ThreatConnect® System Administration Guide

Software Version 7.4

Technical Guide

January 10, 2024

10013-25 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 I F: 703.229.4489
www.ThreatConnect.com

Table of Contents

Overview

A System Administrator account within ThreatConnect works, in many ways, just like a normal Organization account—it even belongs to an Organization that can contain other System Administrator accounts—but it has additional permissions and capabilities that allow the user to configure System Settings within On Premises and Private Cloud ThreatConnect Instances. This guide explains many of the tasks requiring system privileges, particularly the systemwide tasks that are performed primarily on the **System Settings** screen. See *ThreatConnect Account Administration Guide* for instruction on tasks that must be performed by a System Administrator on the **Accounts Settings** screen.

Because of the account's ability to change System Settings, it is advised that the account be used only for these tasks and not for Organization administration, Community administration, or regular analysis. In general, administrative tasks should always be carried out by the least-privileged account possible to help maintain system security and functionality.

Access the System Settings Screen

1. Log into ThreatConnect with a System Administrator account (that is, an account with a System role of Administrator).
2. On the top navigation bar, hover the cursor over **Settings** and select **System Settings**. The **Settings** tab of the **System Settings** screen will be displayed (Figure 1).

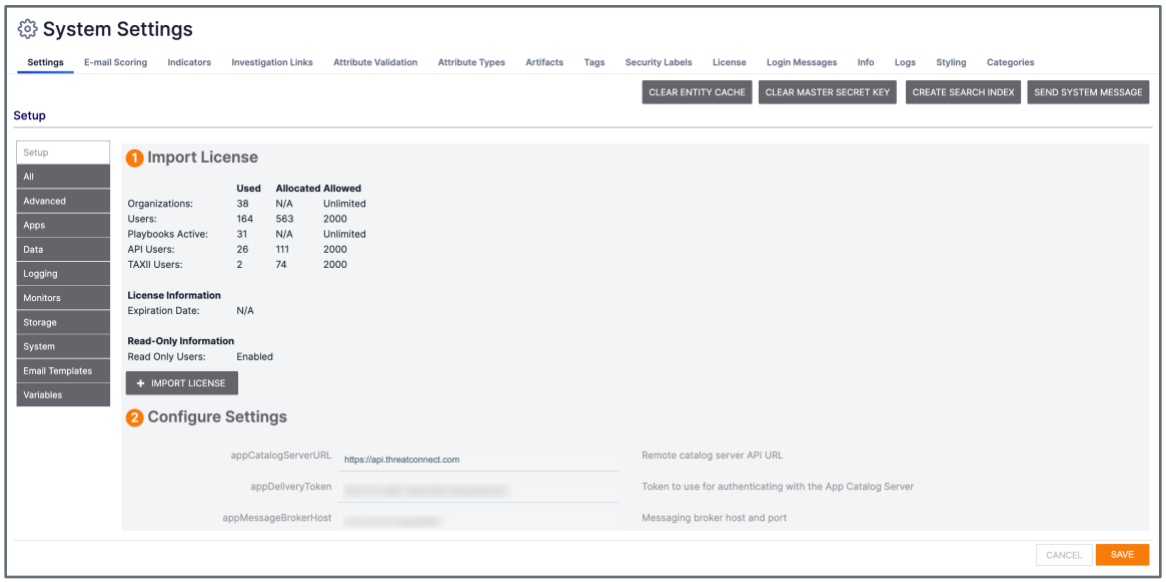

Figure 1

Table 1 provides an overview of the **Settings** menu options. For more information on tasks performed in the **Account Settings** and **Org Settings** screens, refer to *ThreatConnect Account Administration User Guide* and *ThreatConnect Organization Administration User Guide*, respectively.

Table 1

Settings Menu Option	Description
My Profile	Select this option to configure basic user settings for this account, including password changes.
Org Settings	Select this option to create and configure other user accounts within the Organization. Typically, these are other System Administrator accounts.
Org Config	Select this option to modify Attributes, Indicator Exclusion Lists, Security Labels, and Deprecation for a given Organization.
Account Settings	Select this option to create, configure, and manage all Organizations and accounts within an On Premises Instance.

System Settings	Select this option to configure systemwide properties for an On Premises Instance.
TC Exchange™ Settings	Select this option to view installed Apps, install new Apps, and configure System Jobs, among other features.
Help	Select this option to open the ThreatConnect Knowledge Base in a new window.
Logout	Select this option to log out of ThreatConnect.

User Accounts

Create User Accounts

1. Log into ThreatConnect with a System Administrator account.

2. On the top navigation bar, hover the cursor over **Settings** and select **Org Settings**. The **Membership** tab of the **Organization Settings** screen will be displayed (Figure 2).

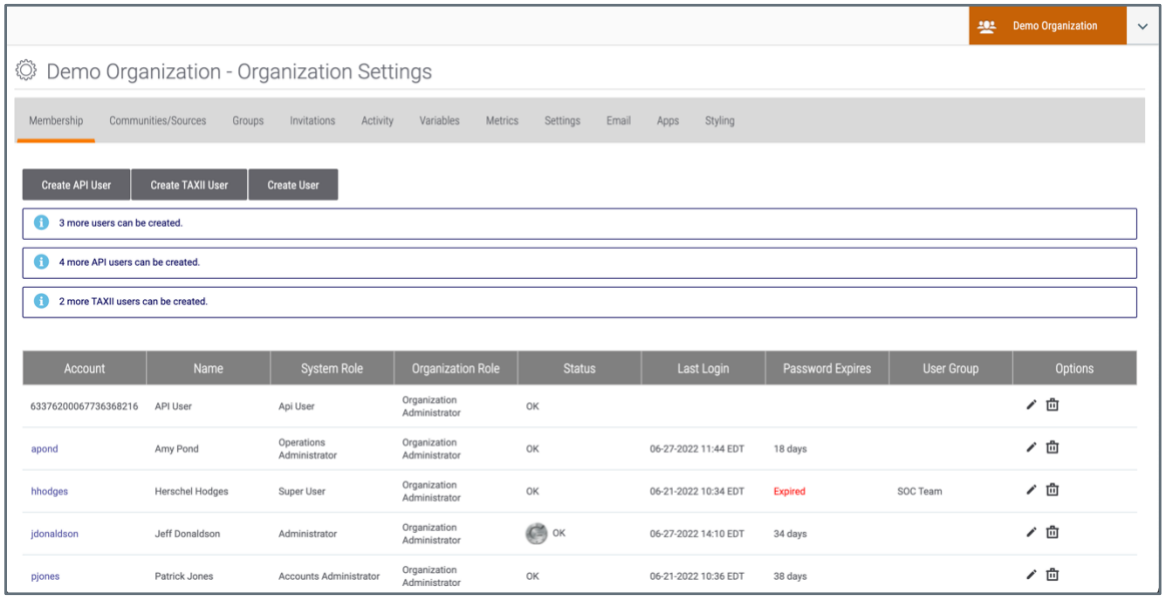

Figure 2

> **Note**: Above the **Accounts** table, the **Organization Settings** screen displays how many more users of each type can be added to the Organization.

3. Click the **Create User** button. The **User Administration** window will be displayed (Figure 3).

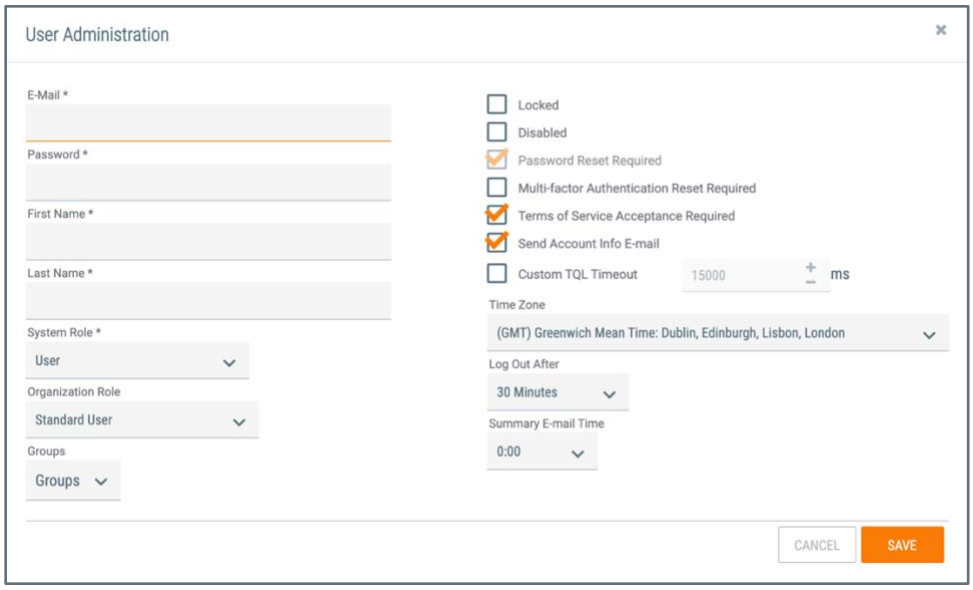

Figure 3

- **E-Mail**: Enter an email address that will also be the name of the user account.
- **Password**: Enter the initial user password, which is subject to the ThreatConnect password policy defined within the system settings.
- **First Name**: Enter the user's first name, which, along with the last name, is what other user accounts see when the user posts within the Organization or in a full-profile Community.
- **Last Name**: Enter the user's last name, which, along with the first name, is what other user accounts see when the user posts within the Organization or in a full-profile Community.
- **System Role**: Select a System role for the user.
- **Organization Role**: Select an Organization role for the user.
- **Groups**: Select user groups to which to add the user, if desired. User groups allow multiple users to be assigned to Workflow Cases and Tasks together.
- **Locked**: Select the checkbox to lock the user account, or clear the checkbox to unlock a user account that has been locked by ThreatConnect.
- **Disabled**: Select the checkbox to disable the user account, which is typically done when a user no longer requires access to ThreatConnect and the Administrator wants to retain log integrity.

- **Password Reset Required**: Select this checkbox to force the user to change the account password upon next login. This checkbox is selected by default upon account creation, and it is cleared once the password has been changed.
- **Multi-Factor Authentication Reset Required**: Select this checkbox to require the user to configure multi-factor authentication (MFA) for their account or to reset MFA for a user who already has it configured (for example, if the user has lost their MFA token). An icon such as the Google Authenticator™ logo will be displayed in the **Status** column for users who have MFA enabled.

  Note: MFA can be disabled for a user on the **Authenticator** tab of the **User Profile** screen for the user. To navigate to this screen, click on the user's account name in the **Account** column of the **Membership** tab of the **Organization Settings** screen (Figure 2).

  Note: MFA can be enforced systemwide via the **twoFactorAuthenticationRequired** system setting. See this setting's entry in the "Setting Descriptions" for more information. If this setting is enabled, then MFA may not be disabled for individual users.
- **Terms of Service Acceptance Required**: Select this checkbox to reset the "terms of service" flag so the user is presented with the terms of service again. It is selected by default when creating a new user.

  Important: The **termsOfServiceRequireNewUserToAccept** system setting must be enabled for the checkbox to be displayed in this window.
- **Send Account Info E-mail**: Select this checkbox to send an email with the account information to the email address entered in the **E-Mail** field. It is selected by default when creating a new user.
- **Custom TQL Timeout**: Select this checkbox to override the system-level ThreatConnect Query Language (TQL) query timeout (i.e., the **tqlQueryTimeout** system setting) for the user. In the field to the right of the checkbox, enter the maximum amount of time, in milliseconds, that TQL queries made by the user will be allowed to run before timing out.
- **Time Zone**: Select the time zone for the user.
- **Log Out After**: Select the amount of time of inactivity after which the user will be logged out.
- **Summary E-mail Time**: Select the time at which the user will receive daily summary emails of followed items or other notifications from ThreatConnect.

4. Click the **SAVE** button to create the user account.

To create Read Only User accounts (including Read Only Commenters), follow the preceding steps, but click the **Create Read Only User** button in Step 3. Note that only **Read Only User** and **Read Only Commenter** are available in the **Organization Role** menu. Users of these types that join a Community or Source will have read-only permissions in that owner as well.

> **Note**: Read Only User accounts do not count against Organization's user license limits as long as they have a System role of Read Only User. Creating Read Only Users requires a license that allows Read Only Users.

Modify User Accounts

1. Click **Edit** to the right of an entry in the table on the **Organization Settings** screen (Figure 2). The **User Administration** screen will be displayed (Figure 4).

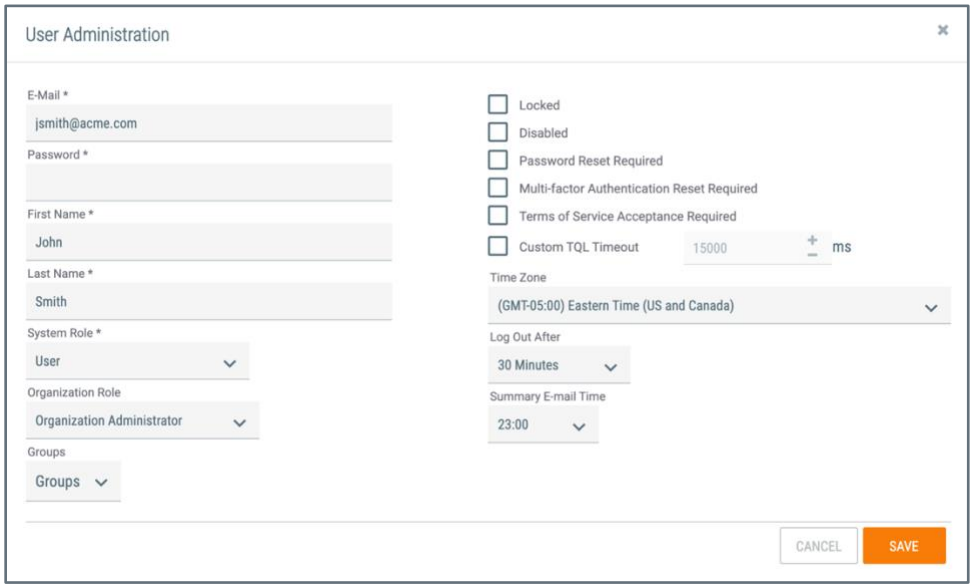

Figure 4

2. Make any desired changes to the account, and click the **SAVE** button.

Edit User Profiles

1. Click an account's username in the **Account** column on the **Organization Settings** screen (Figure 2). The **User Profile** screen will be displayed (Figure 5).

