5. Log out.

6. Log in with username **groupadmin** and the same password, **cavirin123**.

7. Change the password when prompted. Securely record the new password.

8. Log out.

Export

The export process prepares the data sets named in the Introduction for migration to the new system. You can copy and paste grey highlighted text from these procedures into the CLI.

1. Log into the Spring system.

2. Create a directory named *summer18export*:

mkdir summer18export

3. **cd** into the *summer18export* directory:

   cd summer18export

4. Download the zipped file with the migration scripts and other files by clicking the link in Cavirin Zendesk or running the following **wget** command to access the amazon S3 link:

   wget https://s3.amazonaws.com/pulsar-summer-release-2018/migration.zip

5. **unzip** the migration script:

   unzip migration.zip

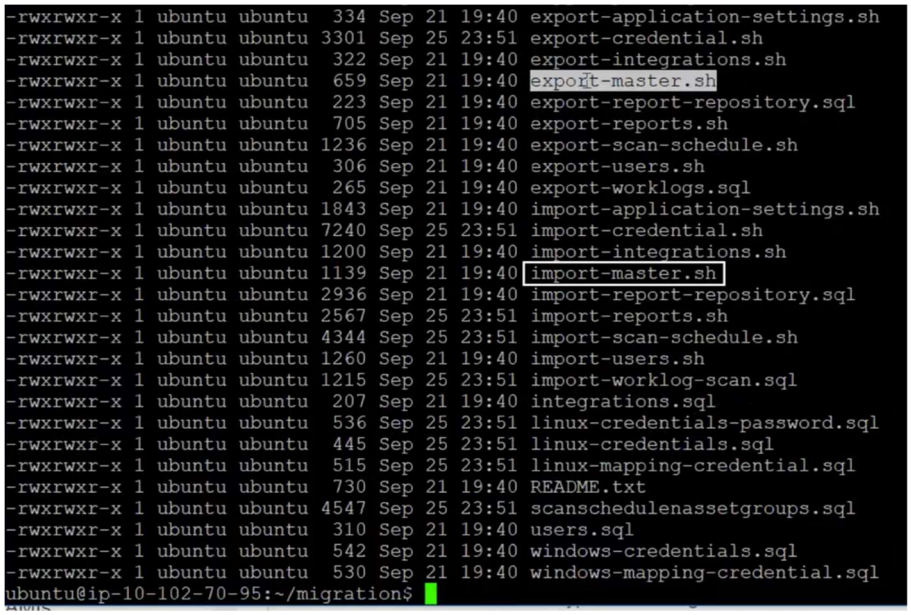
6. Make the script files executable by entering:

   chmod +x -R migration

7. **cd** into the migration folder:

   cd migration

8. Run **ls** and confirm the *migration* folder contains *export-master.sh* and *import-master.sh,* similar to the highlighted fields in the next figure:



9. Run the following to initiate conversion of the data sets described in the Introduction. A message at the bottom of the window ("Yay!!! Done with Export.") confirms the data conversion succeeded.

   cavirin@ip-(*IP addr for Spring instance*)**:~/migration$ ./export-master.sh**

Import

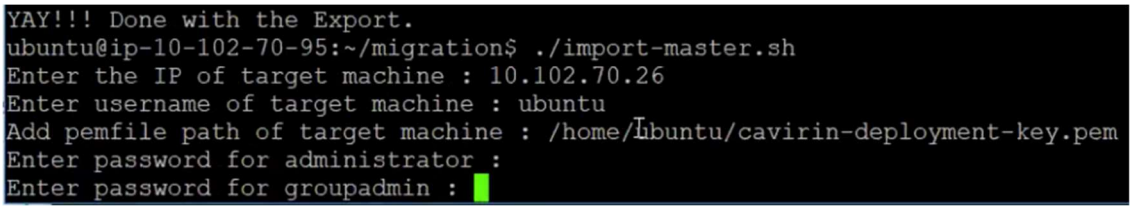
The *import* action copies the *exported* data sets to the new Summer 2018 system. Migration can take up to five minutes and often less than a minute. The duration depends on the volume of data.

> **IMPORTANT**: If you do not have a PEM key file, specify a PEM key on the old Spring system before starting the import. As needed, see Creating a PEM Key File.

Start the import by running the following command from within your local migration directory:

cavirin@ip-(*IP address Spring instance*)**:~/migration$ ./import-master.sh**

The system prompts for the IP address of the destination Summer system. The next figure illustrates the preceding entry and the next several entries and prompts for a Cavirin system in an AWS environment.



10. Enter the IP address of the destination (Summer) system. These prompts follow:

    a. Enter a username for the (destination) target system. *Username* is *cavirin* if the destination is an on-prem Cavirin, *ubuntu* if the destination Cavirin is in AWS.

    b. Enter the full path to the PEM key for the target machine, regardless of current directory.

    c. It prompts you for the password for **administrator** (of the Summer system) and for **groupadmin** (of the Summer system). The data immediately start to migrate.

Followup

This section describes the data verification and other tasks you perform after migration finishes and before you delete the Spring system (no rollback is supported). For detailed information about the tasks in this section, refer to the *Cavirin User Guide Summer 2018*.

NOTE: After you log in, refresh the various screens as needed to see the migrated data.

With Summer 2018 release, access to areas of the system depend on the role in which you log in. For the current followup, you alternately log in with username *administrator* and *groupadmin* to check different functional areas. The following list shows the data sets you confirm and the username you use to log in:

11. Credentials – host and cloud (if applicable): *administrator*

12. User accounts: *administrator*
13. Integrations (Slack, Jira, and so on): *administrator*
14. Application settings – SMTP, custom port settings, SSO: *administrator*
15. Reports: *groupadmin* or *administrator*
16. Asset groups—but not the assets themselves: *groupadmin*
17. Assessment schedules: *groupadmin*

One thing you notice in *Identify > Asset Groups* (*Infrastructure > My Groups* in Spring release) is that no resources are listed. The *Resource Count* column indicates no resources with the "0|0|0|0." These four numbers refer to total resources, non-compute resources (cloud services), compute resources (possessing an OS), and inaccessible resources. See the *Cavirin User Guide* for details about these resource counts.

Log in as *groupadmin*, select each group, and click **Rediscover** (top of screen).

Creating a PEM Key File

The instructions in this section are for generating a PEM key on the Summer release system and securely copying the key to the Spring release system. Except where indicated, the instructions in this section apply to an on-prem Cavirin system and an AWS deployment of a Cavirin system.

> **NOTE**: The specific keywords in this first step are recommended because if you use just the **ssh-keygen** command alone to generate the key, a DSA key is created. However, an RSA key is decrypted a little faster, so changing the key type to RSA is recommended.

1. Enter the following on the Summer system's CLI to create the RSA key:

   ssh-keygen -t rsa -C *<your email address>*

   The system then asks where to store the key.

2. You can click **Enter** to store the key in the default *.ssh* folder. The system asks if you want to specify a passphrase. A passphrase for data migration is optional.
3. If you do not want a passphrase, click **Enter** again.
4. Enter the following on the CLI of the Summer release system: **cd /home/cavirin**
5. Enter: **cd .ssh**
6. Enter: **ls**

You should see the files *id_rsa* (private key) and *id_rsa.pub* (public key). The file transfer method is your choice, but this description illustrates it with WinSCP.

7. Start a WinSCP session (for example) and connect to the Summer release. Then:
    a) Change the File Protocol to SCP (if using WinSCP).
    b) Enter the new IP address as the host name.
    c) Enter the environment-specific username and password pairs:
        - **cavirin**/**NOVAnova** for an on-prem Cavirin instance
        - **ubuntu**/**NOVAnova** for an AWS EC2 instance
8. Find the *id_rsa* and *id_rsa.pub* files.
9. From within the WinSCP window, copy *id_rsa* to the local computer.
10. Open another new WinSCP session and connect to the Spring release system.
11. Copy *id_rsa* to the *summer18export* folder on the old Spring release system.
12. Log back into the old Spring instance via the terminal.
13. Run **ls** and **cd** commands in the *summer18export* directory to be sure *id_rsa* is present.
14. To make the PEM key read-only, enter: **chmod 400 id_rsa**
15. The PEM key has been created and placed in the correct location.
16. When you are prompted to enter a PEM key into the migration sequence, type the entire path regardless of the current directory:

    /home/cavirin/summer18export/id_rsa

First-time Login to a New Cavirin System

This section describes your first-time login on a new system and how to bring the system to a state of readiness for normal operation.

After you complete the mandatory tasks and important optional tasks, users in the role of Group Admin, DevOps, or Analyst can start using the system to discover and assess resources, analyze the results, perform remediation where needed, and so on. Regular use of the Cavirin system is described in the *Cavirin User Guide*.

This section starts after a new VM has been installed. (See

Installing a New Cavirin System for a description of how to do a clean install.)

Initial Tasks on the Cavirin System

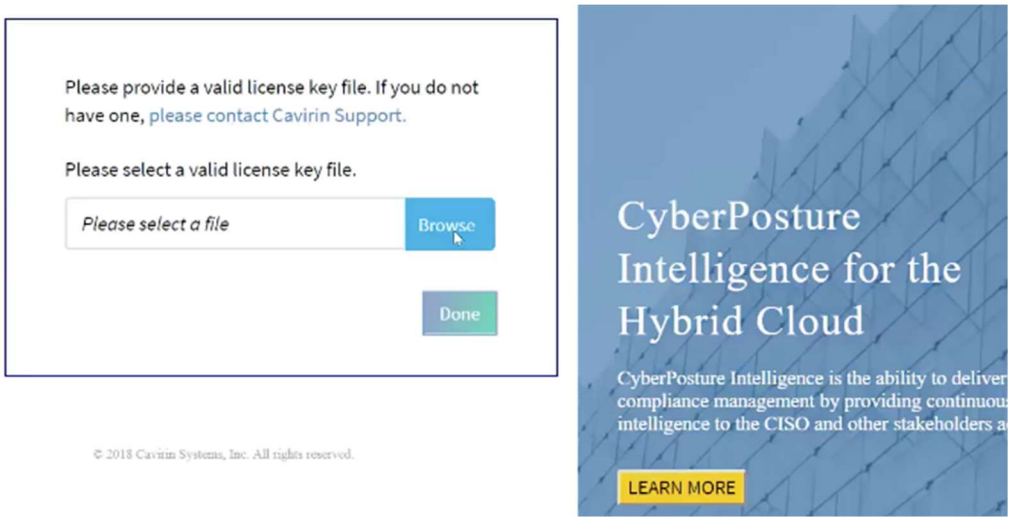
The tasks introduced in this section are:

- Using a browser to reach the IP address of the new Cavirin system (a Chrome incognito window is recommended).
- Uploading a product license that you received from Cavirin and downloaded to a local host. This is the bring-your-own-license (BYOL) model. It applies to on-prem Cavirin installs or any cloud service provider that supports BYOL. An AWS environment can support the BYOL model or a mechanism in the AWS management portal that makes unnecessary a BYOL download/upload process.
- Specifying a unique, strong password for the four default user roles for Cavirin's RBAC. The first role is the SuperAdmin (default username *administrator*), and the second role is Group Admin (default username *groupadmin*).
- Logging in with SuperAdmin role (username *administrator* and new password) to:
    - Configure SMTP.
    - (Optional) Configure one or more third-party integrations for Slack, Jira, PagerDuty, ServiceNow, or Google's Cloud Security Command Center if you plan to use these services. See Integrating Third-party Notification Services for the descriptions.
    - (Optional) Configure single sign-on (SSO) with Okta if SSO is used.

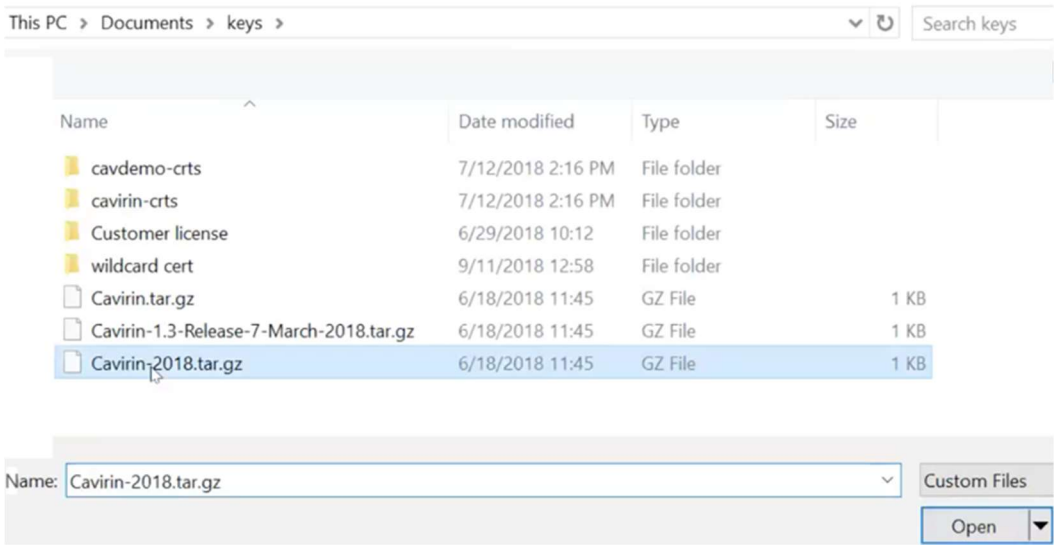
First-time Login

To begin:

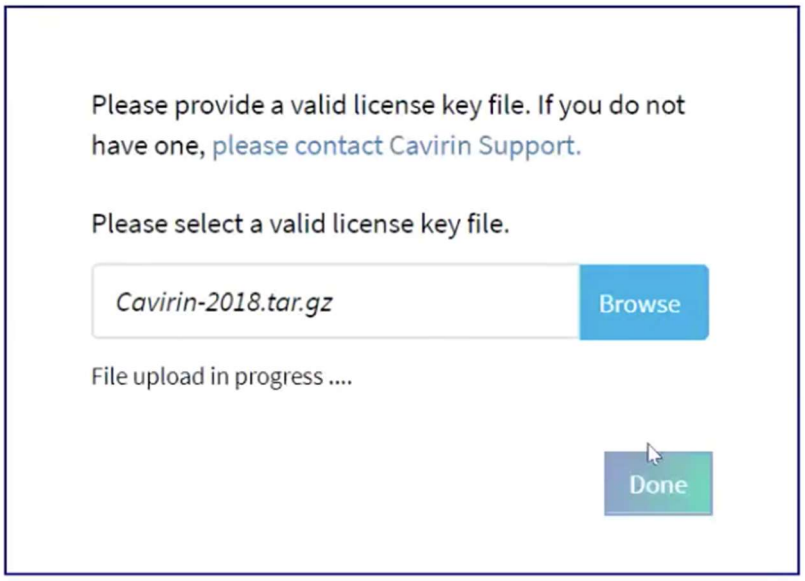
1. Use a browser to navigate to the IP address of the Cavirin system. The request for the Cavirin product license appears as in the next figure. (For a Cavirin system installed in AWS, licensing already might have been arranged through AWS.)



2. Browse to the license (unless already added in AWS as mentioned in Step 1) and click **Open** (a Windows system in the next figure):



3. After the upload finishes and the *Done* button becomes active, click **Done**. The system displays the login area.

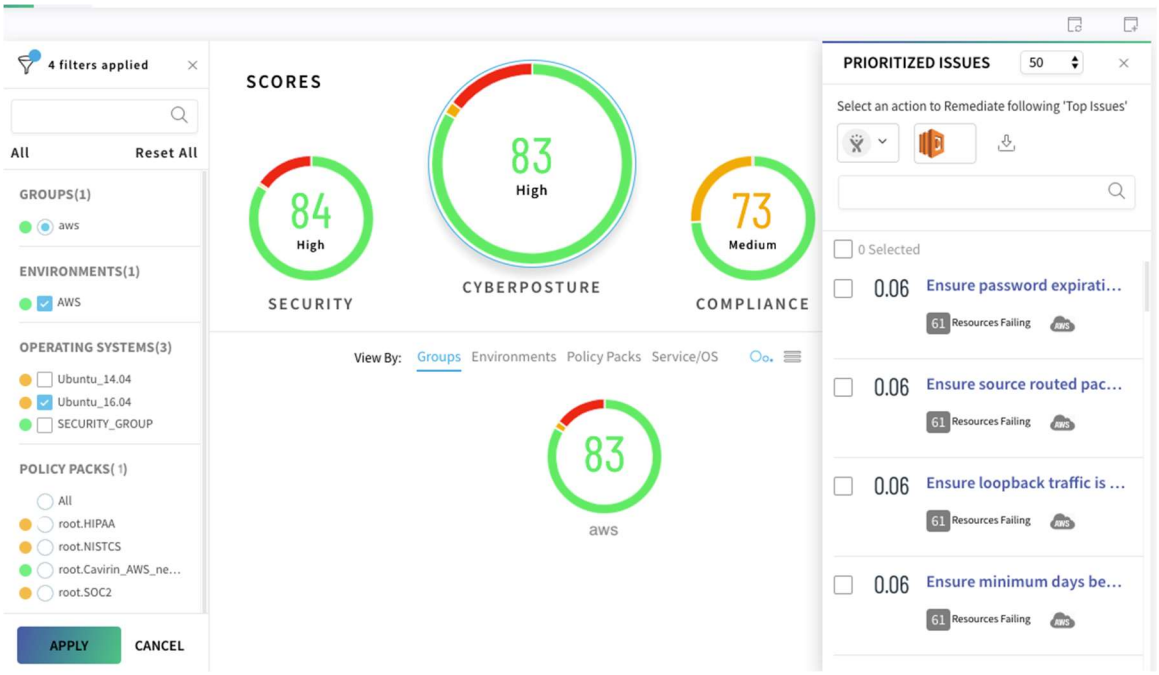


4. Sign in with username *administrator* and the default password that Cavirin provided to you. Subsequently, a popup opens for changing the password.
5. Type a strong password with at least 12 characters and at least 1 special character, typically a dash, underscore, exclamation point, or question mark.

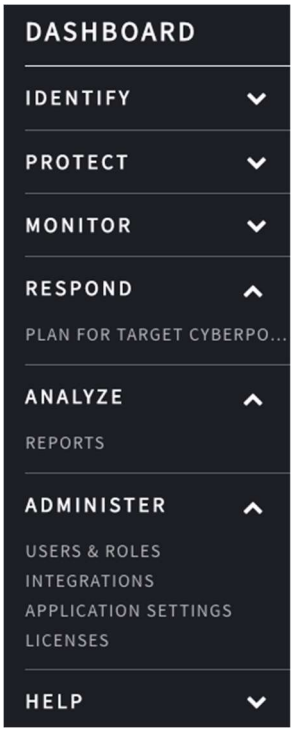
   Allowed characters are $ * ( ) - _ = ! [ ] : ; ? / , . ~ @

   Do not use spaces or # % ^ + { } /\ ' " ` > <
6. Log out.
7. Log in as *groupadmin* and use the same default password as before. Create a different strong password.
8. Repeat the sequence of logging out and back in but with the username *devops* and then *analyst*, creating strong passwords for each.
9. Log out and then log in with the name administrator for the next series of steps.

At this point, Cavirin has no assessment data. (Ignore messages about no data available or the invitation to discover and assess resources.) The next figure illustrates existing data in the CISO Dashboard for an operational system.



10. Click the stacked icon in the upper-left corner (next figure) of the Dashboard to open the navigation pane (subsequent figure). The subsequent figure shows the available areas in the SuperAdmin role.

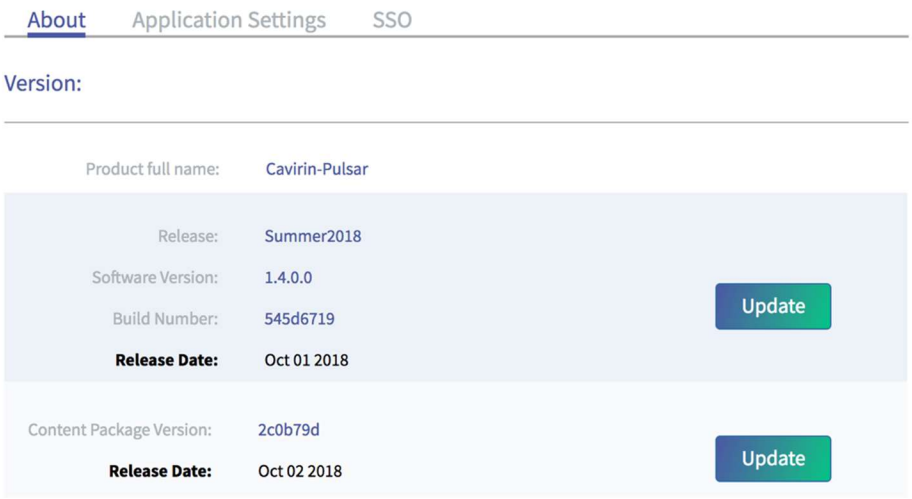


Configuring SMTP

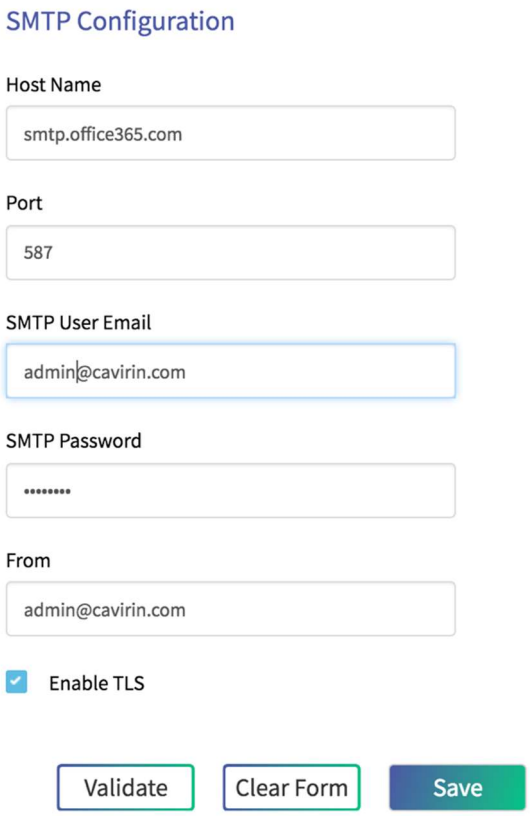
IMPORTANT: SMPT is essential for the Cavirin system to send email to users (with passwords and assessment status, for example).

To set up SMTP:

1. Navigate **Administer** > **Applications Settings**. The next figure illustrates the default screen. The tabs are *About*, *Application Settings*, and *SSO*.
2. Click the **Application Settings** tab.



3. Click the **Application Settings** tab.
4. Scroll to the SMTP part of *Application Settings*. The next figure shows SMTP setup.
5. Type the name of the host you are using, port number **25** or **587**, internal email address of the SMTP server, internal password of the server, and name of the sender that appears to recipients of the email. Enabling TLS is optional.
6. Click **Validate** (or **Clear Form** if necessary).
7. Click **Save**.



Integrating Third-party Notification Services

You can integrate Cavirin with multiple instances or multiple third-party notification services, such as Jira, Slack, PagerDuty, ServiceNow, and Google's Cloud Security Command Center (CSCC). See Integrating Third-party Notification Services for details.

Configure Single Sign-on

If your organization wants to use single sign-on (SSO), Cavirin uses Okta to implement SSO in the current release. You will use the portal at the Okta website and the *SSO* tab in *Administer > Application Settings*. Whether for implementing SSO now or later, you can find the detailed description in Configuring Single Sign-on with Okta.

Detailed Description of Administrator Tasks

The detailed task descriptions that follow pertain to the Administer area of the UI—with the important exception of how each user can modify his or her profile, usually their password. (Users can access their profile from the Dashboard, as this section describes.)

You can perform the tasks in this section only in the SuperAdmin role (except for changing the user's profile, which any can user can do). The subsections describe:

- Privileges for the Default Roles – How to create or modify a *user account* (change user name, suspend user, delete account); how to create a *user group* and create a role.
- Integrating Third-party Notification Services – How to add a third-party service and how each service interoperates with the Cavirin system.
- Application Settings – Provides details about the system and content versions; describes how to specify SMTP and custom TCP ports for SSH, WinRM, and WinRM over HTTPS; and describes how to set up authentication with SSO.

NOTE: By default, WinRM runs with TLS.

- Google Cloud Security Command Center

For a Cavirin system that has been installed in a Google Cloud environment, the Google Cloud Security Command Center (CSCC) provides a dashboard to SecOps engineers. This section describes the tasks you perform in the Google Platform management portal and then in the Cavirin UI before authorized Cavirin users can add CSCC to assessments.

CSCC is a system that accepts and displays Cavirin's assessment findings and recommended remediation for the set of Google Cloud services that Cavirin monitors.

In the current release of the Cavirin system, only one integration between Cavirin and CSCC is supported. Authorized users can use this integration for multiple asset groups.

The most likely users of CSCC are SecOps or DevOps personnel. However, any Cavirin user with the right credentials for Google Cloud can view the CSCC dashboard in Google Cloud. (In contrast, only a Group Admin or DevOps user can associate CSCC with asset groups, as described in the *Cavirin User Guide*.)

Most of the set-up work you do is in the Google Cloud. Therefore, you need to be familiar with Google Cloud Marketplace and the Google Cloud Platform management portal. You will gather information from the Google Platform and then use it for:

- Integrating CSCC with Cavirin
- Providing the CSCC-specific *Project ID* to Group Admin or DevOps users

After finishing the setup by integrating CSCC in the Cavirin UI, you must provide the *Project ID* from GCP for the CSCC project to the DevOps or Group Admin users. Authorized users need this *Project ID* to link a Cavirin asset group to CSCC, as described in the *Cavirin User Guide*.

In the following overview of the workflow, which starts after Cavirin has been added as a managed project in a GCP project via Google Marketplace, you:

1. Launch the Cavirin CyberPosture application from within Marketplace.
2. Sign up your organization for CSCC and get Cavirin's *Cloud SCC Companion App* in Google Marketplace. The *Cloud SCC Companion App* must be on a whitelist in GCP. As of the current release of beta CSCC, we suggest you contact a Google account rep to confirm your *Cloud SCC Companion App* is whitelisted.
3. Go to your Cavirin account and then navigate to **IAM & roles** > **IAM** and confirm that you have all of the following roles for the project at the organization-level in GCP: *Owner*, *Organization-level Administrator*, and *Security Center Administrator*. Obtain these roles and permissions if you do not have them.
4. Navigate to **IAM & roles** > **Services accounts** and click **Create**. Create a service account with a name that indicates its relation to CSCC, such as *cavirin-cscc-app*.
5. Look inside the service account and notice the Keys area.
6. Click **Create** Key.
7. Click **Save** after the key is created.
8. At the top of the *Security Command Center* screen, click **Add Security Sources**. This action takes you to Marketplace. If the card for Cavirin *Cloud SCC Companion* is not visible, use the search box to find it.
9. Click on the card for *Cavirin Cloud SCC Companion* to open the self-service provisioning workflow.
10. Click **Visit Cavirin System Site to Sign Up**. A page requests you to select your organization. In the dropdown, locate and highlight your organization, and then click the **Select** button at right of the dropdown.

    The Source Connect window appears. This page has a box for *Service Account* and a box for *Source ID*. The *Service Account* box shows the account you just created in step 4.

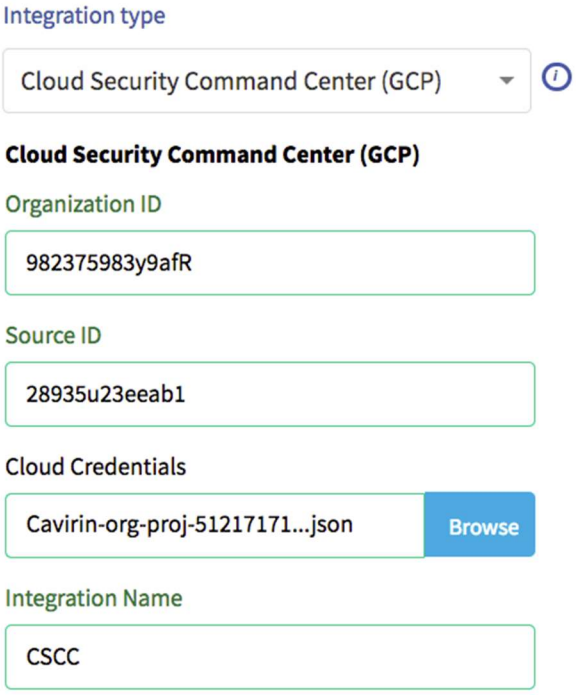
    The Source ID box contains two fields. They are the Organization ID ("*organizations*"), followed by a numeric string, and the Source ID ("*sources*"), also followed by a numeric string. The Organization ID is the Google-generated identifier of your Cavirin account, and the Source ID refers to the *Cavirin Cloud*

Security Companion. When you later integrate CSCC in the Cavirin UI, you will paste or type these numbers into the corresponding boxes in the popup for integrating CSCC with the Cavirin system (next series of steps in this section).

11. Click **Done**. You are returned to the Security Command Center page.
12. Click **Settings** in the upper-right corner of the *Security Command Center* screen. The *Settings* screen appears.
13. Click the **Security Sources** tab at upper-left. A *Security Sources* table for your organization should show the new installation of *Cavirin Cloud Security Companion*. The next step is for downloading the credentials for *Cavirin Cloud Security Companion* to your local host.
14. Return to the *Service accounts* window
15. Select the service account created for the Cavirin Cloud Security Companion. Off to the right of the row for Cavirin Cloud Security Companion are three vertical dots that indicate a drop-down list.
16. Click the drop-down list and, within the list, select **Create key**. A popup for this service account appears.
17. Select the JSON option and click **Create**. Save the key to a place known to you on your local host for subsequent use when you create the integration in the Cavirin UI (in the series of steps after you return to the Cavirin UI).
18. Go to the next series of steps to Integrate CSCC in the Cavirin UI.

To integrate CSCC with the Cavirin System:

1. Navigate to *Add Integration* and select **Cloud Security Command Center (GCP)** for the integration type.
2. Type or paste the *Organization ID* for Cavirin from GCP.
3. Type or paste the *Source ID* for Cavirin from GCP.
4. Upload the key in JSON format that you downloaded from the Google portal. (You downloaded the JSON file from Google Cloud to your local host and now provide it in the *Add Integration* popup.)
5. Type a name for the CSCC integration that indicates this integration is for CSCC.
6. Click **Save** (not shown in figure).

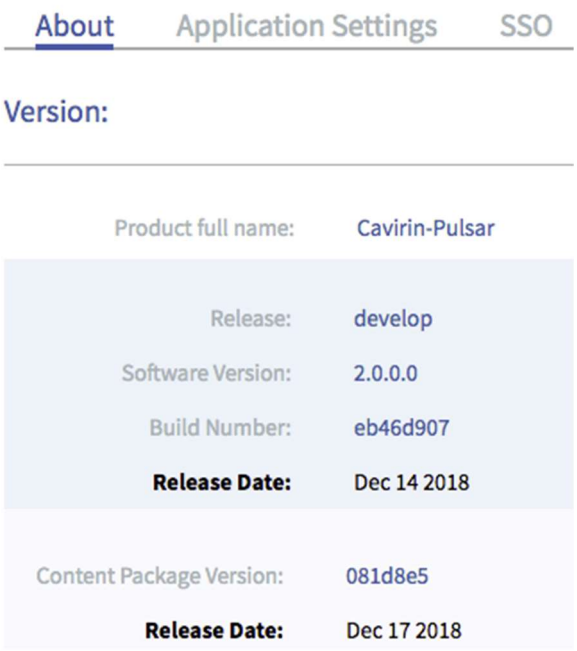


Application Settings

The features in this area provide system information; the ability to specify a custom port number for the services SSH, WinRM, and WinRM over HTTPS; and the SMTP configuration so that the Cavirin system can send email to users.

About (this Cavirin System)

The About section shows release information about the system (Release ID, software version, build number, and release date) and the policy pack content (version and release date). See next figure.

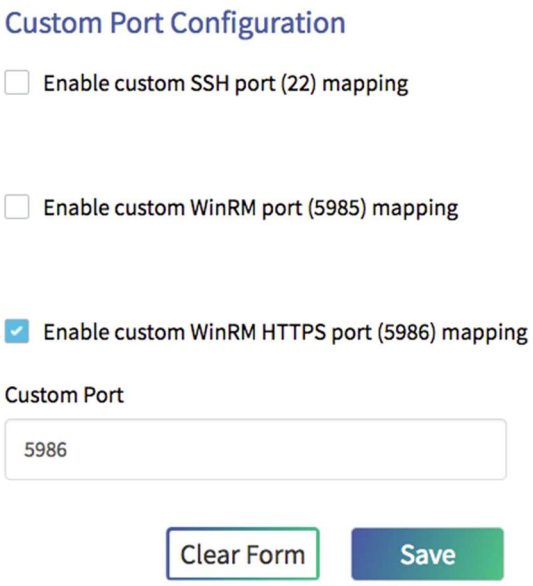


Application Settings

In this page, you can specify an alternative port number for the services SSH, WinRM, and WinRM over HTTPS. This configuration is optional. The reason for specifying alternative port numbers is a security measure but should done after careful consideration of the choice of alternative ports. The SMTP configuration enables the Cavirin system to send email to users and is a critical configuration.

To map SSH, WinRM, or WinRM over HTTPS to alternative ports:

1. Navigate to **Administer** > **Application Settings**. Click the Application Settings tab.
2. Select the protocol whose port you want to customize. The following figure shows all options selected.
3. Type the alternative port number in the *Custom Port* box.



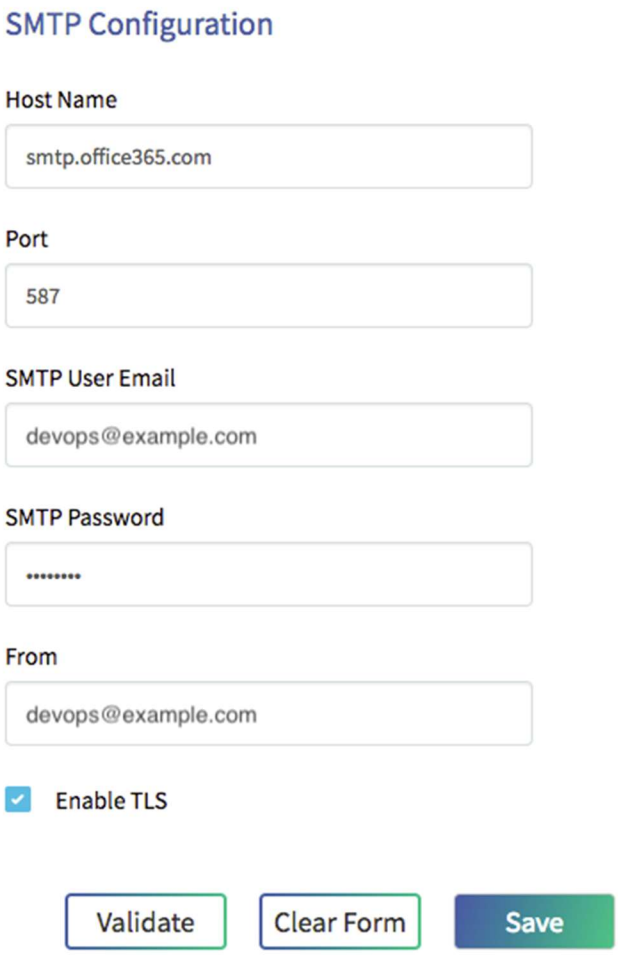
1. Click **Save** when ready (or **Clear Form**).

To set up SMTP:

NOTE: Configuring SMTP is mandatory. Without it, users do not receive email from the Cavirin system. For example, users would not receive a default password and not receive email notification that an assessment has started, stopped, or failed.

1. Navigate to Administer > Application Settings. Click the Application Settings tab.
2. Scroll to the SMTP Configuration area.
3. Type a host name, port number (default 587), an internal email address, internal SMTP password (for which users will not be prompted because this password is internal), a made-up email address that appears as the Sender (From) to recipients of the email.

   Enabling TLS is optional.
4. Click **Validate**.
5. Click **Save** If the setup is valid (or **Clear Form**).



Configuring Single Sign-on with Okta

In the current release, Cavirin uses Okta as the integration service to implement SSO.

NOTE: The prerequisite before beginning this steps in this section is to have "authentication server API" enabled by Okta itself.

The actions in this section involve the Okta portal and Cavirin's UI (Administer > Application Settings > SSO). Refer to Okta's on-line documentation as needed.

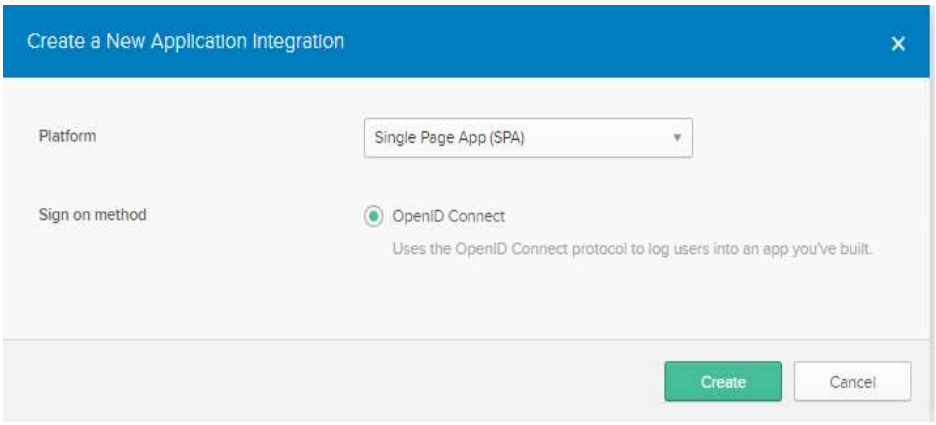
To set up SSO:

1. Go to your Okta management portal.
2. Click **Admin** at upper-right. (The *Add Apps* button is already highlighted.)
3. Click **Applications** in the banner and then select **Applications** in the dropdown that appears. The work area label changes from *Dashboard* to *Applications* and has an *Add Applications* button below the work area label *Applications*.

4. Click **Add Applications**. The display changes to include a *Create New App* button, including the *Create New App* button.

5. Start creating the new app by clicking **Create New App**. The *Create a New Application Integration* area appears as in the next figure.

6. Select **Single Page App (SPA)** in the *Platform* dropdown (next figure). The sign-on method defaults to **OpenID Connect**.

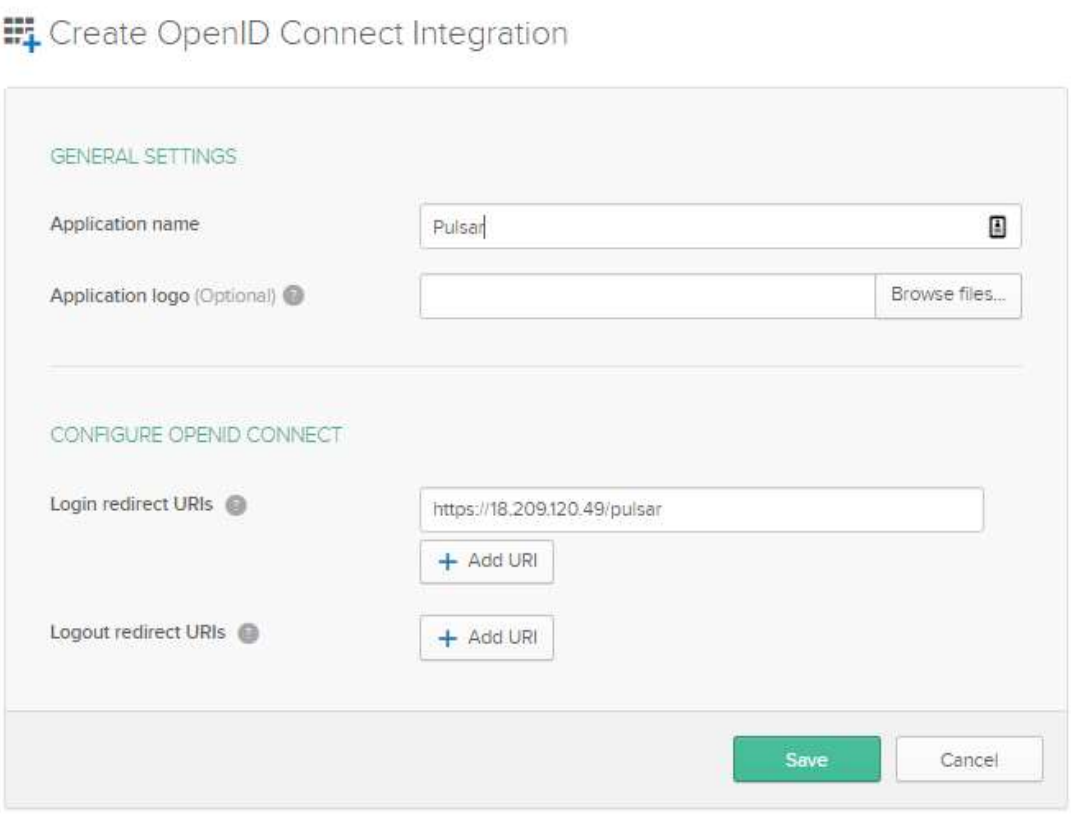


7. Click **Create**. A window named *Create OpenID Connect* opens (see next figure).

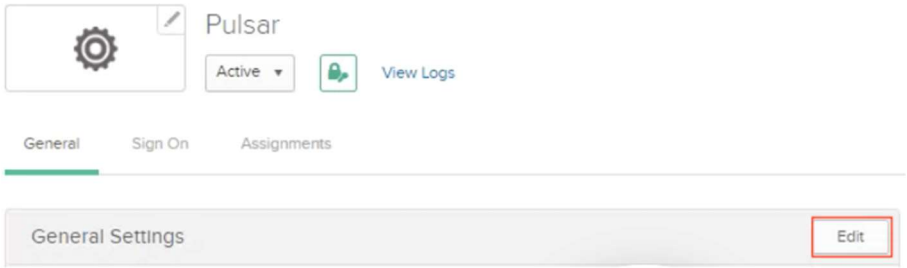
8. In the General Settings area, type a *Platform* name in the *Application name* box (such as "Pulsar").

9. Type your Cavirin system's home page URI in the *Login redirect URIs* field and then do either of the following:

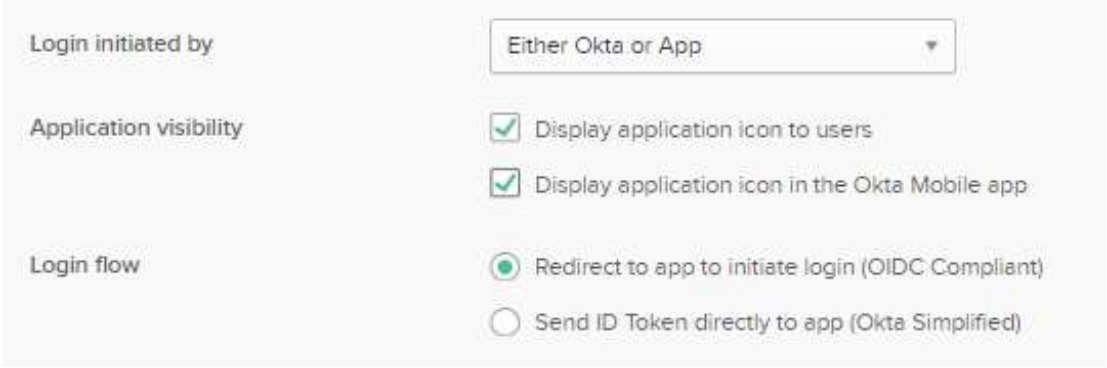
   - Click **Save** now (unless you copy the URI as directed in the next bullet).
   - Copy the URI from the address field of your Cavirin system's browser UI.



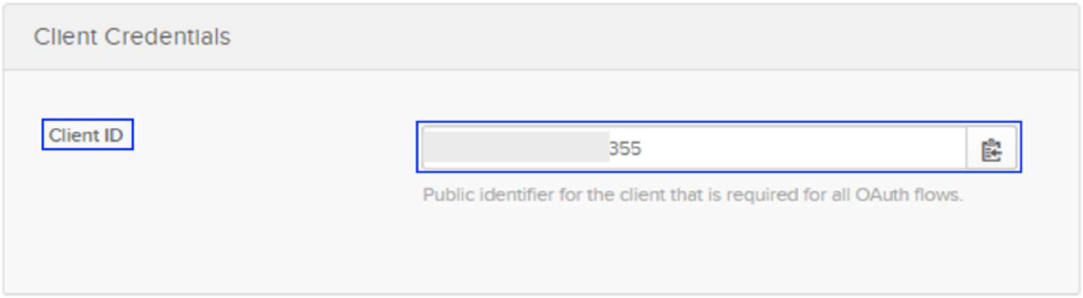
10. Click **Save**. The screen is redrawn, and new UI elements appear (next figure).
11. Click **Edit**, a button that has appeared at lower-right, to edit the settings.