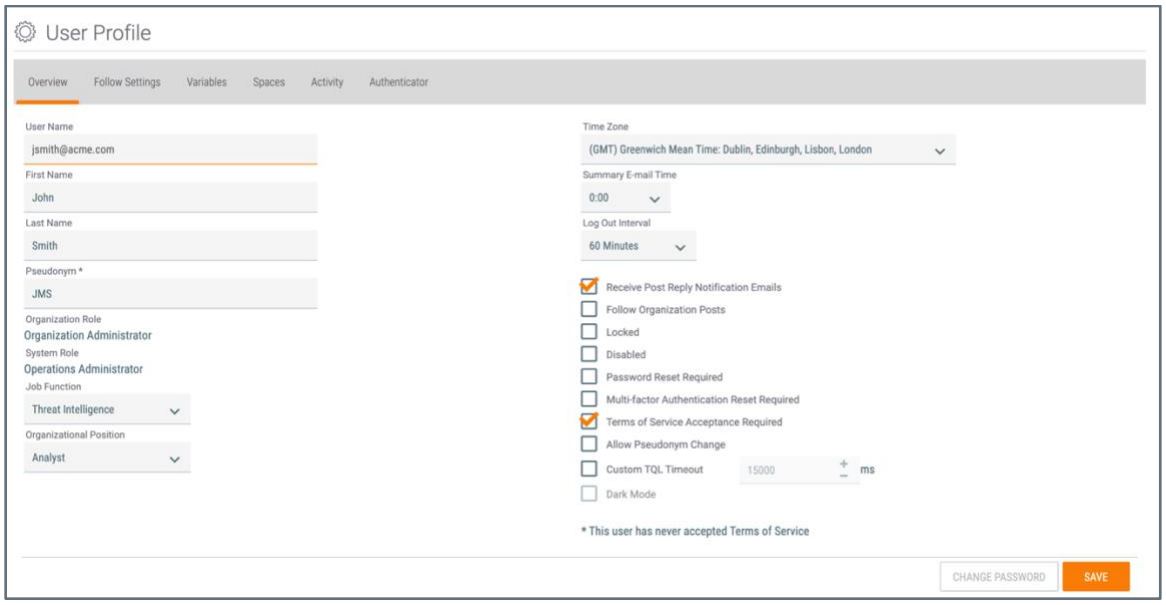

Figure 5

2. Make any desired changes to the account, and click the **SAVE** button. See Figure 3 and the "Overview Tab" section of *My Profile* for more information on the options and checkboxes on this screen.

System Settings

View and Modify System Settings

1. Click **All** in the menu on the left side of the **System Settings** screen (Figure 1) to view a list of settings grouped by category.
2. Make any desired changes to the settings, and then click the **SAVE** button at the bottom right of the screen.

Setting Descriptions

Each system setting or group of settings is defined as follows:

> **Note**: Acceptable values for each setting are defined using configuration-specific boundaries. Specific values or ranges of values are provided for some settings in this section. For all other settings, validation is enforced by the UI when applicable.

advancedJobScheduleEnabled

This setting enables access to advanced Job scheduling.

alertExpirationEnabled

This setting turns on or off the System Alert Expiration Monitor, which, when enabled, deletes system alerts after a period configured in the **alertExpirationInterval** setting. System alerts include alerts for sending notifications to users based on the Follow feature.

alertExpirationInterval

This setting determines the system interval, in hours, at which the alert-expiration purge runs if the Alert Expiration Monitor is enabled.

alertRetentionTime

This setting determines the number of days to keep alerts with no associated records before deleting them.

allowUIErrorCollection

This setting determines whether UI error logs are sent to ThreatConnect.

allowOrganizationPublish

This setting determines whether an Organization can create intelligence packages via the Publish feature (typically limited to Communities and Sources).

> **Note**: Enabling the **allowOrganizationPublish** setting will cause a **Publishing** tab to be displayed on the **Org Config** screen. For more information about this screen, see the "Publishing" section of *ThreatConnect Organization Administration Guide*.

apiIndicatorObservationLimit

This setting specifies the maximum number of observed Indicators that can be returned at a time from v2 of the ThreatConnect API.

appBuilderFileLimitMb

This setting specifies the maximum file size (in MB) for storing a single file in an App development project.

appCatalogServer

This setting allows the server to act as an App Catalog Server.

appCatalogServerURL

This setting corresponds to the remote Catalog Server API URL.

appDeliveryToken

This setting signifies the token that is used to authenticate with the App Catalog Server.

appExecutionDBDaysToKeep

This setting determines the number of days to keep data in the Job-execution table.

appMessageBrokerHost

This setting signifies the messaging broker host and port.

appSharedPlaybookExpirationDays

This setting specifies the number of days before a shared Playbook expires.

appSharingServer

This setting allows the server to act as an App Sharing Server.

> **Important**: To configure additional Sharing Servers or to convert the primary ThreatConnect instance to a Sharing Server, this setting must be enabled.

appSharingServerURLs

This setting corresponds to the App Sharing Server API URL.

appsApiTokenKeepAliveOffsetSeconds

This setting determines the number of seconds to keep an App's API token alive by adding to the user logout interval.

appsApiTokenKey

This setting is the App's API token signing key.

appsApiUrl

This setting should point to the URL for the API at port 8443.
(e.g., **https://api.threatconnect.com:8443)**.

> **Important**: To solve a routing issue, modify the **/etc/hosts** files to allow loopback to resolve to the host in the URL (e.g., **127.0.0.1localhostapi.threatconnect.com**).

appsJavaHome

This setting holds the path to the Java binary.

appsJobMonitorEnabled

This setting is not currently in use.

appsJobNotifyLogFileSizeLimit

This setting is the maximum file size (in MB) of each log file that is attached to the email notifying a user that a Job has finished executing.

appsPythonHome

This setting holds the path to the Python® 3.6.*x* binary.

appsPythonHome311

This setting holds the path to the Python 3.11.*x* binary.

appsRuntimeKillMinutes

This setting indicates the number of minutes that an App will run before being killed automatically.

appsRuntimeThresholdEmail

This setting represents the email used for when an App reaches the threshold minutes limit.

appsRuntimeThresholdMinutes

This setting indicates the number of minutes an App will run before the threshold email is sent (if set).

appsSandboxUser

This setting represents the user account used to execute Jobs.

appServiceAutoStartDelay

This setting determines the number of seconds that the system will wait to automatically start enabled Service Apps after restart.

appsSessionDaysToKeep

This setting indicates the number of days that logs will be kept in the Jobs log directory: **%threatconnect%/exchange/jobs**. It is set to **5** in the Cloud.

appsUploadLimitMb

This setting is the App's catalog file size limit (in MB).

batchApiEnabled

This setting indicates whether batch Indicator upload is enabled.

batchExpireFileDays

This setting indicates the number of days to retain batch Job error files.

batchFileUploadLimit

This setting indicates the batch file size upload limit (in MB).

bulkIndicatorEnabled

This setting turns on the Bulk Indicator Export Service for Communities and Sources.

> **Note**: Document storage is a prerequisite for enabling this service.

bulkIndicatorOnDemandEnabled

This setting determines whether Indicator bulk downloads may be run on demand.

bulkIndicatorTempLocation

This setting tells the system where it will have temporary disk space to build and compile the Bulk Indicator list.

Acceptable Values: A file path to which the system has read/write/edit permissions

bulkReportBatchSize

This setting represents the maximum number of results to process at a time during bulk report creation.

CALEnabled

This setting enables ThreatConnect's Collective Analytics Layer (CAL™), a feature that constantly monitors a user's interaction with the platform's native Indicators. This setting and the following three other CAL settings must be turned on to enable this feature: **CALHost** (system setting), **CALMonitorEnabled** (system setting), and **Enable CAL Data** (account setting specific to each Organization on the instance; see Figure 5 in the *ThreatConnect Account Administration Guide*).

CALHost

This setting identifies the hostname or IP address of the CAL server.

CALMonitorEnabled

This setting enables the CAL integration monitor.

caseResolutionList

This setting is a comma-separated list of possible Case Resolution values.

Default Values: **[Containment Achieved, Deferred / Delayed, Escalated, False Positive, In Progress / Investigating, Not Specified, Rejected, Restoration Achieved]**

componentForkPoolSize

This setting specifies the number of concurrent Component threads allowed per Playbook Worker.

crossOwnerAssociationEnabled

This setting enables the ability to create associations between Cases, Groups, and Indicators in a user's Organization and Groups and Indicators that exist in Communities or Sources to which they have access. It also enables Super Users to create these associations between objects in the Organizations on their instance and between those in the Communities and Sources to which they have access.

> **Note**: If this setting is disabled after being enabled previously, users can still view and remove cross-owner associations created while it was enabled. However, they will not be able to create new cross-owner associations.

defaultDashboard

This setting indicates the name of the default dashboard layout to use for all new Organizations, users, etc.

defaultUserTheme

This setting indicates the default theme for new users.

diskSpaceMonitorInterval

This setting indicates the system interval the disk space monitor runs (in minutes).

diskSpaceMonitorThresholdFactor

This setting indicates the percentage of disk used when the monitor takes action.

diskSpaceMonitorInodeFactor

This setting indicates the percentage of inodes used when the monitor takes action.

diskSpaceMonitorAlertFactor

This setting indicates the percentage of disks used when the monitor sends an email notification.

diskSpaceMonitorAlertEmail

This setting indicates the e-mail addresses or alias to receive alert notifications (comma separated).

diskSpaceMonitorInodeHoursToKeep

This setting indicates the number of hours retained for session logs when the inodes threshold factor is reached.

diskSpaceMonitorIntodeFileSystem

This setting indicates the filesystem where inodes are checked.

diskSpaceMonitorDaysToKeepDeleteFactor

This setting indicates the percentage reduced for existing days to keep settings.

dnsBounceDailyLimit

This setting determines the maximum number of DNS daily changes before Bounce Protection is activated, if DNS Bounce Protection is enabled (under the **dnsBounceProtectionEnabled** setting).

dnsBounceProtectionEnabled

This setting turns the System DNS Bounce Protection on or off. DNS Bounce Protection monitors Host Indicators, with DNS monitoring turned on for excessive DNS fluxing. If a Host Indicator changes its DNS enough times to meet the maximum value specified in the **dnsBounceDailyLimit** setting, then its DNS monitoring will be turned off.

dnsEnabled

This setting turns the System DNS monitor on or off, as well as supports DNS tracking. The DNS monitor sends periodic DNS requests for Host Indicators, with DNS monitoring turned

on, and logs responses as DNS Resolutions. The period of DNS requests is determined by the **dnsRefreshInterval** setting.

dnsRefreshInterval

This setting determines the system interval, in minutes, at which Host Indicator DNS resolutions are performed.

Acceptable Values: This setting is set within the **On Premises Instance** license; it is not configurable.

dnsRefreshMaximumHostLimit

This setting determines the maximum number of Host Indicators that will be refreshed during a DNS monitor run.

> **Note**: If no limit is to be enforced, enter a value of **0** for this setting.

dnsServerList

This setting determines the DNS servers that the DNS monitor requires for resolution.

Acceptable Values: Comma-separated IPv4 addresses

documentAwsAccessID

This setting determines the access ID required by Amazon Web Services® (AWS), if using AWS for document storage.

Acceptable Values: Valid AWS access key ID (e.g., **ACLBMQG9NSOILNSOIH8D**)

documentAwsBucketName

This setting determines the globally unique bucket name for S3 document storage.

Acceptable Values: Valid AWS bucket name (e.g., **example-bucket-ace39bf-23d0a9e**)

documentAwsKMSCmkId

This setting is the AWS KMS-managed customer master key (enables client and server-side encryption).

documentAwsRegion

This setting determines the AWS Region for document storage.

Acceptable Values: A valid AWS Region: **[AF_SOUTH_1, AP_EAST_1, AP_NORTHEAST_1, AP_NORTHEAST_2, AP_NORTHEAST_3, AP_SOUTH_1, AP_SOUTH_2, AP_SOUTHEAST_1, AP_SOUTHEAST_2, AP_SOUTHEAST_3, AP_SOUTHEAST_4, CA_CENTRAL_1, CN_NORTH_1, CN_NORTHWEST_1, EU_CENTRAL_1, EU_CENTRAL_2, EU_NORTH_1, EU_SOUTH_1, EU_SOUTH_2, EU_WEST_1, EU_WEST_2, EU_WEST_3, GovCloud, ME_CENTRAL_1, ME_SOUTH_1, SA_EAST_1, US_EAST_1, US_EAST_2, US_GOV_EAST_1, US_ISO_EAST_1, US_ISO_WEST_1, US_ISOB_EAST_1, US_WEST_1, US_WEST_2]**

documentAwsSecretKey

This setting determines the secret access key used to authenticate to AWS for document storage.

Acceptable Values: Valid AWS secret access key

documentStorageFileLimit

This setting determines the maximum size, in megabytes, of a single upload document if document storage is enabled.

documentStorageLocalPath

This setting determines the location on the local server to store documents, if document storage is enabled and set to the **local** setting (rather than using AWS).

Acceptable Values: Valid path on the ThreatConnect server with appropriate permissions

Warning: DO NOT set this value to "/tmp". A location like "$TC_HOME/docstorage" is recommended.

Note: This setting needs to reside on a highly available storage system such as a SAN/RAID-backed filesystem.

documentStorageType

This setting determines whether document storage is enabled, and, if so, the type of storage to use (i.e., local or AWS).

Acceptable Values: [**NONE**, **AWS**, **LOCAL**]

emailEnabled

This setting determines whether the System will send notifications, invites, and other emails.

emailScoreEvil

This setting determines the breakpoint for an "Evil" email when submitted for header analysis. Any value below this limit, but above the **emailScoreSuspicious** value, will be rated as "Evil."

Acceptable Values: Positive whole numbers greater than the value set for **emailScoreSuspicious**

emailScoreSafe

This setting determines the breakpoint for a "Safe" email when submitted for header analysis. Any value below this limit will be rated as "Safe."

emailScoreSuspicious

This setting determines the breakpoint for a "Suspicious" email when submitted for header analysis. Any value below this limit, but above the **emailScoreSafe** value, will be rated as "Suspicious."

Acceptable Values: Positive whole numbers greater than the value set for **emailScoreSafe**

emailScoreVeryEvil

This setting determines the breakpoint for a "Very Evil" email when submitted for header analysis. Any value below this limit, but above the **emailScoreEvil** value, will be rated as "Very Evil."

Acceptable Values: Positive whole numbers greater than the value set for **emailScoreEvil**

emailSesAccessID

This setting determines the AWS access key ID to use for Amazon Simple Email Service (SES)™.

Acceptable Values: Valid AWS access key ID (e.g., **ACLBMQG9NSOILNSOIH8D**)

emailSesEnabled

This setting determines whether to send emails with Amazon SES.

emailSesRegion

This setting determines the AWS Region to use for Amazon SES.

Acceptable Values: A valid AWS Region: **[AF_SOUTH_1, AP_EAST_1, AP_NORTHEAST_1, AP_NORTHEAST_2, AP_NORTHEAST_3, AP_SOUTH_1, AP_SOUTH_2, AP_SOUTHEAST_1, AP_SOUTHEAST_2, AP_SOUTHEAST_3, AP_SOUTHEAST_4, CA_CENTRAL_1, CN_NORTH_1, CN_NORTHWEST_1, EU_CENTRAL_1, EU_CENTRAL_2, EU_NORTH_1, EU_SOUTH_1, EU_SOUTH_2, EU_WEST_1, EU_WEST_2, EU_WEST_3, GovCloud, ME_CENTRAL_1, ME_SOUTH_1, SA_EAST_1, US_EAST_1, US_EAST_2, US_GOV_EAST_1, US_ISO_EAST_1, US_ISO_WEST_1, US_ISOB_EAST_1, US_WEST_1, US_WEST_2]**

emailSesSecretKey

This setting determines the AWS secret access key to use for Amazon SES.

Acceptable Values: A valid AWS secret access key.

escapeExternalLinks

This setting prevents external links from being rendered in the notification message center.

excludeFromDetailsEnabled

For Dedicated Cloud instances, this setting determines whether to allow Organization and System Administrators to add an Indicator to an Organization-level Exclusion List from the Indicator's **Details** screen. When this setting is enabled, the **Add to Exclusion List** checkbox will be displayed in the **Indicator Status** section of the **Details** screen for all Indicators.

exclusionListMaxItems

This setting indicates the maximum number of items contained in any single Indicator exclusion list.

highPriorityNotificationLimit

This setting specifies the number of days that high-priority notifications are retained before being automatically deleted.

importLimitIndicator

This setting determines the maximum number of Indicators that can be imported at one time. Depending on browser and system-timeout settings, making the limit too high may result in failed import attempts.

importLimitIndicatorFileSize

This setting determines the maximum file size, in kilobytes, that can be uploaded per Indicator import. Depending on browser and system-timeout settings, making the limit too high may result in failed import attempts.

importSignatureAllowedMediaTypes

This setting determines the File Media Types allowed for Signature files during the Signature upload. Typical File Media Types include XML and plain text.

Acceptable Values: Java-compatible regular expression

importSignatureFileSize

This setting determines the maximum file-size limit, in kilobytes, for a Signature file during the Signature upload. Depending on browser- and system-timeout settings, making the limit too high may result in failed import attempts.

importSignatureTypes

This setting is a comma-separated list of Signature file types allowed in the Signature upload.

Default Values: **[Snort, YARA, CybOX, OpenIOC, ClamAV, Suricata, Bro, Regex, SPL, Sigma, Iris Search Hash, TQL Query, KQL, STIX Pattern]**

inAppInteractionEnabled

Setting this value to **true** enables in-app tours, guides, and surveys provided by ThreatConnect, for the user's benefit, through a third-party analytics service.

> **Important**: By activating this feature, the customer is consenting to ThreatConnect's collection and use of the customer's user-activity data and information to improve the product and user experience.

indicatorDeleteInterval

This setting specifies the interval, in hours, at which deleted Indicator transactions are deleted.

indicatorDeleteRetentionTime

This setting specifies the number of units to retain Indicator delete history. The value entered for this setting corresponds to the unit of time selected for the **indicatorDeleteRetentionUnits** setting.

indicatorDeleteRetentionUnits

This setting specifies the unit of time used when retaining Indicator delete history. For example, if **indicatorDeleteRetentionTime** is set to **2** and **indicatorDeleteRetentionUnits** is set to **HOURS**, Indicator delete history will be retained for two hours.

Acceptable Values: [**DAYS**, **HOURS**]

indicatorExportLimit

This setting determines the maximum number of Indicators that a user can export at one time.

> **Important**: The default value of **5000** is the maximum recommended value. Using a value that is significantly higher may result in system instability when larger exports are run.

indicatorStatusLock

This setting determines whether to prevent automated system processes, except for scheduled Threat Deprecation, from modifying the Indicator Status for all Indicators on the ThreatConnect instance. When this setting is enabled, the default Indicator Status for new Indicators will be **Active**, and the Indicator Status of Indicators in each owner will remain constant regardless of activity affecting the Indicator Status of the same Indicators in other owners or CAL.

intelReqResultsRefreshExecutionTime

This setting determines the system time at which the Intelligence Requirement (IR) results refresh monitor will poll ThreatConnect and the ThreatConnect Global Intelligence Dataset for new local and global results, respectively, for IR keyword queries.

intelReqResultsRefreshMonitorEnabled

This setting turns the Intelligence Requirement (IR) results refresh monitor on or off. If this setting is turned off, results will not be retrieved automatically for IR keyword queries. In this scenario, users must click the **Retrieve Results** button on the **Overview** tab of an IR's **Details** screen to manually retrieve the most recent results for the IR's keyword query.

ipGeoBrokerURL

This setting determines the URL to which the IP GeoLocation Service will send queries. Changing this value may result in the IP GeoLocation Service not being able to retrieve location and other amplifying data for Address Indicators.

Acceptable Values: The full URL of the IP GeoLocation Service

ipGeoDbRefreshInterval

This setting specifies the system interval, in days, at which to check for a new IP Geo data file.

ipGeoMonitorInterval

This setting determines the system interval, in minutes, at which the IP GeoLocation Service searches for new IP addresses to check for geographic data. Newly imported Address Indicators may not show IP GeoLocation information until the IP GeoLocation Service performs another query.

jobLoggingResetInterval

This setting specifies the interval to reset Job logging back to INFO.

keychainEnabled

If this setting is enabled, the user is forced to generate a master key to encrypt the secret keys used in Jobs. If the keys are persisted, it will encrypt the master key and store it in the database. If persist is not selected, the user is forced to enter the master key while logged in as an Admin for each restart.

loggingLevel

This setting determines the lowest level of logging that will be logged.

Acceptable Values: One of (**TRACE**, **DEBUG**, **INFO**, **WARN**, **ERROR**, **FATAL**)

Note: Refer to https://docs.jboss.org/process-guide/en/html/logging.html for more information.

loggingLocation

This setting determines the name and location of the log file for this deployment.

Acceptable Values: Full-system path and file name/extension

loggingMaxBackupIndex

This setting determines the maximum number of logging files that will remain in the logging directory.

loggingMaxFileSize

This setting determines the maximum size, in bytes, of a single logging file.

loggingPattern

This setting determines the log4j pattern for what will be logged.

Acceptable Values: Valid log4j pattern (e.g., **Systemd{yyyy-MM-dd HH:mm:ss,SSS} System5p [Systemt] (SystemF:SystemL) – SystemmSystemn**)

loggingSyslogHost

This setting determines the syslog host(s) to which logs will be sent. If using more than one syslog host, separate each one with a comma.

Acceptable Values: A host and port combination (e.g., **localhost:514**)

logToFile

This setting turns on application-level logging to system setting **loggingLocation**.

logToSearchCluster

This setting turns on logging to OpenSearch®.

logToSyslog

This setting turns on application-level logging to a syslog server.

logTraceforClass

This setting turns on TRACE logging for a list of comma-separated fully qualified class names.

lowPriorityNotificationLimit

This setting specifies the number of days that low-priority notifications are retained before being automatically deleted.

mailConnectionTimeout

This setting specifies the timeout length, in minutes, for the Mailbox Trigger in Playbooks.

mailInboundDomain

This setting indicates the appropriate specified domain to be used for inbound email inboxes.

Acceptable Values: A valid host that has a DNS MX record configured for it, typically pointing to ThreatConnect (e.g., **tcsoar.mydomain.com**).

mailInboundEnabled

This setting enables the email-ingestion capability.

mailInboundEnableTLS

This setting determines whether TLS is enabled on inbound mail. If the Enabled box is selected, inbound emails that come from SMTP and SMTPS connections will be allowed.

mailInboundKeyStore

This setting indicates the path to the Java Keystore.

mailInboundKeyStorePassword

This setting specifies the password for the Java Keystore.

mailInboundPort

This setting specifies the port used by the ThreatConnect mail server.

Acceptable Values: A valid port (e.g., 2500)

mailInboundRequireTLS

This setting specifies whether TLS is required on inbound mail. If the Enabled box is checked, only inbound emails that come from SMTPS connections will be allowed.

managementAPISubscriberIntervalSeconds

This setting specifies the minimum interval for triggering alerts.

managementApiSubscriberMaxHourlyAlerts

This setting specifies the maximum number of alerts that can be triggered in one hour.

maxDailyNotificationsPerPlaybook

This setting specifies the maximum number of email failure notifications that can be sent daily for a Playbook.

mediumPriorityNotificationLimit

This setting specifies the number of days that medium-priority notifications are retained before being automatically deleted.

organizationStatusMonitorEnabled

This setting turns on the Organization Status Monitor.

organizationStatusMonitorinterval

This setting determines the interval, in minutes, at which the system checks for and handles expired Organizations.

passwordFailureLockCount

This setting determines the number of failed login attempts after which a user account is locked.

passwordLower

This setting determines the number of lowercase letters required for a password.

passwordMaxAge

This setting determines the number of days before a user's password expires. After a user's password expires, they will be required to reset it during their next login attempt.

passwordMinimum

This setting determines the minimum number of characters required for a password.

passwordNumber

This setting determines the number of numerical characters required for a password.

passwordSpecial

This setting determines the number of special characters required for a password.

passwordUpper

This setting determines the number of uppercase characters required for a password.

playbookExecutorAotDepth

This setting specifies the number of levels to AOT launch in Playbook execution.

playbookExecutorAotPoolSize

This setting specifies the process cache size for AOT launched Apps.

playbookExecutionDBDaysToKeep

This setting specifies the number of days to keep data in the Playbook execution table.

playbookFailedInteractiveSessionCount

This setting specifies the number of **Interactive Mode** sessions to keep for a Playbook.

playbookForkPoolSize

This setting specifies the number of concurrent threads allowed per Playbook Worker.

playbookSessionPurgeTimeoutSeconds

This setting determines the number of delay seconds after which a Playbook session is purged.

playbookVersionArchiveLimit

This setting specifies the number of archived Playbook versions that are allowed.

playbookWebHookPathByOrg

This setting determines if WebHook URLs are isolated per Organization.

playbooksCompletedSessionDaysToKeep

This setting determines the number of days for which to keep session data for Playbook executions.

playbooksDbCredentialsEnabled

This setting determines whether a username and password are required to interact with the Playbooks database on Redis®. If **playbooksDbUsername** and **playbooksDbPassword** both have values, ThreatConnect will use them to authenticate to the Playbooks Redis database.

playbooksDbHost

This setting specifies the Playbooks Redis database host.

playbooksDbPassword

This setting determines the password to use to authenticate with the Playbooks Redis database.

playbooksDbPort

This setting specifies the Playbooks Redis database port.

playbooksDbUsername

This setting determines the username to use to authenticate with the Playbooks Redis database.

playbooksDefaultRoiDollarsPerHour

This setting specifies the default Playbooks return on investment (ROI) dollars per hour.

playbooksDefaultRoiMinutes

This setting specifies the default Playbooks ROI minutes.

playbooksDisplayFailureNotifications

This setting determines if email notifications are enabled for failed Playbooks.

playbooksEnabled

This setting enables Playbooks when set to **true**.

> **Note**: A System Administrator can run Playbooks in Cloud for an Organization that cannot activate this feature. Furthermore, a System Administrator can see any Playbook (using a direct link).

playbooksEndpointLimitMb

This setting specifies the maximum number of megabytes allowed for a Playbook endpoint.

playbooksLoggingLevel

This setting determines the lowest level of playbooks logging that will be logged.