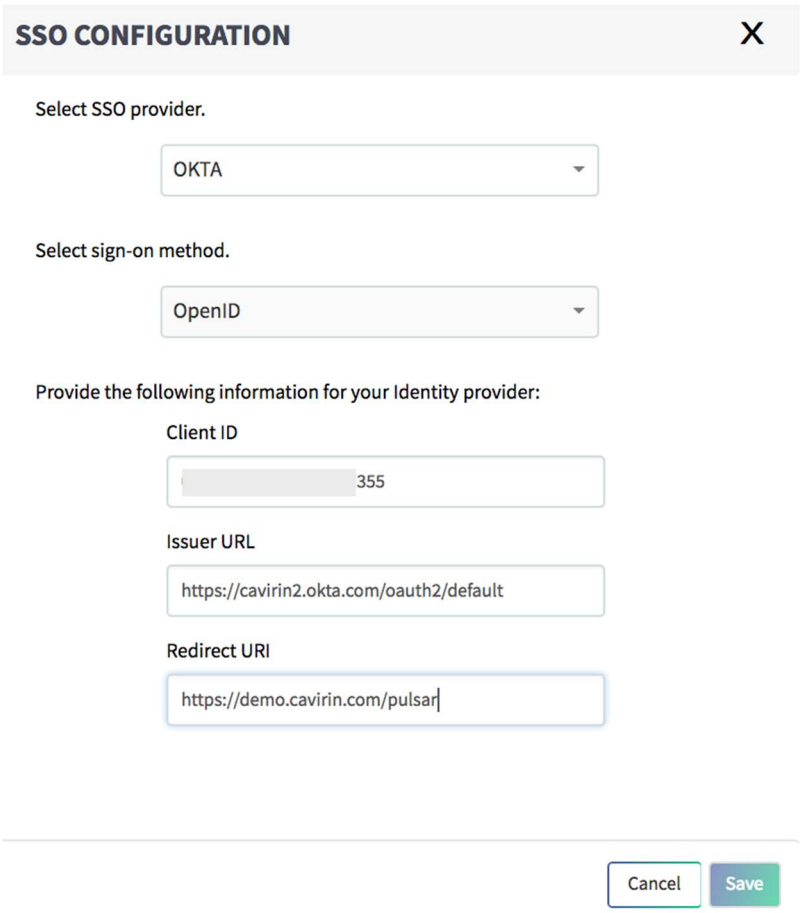
12. Select **Either Okta or App** in the dropdown for the value of *Login initiated by* (in the redrawn General Settings screen, next figure).
13. For Application visibility (next figure), marking both checkboxes is optional but recommended. The decision depends on an organization needs. Marking the first box lets a user have a chiclet in the Okta portal that logs them into the Cavirin system. Marking the second box lets a user log into Cavirin from a mobile device.
14. Clicks **Save** (not shown in next figure screen).



15. Copy the *Client ID* value (next figure) from Okta (Client Credentials area below the General Settings area). After you log into the Cavirin system and navigate as directed (next step), paste the *Client ID* in Cavirin's SSO Configuration.



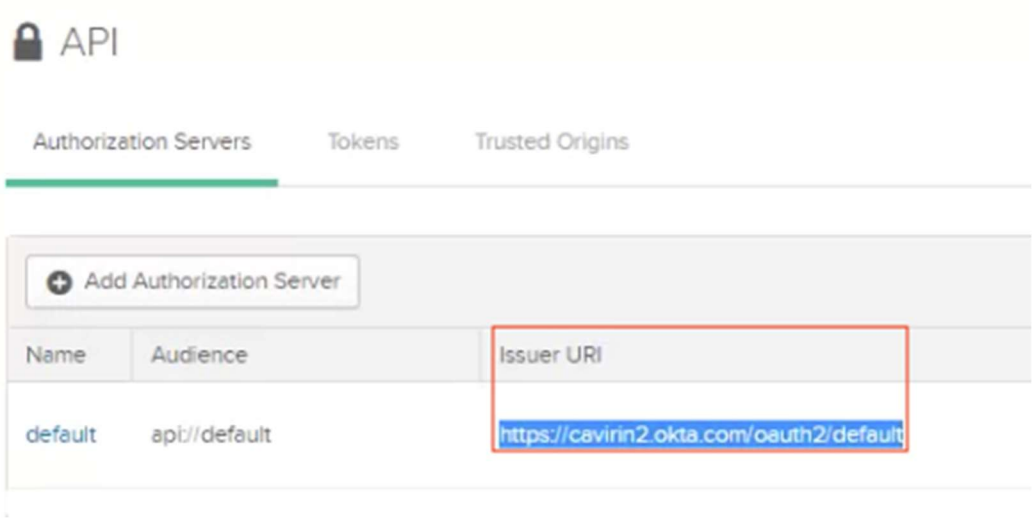
16. Log into the Cavirin system; navigate to **Administer** > **Application Settings** > **SSO**. The SSO Configuration window pops up.



17. Paste the *Client ID* from Okta into the Client ID box in the SSO Configuration.

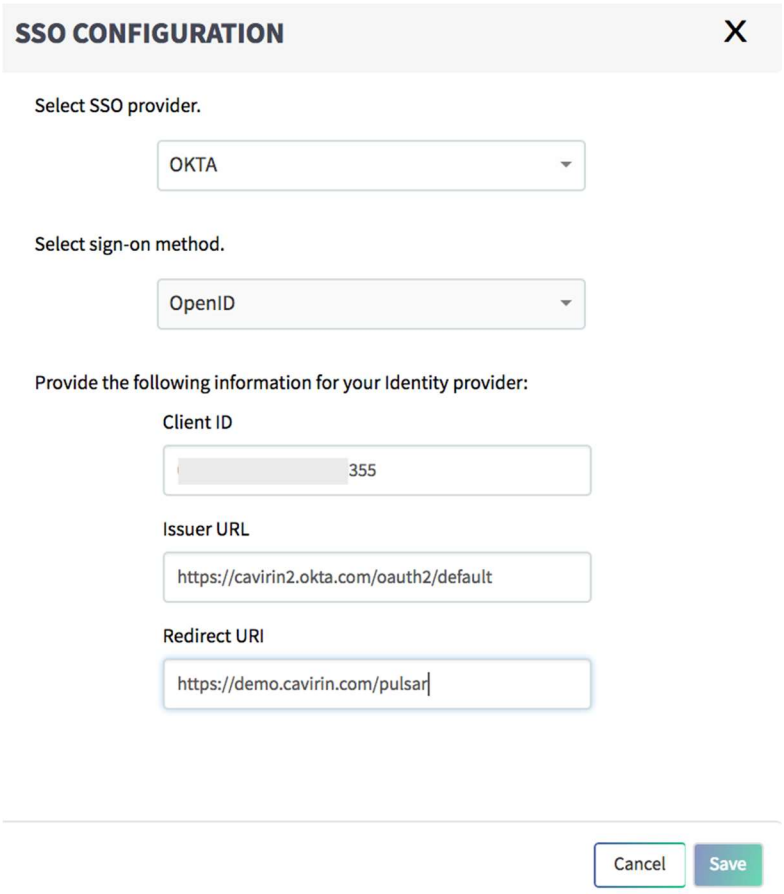
The next step is for copying the *Issuer URI* in Okta and pasting it in the Cavirin SSO Configuration (the previous figure shows it was already pasted).

18. In Okta, navigate to **Security** > **API** (next figure), copy the value of *Issuer URI* in the third column, and paste it into the Issuer URI field of the system's open SSO Configuration popup (subsequent figure).



19. Specify the Redirect URI in the SSO Configuration popup. This is the home page of the Cavirin instance and is identical to the Okta redirect, so you can copy it from Okta or just type it.

NOTE: For completeness, all fields in SSO Configuration should be populated.



20. Click one time outside the *Redirect URI* box before the next step.

21. Click **Save** *only once* In the Cavirin SSO Configuration popup. The system should display a confirmation of valid information.

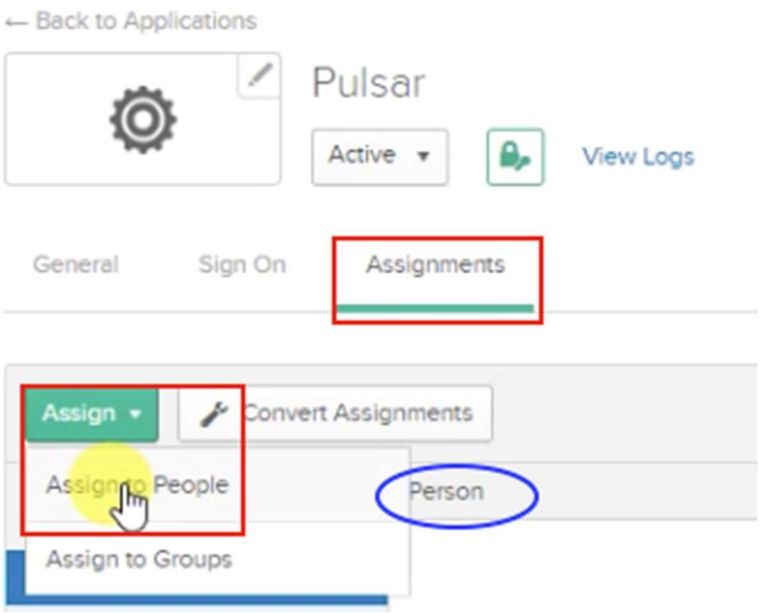
22. The SSO page shows the details of the Okta integration.

The next task is for specifying the Cavirin users that are authorized to use SSO. (An *authorized user* has access to the app/chiclet available from the Okta portal.)

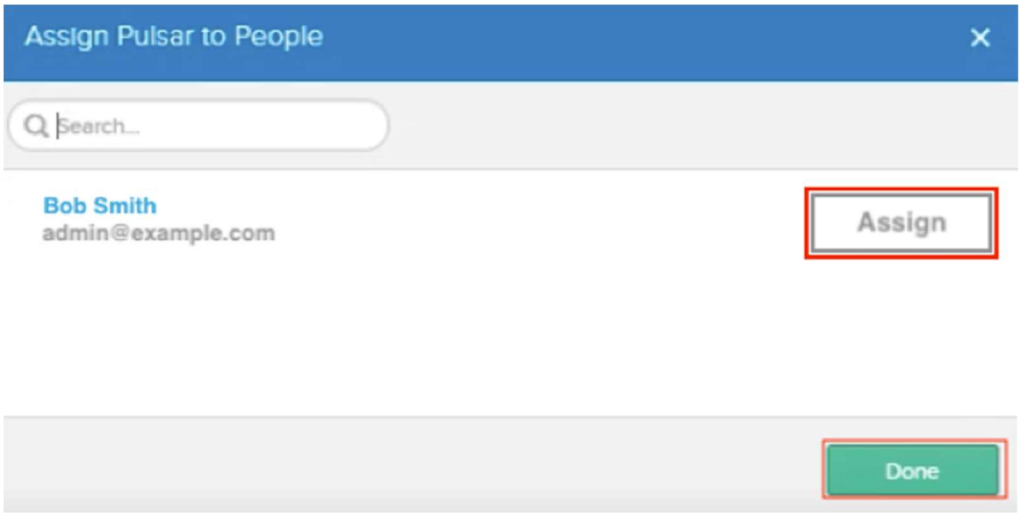
23. Return to the Okta portal (log in if necessary).

24. Click **Assignments** at top-left in the Okta Dashboard (next figure); then click **Assign** to see its dropdown menu; and then select **Assign to People**. The subsequent figure pops up. (This example shows "Pulsar" has not yet been assigned, so the *Person* column is empty.)

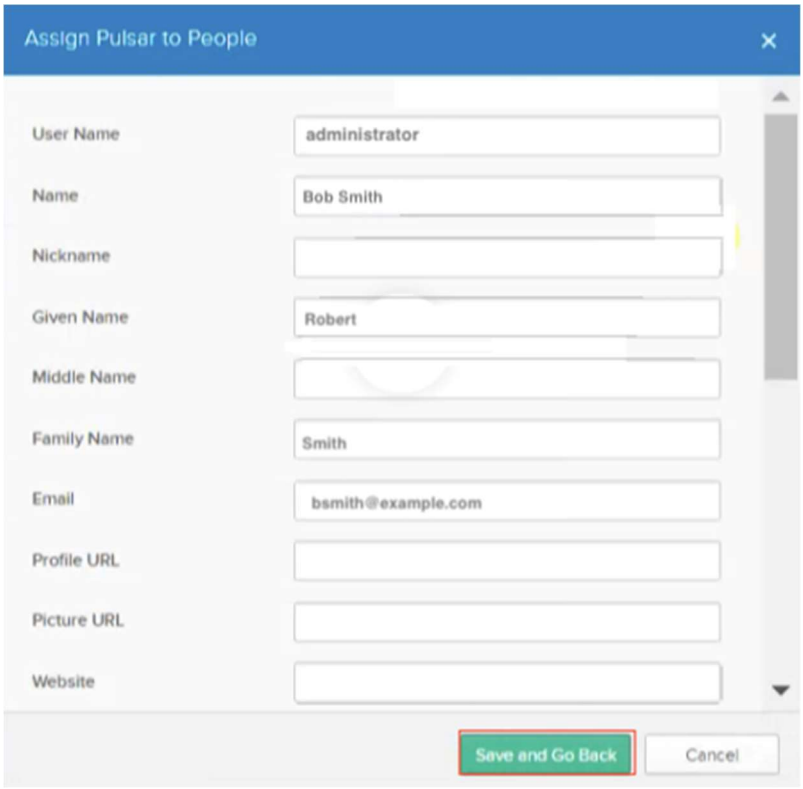
A list of Cavirin users, labeled *Assign Pulsar to People*, pops up, as the subsequent figure shows for just one employee.



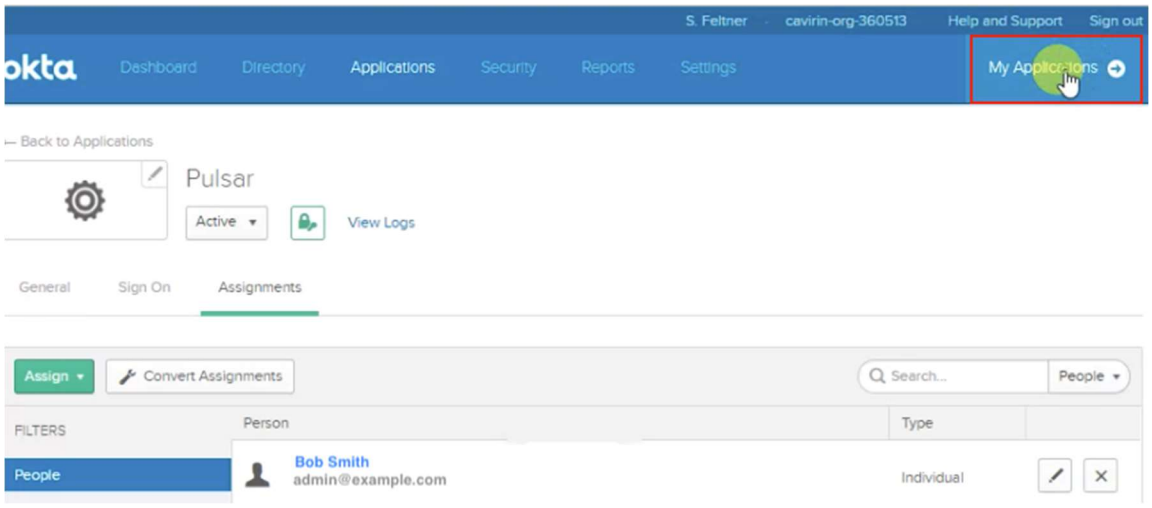
25. Click **Assign** next to the member intended to receive the Pulsar assignment, as in the next figure. This action opens another popup that lets you specify details about this user. At this juncture, you can press **Done** at the bottom of the next screen or add or modify details in the popup in the subsequent screen.



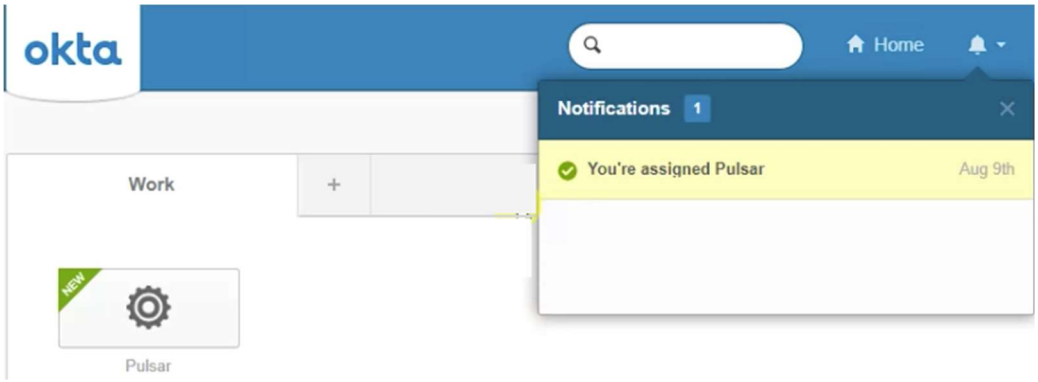
26. Accept the current user profile as-is or modify it as in the next figure. When ready, click **Save and Go Back** to assign Pulsar SSO to another user.



27. Click **My Applications** in the upper-right corner of the next figure. (Notice at the bottom of the next figure that the user name now appears in the *Person* column.)

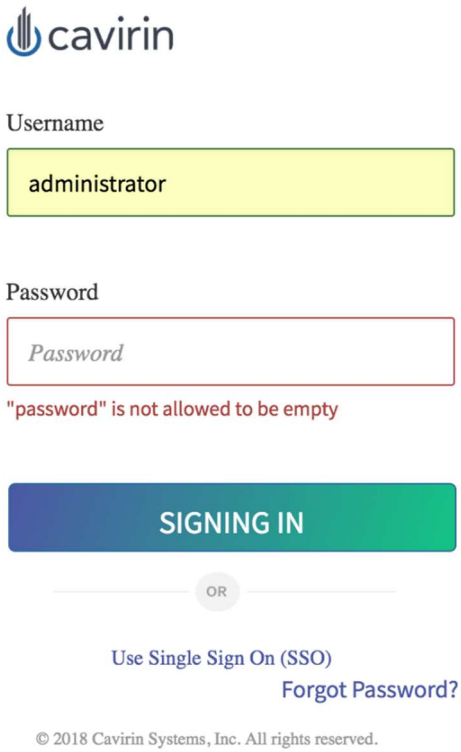


A popup confirms that SSO use with Pulsar has been granted (see "Notifications" and "You're assigned Pulsar"):



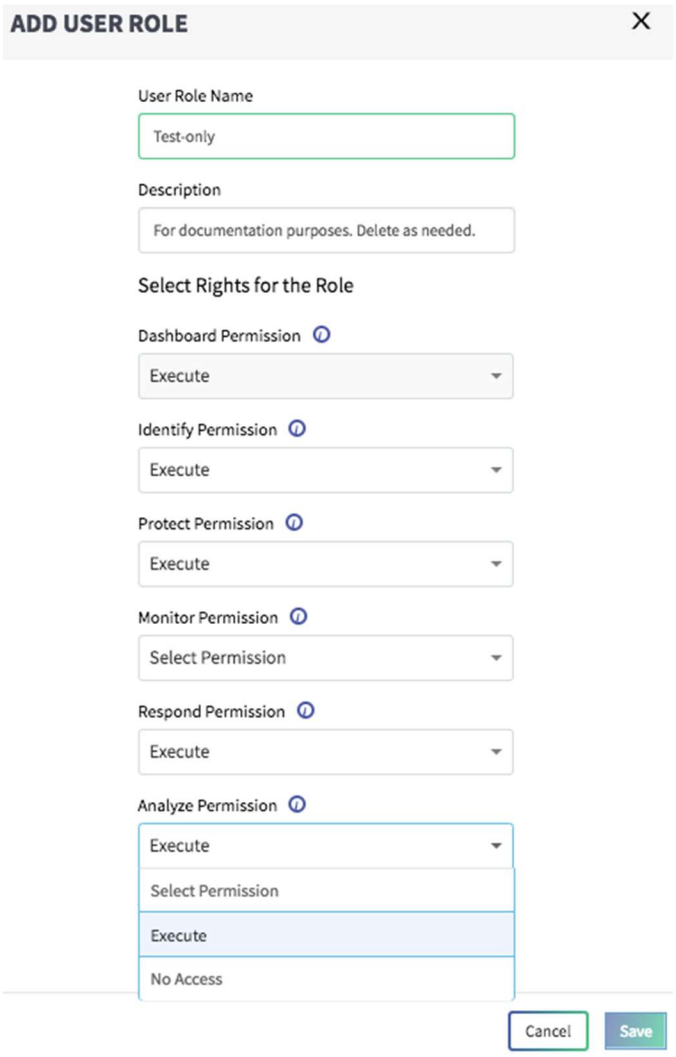
28. You can test the SSO login on Cavirin (first log out if already logged in). The login page should display the SSO sign-in option.

29. Click **Single Sign On** and receive access to the CISO Dashboard.



- Product Licenses – Provides details about the current Cavirin license and the way to upload a new license.
- Creating a Custom RBAC Role
- You can create RBAC roles with your own mix of rights for a role. To do so:

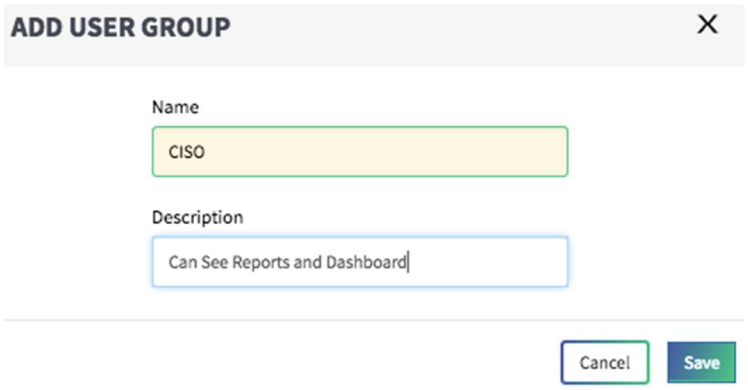
1. Navigate: **Administer** > **Users & Roles**.
2. Click **Add Role**. A form opens for naming the role and selecting the authorizations. (Super Admin role is inaccessible.) Click **Save** when ready.



Creating a User Group

You can create any number of user groups beyond Default User Group. Subsequently, a new or edited user account can be assigned to the new group:

1. Navigate: **Administrator** > **Users & Roles** > **User Groups**.
2. Click **Add User Group** at top of the table. The form for adding a group opens.
3. Specify a descriptive name and description for the user group.
4. Click **Save**.



- How Users Can Change Their Profile – Users can change their profile details (first/last name, email address, role, password, and so on).

Privileges for the Default Roles

To see the capabilities authorized for each role, click the **Roles & Rights** tab. The following table lists the default roles. Each row shows the title of the role, the role's default login name, and the authorization for each functional area in the UI.

Role Description	Username	Dash-board	Identify	Protect	Monitor	Respond	Analyze	Admini-ster
DevOps	devops	Execute	Execute	Execute	Execute	No Access	No Access	No Access
Group Admin	groupadmin	Execute	Execute	Execute	Execute	Execute	Execute	No Access
Security Analyst	analyst	Execute	No Access	No Access	No Access	Execute	Execute	No Access
SuperAd-min	administrator	Execute	Execute	No Access	Execute	Execute	Execute	Execute

Creating and Modifying User Accounts

This section describes how users in the SuperAdmin role create or modify a user account.

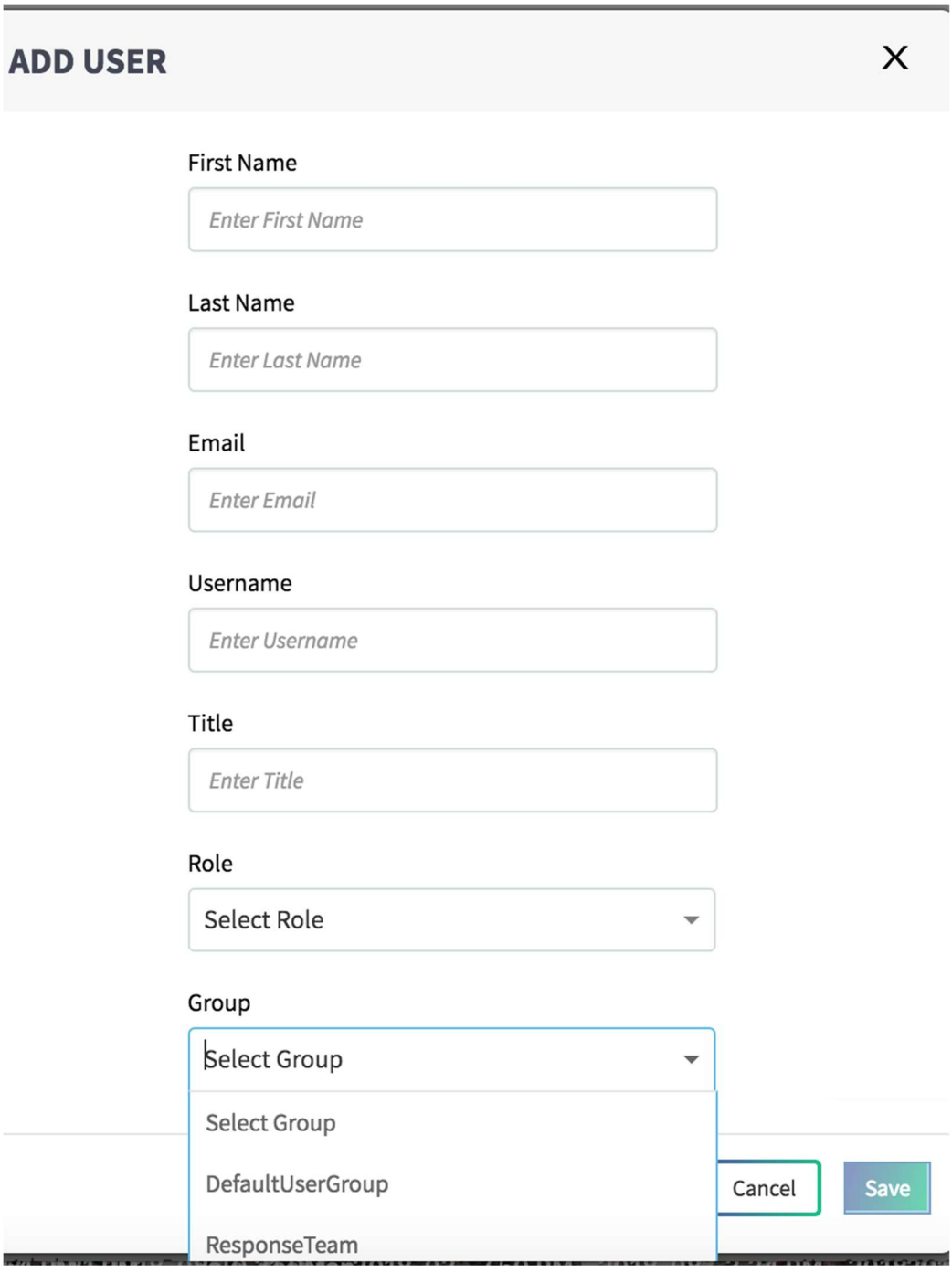
In accordance with Cavirin's support for role-based access control (RBAC) in the current release, a user can have one role and belong to one user group.

To create a user account:

1. Navigate to **Administer** > **Users & Roles**. The default tab is *Users*.
2. Click **Add User**. The form for adding an account opens as in the next figure, with the following fields:

- First and last names
- Email address
- Username
- Job title (text entry)
- Role (dropdown with default roles and custom roles, if applicable)
- User group (DefaultUserGroup) or a custom user group, if one exists)

3. Click **Save** when ready.


ADD USER
First Name
Enter First Name
Last Name
Enter Last Name
Email
Enter Email
Username
Enter Username
Title
Enter Title
Role
Select Role
Group
Select Group
Select Group
DefaultUserGroup
ResponseTeam
Cancel
Save

Modifying a user account means editing, suspending, or deleting the account.

- Editing the account can change first or last name, login name, email address, job title, role (can be a default roles or a custom role), or user group.
- Suspending but not deleting the account.
- Deleting the account.

To modify a user account:

1. Navigate to Administer > Users & Roles.
2. Mark the check box next to the user name on the account. The three options that become active are **Edit User**, **Suspend User**, and **Delete User**.
3. Click **Edit User**. The form that opens has the same fields as the form for creating the user account:
    - First name, last name
    - Email address
    - Username
    - Job title (text entry)
    - Role (dropdown with default roles and custom roles, if applicable)
    - User group (the default group or a custom user group, if available)
4. Click **Save** when ready.

To suspend and then re-activate a user's account:

1. Navigate: **Administer** > **Users & Roles**.
2. Mark the check box next to the user name on the account. The three options that become active are **Edit User**, **Suspend User**, and **Delete User**.
3. Click **Suspend User**. A challenge for you to confirm the suspension opens.
4. Click **Yes**. The account remains in the account list, but the status of the account turns from Active to Suspended.
5. To reactivate the account by clicking the user name and clicking **Activate User**.
6. A challenge pops up for you to confirm the reactivation.
7. Click **Yes**.

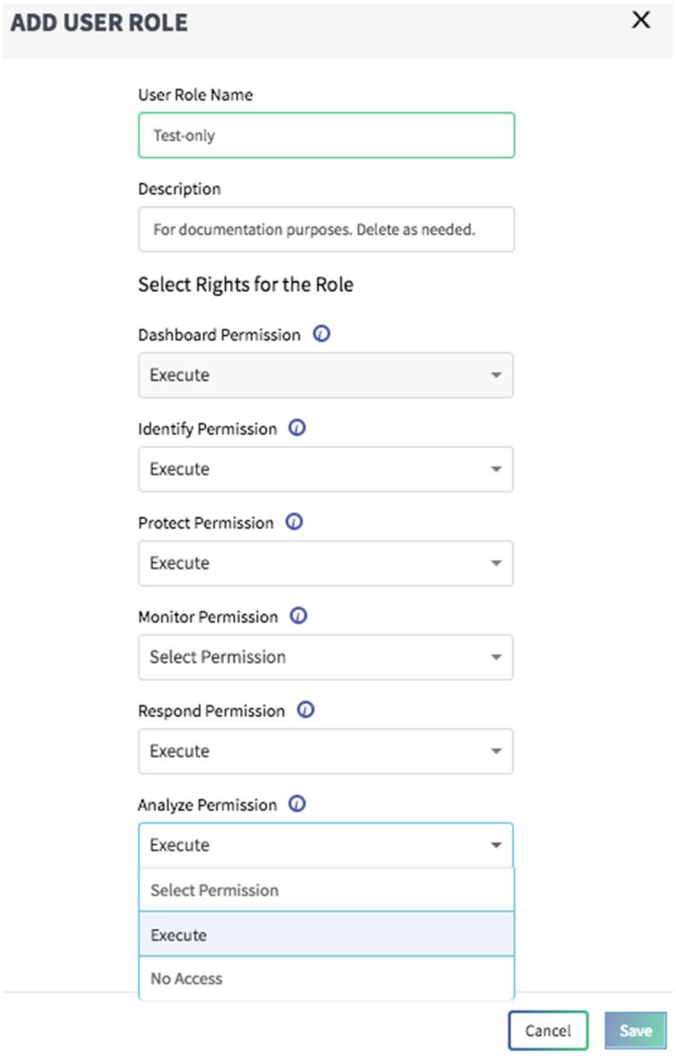
To delete a user's account:

1. Navigate: **Administer** > **Users & Roles**.
2. Mark the check box next to the user name on the account. The three options that become active are **Edit User**, **Suspend User**, and **Delete User**.
3. Click **Delete User**. A challenge opens for you to confirm the deletion.
4. Click **Yes**.

Creating a Custom RBAC Role

You can create RBAC roles with your own mix of rights for a role. To do so:

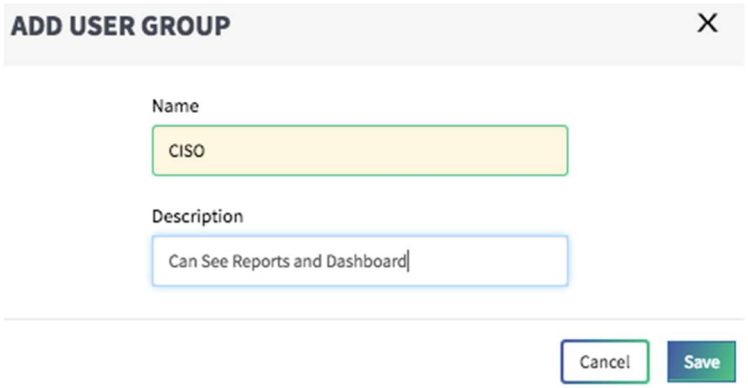
3. Navigate: **Administer** > **Users & Roles**.
4. Click **Add Role**. A form opens for naming the role and selecting the authorizations. (Super Admin role is inaccessible.) Click **Save** when ready.



Creating a User Group

You can create any number of user groups beyond Default User Group. Subsequently, a new or edited user account can be assigned to the new group:

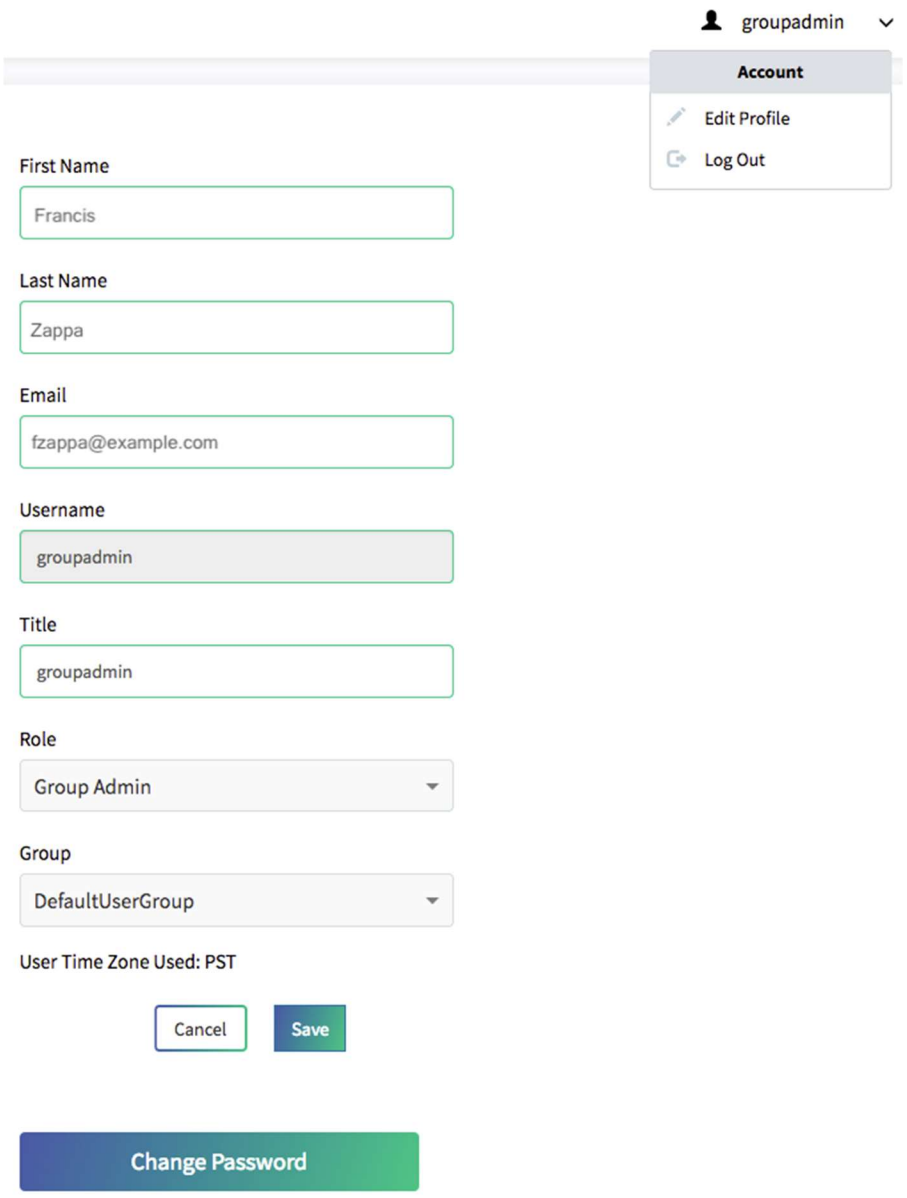
5. Navigate: **Administrator** > **Users & Roles** > **User Groups**.
6. Click **Add User Group** at top of the table. The form for adding a group opens.
7. Specify a descriptive name and description for the user group.
8. Click **Save**.



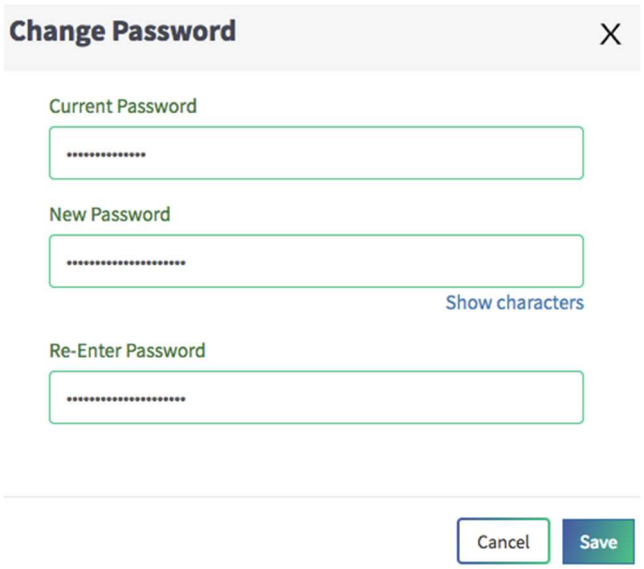
How Users Can Change Their Profile

Any user can change his or her profile (including password). To change a profile, a user:

2. Clicks the dropdown next to the login name in the upper-right corner of the UI to open the profile popup (next figure).
3. Modify as needed the fields and click **Save** if not changing the password (step 3).



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



Integrating Third-party Notification Services

This section describes how to integrate third-party services with the Cavirin system. These services take information from the system and fulfill the purpose of the service, such as creating Jira tickets, sending messages to a Slack channel, or sending assessment data to the Google Security Command Center.

Before you configure an integration, your organization must have an account with the third-party provider. Cavirin supports a subset of services offered by the third parties. For example, ServiceNow offers services that are not relevant to Cavirin's mission, so Cavirin makes no attempt to support them. Further, the integration with Goggle Could described in this section is for just Google's Cloud Security Command Center (CSCC), which displays the results of Cavirin assessments and monitoring in your GCP environment.

Cavirin supports multiple instances of a service (for example, multiple Slack channels):

- The name assigned to each instance of a service must be unique. For example, you could specify Slack channel "Support" and Slack channel "Dev."
- The unique name for a one service can be used for other services, for example, "Support" for Slack, ServiceNow, and Jira.

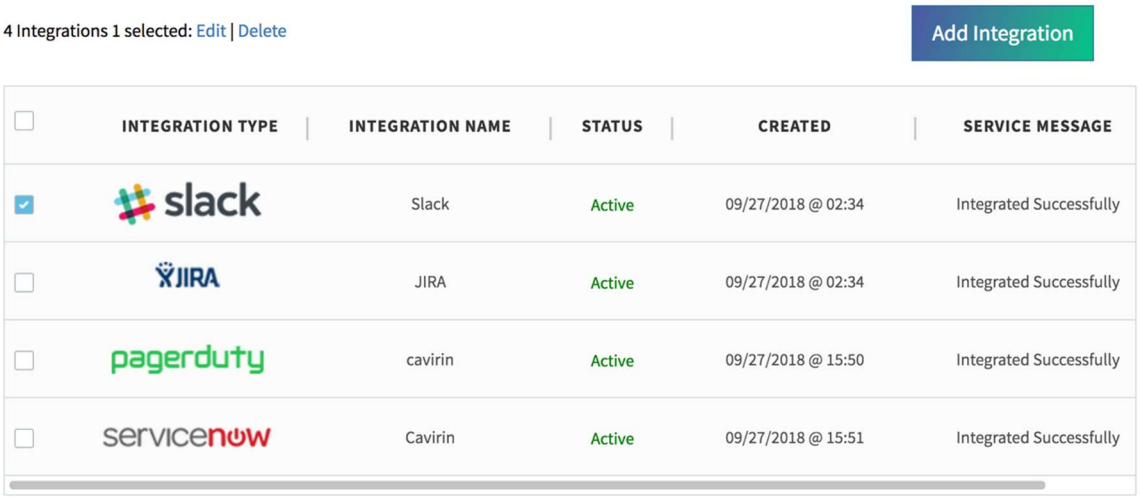
The following table shows the notification services and where they are supported:

Service	Assessment Schedule & Notification	Monitoring	Dashboard Prioritized Issues
Jira	X	X	Yes
Slack	Yes	Yes	Yes
PagerDuty	Yes	Yes	Yes
ServiceNow	X	X	Yes
Google CSCC	X	Yes*	X

* Although you integrate CSCC with the Cavirin system, the results of monitoring are visible in the Google Platform. See Google Cloud Security Command Center for details.

To see a list of service integrations and then add another integration:

1. Click **Integrations**. The next figure shows current integrations.
2. Click **Add Integration**. To see details about each notification service, proceed to one of the following:



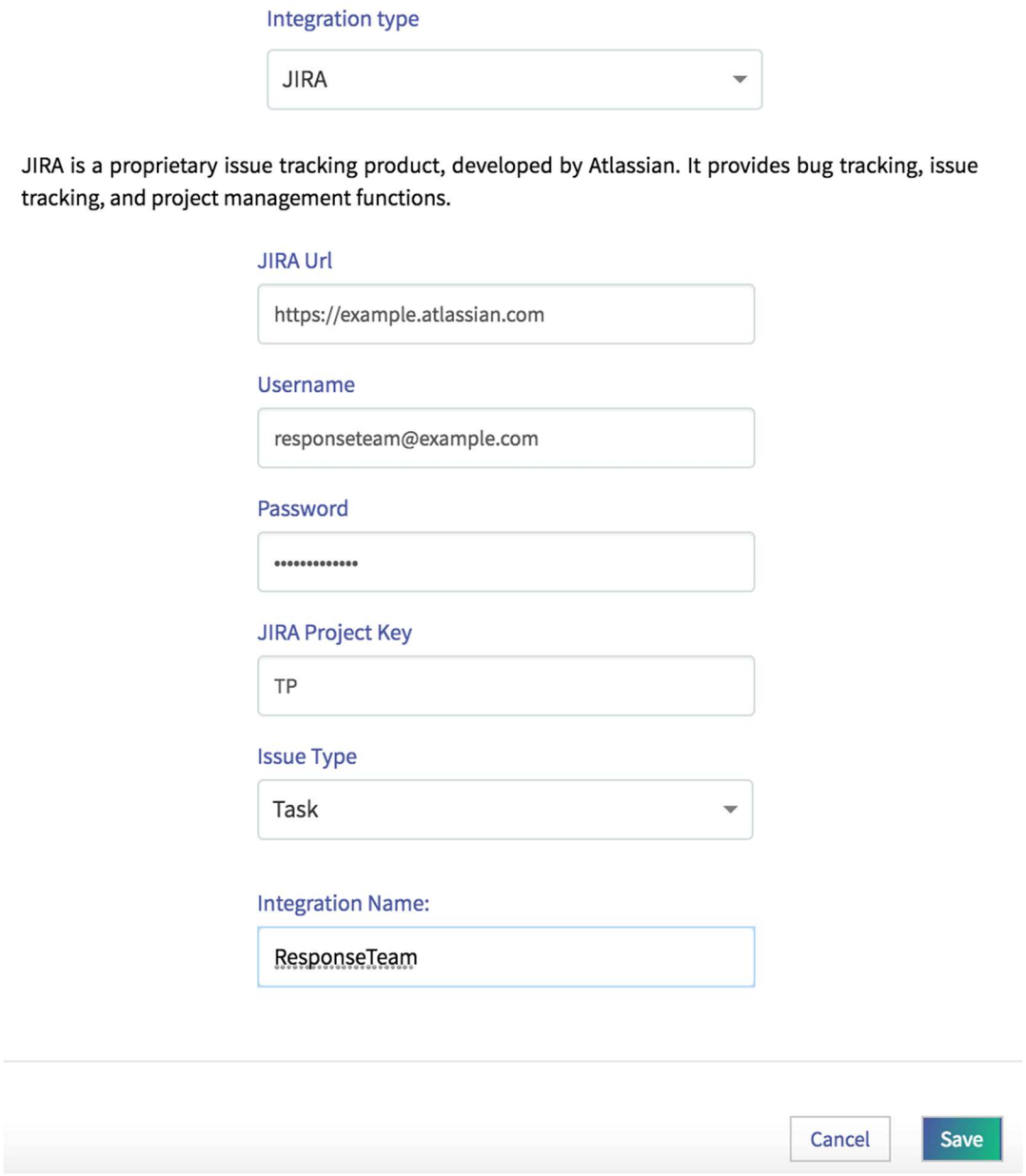
Jira Integration and Use Case

Cavirin supports Jira to generate tickets and notifications. In the current release, you can generate a Jira ticket from the Dashboard's Prioritized Issues area or from an HTML report

in the Reports area. In a report, you drill down to all policies for a resource in Device view and request a ticket. This description illustrates a workflow and the result—a Jira ticket.