Acceptable Values: **[TRACE**, **DEBUG**, **INFO**, **WARN**, **ERROR**, **FATAL]**

playbooksLoggingLocation

This setting specifies the name and location of the Playbooks log file for this deployment.

playbooksLoggingMaxBackupIndex

This setting determines the maximum Playbooks logging files that will remain in the logging directory.

playbooksLoggingMaxFileSize

This setting specifies the maximum size of a Playbooks logging file, in bytes.

playbooksLogToFile

This setting turns on or off Playbooks logging to file.

playbooksMaxDailyExecutions

This setting specifies the number of Playbook executions allowed in a single day.

playbooksMaxLoopLimit

This setting specifies the maximum number of iterations allowed in a Playbook loop.

playbooksRuntimeKillMinutes

This setting specifies the number of minutes after which the Playbook session reaper will kill a running or sleeping Playbook.

potentialAssociationMode

This setting determines how potential associations are suggested on the ThreatConnect instance. Acceptable values include the following:

- **Matched**: Potential associations will be based on matching Artifacts to Indicators on the ThreatConnect instance.
- **Associated**: Potential associations will be based on second-degree associations to objects on the ThreatConnect instance.
- **Both**: Potential associations will be based on matching Artifacts to Indicators on the ThreatConnect instance AND on second-degree associations to objects on the ThreatConnect instance.

privateIndicatorsEnabled

This setting, when set to **true**, allows CAL data retrieval to be disabled for individual Indicators.

proxyHost

This setting determines the appropriate proxy host if a proxy server is required.

Acceptable Values: Valid IP address or host name for a proxy accessible by the ThreatConnect instance

proxyPassword

This setting determines the password required for authenticating with the proxy.

Acceptable Values: Blank or valid proxy password

proxyPort

This setting determines the proxy port to use if a proxy server is required.

Acceptable Values: Valid port number

proxyRequired

This setting determines whether an HTTP proxy is required for HTTP data services. If **proxyUsername** and **proxyPassword** both have values, ThreatConnect will use them to authenticate to the proxy server.

proxyUsername

This setting determines the username required for authenticating with the proxy.

Acceptable Values: Blank or valid proxy username

reverseWhoisBrokerURL

This setting determines the URL to which the Reverse WHOIS Track service sends queries. Changing this value may result in the Reverse WHOIS service not being able to retrieve results for Reverse WHOIS Track queries and monitoring.

Acceptable Values: The full URL of the Reverse WHOIS service

reverseWhoisEnabled

This setting determines whether the Reverse WHOIS Monitor, and support for Reverse WHOIS Tracks, is turned on or off. The Reverse WHOIS Monitor checks for results when users run a Reverse WHOIS Track and, periodically, for new results from existing Tracks.

reverseWhoisInterval

This setting determines the system interval, in hours, at which Reverse WHOIS alerts are checked.

reverseWhoisMonitorConcurrency

This setting determines the number of concurrent Reverse WHOIS Monitors to run.

reverseWhoisTimerStart

This setting determines the time of day at which to start Reverse WHOIS queries for the previous day. The time is configured as Coordinated Universal Time (UTC) in Cloud versions of ThreatConnect. The default time zone is set by the operating system, so the time zone may vary.

searchAdminPassword

This setting specifies the OpenSearch admin password.

searchAdminUsername

This setting specifies the OpenSearch admin username.

searchBackupHour

This setting indicates the hour of the day when the OpenSearch backup should be run.

searchCluster

This setting specifies the OpenSearch cluster name. It must match the one specified in **opensearch.yml**.

searchEnabled

This setting determines whether the OpenSearch service is enabled.

> **Important**: This setting must be enabled in order to enable ThreatConnect to use the DataStore.

searchSecurityEnabled

This setting turns on or off security for OpenSearch on the system.

searchUrl

This setting determines the URL for the OpenSearch server.

Acceptable Values: A valid URL and port specification (e.g., http://localhost:9200)

> **Important**: This setting must be defined to enable ThreatConnect to use the DataStore.

secureProxyBlacklist

This setting is a comma-separated list of domains or IP addresses that are blocked by the Spaces Secure Proxy. This is a security feature to prevent unauthorized access to application resources.

secureSystemUrl

This setting determines the URL used to create linked content. For example, a System Indicator will have the following URL if this setting's value is **https://app.threatconnect.com**: **https://app.threatconnect.com/tc/auth/indicators/details/address.xhtml?address=1.2.3.4**.

Acceptable Values: The desired System's URL

sourceFeedMonitorEnabled

This setting enables the Source Feed Monitor, which searches for updates to pre-configured source feeds.

sourceFeedMonitorInterval

This setting specifies the frequency, in minutes, on which the Source Feed Monitor runs.

summaryEmailRefreshInterval

This setting determines the system interval, in minutes, at which the system sends out a summary-notification email. Summary notifications are configured in the user settings for each user.

synchronousBatchSaveLimit

This setting determines the kilobyte limit for processing batch save requests synchronously.

syslogIncludePlaybookExecution

This setting, when enabled, causes Playbook and Playbook App execution logs to be sent to the syslog host configured for the **loggingSyslogHost** system setting.

systemDisplayName

This setting determines the display name for the system, as used in system emails. Its value should be the desired system name as seen in notifications, invites, and other system-generated emails.

systemEmailAddressAccount

This setting determines the email address used by the system when sending account information.

Acceptable Values: A valid email address

systemEmailAddressNotification

This setting determines the email address used by the system when sending notifications.

Acceptable Values: A valid email address

systemSubjectName

This setting determines the first string in the subject field of system-generated emails.

systemUrl

This setting determines the system URL used in system emails and graphics within HTML-formatted emails. This setting, by default, will point to the **Cloud Instance** of ThreatConnect.

Acceptable Values: A valid URL

taskEmailMonitorEnabled

This setting determines whether the system creates emails for monitored tasks (escalation, overdue, etc.).

taskEmailMonitorInterval

This setting determines the system interval, in minutes, at which the task email monitor looks for tasks to escalate or flag as overdue.

taxiiExchangeMonitorEnabled

This setting turns the Trusted Automated eXchange of Indicator Information (TAXII™) Exchange–related maintenance task on or off.

taxiiExchangeMonitorInterval

This setting is the system interval, in minutes, at which TAXII Exchange is done.

taxiiPollServiceIndicatorExportLimit

This setting indicates the limit of Indicators the TAXII Server can provide for each request. Subsequent Indicators can be pulled via multi-part poll exchange.

taxiiPollServiceMaxDataRange

This setting indicates the maximum time frame for which data may be pulled via the TAXII Service.

tempPasswordDuration

This setting determines the duration, in minutes, for which a temporary password is valid.

termsOfServiceRequireNewUserToAccept

This setting requires that new users accept the existing Terms of Service.

thirdPartyEnrichmentAPILimit

This setting determines the maximum number of Indicators API users can enrich in a single request to the `/v3/indicators/enrich` ThreatConnect v3 API endpoint.

thirdPartyEnrichmentCacheLimit

This setting determines the number of days to cache third-party enrichment data. The cache will hold data retrieved from enrichment services for the number of days specified (the default is **30**), and all enrichment data requests will retrieve data from the cache unless the user clicks the **Retrieve Data** button on the **Enrichment** tab of the **Details** screen. After the specified number of days has passed, the data are automatically cleared from the cache.

threatAssessIntervalCount

This setting determines the number of Indicators to process per monitor cycle.

threatAssessMonitorEnabled

This setting turns the Threat Assessment maintenance task on or off.

threatAssessMonitorInterval

This setting determines the system interval, in minutes, at which Threat Assessment is performed.

threatAssessRefreshInterval

This setting determines the system interval, in days, at which a Threat Assessment for a given Indicator is updated.

threatDeprecationMonitorEnabled

This setting turns the Threat Deprecation maintenance task on or off.

threatDeprecationMonitorInterval

This setting determines the interval, in minutes, at which Threat Deprecation is performed.

tqlAssociationExecutionTime

This setting determines the system time at which the monitor will execute each user query and apply the results as associations.

tqlAssociationMonitorEnabled

This setting turns the TQL Association Monitor on or off. If this setting is turned off, TQL queries added to Groups will not run automatically and must be run manually by a user.

tqlAssociationTotalAssignable

This setting determines the maximum number of TQL queries that can be assigned and used for TQL associations on the ThreatConnect instance.

> **Important**: This setting *does not* determine the maximum number of TQL queries that can be assigned to a single Group. That limit is two queries (one Group query and one Indicatory query) and cannot be modified.

tqlQueryTimeout

This setting determines the maximum amount of time, in milliseconds, that a TQL query is allowed to run before timing out. System Administrators and Operations Administrators may override this setting for individual users in the **User Administration** window for the user on the **Membership** tab of the **Organization Settings** screen.

twoFactorAuthenticationRequired

When enabled, this setting requires multi-factor authentication (MFA) for all user accounts on the instance upon login.

userFirstNameRegex

This setting specifies the regular expression validation rules to be applied when creating or modifying a user's first name.

userJobFunctionRegex

This setting specifies the regular expression validation rules to be applied when creating or modifying a user's job function.

userJobRoleRegex

This setting specifies the regular expression validation rules to be applied when creating or modifying a user's job role.

userLastNameRegex

This setting specifies the regular expression validation rules to be applied when creating or modifying a user's last name.

userPseudonymRegex

This setting specifies the regular expression validation rules to be applied when creating or modifying a user's pseudonym.

v3ApiCreateLimit

This setting specifies the maximum number of items that can be created at a time using v3 of the ThreatConnect API.

v3ApiBulkDeleteAllowed

When enabled, this setting determines whether bulk delete operations are available using v3 of the ThreatConnect API.

v3ApiIntelLinkLimit

This setting determines the maximum number of association levels that can be retrieved at one time for intelligence items using v3 of the ThreatConnect API.

v3ApiReadLimit

This setting specifies the maximum number of items that can be read at a time using v3 of the ThreatConnect API.

v3ApiTurboMode

This setting activates a performance-improved algorithm for fetching large numbers of certain types of child objects (e.g., Attributes, Tags, associations, etc.) within the context of a v3 API request. You can enable this setting for threat intelligence only, Workflow only, or both.

Acceptable Values: **[Disabled, Intel Only, Workflow Only, Intel + Workflow]**

v3ApiTurboModeBatchSize

This setting determines the number of unique child items fetched per batch within a turbo-enabled lookup.

v3ApiTurboModeExemptionLimit

This setting determines the maximum number of child items per batch for which turbo lookups will be performed. Turbo lookups for child items that exceed this limit will be skipped and performed separately. This setting may be disabled by setting its value to -1.

whoisBrokerURL

This setting determines the URL of the WHOIS Monitor service. Changing this value may result in the WHOIS service not being able to retrieve WHOIS records for Host Indicators.

Acceptable Values: The full URL of the WHOIS service

whoisEnabled

This setting determines whether the System WHOIS Monitor service (and support for WHOIS functions) is turned on or off. The WHOIS Monitor service queries a third party for domain WHOIS information for Host Indicators with WHOIS tracking enabled.

whoisMonitorInterval

This setting determines the system interval, in minutes, at which the WHOIS Monitor searches for new Host Indicators for which to check WHOIS.

whoisRefreshInterval

This setting determines the system interval, in days, at which WHOIS lookups are performed.

Email Templates

Emails that are sent by the platform can be customized using the corresponding template. A list of Email Templates is located in System Settings.

Note: ThreatConnect uses FreeMarker™ as the parser for email templates.

1. Click **Email Templates** in the menu on the left side of the **System Settings** screen. The **Email Templates** screen will be displayed (Figure 6).

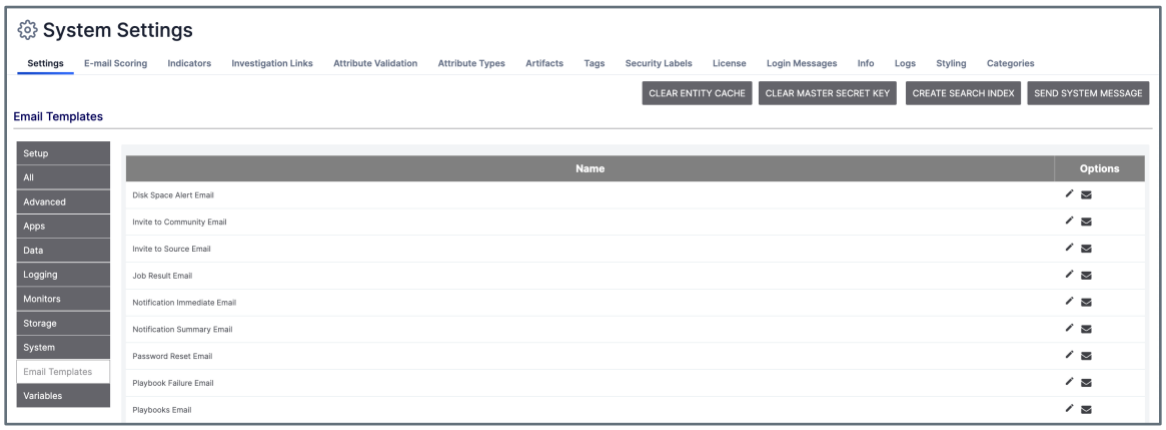

Figure 6

2. Select an email template from the list and click **Edit** . A window will be displayed with the name of the email template (**Invite to Community Email** this example) (Figure 7).