First, in the *Administer* screen:

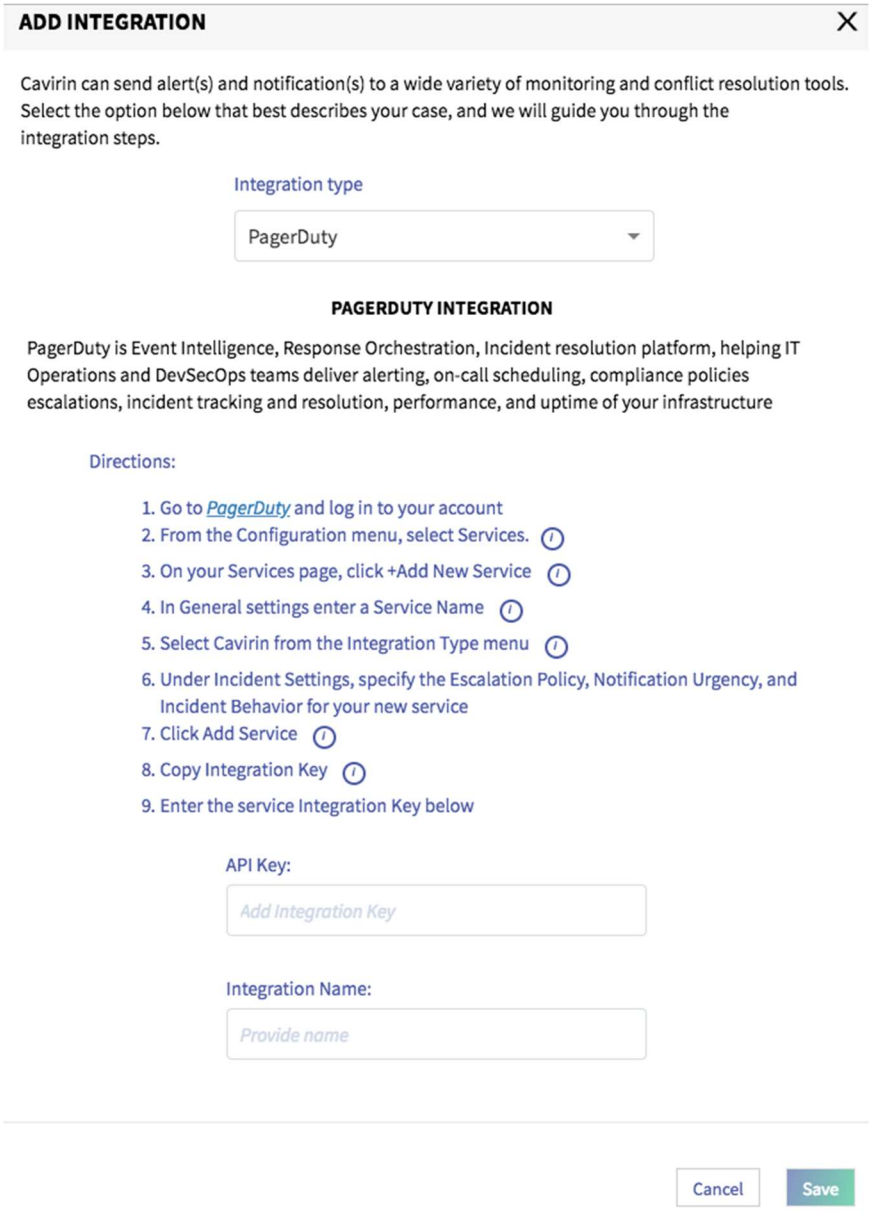
1. Click **Integrations** and then the **Add Integration** button. The default popup opens.
2. Select **Jira** in the *Integration type* dropdown.
3. Enter the Jira URL, username, password, Jira project key (the prefix for Jira tickets), issue type, and name for this integration. See the subsequent figure.
4. **Save** the configuration.



PagerDuty Integration

To integrate Cavirin with PagerDuty (default in the list of third-party notification provider):

1. Select Integrations in the Administer area (see next figure). Click any of the ❶ icons to open helpful guidance for the associated step.
2. Provide the API key for the organization's account. PagerDuty provides this key (see Step 8 of the next figure.)
3. Click **Save** when ready.



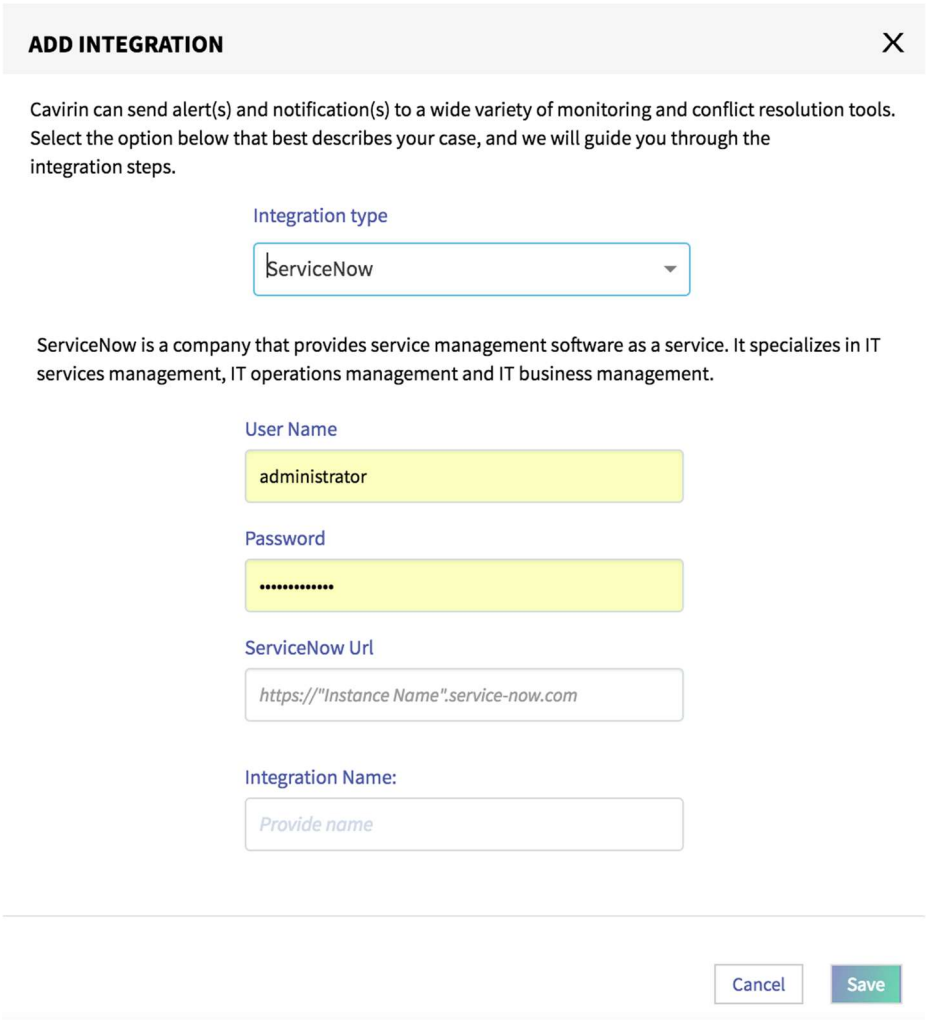
ServiceNow Integration

Cavirin's supports ServiceNow to create trouble tickets. In the Dashboard's *Prioritize Issues* area, users generate a ticket to the ServiceNow account. This section describes how you integrate the Cavirin system with your organization's ServiceNow account.

In the *Add Integration* popup, specify:

1. The SuperAdmin credentials you enter for logging into ServiceNow accounts
2. The URI that points to the organization's ServiceNow account

After completing the fields illustrated in the next figure, click **Save**.



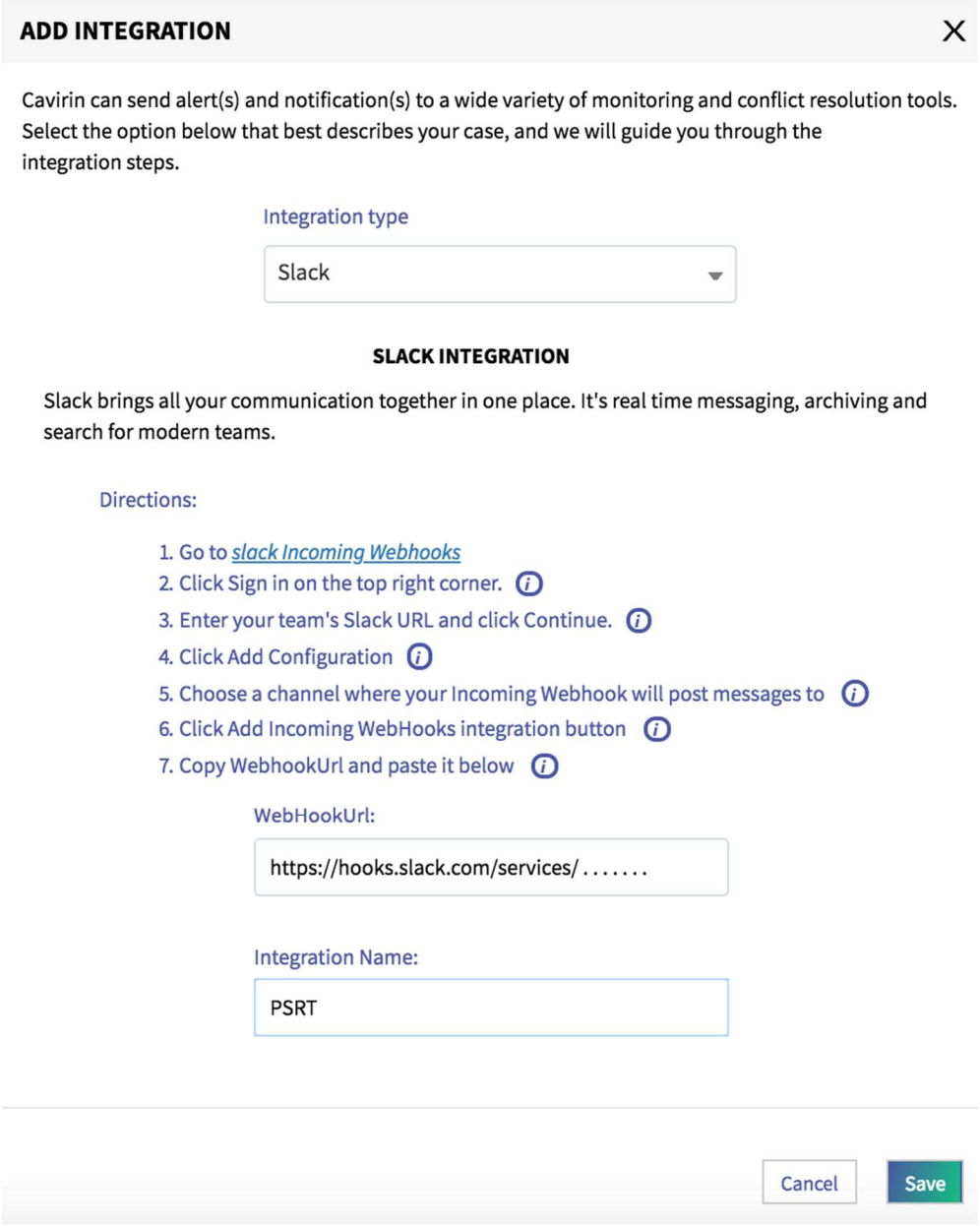
Slack Integration

Slack notification is available for the following functions in the current release:

- Schedule Assessments, the third of the three Discover & Assess wizards
- Prioritized Issues area of the CyberPosture Dashboard
- Monitoring

To create a Slack integration:

1. Click **Integrations** in the *Administer* area.
2. Click Add Integration.
3. Select **Slack** to open the configuration form. See next figure.
4. Do each step under *Directions*. For help with the meaning of a field, click the ❶ icon, as the next figure illustrates for multiple fields.
5. Click **Save** when done.



Google Cloud Security Command Center

For a Cavirin system that has been installed in a Google Cloud environment, the Google Cloud Security Command Center (CSCC) provides a dashboard to SecOps engineers. This section describes the tasks you perform in the Google Platform management portal and then in the Cavirin UI before authorized Cavirin users can add CSCC to assessments.

CSCC is a system that accepts and displays Cavirin's assessment findings and recommended remediation for the set of Google Cloud services that Cavirin monitors.

In the current release of the Cavirin system, only one integration between Cavirin and CSCC is supported. Authorized users can use this integration for multiple asset groups.

The most likely users of CSCC are SecOps or DevOps personnel. However, any Cavirin user with the right credentials for Google Cloud can view the CSCC dashboard in Google Cloud. (In contrast, only a Group Admin or DevOps user can associate CSCC with asset groups, as described in the *Cavirin User Guide*.)

Most of the set-up work you do is in the Google Cloud. Therefore, you need to be familiar with Google Cloud Marketplace and the Google Cloud Platform management portal. You will gather information from the Google Platform and then use it for:

- Integrating CSCC with Cavirin
- Providing the CSCC-specific *Project ID* to Group Admin or DevOps users

After finishing the setup by integrating CSCC in the Cavirin UI, you must provide the *Project ID* from GCP for the CSCC project to the DevOps or Group Admin users. Authorized users need this *Project ID* to link a Cavirin asset group to CSCC, as described in the *Cavirin User Guide*.

In the following overview of the workflow, which starts after Cavirin has been added as a managed project in a GCP project via Google Marketplace, you:

19. Launch the Cavirin CyberPosture application from within Marketplace.
20. Sign up your organization for CSCC and get Cavirin's *Cloud SCC Companion App* in Google Marketplace. The *Cloud SCC Companion App* must be on a whitelist in GCP. As of the current release of beta CSCC, we suggest you contact a Google account rep to confirm your *Cloud SCC Companion App* is whitelisted.
21. Go to your Cavirin account and then navigate to **IAM & roles** > **IAM** and confirm that you have all of the following roles for the project at the organization-level in GCP: *Owner*, *Organization-level Administrator*, and *Security Center Administrator*. Obtain these roles and permissions if you do not have them.
22. Navigate to **IAM & roles** > **Services accounts** and click **Create**. Create a service account with a name that indicates its relation to CSCC, such as *cavirin-cscc-app*.
23. Look inside the service account and notice the Keys area.
24. Click **Create** Key.
25. Click **Save** after the key is created.
26. At the top of the *Security Command Center* screen, click **Add Security Sources**. This action takes you to Marketplace. If the card for Cavirin *Cloud SCC Companion* is not visible, use the search box to find it.
27. Click on the card for *Cavirin Cloud SCC Companion* to open the self-service provisioning workflow.

28. Click **Visit Cavirin System Site to Sign Up**. A page requests you to select your organization. In the dropdown, locate and highlight your organization, and then click the **Select** button at right of the dropdown.

    The Source Connect window appears. This page has a box for *Service Account* and a box for *Source ID*. The *Service Account* box shows the account you just created in step 4.

    The Source ID box contains two fields. They are the Organization ID ("*organizations*"), followed by a numeric string, and the Source ID ("*sources*"), also followed by a numeric string. The Organization ID is the Google-generated identifier of your Cavirin account, and the Source ID refers to the *Cavirin Cloud Security Companion*. When you later integrate CSCC in the Cavirin UI, you will paste or type these numbers into the corresponding boxes in the popup for integrating CSCC with the Cavirin system (next series of steps in this section).

29. Click **Done**. You are returned to the Security Command Center page.

30. Click **Settings** in the upper-right corner of the *Security Command Center* screen. The *Settings* screen appears.

31. Click the **Security Sources** tab at upper-left. A *Security Sources* table for your organization should show the new installation of *Cavirin Cloud Security Companion*. The next step is for downloading the credentials for *Cavirin Cloud Security Companion* to your local host.

32. Return to the *Service accounts* window

33. Select the service account created for the Cavirin Cloud Security Companion. Off to the right of the row for Cavirin Cloud Security Companion are three vertical dots that indicate a drop-down list.

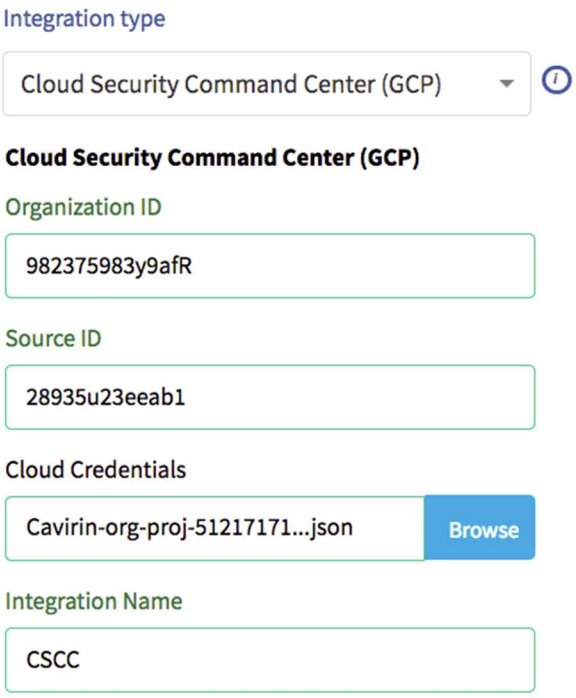
34. Click the drop-down list and, within the list, select **Create key**. A popup for this service account appears.

35. Select the JSON option and click **Create**. Save the key to a place known to you on your local host for subsequent use when you create the integration in the Cavirin UI (in the series of steps after you return to the Cavirin UI).

36. Go to the next series of steps to Integrate CSCC in the Cavirin UI.

To integrate CSCC with the Cavirin System:

7. Navigate to *Add Integration* and select **Cloud Security Command Center (GCP)** for the integration type.
8. Type or paste the *Organization ID* for Cavirin from GCP.
9. Type or paste the *Source ID* for Cavirin from GCP.
10. Upload the key in JSON format that you downloaded from the Google portal. (You downloaded the JSON file from Google Cloud to your local host and now provide it in the *Add Integration* popup.)
11. Type a name for the CSCC integration that indicates this integration is for CSCC.
12. Click **Save** (not shown in figure).

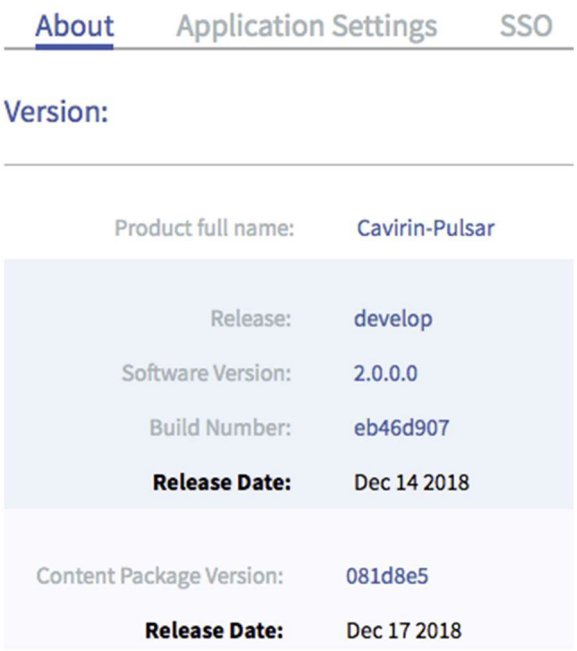


Application Settings

The features in this area provide system information; the ability to specify a custom port number for the services SSH, WinRM, and WinRM over HTTPS; and the SMTP configuration so that the Cavirin system can send email to users.

About (this Cavirin System)

The About section shows release information about the system (Release ID, software version, build number, and release date) and the policy pack content (version and release date). See next figure.

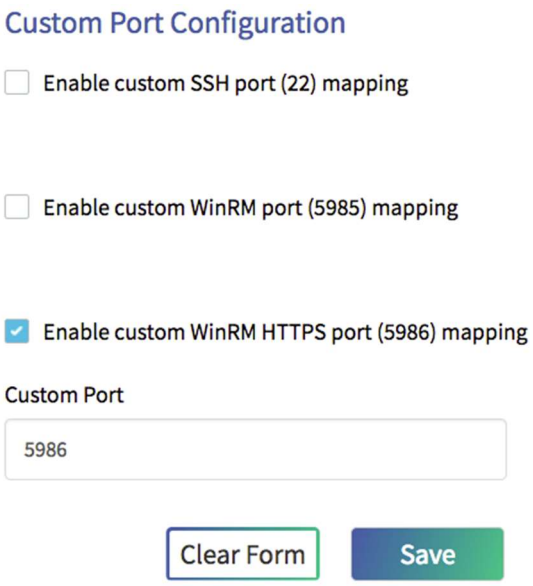


Application Settings

In this page, you can specify an alternative port number for the services SSH, WinRM, and WinRM over HTTPS. This configuration is optional. The reason for specifying alternative port numbers is a security measure but should done after careful consideration of the choice of alternative ports. The SMTP configuration enables the Cavirin system to send email to users and is a critical configuration.

To map SSH, WinRM, or WinRM over HTTPS to alternative ports:

4. Navigate to **Administer** > **Application Settings**. Click the Application Settings tab.
5. Select the protocol whose port you want to customize. The following figure shows all options selected.
6. Type the alternative port number in the *Custom Port* box.



7. Click **Save** when ready (or **Clear Form**).

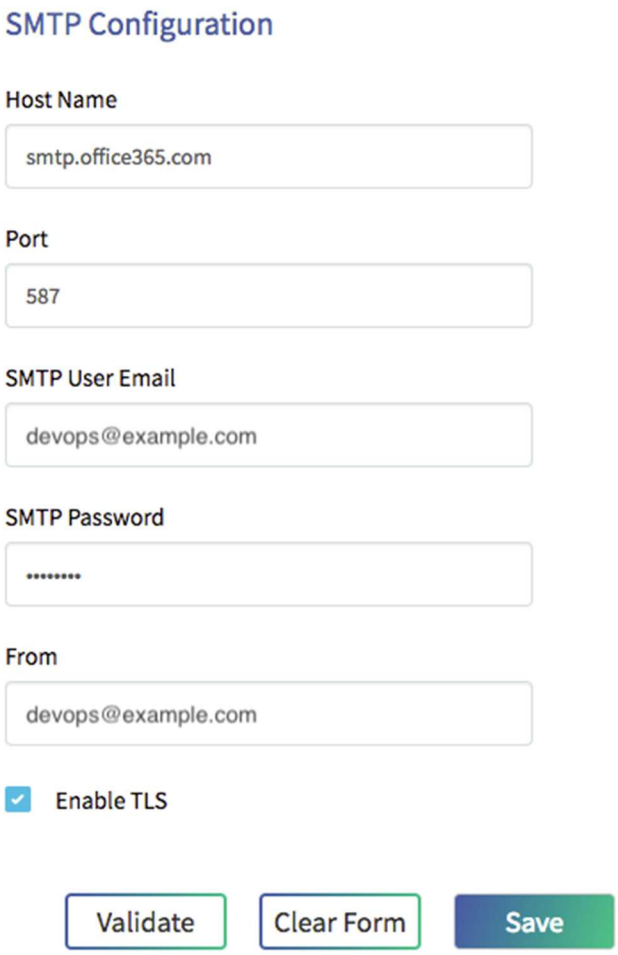
To set up SMTP:

NOTE: Configuring SMTP is mandatory. Without it, users do not receive email from the Cavirin system. For example, users would not receive a default password and not receive email notification that an assessment has started, stopped, or failed.

6. Navigate to Administer > Application Settings. Click the Application Settings tab.
7. Scroll to the SMTP Configuration area.
8. Type a host name, port number (default 587), an internal email address, internal SMTP password (for which users will not be prompted because this password is internal), a made-up email address that appears as the Sender (From) to recipients of the email.

   Enabling TLS is optional.

9. Click **Validate**.
10. Click **Save** If the setup is valid (or **Clear Form**).



Configuring Single Sign-on with Okta

In the current release, Cavirin uses Okta as the integration service to implement SSO.

NOTE: The prerequisite before beginning this steps in this section is to have "authentication server API" enabled by Okta itself.

The actions in this section involve the Okta portal and Cavirin's UI (Administer > Application Settings > SSO). Refer to Okta's on-line documentation as needed.