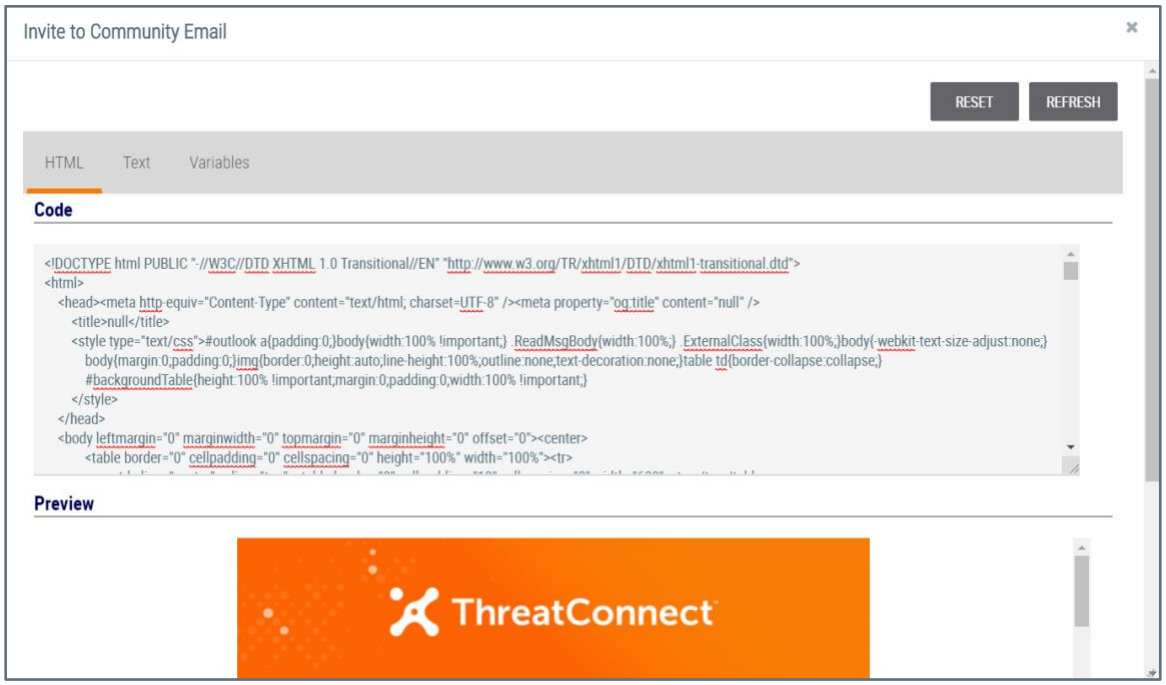

Figure 7

3. Click the **HTML** or the **Text** tab for HTML- or text-supported emails, respectively, and enter the desired changes into the **Code** window.
4. Click the **Variables** tab to see a list of predefined variables. These variables are not configurable, but the **image1-4** options allow a user to upload images that can be inserted into the email.
5. Return to the **HTML** or **Text** screen and click the **REFRESH** button. The modified email template will be displayed in the **Preview** or **Text Preview** window.
6. If satisfied with the changes, click the **SAVE** button. Otherwise, click the **RESET** button and the original text will be displayed.
7. To receive a system-generated email for review, click **Test Email** ✉ next to any of the available Email Templates. The **Send Test Email** window will be displayed.
8. Enter a destination email address, and click the **SEND** button.

Variables

Variables can be preconfigured and used to populate certain fields, such as the **ThreatConnect API Access ID** or **Secret Key**.

1. Click the **Variables** button in the menu located on the left side of the **System Settings** screen (Figure 1). The **Variables** screen will be displayed (Figure 8).

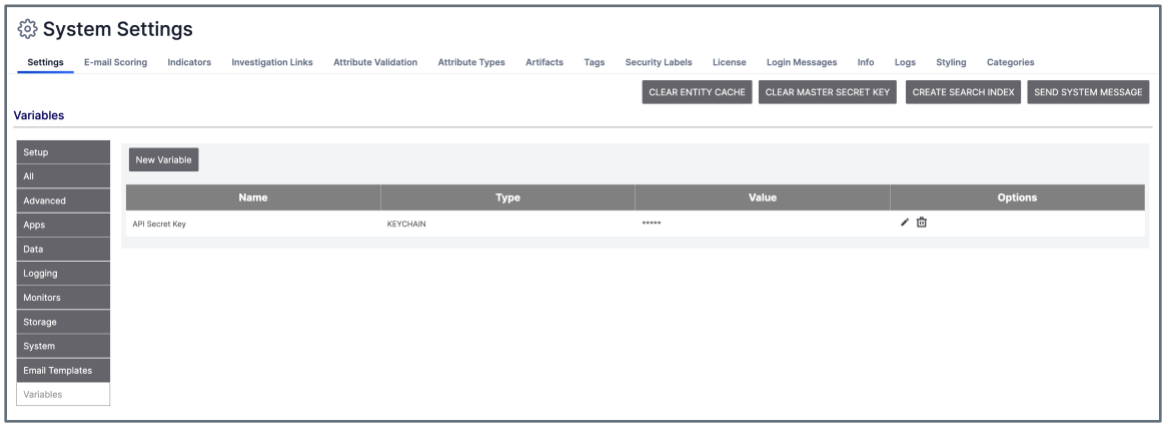

Figure 8

2. Click the **New Variable** button. The **Property** window will be displayed (Figure 9).

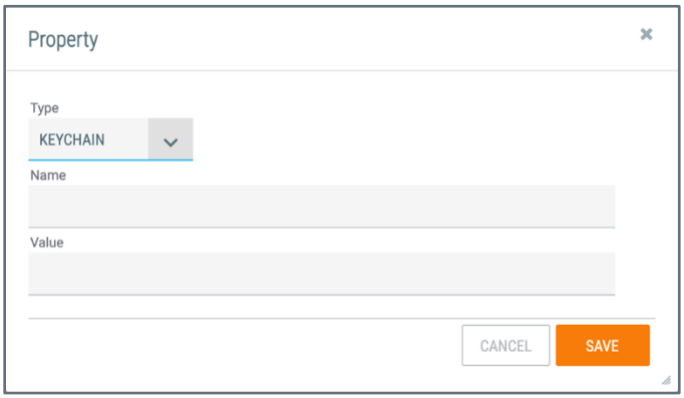

Figure 9

- **Type**: Select the variable's type. Available options include **KEYCHAIN**, **TEXT**, and **FILE**.
- **Name**: Enter a name for the variable.
- **Value**: Enter a value for the variable.
- Click the **SAVE** button to create the new variable.

Email-Scoring Rules

From the **System Settings** screen, an Administrator can click on the **E-mail Scoring** tab to view, create, and edit System-wide rules for scoring email headers when imported into ThreatConnect.

How the Scoring Engine Works

All email-scoring rules use Java®-compatible regular expressions for pattern matching on an email header. There are two basic types of rules used by the email-scoring engine: those that match on an Indicator (e.g., host, IP address, or email address) within the email header, and those that match on a non-Indicator pattern within the email header (e.g., X-Mailer or Sender Policy Framework (SPF) value). Several rules have been pre-populated into the **On Premises Instances**, but the user may modify or add to these default rule sets.

All scoring rules require a Header Name Field with a specified range for finding the pattern within the email header. For example, to find an email sent by the **FastMail 1.6 [cn]** mail tool, search for the text string **FastMail 1.6 [cn]** in the X-Mailer field of the header. To define this rule in the **Email Header Scoring Engine**, set a regex to define the Header Field Name as **\bX-Mailer\b** and the Header Field Value as **FastMail 1\.6 \[cn\]**.

For rules that match on Indicators, the score given to an email header based on a match is calculated from the Indicator's Threat Rating (i.e., the number of skulls it is assigned). For rules that do not match on an Indicator, the score must be given a value.

Create an Email-Scoring Rule

1. Click the **E-mail Scoring** tab on the **System Settings** screen (Figure 1). The **E-mail Scoring** screen will be displayed (Figure 10).

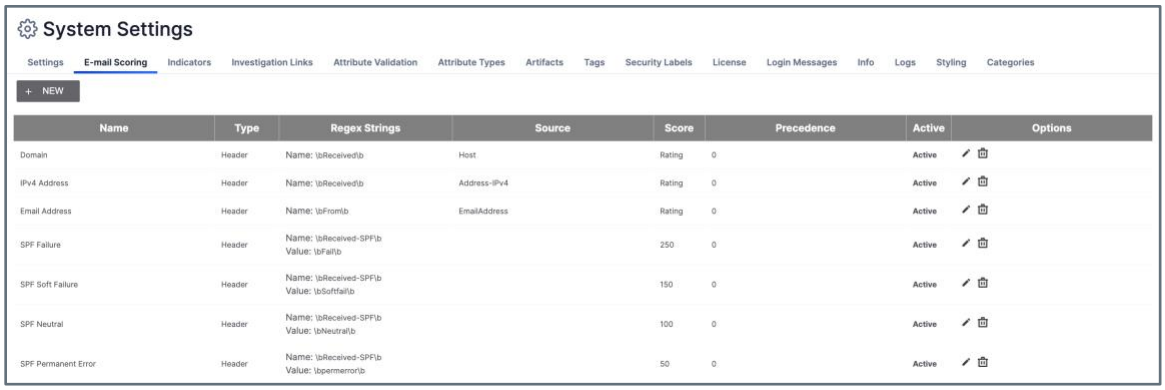

Figure 10

2. Click the **+ NEW** button. The **E-mail Scoring Rule** window will be displayed (Figure 11).

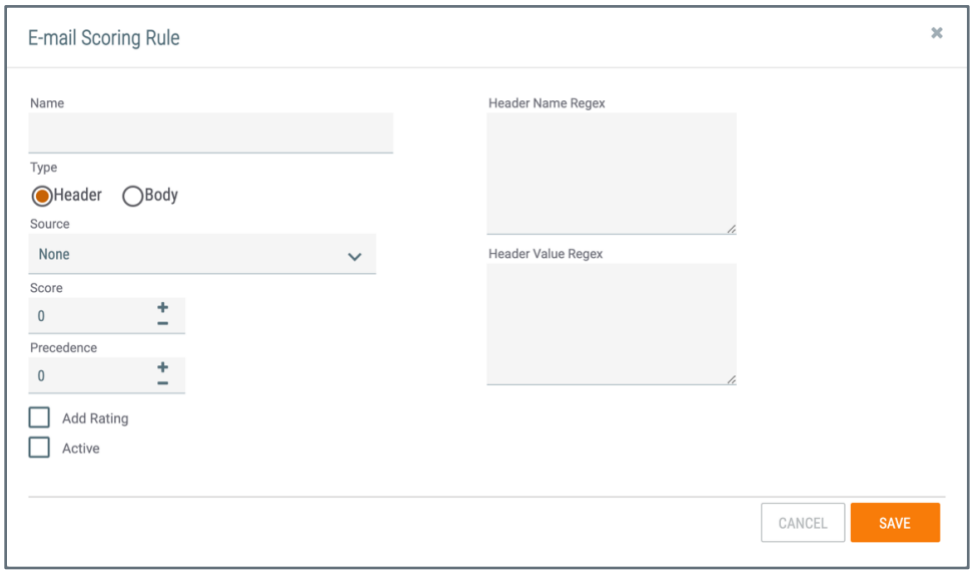

Figure 11

- **Name**: Enter the name of the rule.
- **Type**: Select either the **Header** or **Body** email component.
- **Source**: Select an Indicator as the source of a rule's score, if this rule will match on an Indicator string. If this rule will match on a non-Indicator string, leave this field set to **None**.
- **Score**: Enter a base score for the email if there is a match on the rule in the **Score** field, or use the plus and minus buttons to add or subtract increments of 1, respectively. Points may be added to the rule if the rule is matching on an Indicator and the **Add Rating** checkbox is selected.

- **Precedence**: Enter the Precedence value, which is used if two rules exist for different Indicator types, or use the plus and minus buttons to add or subtract increments of 1, respectively. A rule with a higher Precedence value will be counted instead of a rule with a lower Precedence value that matches on the same header value. If the rules match on Indicators of different types, the rule with the higher Precedence value will determine the type.
- **Add Rating**: Select the checkbox to add an Indicator's Threat Rating (i.e., number of skulls) to the score's value when a match occurs. This feature is applicable only for rules that match on an Indicator.
- **Active**: Select the checkbox to specify whether the rule is active. The rule will not be included in the Email-Scoring Engine unless this checkbox is selected.
- **Header Name Regex (Header Only)**: Enter a Java-compatible regular expression that defines the email header field in which the header value will be found.
- **Header Value Regex or Body Value Regex**: Enter a Java-compatible regular expression that defines the email header or body value that will result in a match for the rule.
- Click the **SAVE** button to create the rule.

Edit an Email-Scoring Rule

1. Click **Edit** in the **Options** column for the rule that is to be edited. The **E-mail Scoring Rule** window will be displayed (Figure 11).
2. Make any changes to the rule, and click the **SAVE** button.

Indicators

From the **System Settings** screen, an Administrator can click on the **Indicators** tab to view, create, and edit custom Indicator types, custom Indicator-to-Indicator associations, Indicator import rules, and Indicator exclusion lists, as well as enable and configure built-in enrichment tools for available Indicator types.

All Indicator-matching rules use Java-compatible regular expressions for pattern matching on Indicator creation and import. In ThreatConnect, there are currently 12 native Indicator types: Address, ASN, CIDR, Email Address, Email Subject, File (MD5, SHA1, SHA256), Hashtag, Host, Mutex, Registry Key, URL, and User Agent, although seven of these types are configured as custom Indicator types. For users with a Dedicated or On Premises Instance, ThreatConnect can be extended to create custom Indicator types to support different use cases. Indicator-matching rules have been pre-populated into the On Premises Instance for each built-in Indicator type, but the user may modify or add to these default rule sets.

Custom Indicator Types

For ThreatConnect users with a Dedicated Cloud or On-Premises subscription, ThreatConnect can be extended to create custom Indicator types to support different use cases.

Custom Indicators are treated in the same manner as built-in Indicator types, such as URL or File, and they can be associated with Groups, such as Threats, Incidents, and Emails, as well as with other Indicators via the custom Associations functionality (see the "Custom Associations" section). Once they are added into ThreatConnect, they will be displayed in menus and lists along with built-in Indicator types. Users will not be able to tell the difference between a custom Indicator and a built-in Indicator.

For example, if users wish to keep track of unique Bitcoin strings generated by malicious binaries in HTTP traffic, they could create a Bitcoin custom Indicator type to store strings they may wish to filter and alert on in their environment.

Warning: Improperly configured custom Indicator types could damage the ThreatConnect instance. Please contact a ThreatConnect Customer Success Engineer for guidance about defining custom Indicator types.

Note: Because of database constraints, a custom Indicator's descriptive name is limited to 50 characters, and the total number of characters used in the value of the Indicator (i.e., Fields 1–3) itself cannot exceed 500. Also because of database constraints, custom Indicator regexes that do not constrain total character length are incompatible with custom Indicators.

Note: System Administrators can edit and delete custom Indicators at any time.

Create a Custom Indicator Type

1. Click the **Indicators** tab on the **System Settings** screen (Figure 1). The **Indicators** screen will be displayed with the **Types** option selected from the menu on the left side of the screen (Figure 12).

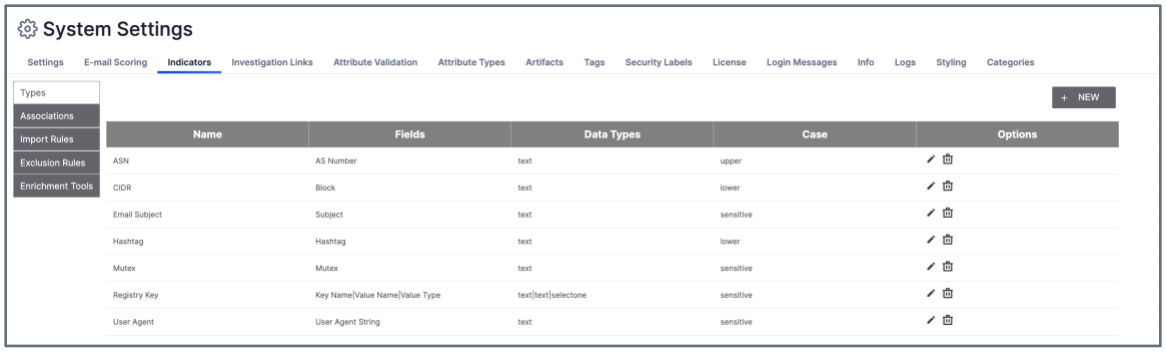

Figure 12

2. Click the **+ NEW** button. The **Create Custom Indicator Type** window will be displayed (Figure 13).

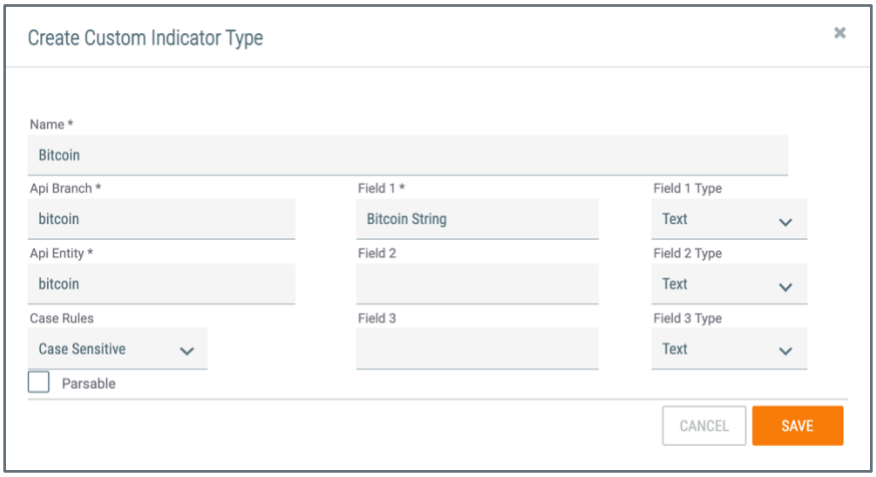

Figure 13

- **Name**: Enter a name for the custom Indicator (e.g., **Bitcoin**).

  > **Note**: Once a custom Indicator has been created, its name may not be changed.

- **Api Branch**: Set this parameter to the mapped API field in ThreatConnect (e.g., **bitcoin**).
- **Api Entity**: Set this parameter to the mapped entity fields in ThreatConnect. In this case, the entity type would be **bitcoin**.
- **Case Rules**: Specify whether text fields require lowercase, uppercase, or case-sensitive letters. The case rule applies to all text fields; it is not possible to choose separate case rules for separate fields. All data imported into a text field will be changed to conform to the case rule. For example, if **Lowercase** is chosen, any uppercase letters imported into the field will be changed to lowercase letters, and if **Uppercase** is chosen, any lowercase letters imported into the field will be changed to uppercase letters. If **Case Sensitive** is chosen, then all data will remain the same.
- **Parsable**: Select this checkbox if the Indicator will be parsable within ThreatConnect. If an Indicator is parsable, it will be verified against the Indicator import rules to determine whether an unstructured import can be performed.

  > **Note**: Multi-value custom Indicator types are not parsable.

- **Field 1**: Set a label for the primary field (e.g., **Bitcoin String**).
- **Field 1 Type**: Set the field's data type (i.e., **Text**, **Number** or **Select One**). If **Select One** is chosen, a **Field 1 Options List** box will be displayed below the **Field 1 Type** box. Items entered into this box should be separated by semicolons.

  > **Note**: In this example, the **Bitcoin String** field would require the **Type** to be **Text**, while a credit card number would require the **Type** to be **Number**.

- Optionally, configure secondary fields in the same manner as any of the primary fields. Secondary fields will be concatenated with the primary field, and the resulting value will be treated as a unique Indicator.

  > **Note**: Fields 1–3 may store up to a combined total of 500 characters of text. Attempts to store more characters than that between the three fields could lead to stability or performance issues, rendering the system inoperable. Number fields may store up to 20 characters per field.

> **Note**: ThreatConnect uses colons to distinguish between the fields used in multi-value Indicators. For that reason, multi-value custom Indicator types may not use colons. However, single-value custom Indicator types can still use colons.

- Click the **SAVE** button to save the changes.

> **Note**: The maximum length for all fields combined is limited to 500 characters, which may be helpful for Indicators that would otherwise be duplicates. For instance, a primary field of **User Agent String** and a secondary field of **Process Name** may uniquely identify an Indicator for a malicious binary that is spoofing a legitimate string, such as **Internet Explorer:evil.exe**.

Edit or Delete a Custom Indicator Type

To edit or delete a custom Indicator type, click **Edit** or **Delete** , respectively, in the **Options** column.

Import Rules for Custom Indicator Types

Follow the steps in the "Indicator Import Rules" section to create import rules for custom Indicators. Make sure to define a regular expression that must be matched (in order) for new Indicators of that type and to select the **Active** checkbox to designate the rule as active. It is recommended that the regular expressions be used to define the three fields of a custom Indicator so that they conform to the character-limit rules. Each field of a custom Indicator must have at least one import rule defined before Indicators of that type can be created.

Custom Associations

Custom associations allow Indicators to be associated to other Indicators. These Indicators can be native Indicators [Address, ASN, CIDR, Email Address, Email Subject, File (MD5, SHA1, SHA256), Hashtag, Host, Mutex, Registry Key, URL, and User Agent] or custom Indicators created by the System Administrator. The details of these associations are found on the **Browse** screen. Table 2 displays the built-in custom associations provided by ThreatConnect.

Table 2

Name	API Branch	Primary	Target
ASN to Address	asnToAdress	ASN	Address
ASN to CIDR	asnToCidr	ASN	CIDR
Address to User Agent	addressToUserAgent	Address	User Agent
CIDR to Address	cidrToAddress	CIDR	Address
Domain Registrant Email	domainRegistrant	Host	EmailAddress
File Download	fileDownload	URL	File
DNS PTR Record	dnsPtrRecord	Address	Host
URL Host	urlHost	URL	Address, Host

Create a Custom Association

1. Click **Associations** in the menu on the left side of the **Indicators** screen (Figure 12). The **Associations** screen will be displayed (Figure 14).

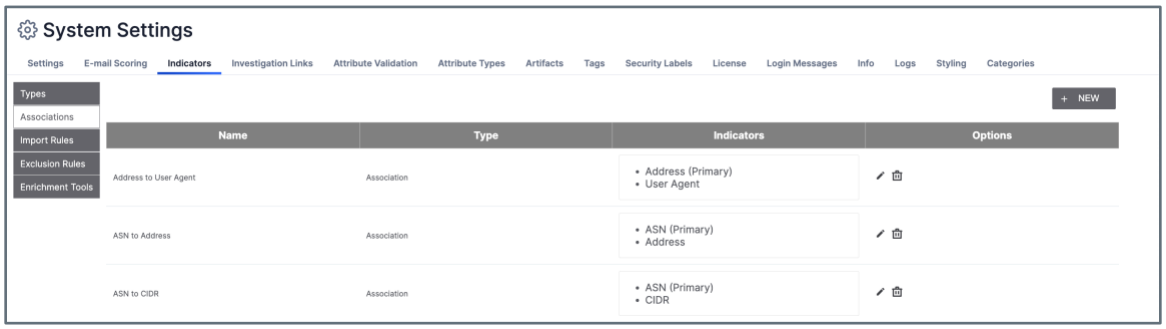

Figure 14

2. Click the **+ NEW** button. The **Create Custom Indicator Association** window will be displayed with the **Association** option selected (Figure 15).

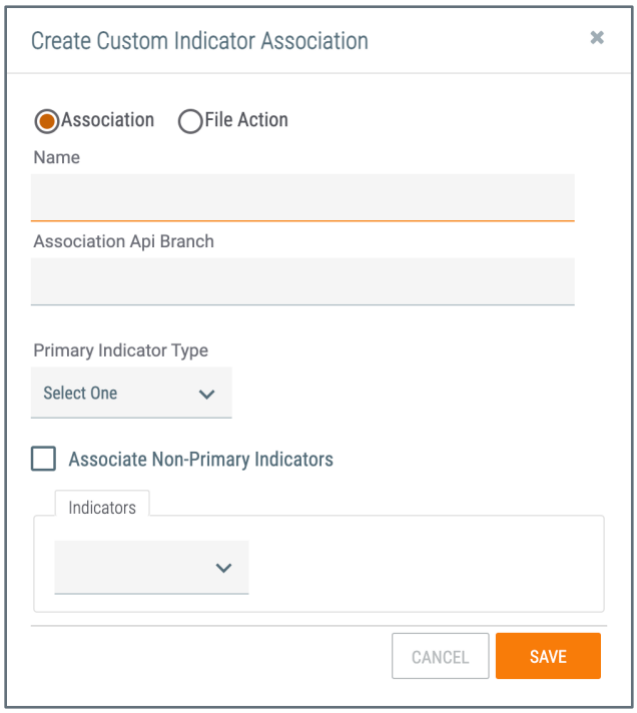

Figure 15

- **Name**: Enter a name for the custom association (e.g., **Address to CIDR**).

- **Association Api Branch**: Set this parameter to the mapped API field in ThreatConnect (e.g., **addressToCidr**).
- **Primary Indicator Type**: Select the primary Indicator type.
- **Associate Non-Primary Indicators**: Select this checkbox to allow non-primary Indicators that are associated with the primary Indicator to be associated with each other.

  > **Important**: If this checkbox is not selected, an association between two Indicators is commutative. That is, the designation of primary vs. non-primary is insignificant: The association works equally in both directions, and non-primary Indicators associated with a given primary Indicator are not associated with each other. If this checkbox is selected, non-primary Indicators of a given Indicator are also associated with each other.

- **Indicators**: Select one or more Indicators to associate with the primary Indicator type.
- Click the **SAVE** button to create the custom association.

Create a File Action

File Actions are a sub-type of custom associations that allow the File Indicator type to be associated to other Indicators. The details of these associations are found on the **Browse** screen. ThreatConnect provides three built-in File Action types: **File Mutex**, **File Registry Key**, and **File User Agent**.

1. Click the **+ NEW** button on the **Associations** screen (Figure 14). The **Create Custom Indicator Association** window will be displayed with the **Association** radio button selected (Figure 15).
2. Select the **File Action** option (Figure 16).

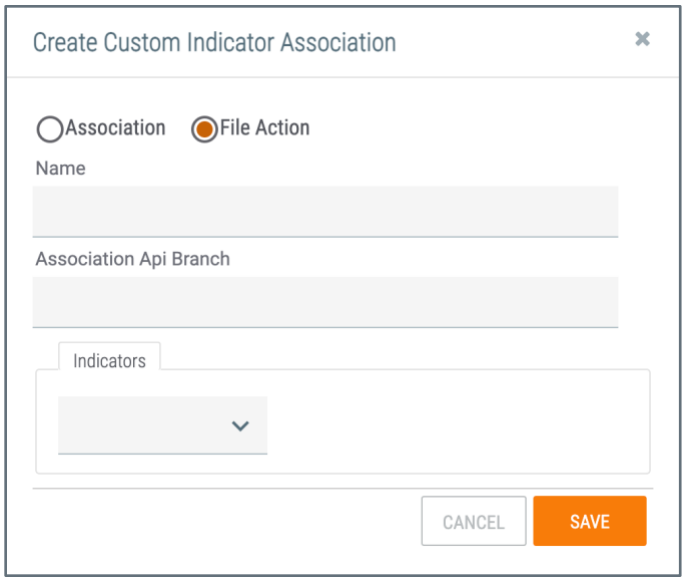

Figure 16

- **Name**: Enter a name for the custom association (e.g., **File CIDR**).
- **Association API Branch**: Set this parameter to the mapped API field in ThreatConnect (e.g., **cidr**).
- **Indicators**: Select one or more Indicators to associate with the File.
- Click the **SAVE** button to create the File Action.