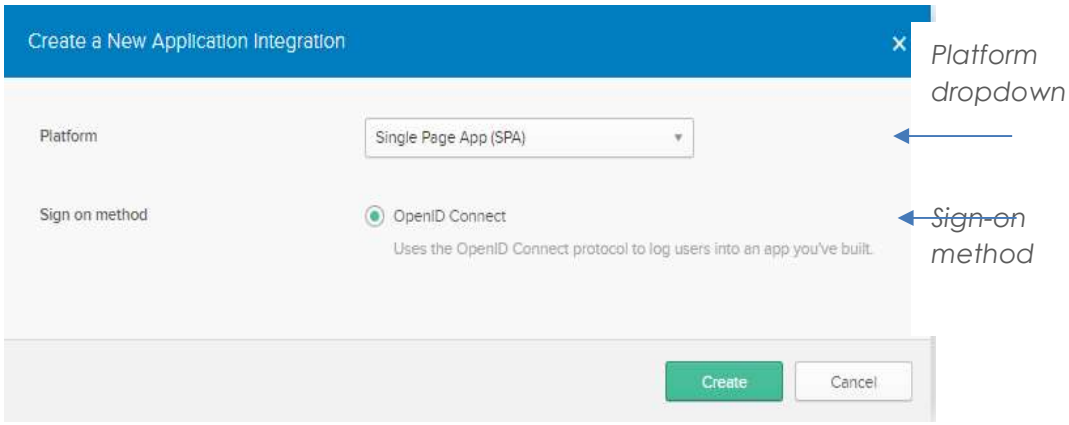
To set up SSO:

30. Go to your Okta management portal.
31. Click **Admin** at upper-right. (The *Add Apps* button is already highlighted.)
32. Click **Applications** in the banner and then select **Applications** in the dropdown that appears. The work area label changes from *Dashboard* to *Applications* and has an *Add Applications* button below the work area label *Applications*.

33. Click **Add Applications**. The display changes to include a *Create New App* button, including the *Create New App* button.

34. Start creating the new app by clicking **Create New App**. The *Create a New Application Integration* area appears as in the next figure.

35. Select **Single Page App (SPA)** in the *Platform* dropdown (next figure). The sign-on method defaults to **OpenID Connect**.

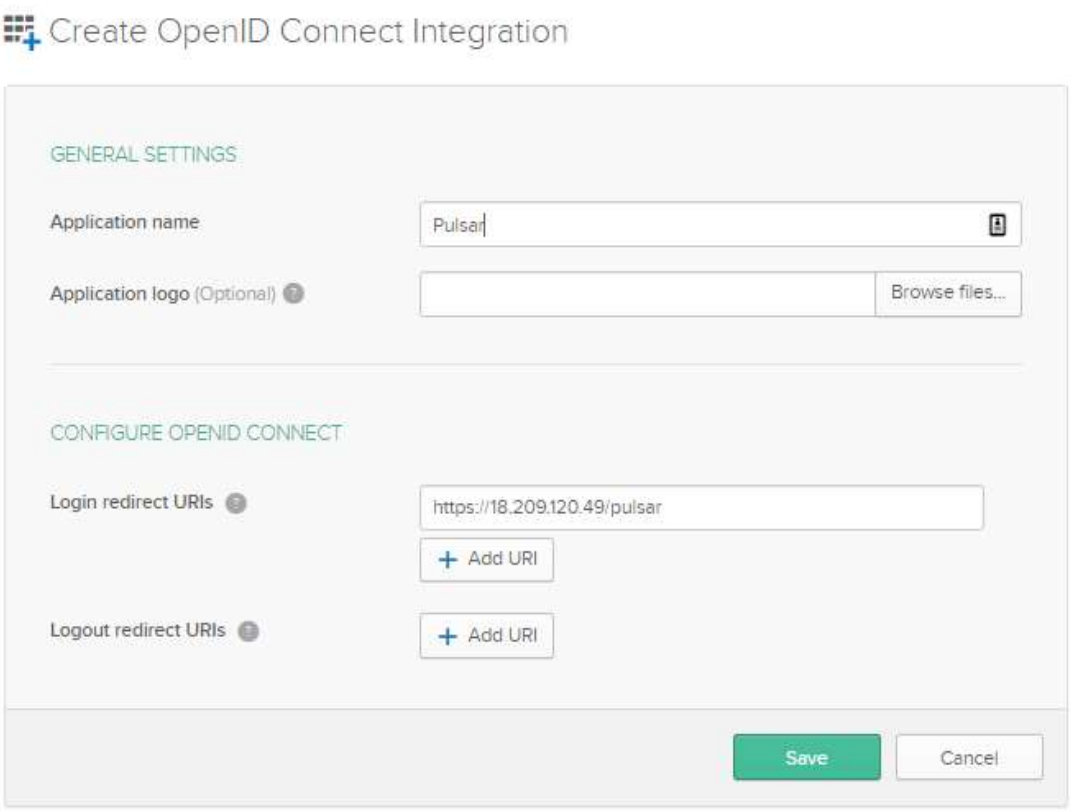


36. Click **Create**. A window named *Create OpenID Connect* opens (see next figure).

37. In the General Settings area, type a *Platform* name in the *Application name* box (such as "Pulsar").

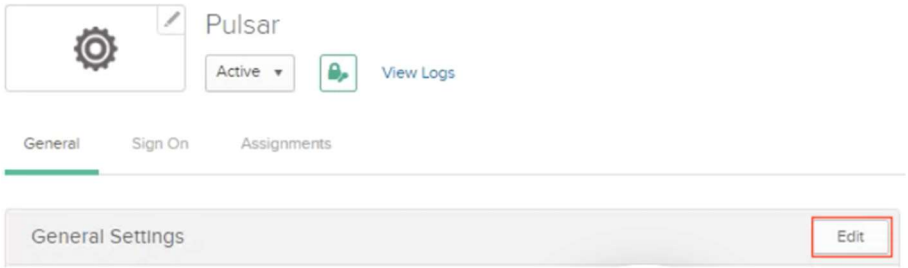
38. Type your Cavirin system's home page URI in the *Login redirect URIs* field and then do either of the following:

    - Click **Save** now (unless you copy the URI as directed in the next bullet).
    - Copy the URI from the address field of your Cavirin system's browser UI.



39. Click **Save**. The screen is redrawn, and new UI elements appear (next figure).

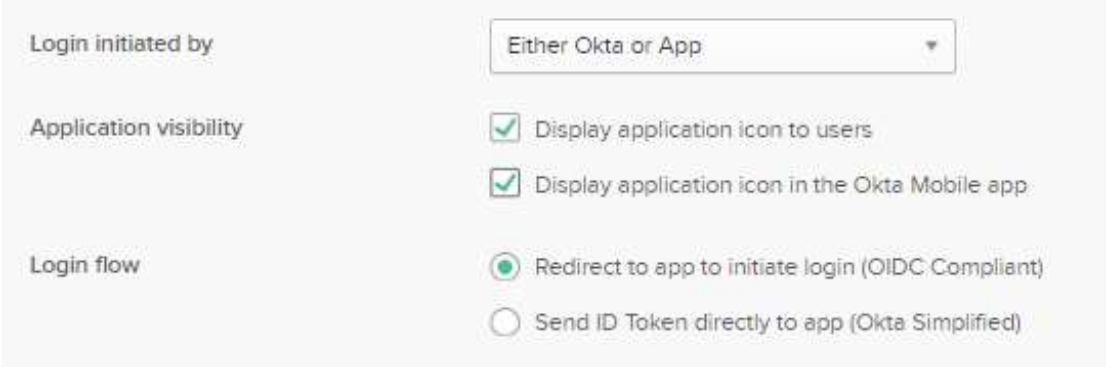
40. Click **Edit**, a button that has appeared at lower-right, to edit the settings.



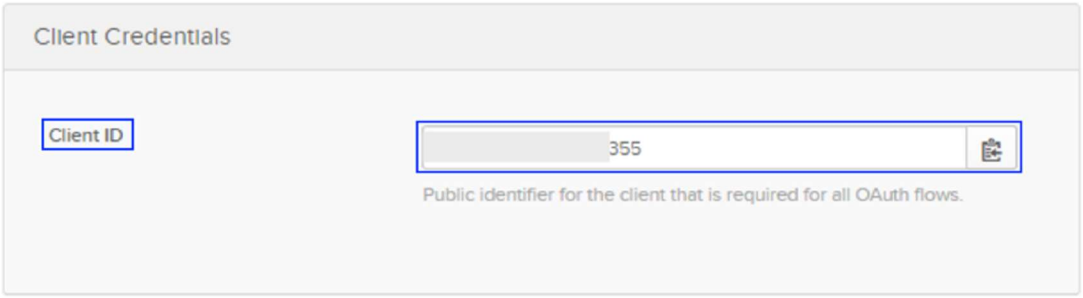
41. Select **Either Okta or App** in the dropdown for the value of *Login initiated by* (in the redrawn General Settings screen, next figure).

42. For Application visibility (next figure), marking both checkboxes is optional but recommended. The decision depends on an organization needs. Marking the first box lets a user have a chiclet in the Okta portal that logs them into the Cavirin system. Marking the second box lets a user log into Cavirin from a mobile device.

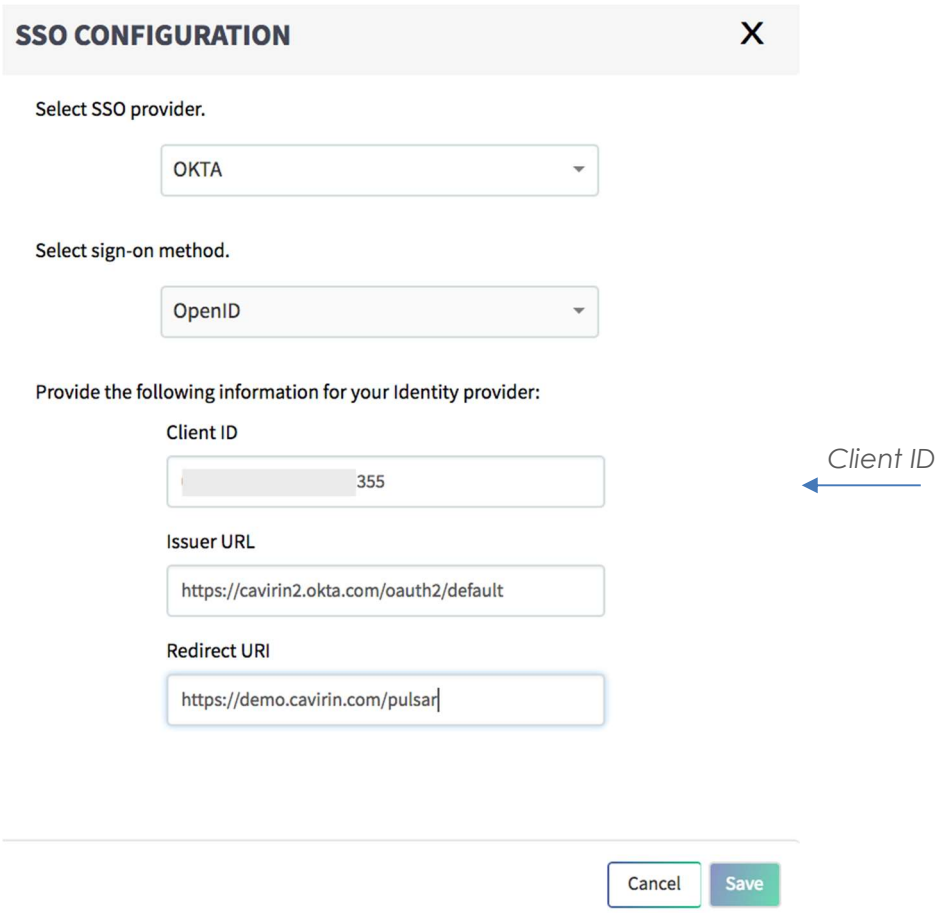
43. Clicks **Save** (not shown in next figure screen).



44. Copy the *Client ID* value (next figure) from Okta (Client Credentials area below the General Settings area). After you log into the Cavirin system and navigate as directed (next step), paste the *Client ID* in Cavirin's SSO Configuration.



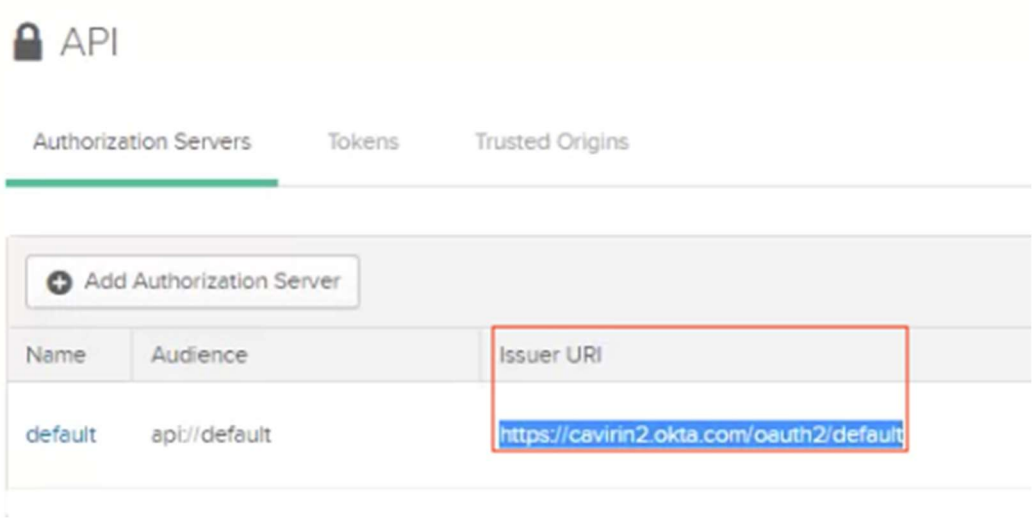
45. Log into the Cavirin system; navigate to **Administer** > **Application Settings** > **SSO**. The SSO Configuration window pops up.



46. Paste the *Client ID* from Okta into the Client ID box in the SSO Configuration.

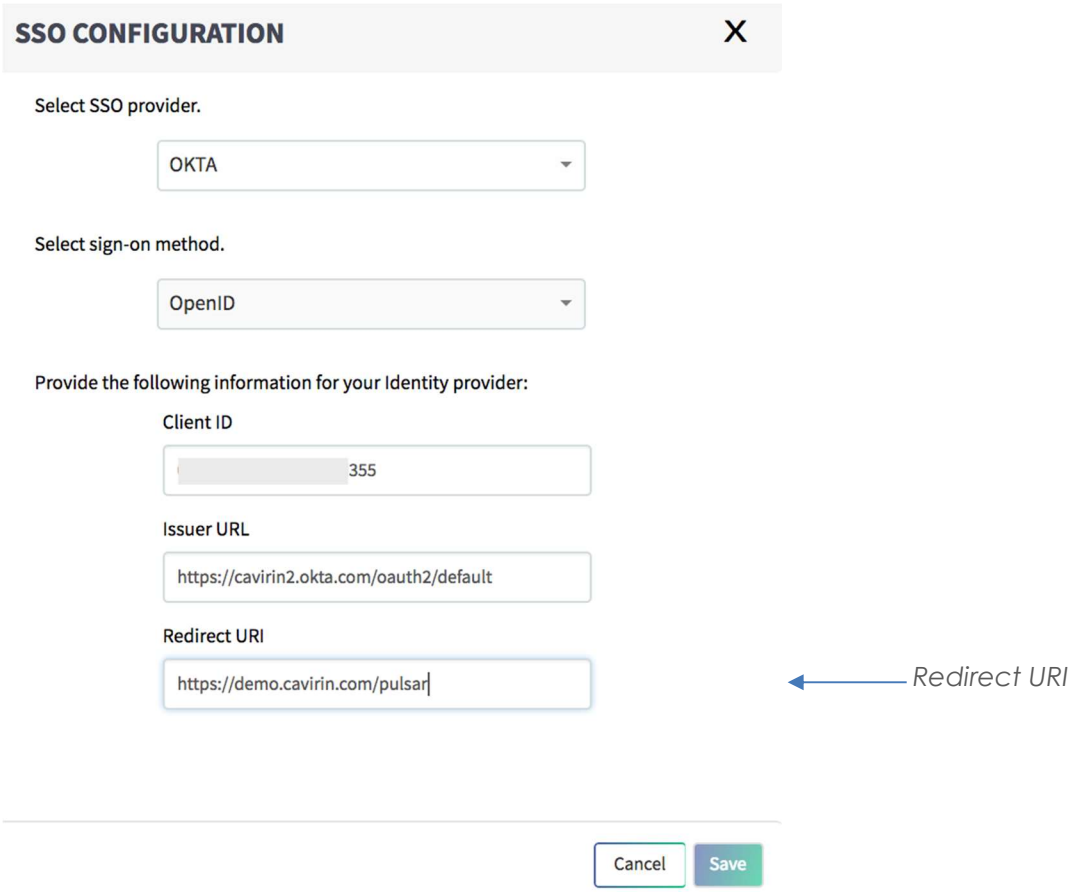
The next step is for copying the *Issuer URI* in Okta and pasting it in the Cavirin SSO Configuration (the previous figure shows it was already pasted).

47. In Okta, navigate to **Security** > **API** (next figure), copy the value of *Issuer URI* in the third column, and paste it into the Issuer URI field of the system's open SSO Configuration popup (subsequent figure).



48. Specify the Redirect URI in the SSO Configuration popup. This is the home page of the Cavirin instance and is identical to the Okta redirect, so you can copy it from Okta or just type it.

NOTE: For completeness, all fields in SSO Configuration should be populated.



49. Click one time outside the *Redirect URI* box before the next step.

50. Click **Save** *only once* In the Cavirin SSO Configuration popup. The system should display a confirmation of valid information.

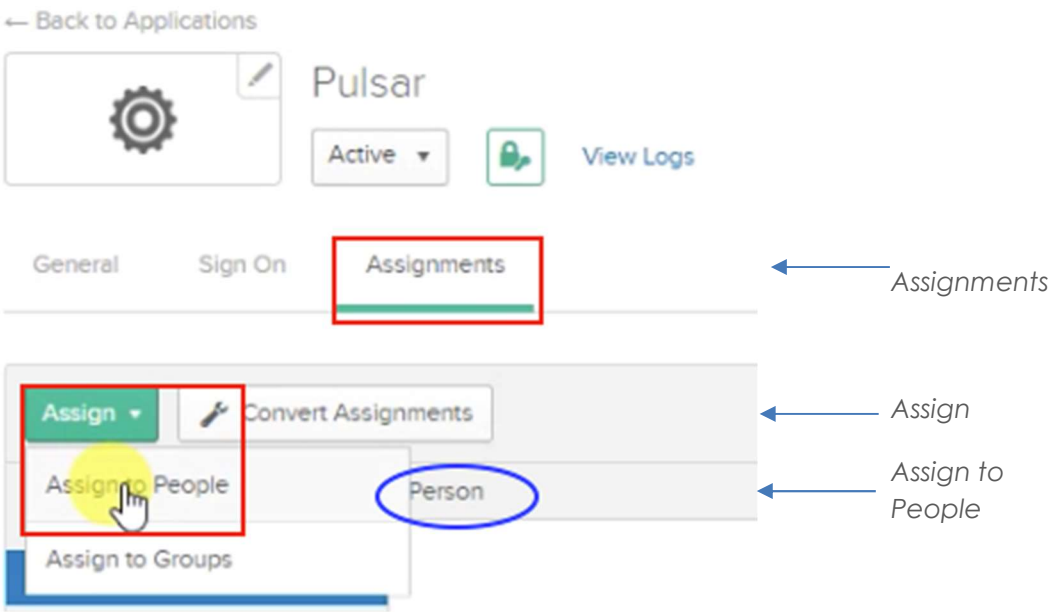
51. The SSO page shows the details of the Okta integration.

The next task is for specifying the Cavirin users that are authorized to use SSO. (An *authorized user* has access to the app/chiclet available from the Okta portal.)

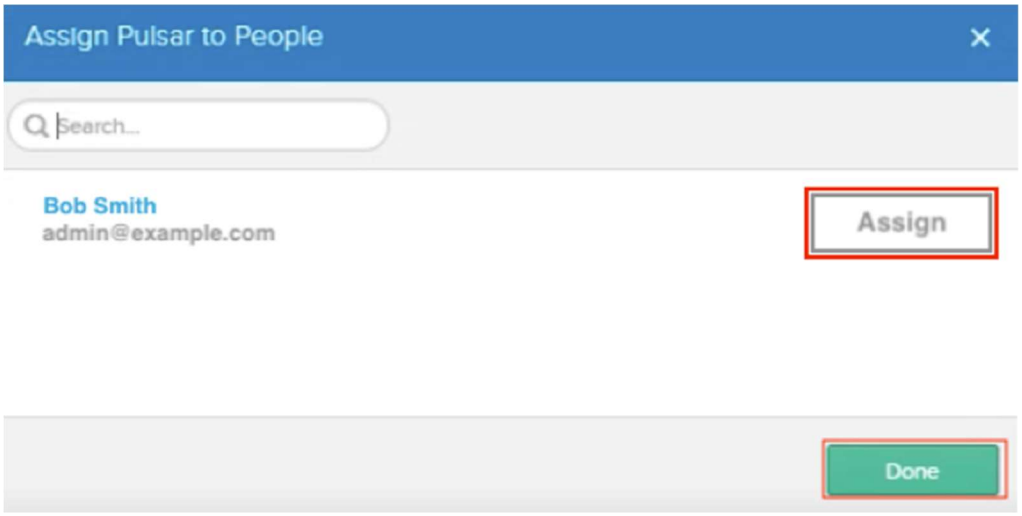
52. Return to the Okta portal (log in if necessary).

53. Click **Assignments** at top-left in the Okta Dashboard (next figure); then click **Assign** to see its dropdown menu; and then select **Assign to People**. The subsequent figure pops up. (This example shows "Pulsar" has not yet been assigned, so the *Person* column is empty.)

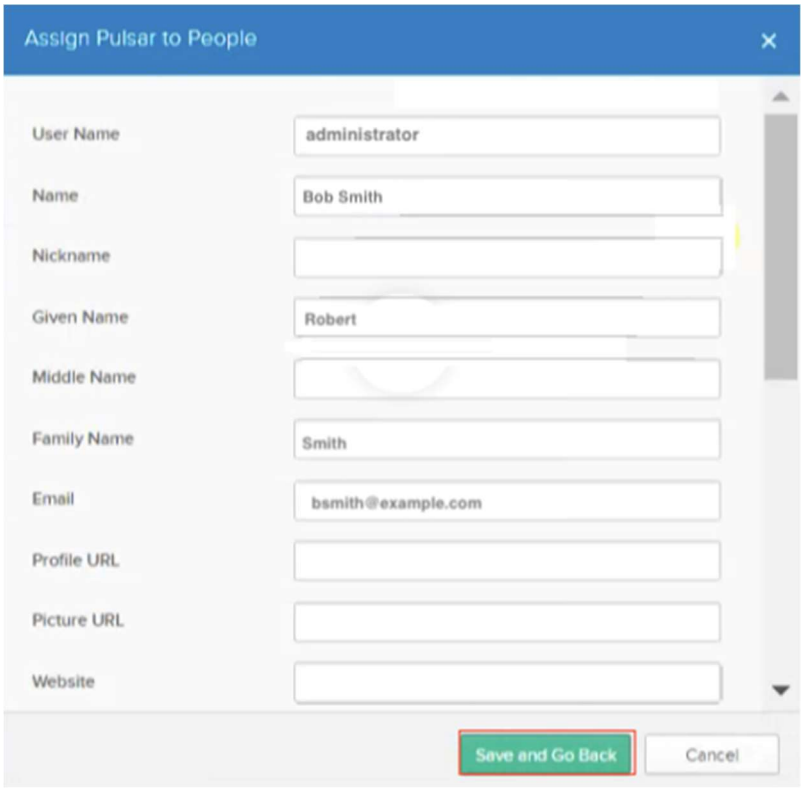
A list of Cavirin users, labeled *Assign Pulsar to People*, pops up, as the subsequent figure shows for just one employee.