Edit or Delete a Custom Association or File Action

To edit or delete a custom Indicator association or File Action, click **Edit** or **Delete**, respectively, in the **Options** column.

Indicator Import Rules

Create an Indicator Import Rule

1. Click **Import Rules** in the menu on the left side of the **Indicators** screen (Figure 12). The **Import Rules** screen will be displayed (Figure 17).

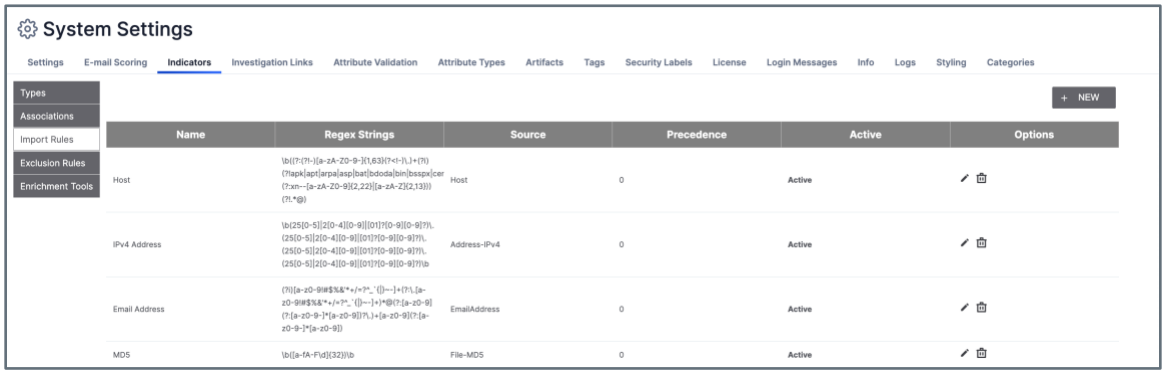

Figure 17

2. Click the **+ NEW** button. The **Create Indicator Import Rule** window will be displayed (Figure 18).

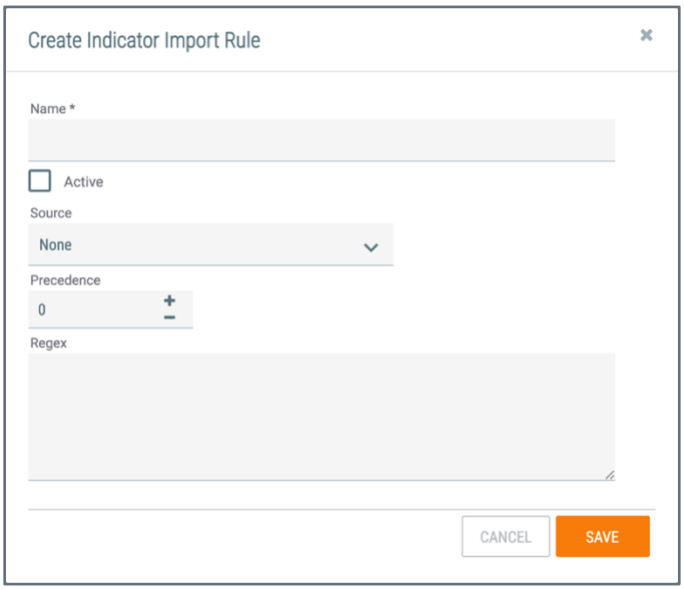

Figure 18

- **Name**: Enter the name of the rule.
- **Active**: Select the checkbox to designate the rule as active. The rule will not be included for Indicator validation unless this checkbox is selected.

- **Source**: Select the Indicator type on which the rule will match.
- **Precedence**: Enter the Precedence value, which is used if two rules exist for different Indicator types and if the regular expressions both match on the import content, or use the plus and minus buttons to add or subtract increments of 1, respectively. A rule with a higher Precedence value will be counted instead of a rule with a lower Precedence value.
- **Regex**: Enter a Java-compatible regular expression to define the Indicator that will result in a match for the rule.
- Click the **SAVE** button to create the rule.

Important: System Administrators should be cautious when creating Indicator import rules that allow empty strings so as not to cause unexpected errors in ThreatConnect.

Edit or Delete an Indicator Import Rule

To edit or delete an Indicator import rule, click **Edit** or **Delete** , respectively, in the **Options** column.

Indicator Exclusion Lists: System Level

The purpose of creating an Indicator Exclusion List is to prevent the importation of Indicators that may be deemed legitimate or non-hostile by an Administrator. ThreatConnect is prepopulated with default Indicator Exclusion Lists, but the system allows users to create custom Exclusion Lists at the System, Organization, Community, or Source level. The System-level List is configured through the **System Settings** screen by a System Administrator. Table 3 displays a list of what is and is not blocked by an Indicator Exclusion List.

Table 3

Item	Yes	No
Manual Creation	✓	
Structured Import	✓	
Unstructured Import	✓	
E-mail Ingestion (Phishing and Feed)	✓	
Source Feed Monitor	✓	
STIX™/TAXII Feeds	✓	
API Creation	✓	
API Bulk Import	✓	
Contribute/Copy to My Org		✓
pDNS		✓
Track Imports		✓
DNS Monitoring		✓

1. Click **Exclusion Rules** in the menu on the left side of the **Indicators** screen (Figure 12). The **Exclusion Rules** screen will be displayed (Figure 19).

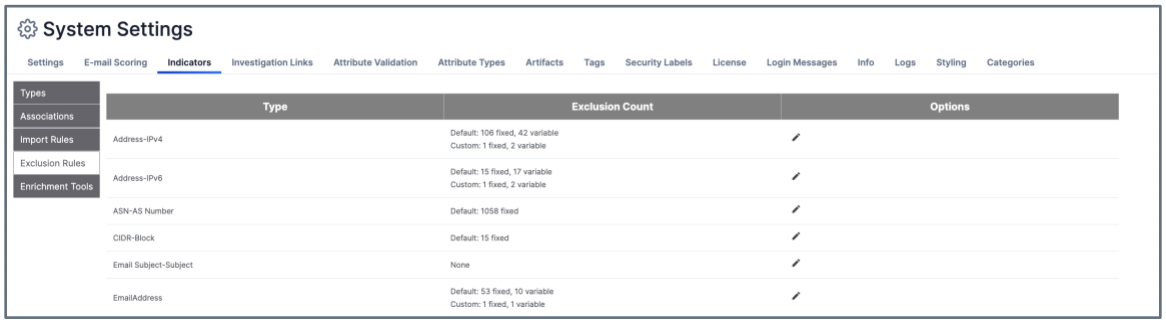

Figure 19

2. Click **Edit** in the **Options** column for an Indicator (**Address-IPv6** for this example). The **Exclusion Details** window will be displayed (Figure 20).

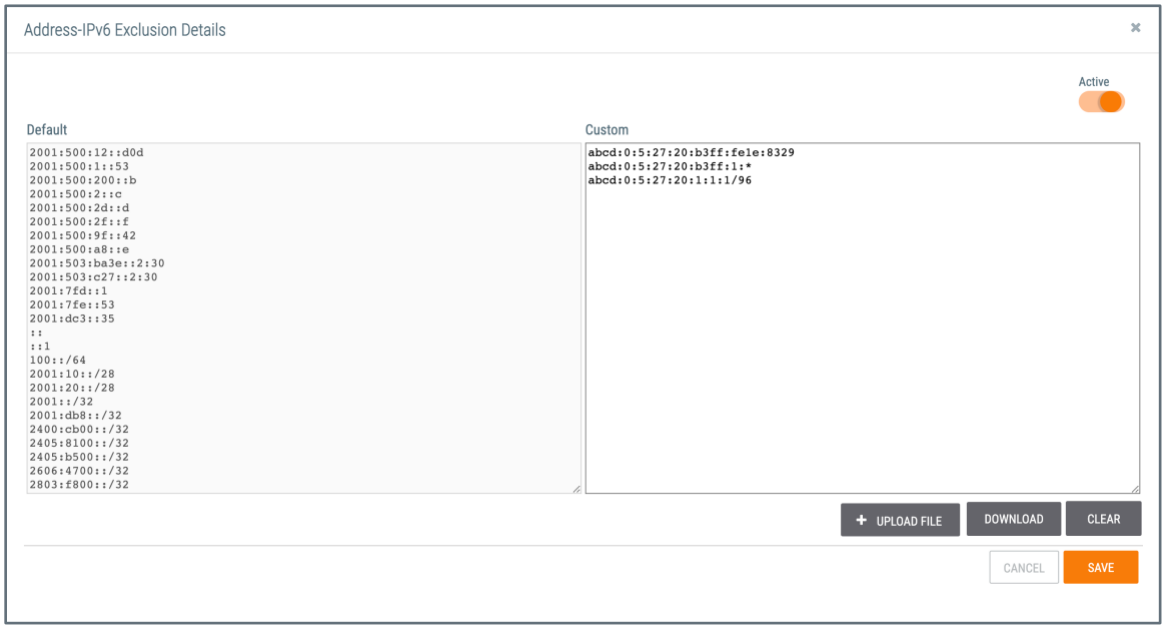

Figure 20

3. If the slider at the top right of the window is toggled on (orange), the **Default** Exclusion List on the left side of the screen will be used, as well as any Indicators that have been added to the **Custom** Exclusion List on the right. If the slider is toggled off (gray), only the **Custom** Exclusion List will be used.

> **Note**: The List on the **Default** side cannot be modified.

4. When creating a new Exclusion List, enter the information directly into the **Custom** text box, and click the **SAVE** button. Alternatively, click the **+ UPLOAD FILE** button to locate and select a file upload. After the file is uploaded, click the **SAVE** button.

   Note: The file must be in .txt format. Also, place an asterisk (*) at the beginning and end of the Indicator to exclude all results. For example, ***xyz.com*** in the URL Exclusion List would exclude any URL that contains the string **xyz.com**.

5. To modify an existing Exclusion List, edit it directly from the **Custom** text box, and click the **SAVE** button. Alternatively, click the **DOWNLOAD** button to download and edit a file, and then click the **+ UPLOAD FILE** button to upload the edited file. After the file is uploaded, click the **SAVE** button.

   Note: When trying to create an Indicator that has been placed on an Exclusion List, a message will be displayed in the **Create** window warning that the Indicator is contained on a System-wide Exclusion List.

6. To remove an existing **Custom** Exclusion List, click the **CLEAR** button, and the **Remove Exclusions** window will be displayed.
7. Click the **YES** button, followed by the **SAVE** button.

Enrichment Tools

ThreatConnect includes built-in enrichment services that, when enabled, retrieve data from a third-party enrichment service and then display those data on the **Enrichment** tab of the **Details** screen for supported Indicator types.

To use a built-in enrichment service, a valid API key for the enrichment service's vendor must be provided. At this time, the following third-party enrichment services are available in ThreatConnect:

- **DomainTools®**: Available for Host Indicators only.
- **Farsight Security®**: Available for Address and Host Indicators only.
- **RiskIQ®**: Available for Host Indicators only.
- **Shodan®**: Available for Address Indicators only.
- **urlscan.io**: Available for URL Indicators only.
- **VirusTotal™**: Available for Address, File, Host, and URL Indicators only.

Enabling an Enrichment Service

1. Click **Enrichment Tools** in the menu on the left side of the **Indicators** screen (Figure 12). The **Enrichment Tools** screen will be displayed (Figure 21).

Figure 21

2. Click **Edit** in the **Options** column for an enrichment service. The **Edit Vendor** window will be displayed.
3. Fill out the configuration options for the **DomainTools**, **Farsight**, **RiskIQ**, **Shodan**, **URLScan**, or **VirusTotal** enrichment service.

When an enrichment service is enabled, a value of **true** will be displayed in the **Enabled** column of the table displayed on the **Enrichment Tools** screen (Figure 21).

Important: Enabling the Farsight Security enrichment service allows users to view and retrieve passive DNS data for Address and Host Indicators on the **Enrichment** tab of the new **Details** screen. To view passive DNS data on the legacy **Details** screen for these Indicator types, Farsight Security must be enabled on the **Settings** tab of the **Organization Settings** screen. See the "Passive DNS" section of *ThreatConnect Organization Administration Guide* for more information.

Investigation Links

ThreatConnect includes dozens of third-party enrichment links to specific sources. To view the links for a particular Indicator, navigate to that Indicator's **Details** screen. Administrators can also add custom sources for each Indicator type.

1. Click the **Investigation Links** tab on the **System Settings** screen (Figure 1). The **Investigation Links** screen will be displayed (Figure 22).