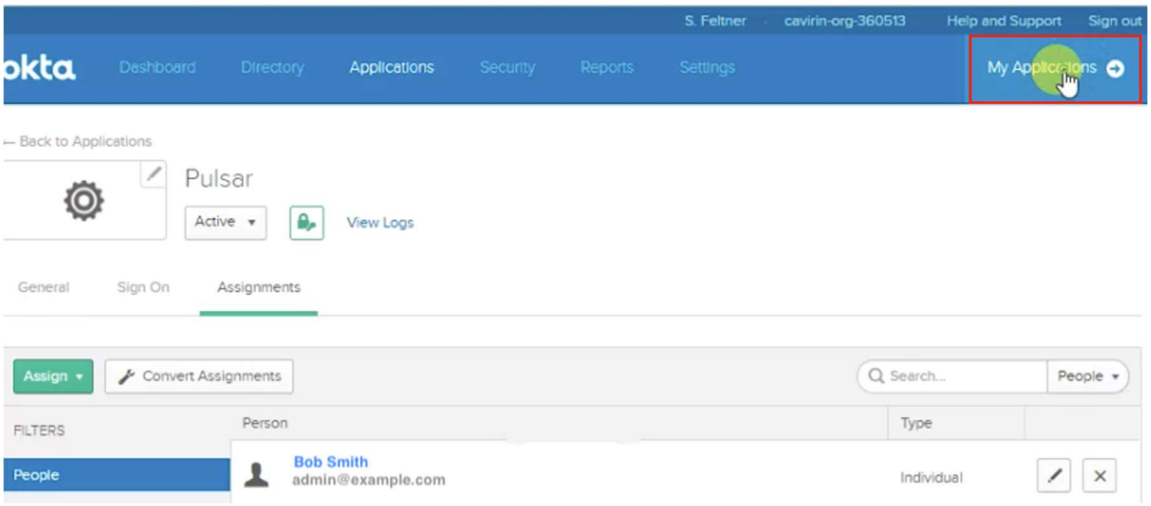
54. Click **Assign** next to the member intended to receive the Pulsar assignment, as in the next figure. This action opens another popup that lets you specify details about this user. At this juncture, you can press **Done** at the bottom of the next screen or add or modify details in the popup in the subsequent screen.



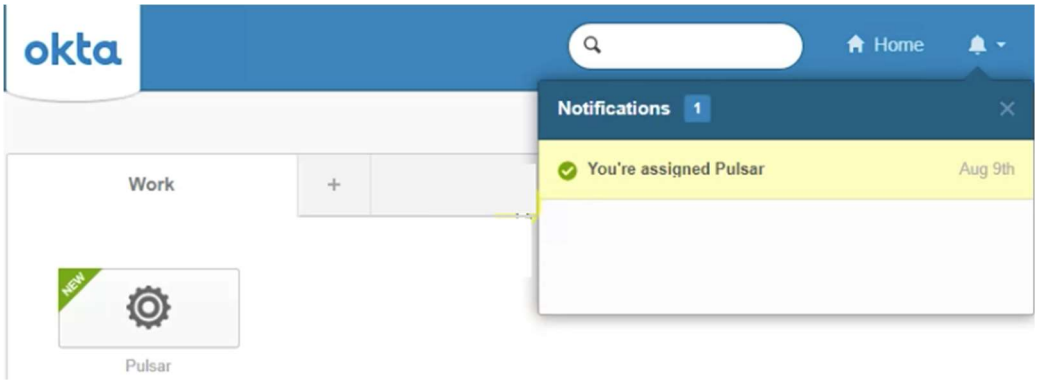
55. Accept the current user profile as-is or modify it as in the next figure. When ready, click **Save and Go Back** to assign Pulsar SSO to another user.



56. Click **My Applications** in the upper-right corner of the next figure. (Notice at the bottom of the next figure that the user name now appears in the *Person* column.)

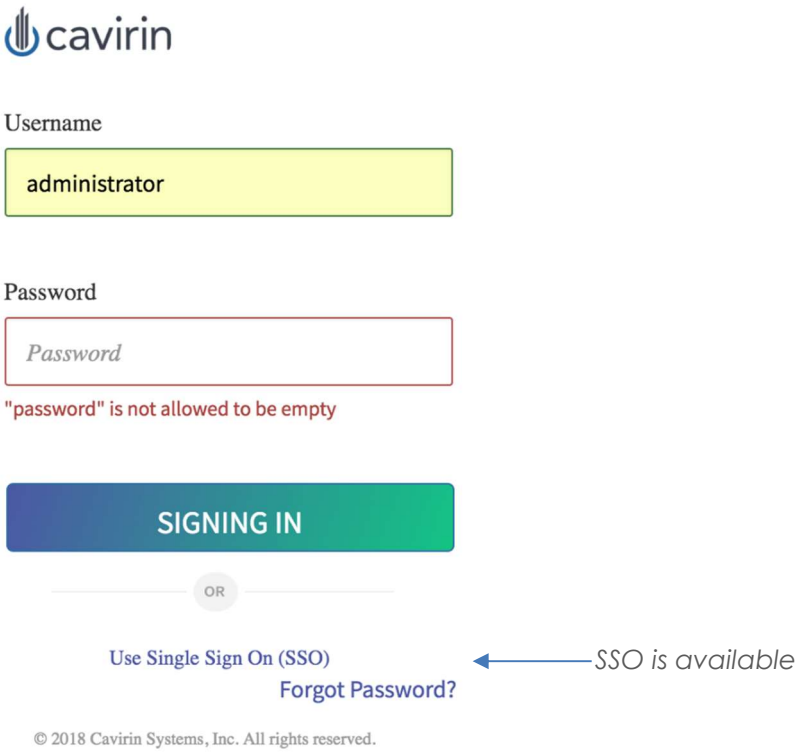


A popup confirms that SSO use with Pulsar has been granted (see "Notifications" and "You're assigned Pulsar"):



57. You can test the SSO login on Cavirin (first log out if already logged in). The login page should display the SSO sign-in option.

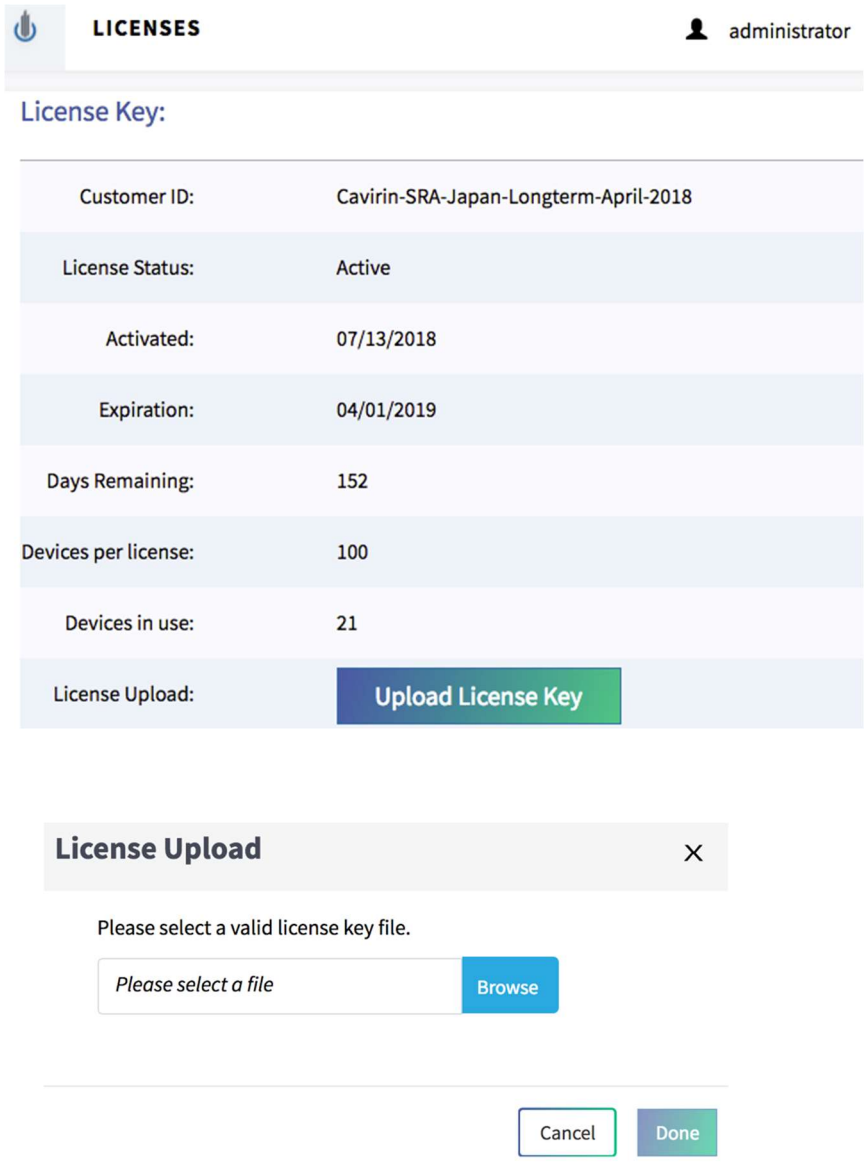
58. Click **Single Sign On** and receive access to the CISO Dashboard.



Product Licenses

The description in this section applies to Cavirin systems that are on-prem, in Azure, or in Google Cloud Platform, but not AWS. (AWS uses a mechanism for obtaining a license that does not involve a Cavirin administrator.) To upload a license (SuperAdmin role):

1. Navigate to **Administer** > **Licenses**. The popup in the following figure opens. It shows details about the current license (for an operational system in this figure).
2. Click **Upload License**. The popup in the subsequent figure requests you to browse the location of a valid license on the local host computer.
3. Select the license; click **Done**.


LICENSES
administrator
License Key:
Customer ID:
Cavirin-SRA-Japan-Longterm-April-2018
License Status:
Active
Activated:
07/13/2018
Expiration:
04/01/2019
Days Remaining:
152
Devices per license:
100
Devices in use:
21
License Upload:
Upload License Key
License Upload
Please select a valid license key file.
Please select a file
Browse
Cancel
Done

Setting Up GCP for Auto-remediation or Monitoring

Before a user in the role of Group Admin or DevOps can enable auto-remediation or monitoring for a Google Cloud account in the Cavirin UI, the Cavirin system must be configured at its back-end to support these features. This section provides the back-end configuration steps for auto-remediation and monitoring.

Setting Up the GCP Monitoring

This section describes how to set up monitoring for the Google Cloud Platform (GCP) environment. The minimum prerequisites and versions for this process are:

- Python 3.5
- Google SDK version 228
- Cavirin instance installed in a GCP environment

You can set up monitoring at the organization level or the project level. A single GCP project or multiple projects can be monitored. For monitoring more than one project, the default project is used to connect to the additional projects.

During this process, you will create service accounts. These service accounts can be removed after the initial set-up if the needed permissions for normal operation are in place, as this section describes.

Monitoring at the Organization Level

Log into Cavirin with SSH and an appropriate key. Then:

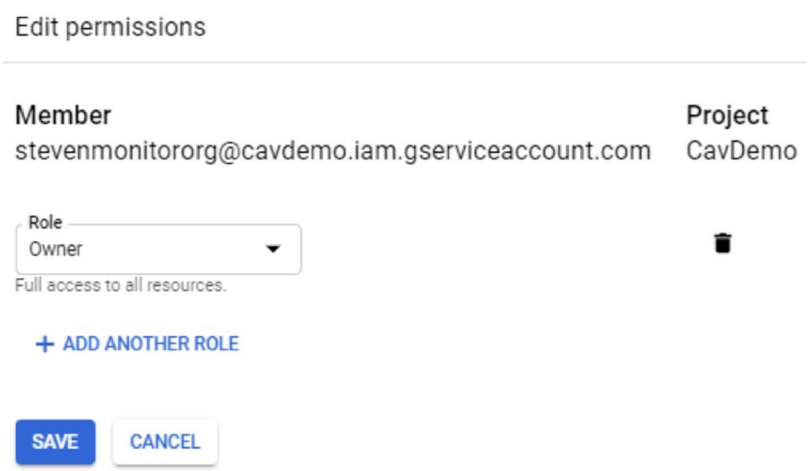
1. Navigate as follows: **cd /var/lib/cavirin/tools/gcp-monitoring**.
2. Unzip the archive: **unzip gcp-monitoring-org.zip.**
3. Navigate as follows: **cd cloudinstall.**
4. Open the following file for editing: **vi gcp-config-org.json.**
5. Enter values for *organizationID*, *defaultProjectID*, *keyPath*, *projectsList*, and *cloudFunctionName* to set up the GCP monitoring at organization level.
6. Run: **python3.5 cavirin-gcp-setup-monitoring-org.py**

   A user in the Group Admin or DevOps role uses some output values for enabling or modifying the monitoring function in a Google Cloud account on the Cavirin system. Specifically, a user must specify the *project ID* and *subscription name*.
7. **Copy** the *project ID* and *subscription name* (and paste in the Cavirin UI if appropriate now) or record for later entry.

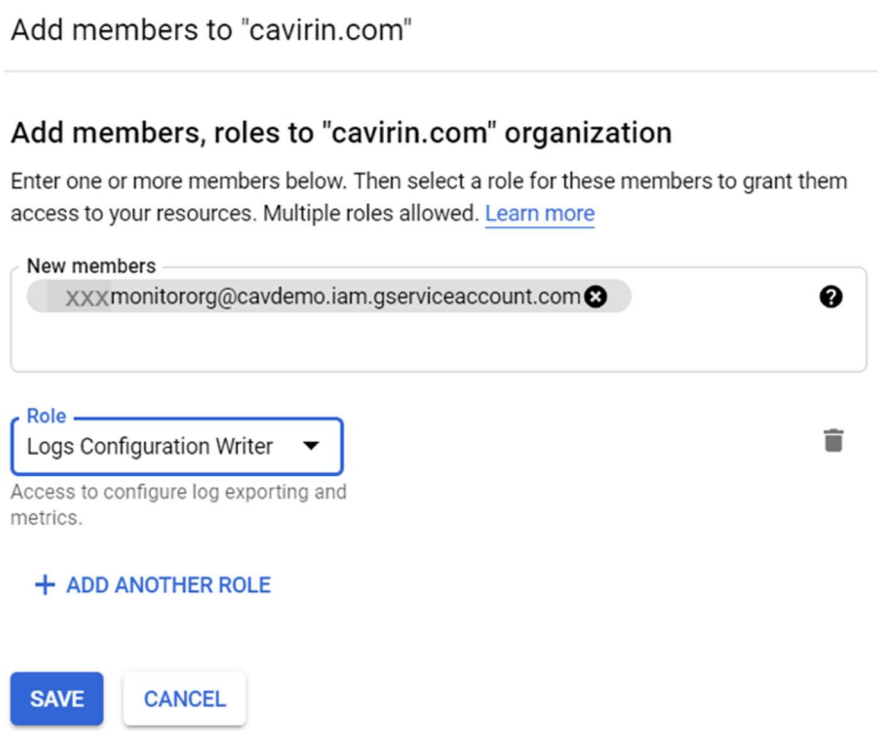
Create a Service Account at the Project Level

Create a service account at the project level (the default project), as follows:

1. Copy the Service account email alias.
2. Create a key for the service user.
3. Assign the *Project Owner Role* to the service user.



4. Navigate to the organization IAM.
5. Add User.
6. Enter the service account email address copied earlier.
7. Assign the Log Configuration Writer Role.
8. **Save**.



The APIs to Enable

To enable, navigate to API and Services -> Library.

Search for each of the following and enable them for the project:

- PubSub
- IAM
- cloudresourcemanager
- cloudfunction

Add the service account to all additional projects you wish to monitor.

Monitoring at the Project Level

Log into Cavirin with SSH and an appropriate key. Then:

1. Navigate to: **cd /var/lib/cavirin/tools/gcp-monitoring**.
2. Unzip the following: **unzip gcp-monitoring-project.zip**.
3. Navigate to: **cd cloudinstall**.
4. Edit the following: **vi gcp-config-project.json**.

5. Enter values for *defaultProjectID*, *keyPath*, and *cfName* to set up the GCP Monitoring at the Project level.

6. Execute: **python3.5 cavirin-gcp-setup-monitoring-project.py**.

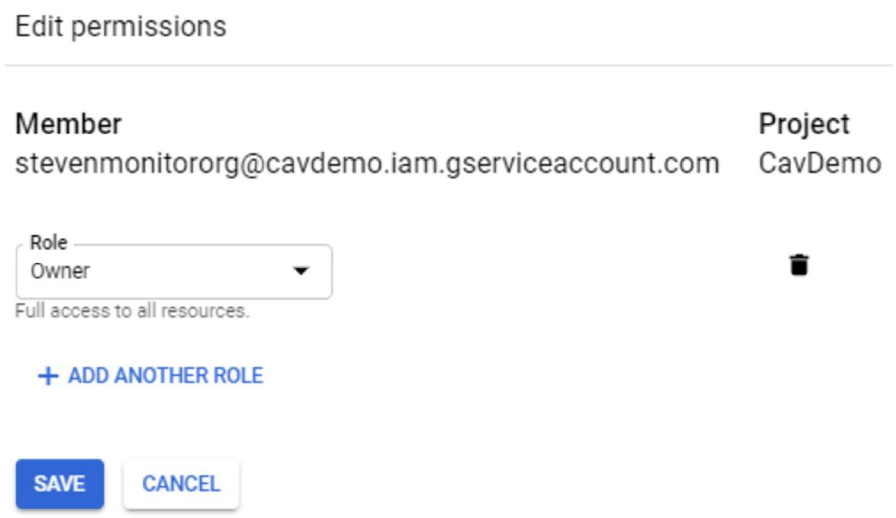
   A user in the Group Admin or DevOps role uses some output values for enabling or modifying the monitoring function in a Google Cloud account on the Cavirin system. Specifically, a user must specify the *project ID* and *subscription name*.

7. **Copy** the *project ID* and *subscription name* (and paste in the Cavirin UI if appropriate now) or record for later entry.

Creating the Needed Service Account for the Project

To create a service account at the project level (the default project):

1. Copy the service account email alias.
2. Create a key for the service user.
3. Assign the Project *Owner* role to the service user.



The APIs to Enable

This section lists the needed APIs to enable:

1. Navigate to: **API and Services** > **Library**
2. Search for each API and enable it for the project:
    - PubSub
    - IAM
    - cloudresourcemanager
    - cloudfunction

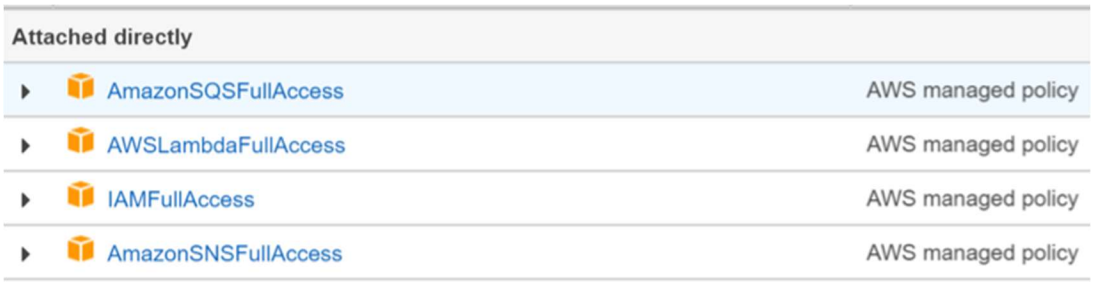
Setting Up AWS for Lambda-remediation or Monitoring

Before a user in the role of Group Admin or DevOps can enable Lambda remediation or monitoring for an AWS cloud account in the Cavirin UI, the Cavirin system must be configured at its back-end to support these features. This section provides the back-end configuration steps for Lambda-remediation and monitoring.

Setting Up the AWS Account for Lambda Remediation

Log into the Cavirin system with SSH and an appropriate key. Then:

1. Run **aws configure**.
2. Add your key, secret, and region. The policy on this key needs to be:



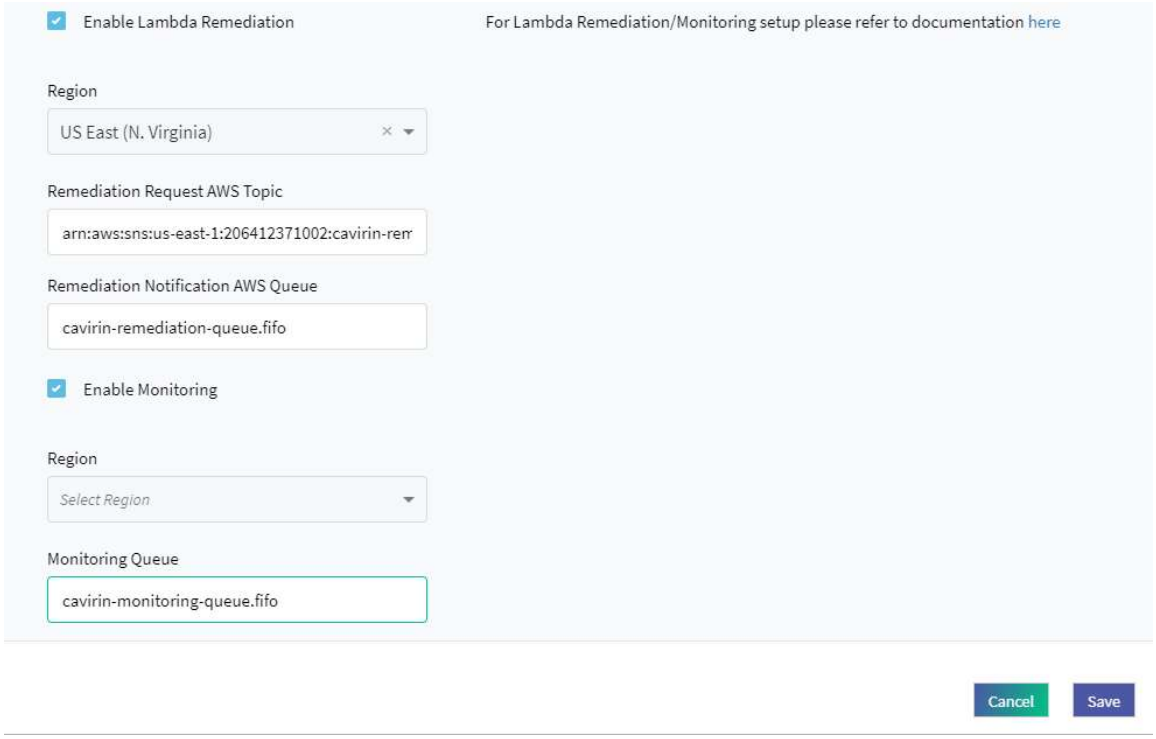
3. Navigate to: **cd /var/lib/cavirin/tools/aws-remediation**
4. Unzip the file: **unzip aws-remediation.zip**
5. Navigate: **cd cloudinstall**.
6. Run: **vi cavirin-config.json**. See next figure.
7. Specify a region and then save and close the file: "**region**":"*<desired region>*"

8. Run the script: **python3.5 cavirin_setup_remediation.py**

   Notice the topic and queue values at the bottom of the success message. A user in the role of Group Admin or DevOps must provide these values in the Cavirin UI (subsequent figure) if enabling Lambda remediation for a cloud account.

```
==========================================================================================
================================Cavirin Remediation Succesfully Setup=====================
==========================================================================================
Please use the following values to Input on the UI in Cloud Account Pop Up after enabling Remediation
Region: us-east-1
Remediation Request AWS Topic: arn:aws:sns:us-east-1:206412371002:cavirin-remediation-topic
Remediation Notification AWS Queue: cavirin-remediation-queue.fifo
```

The next figure shows where the Group Admin or DevOps user enters the values for AWS Topic and AWS Queue from the preceding script into the Cavirin UI. The user also must select the region in which the Lambda remediation engine will run. The configuration values for these values appear when the *Enable Lambda Remediation* box is marked.



9. Remove the .AWS folder: **rm -rf /home/ubuntu/.aws**.

This concludes the pre-requisite steps for setting up Lambda remediation.

Setting Up the Monitoring of an AWS Account

Monitoring focuses on the cloud environment instead of resources and watches for events that might indicate a breach of the cloud environment.

The steps in this section are for the back-end setup of monitoring and related steps un the Cavirin UI, specifically in the page for adding an AWS cloud account and the enable for monitoring. It also includes the steps for deleting the configuration.

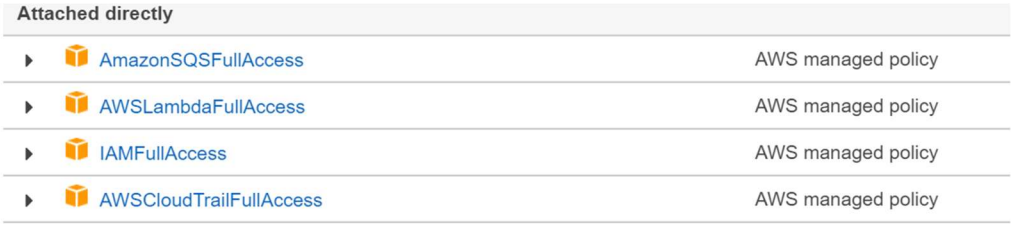
The pre-requisite resources for this section are as follows:

- AWS Boto3
- Python 3.5
- aws-cli/1.16.24 or above
- SSH access
- A FIFO queue

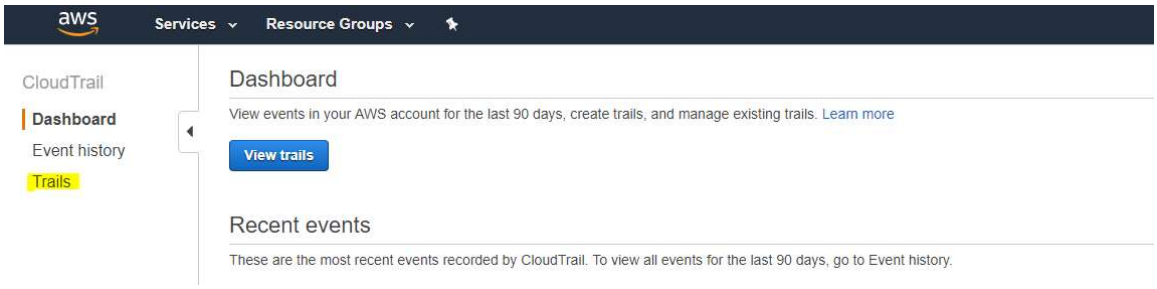
  NOTE: Although monitoring and remediation can be applied to any region, the FIFO queues for these functions are supported in a subset of all regions. The number of regions that support the FIFO queues changes. As of this release of the *Cavirin Administrator Guide*, FIFO queues are available in the US East (Ohio), US East (N. Virginia), US West (N. California), US West (Oregon), Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), Canada (Central), EU (Frankfurt), EU (Ireland), EU (London), EU (Paris), and South America (São Paulo) regions. To see the current regions, go here: [FIFO Region Support.]

To set up monitoring:

1. Log into Cavirin with SSH and an appropriate key.
2. Run ***aws configure***; add your key and secret; the policy on this key needs to be:



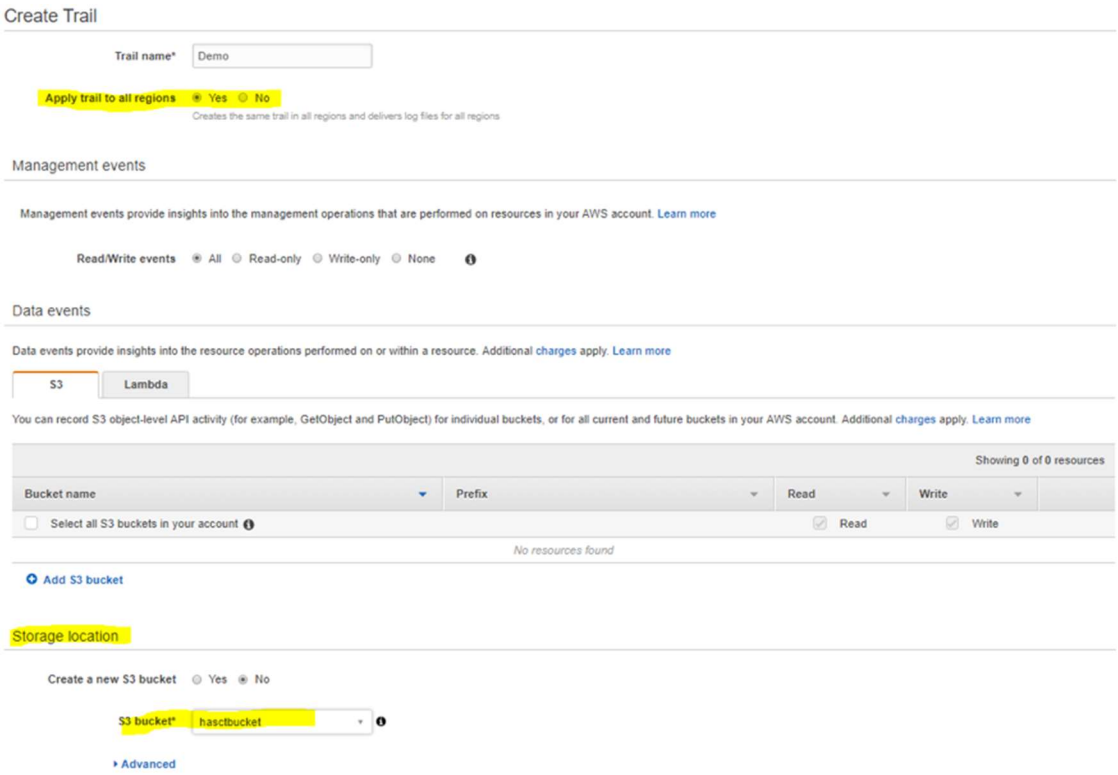
3. Navigate: **cd /var/lib/cavirin/tools/aws-monitoring**
4. Unzip the file: **unzip aws-monitoring.zip**
5. Navigate: **cd cloudinstall**
6. Open the AWS Console.
7. Navigate to AWS console -> Cloudtrail -> Trails.



8. Click **Create trail**:

9. Add the name for the trail. Store this name because you will need it later.

10. Select an existing s3 bucket or create a new one.

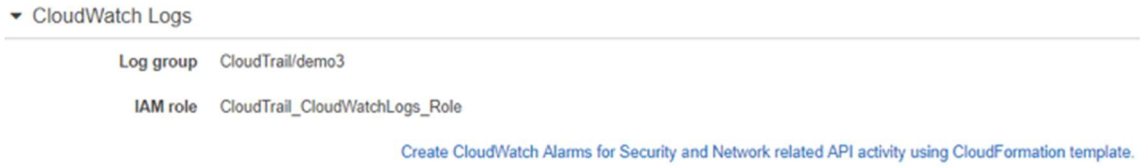


11. Click **Create**.

10. Click on the newly created trail.

11. Click **Configure** under the CloudWatch Logs**:**

12. Provide a name for the log group.
13. Select **Continue**.
14. Select **Allow**.



15. Return to the Cavirin SSH console.
16. Open this file for editing: **vi cavirin-config.json**
17. Edit the following lines and save the file:

"region":"*<desired region>*", where the region supports FIFOs.

"cloudtrail-region":"*<Region where cloudtrail is located/created (Home Region)>*"

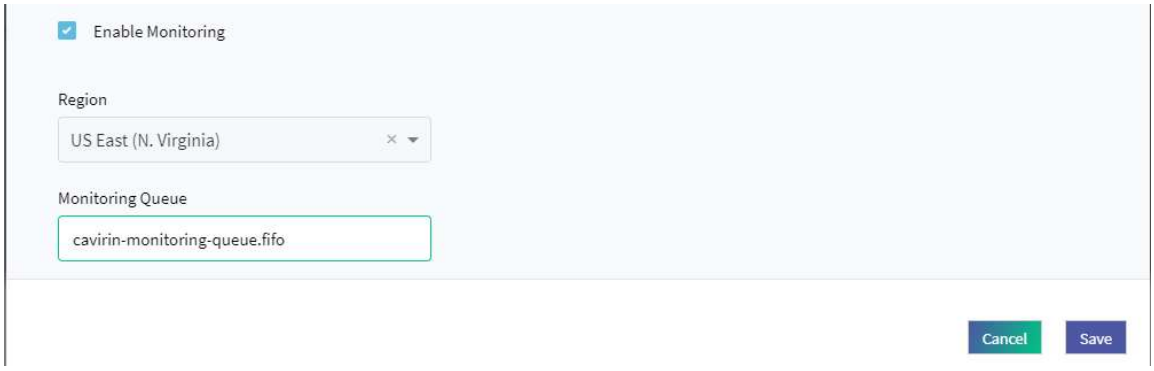
"CloudTrailName":"*<Name of trail>*"

```
ubuntu@ip-172-31-78-13:/var/lib/cavirin/tools/monitoring/cloudinstall$ vi cavirin-config.json
{
  "region":"us-east-1",
  "cloudtrail-region":"us-east-1",
  "CloudTrailName":"Demo",
  "FilterName":"cavirin-monitoring-filter",
  "FilterPattern":"{ $.eventName = AuthorizeSecurityGroupIngress && $.errorCode NOT EXISTS }",
  "SQSName":"cavirin-monitoring-queue",
  "PolicyName": "cavirin-monitoring-policy",
  "RoleName" : "cavirin-monitoring-role",
  "cavirin-monitoring-lambda-function": "cavirin-monitoring-lambda",
```

12. Run script: ***"python3.5 cavirin_setup_monitoring.py"***

```
================================================================================
================================Cavirin Monitoring Succesfully Setup============
================================================================================
Please use the following values to Input on the UI in Cloud Account Pop Up after enabling Monitoring
Region: us-east-1
Monitoring Notification AWS Queue: cavirin-monitoring-queue.fifo
ubuntu@ip-172-31-78-13:/var/lib/cavirin/tools/monitoring/cloudinstall$
```

1. Copy the AWS Queue and Region to the UI. Cloud Credentials -> Select AWS Account -> Edit -> Select Enable Monitoring.
2. Remove the .AWS folder: **rm -rf /home/ubuntu/.aws**



The subsequent descriptions are for removing a setup for Lambda or monitoring.

Tear-Down Scripts for AWS Monitoring or Lambda Remediation

This section lists the steps for two tasks. These tasks are: tearing down (removing) AWS monitoring and tearing down Lambda remediation.

Removing AWS Cloud Monitoring

To tear down the monitoring function:

1. Log into the system Cavirin by using SSH with an appropriate key.
2. Run **aws configure** and add your key, secret, and region.
3. Navigate to: **cd /var/lib/cavirin/tools/aws-monitoring/cloudfunction**.
4. Copy file: **cp config.json ../cloudinstall/cavirin-tdconfig.json**
5. Navigate to: **cd .. /cloudinstall**
6. Run: **python3.5 cavirin_teardown_monitoring.py**

Removing Lambda Remediation

To tear down the Lambda remediation setup:

1. Log into Cavirin via SSH with an appropriate key
2. Run **aws configure** – Specify your key and secret.
3. Navigate: **cd /var/lib/cavirin/tools/aws-remediation/cloudfunction/**
4. Copy file: **cp config.json ../cloudinstall/cavirin-tdconfig.json**
5. Navigate: **cd .. /cloudinstall**
6. Run: **python3.5 cavirin_teardown_remediation.py**

Information for Adding a Proxy Server

This section illustrates the steps that a user in the Group Admin or DevOps role takes to configure one or more proxy servers to sit between the Cavirin system and the asset groups in a subnet or segment. As a SuperAdmin, you do not perform these steps; this section just illustrates the information that a Group Admin or DevOps user needs.

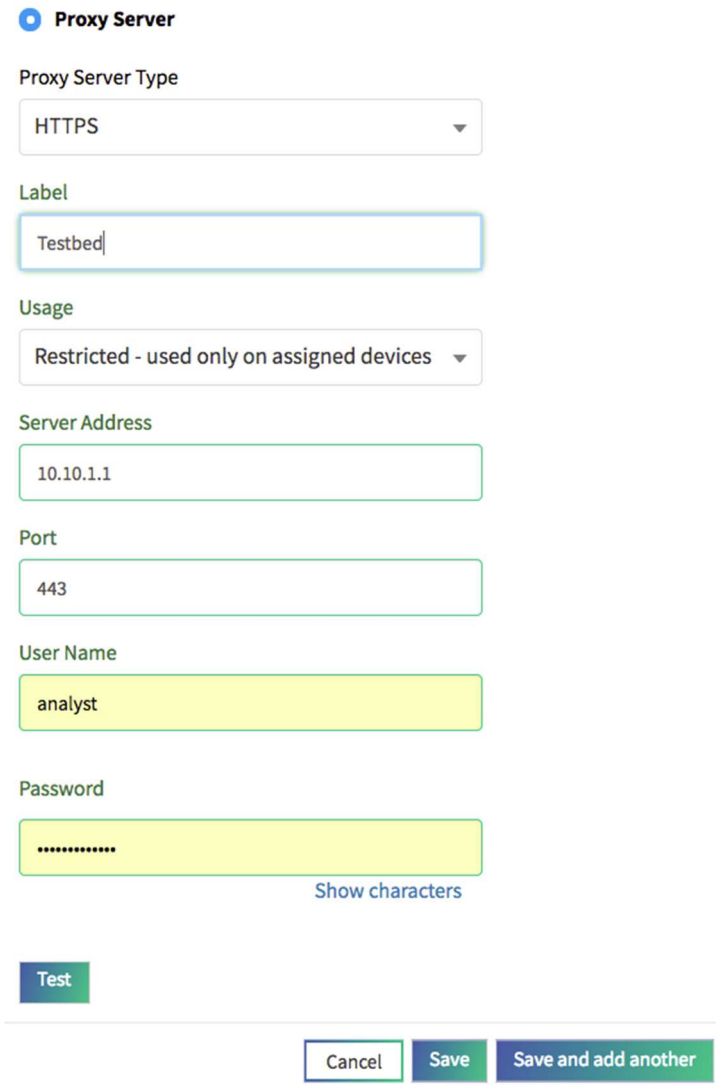
The supported server types are HTTP, HTTPS, SOCKS4, and SOCKS5 on port 80, 443, or 1080. Two places allow a user to specify a proxy server or see and modify existing servers: the *Discovery & Assess Resources* wizard for a new asset group and the editing popup for existing asset groups.

To configure a proxy server, the user:

1. Navigates to **Protect** > **Proxy Servers**. Clicks **Add Proxy Servers** and sees the configuration popup in the next figure illustrates.

2. Fills in the all the fields and clicks **Test** to confirm the validity of the configuration and the reachability of the server.

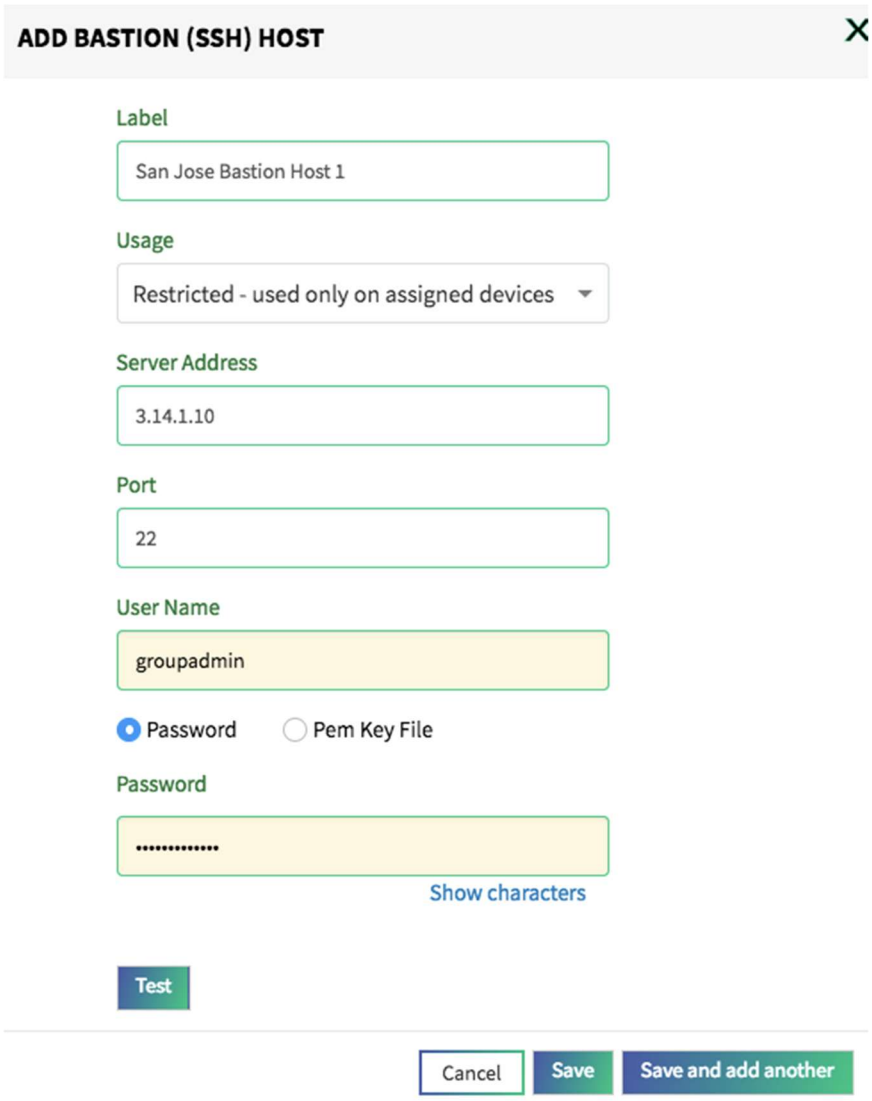
3. Clicks **Save** or **Save and add another**.


Proxy Server
Proxy Server Type
HTTPS
Label
Testbed
Usage
Restricted - used only on assigned devices
Server Address
10.10.1.1
Port
443
User Name
analyst
Password
Show characters
Test
Cancel
Save
Save and add another

Information for Adding a Bastion Host

A user in the role of Group Admin or DevOps can specify one or more bastion hosts to enhance the security of assets in subnets and segments. No back-end configuration of the Cavirin system by you is involved for bastion hosts. Instead, you or your organization must provide the following information to a user in the Group Admin or DevOps role when he or she specifies a bastion host in the *Protect > Bastion Hosts* screen (as they are directed in the *Cavirin User Guide*):

- A *label* is a meaningful name of this bastion configuration.
- *Usage* - The Cavirin system offers user-specified login credentials to the bastion host when it seeks to communicate with the bastion host. The *usage* is *restricted* or *global* (same meaning for host credentials): restricted credentials are offered to the bastion host that the user specifies in the Cavirin UI, and global means credentials are offered to all bastion hosts.
- *IP address* of the bastion host.
- TCP *port* number (always 22 because SSH is the protocol for bastion hosts).
- *Username* for the Cavirin system when the bastion host requests Cavirin's credentials.
- The Cavirin system offers a *password* or a *PEM key file* and an optional *PEM passphrase* to the bastion host when it authenticates the Cavirin system.


ADD BASTION (SSH) HOST
Label
San Jose Bastion Host 1
Usage
Restricted - used only on assigned devices
Server Address
3.14.1.10
Port
22
User Name
groupadmin
Password
Pem Key File
Password
Show characters
Test
Cancel
Save
Save and add another

Upgrading the Content of a Policy Pack

The procedure for upgrading a policy pack is the same for all policy packs. This description uses the Cavirin Patches and Vulnerabilities Policy Pack as the example.

1. Copy the new-content file from the Cavirin S3 bucket to the local directory on the Cavirin system, for example:

   /home/ubuntu/latest-content/latest (compliance and P+V bundle).

2. Make the file executable: **chmod +x latest**

3. Execute the script to install the latest content packages: **./latest**

Changing the Rate of Auto-assessments Based on Event Threshold

Auto-assessment means that when security events in a monitored environment cross a threshold, an assessment is automatically initiated. The assessment applies wherever the asset group exists. For example, if an asset group has been created to exist in three AWS regions and Cavirin determines that the threshold of suspicious events was crossed in one region, the assessment applies to all regions where the asset group exists. Also, when the assessment begins, the event counter is reset.

If the Cavirin system detects that monitored events in a cloud cross a threshold in an up or down deviation from a baseline of events, an assessment immediately begins. (The exception to this action is when an assessment on the same, targeted asset group is in the pre-scan state, in which case Cavirin lets the current assessment proceed.)

The number of monitored events might initiate too many auto-assessments. This section describes how to reduce the number of auto-assessments by changing the threshold. The instructions apply to any cloud that has enabled monitoring.

> **NOTE**: In the current release of the Cavirin system, cloud monitoring and auto-assessments are linked in the following way: if you set up monitoring and a user in the role of Group Admin or DevOps enables monitoring for a specific cloud account, the auto-assessment function is on by default and cannot be disabled.

After the automatic assessment, the baseline remains the same, and the event count is reset. Also, the assessment clears the related events in the Alerts screen.

The default threshold is a deviation of 10% from the preceding period of monitoring. For example, if 100 events were detected in the preceding 15-minute period and 89 or 111 events are detected in the current 15-minute period, Cavirin automatically starts an assessment. (The threshold is not crossed with 90 or 110 events—these are the thresholds.)

The deviation in the configuration file is expressed as a decimal value, so the default of 0.1 means a 10% deviation. However—and especially if an excessive number assessments are interfering with operations or just becoming inconvenient—you can raise the threshold for triggering an assessment. The higher the percent of deviation, the fewer auto-assessments will be triggered.

To modify the threshold:

1. Navigate: **cd /var/lib/cavirin/pulsar-workflow-monitoring/conf**
2. Open the configuration file in the *conf* directory: **vi config.json**
3. Locate the *monitoring_threshold_count* setting in the configuration file.
4. You can:
   - *Increase* the value to *reduce* the occurrence of auto-assessments
   - *Reduce* the value to increase the number of assessments

   For example, if you change the value of *monitoring_threshold_count* from the default .1 to 1(100%), the number of auto-assessment will be one tenth of the previous number. The threshold becomes 1100 events in an hour.
5. Save and close the *config.json* file.

This is the end of the *Cavirin Administrator Guide* for Winter release.