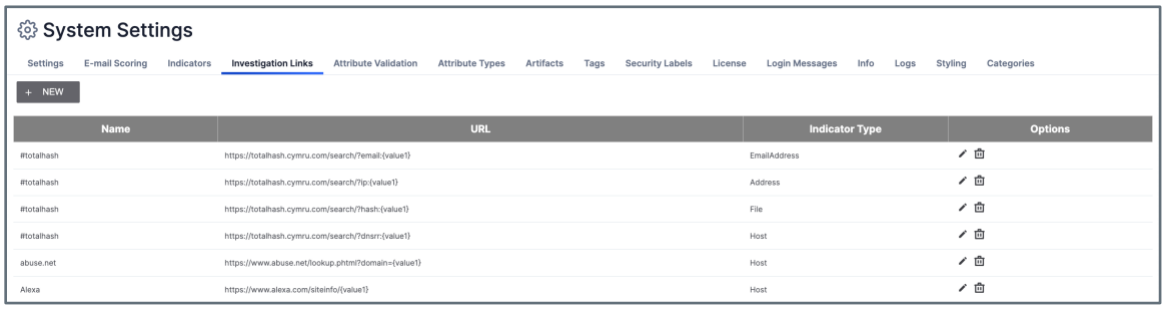

Figure 22

2. Click the **+ NEW** button. The **Create External Link** window will be displayed (Figure 23).

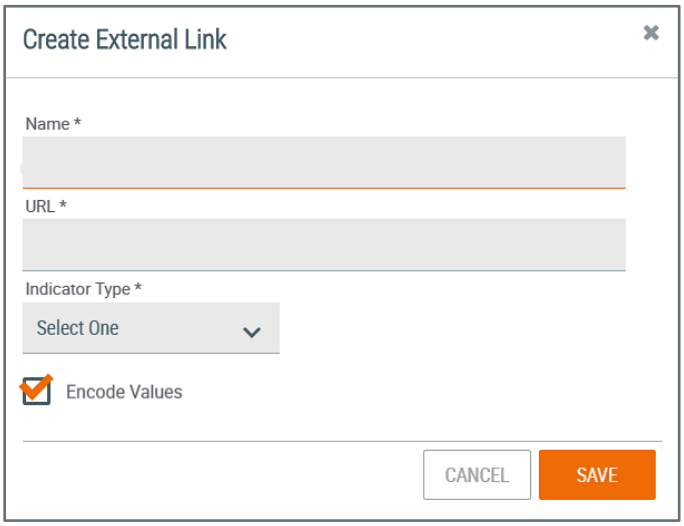

Figure 23

- **Name**: Enter the name of the external link.
- **URL**: Enter the URL of the external link
- **Indicator Type**: Select the Indicator type to which the external link applies.

- **Encode Values**: Select the checkbox to URL encode the Indicator to which the external link applies.
- Click the **SAVE** button.

Note: It is best practice for System Administrators to click the **Clear Entity Cache** button on the **Settings** tab after creating Investigation Links. Otherwise, the links may not populate for all users viewing the Indicators.

Attribute Validation

ThreatConnect is preloaded with a variety of Validation Rules to ensure that Attribute Types (see the "Attribute Types" section) conform to a valid input range and format. For example, a System Administrator may want country codes to follow a specific two-letter scheme or email addresses to match a proper regular expression. With ThreatConnect, System Administrators are capable of creating additional Validation Rules, which can be used by System, Community, and Organization Administrators when creating Attribute Types at their respective levels.

Create System Attribute Type Validation Rules

1. Click the **Attribute Validation** tab on the **System Settings** screen (Figure 1). The **Attribute Validation** screen will be displayed (Figure 24). The **Attribute Validation** screen displays the existing System Attribute Validation Rules.

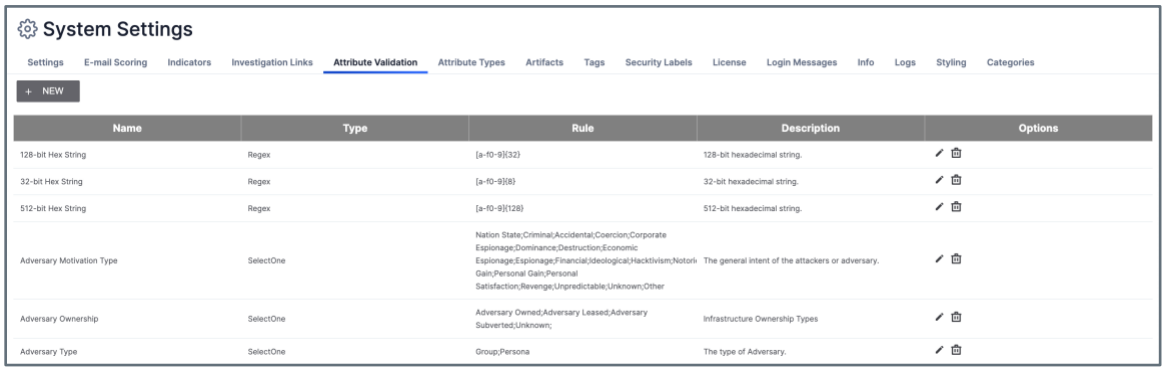

Figure 24

2. Click the **+ NEW** button. The **Create Attribute Validation Rule** window will be displayed (Figure 25).

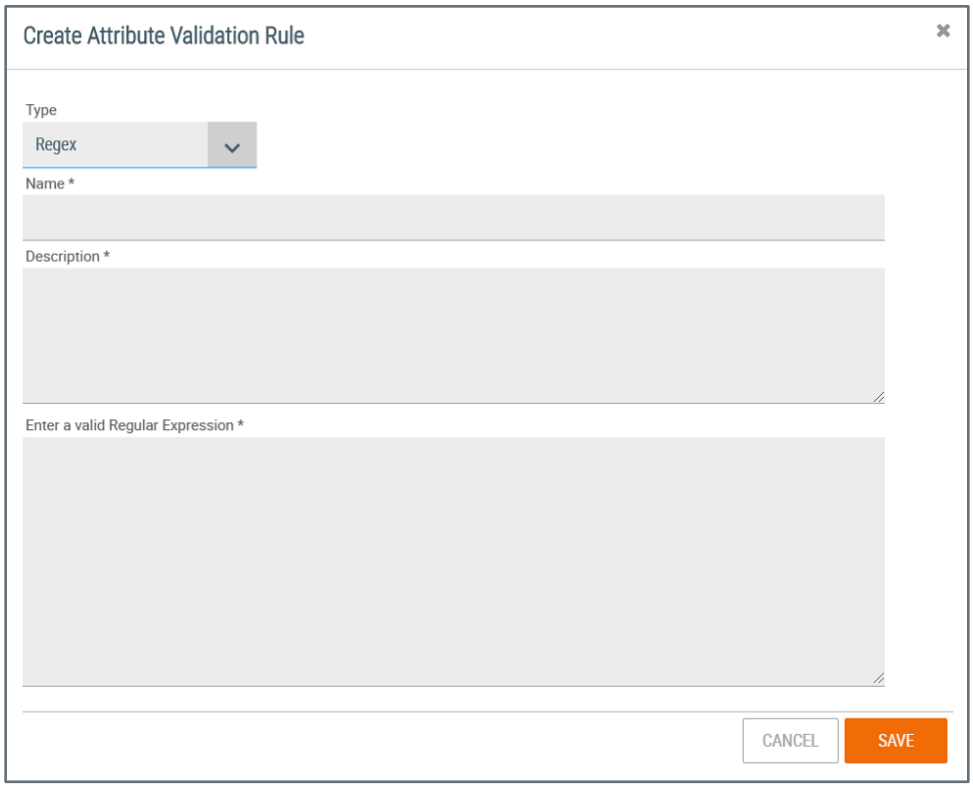

Figure 25

- **Type**: Select the schema for the Validation Rule. Each option offers the flexibility to determine the valid domain for each Attribute Type:
  - **Regex**: A regular expression that considers only matching inputs to be valid (e.g., an IP address or email address on a certain domain)
  - **Xsd**: An XML Schema Definition used to validate input (useful for attaching logs from a vendor product)
  - **Select One Picklist**: Presented as a dropdown menu of options—after the Administrator defines the options in the text box at the bottom of the window—from which users may only select one value (e.g., high, medium, or low priorities)
  - **Select One Radio**: Similar to Select One Picklist, but presented as a series of radio buttons
  - **Date**: A date in the YYYY/MM/DD format.
  - **Date/Time**: A date and time in the YYYY-MM-DD HH:MM UTC format.
  - **Integer**: A whole number, valid in the range specified in the right-hand text box (e.g., 0:1440 for "minutes worked")

- **Name**: Enter the name of the Validation Rule as it will be displayed in the Validation Rules table of the Attribute Validation screen.
- **Description**: Enter a general description of the Validation Rule.
- **Enter a Valid Regular Expression**: If applicable, enter the parameters for a Validation Rule as defined previously.
- Click the **SAVE** button to save and use the new **System Attribute Validation Rule**.

> **Important**: A System Attribution Validation Rule must be attached to an actual Attribute Type to validate user input.

Edit System Attribute Validation Rules

1. Click **Edit** for the Validation Rule to be edited in the **Options** column of the **Attribute Validations** screen (Figure 24). The **Create Attribute Validation Rule** window will be displayed with pre-entered values for the selected rule.
2. Make any desired changes to the rule, and click the **SAVE** button.

Attribute Types

Attribute Types are used to describe similar types of data within ThreatConnect. They can be used to articulate aspects of the Diamond Model or dictate how to deal with a certain Group or Indicator. ThreatConnect is deployed with a default set of System Attribute Types, which may be affixed to Groups and Indicators by any Organization or Community. System Administrators can add or edit System Attribute Types to make them available to the entire user base.

View System Attribute Types

Click the **Attribute Types** tab on the **System Settings** screen (Figure 1). The **Attribute Types** screen will be displayed (Figure 26).

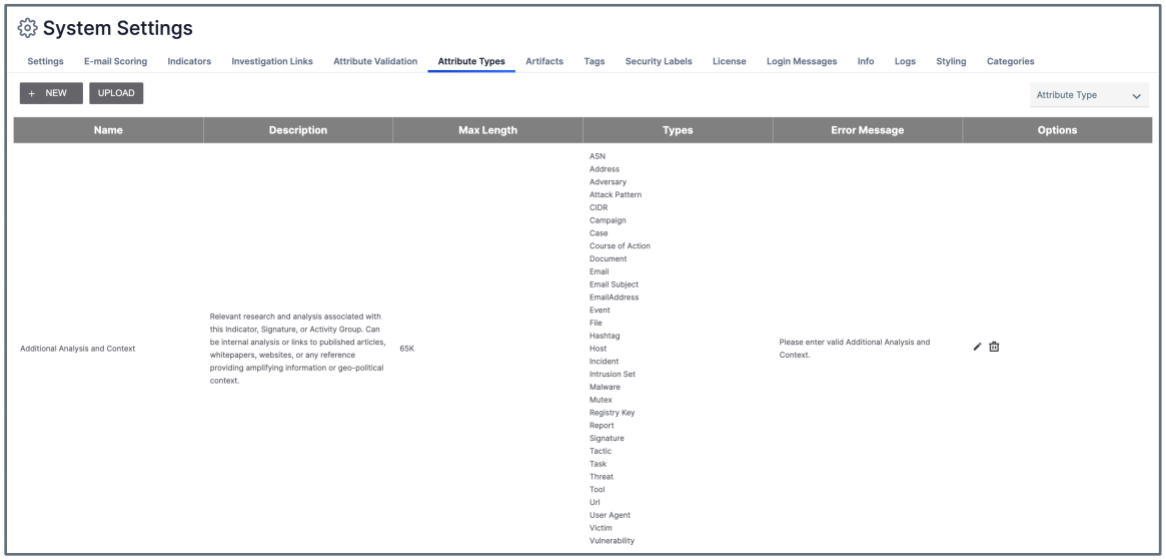

Figure 26

Create System Attribute Types

To create a custom System Attribute Type, click the **+ NEW** button on the **Attribute Types** screen (Figure 26). The **Configure Attribute Type** window will be displayed (Figure 27).

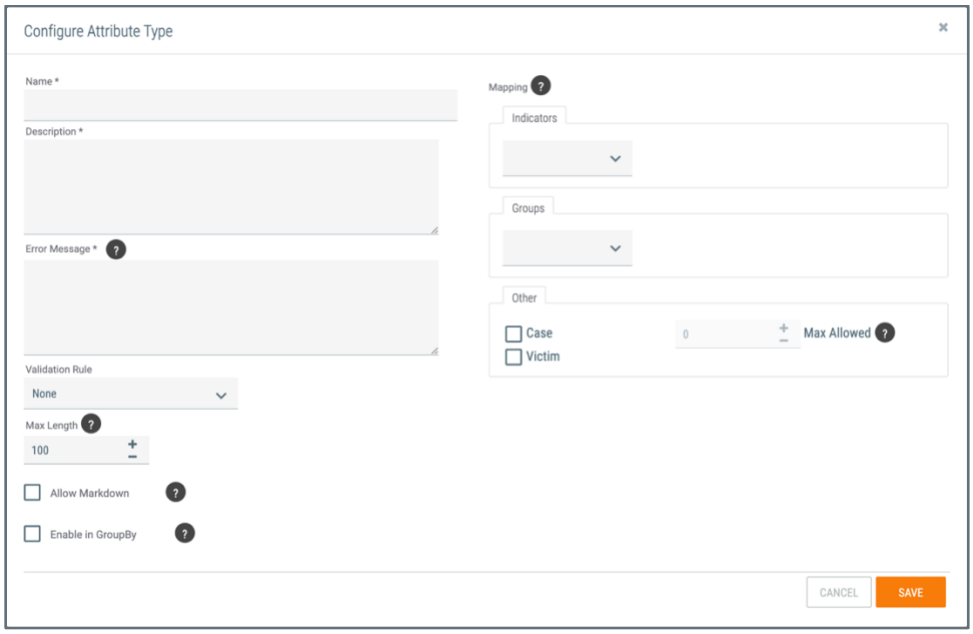

Figure 27

- **Name**: Enter the name of the System Attribute Type as it will be displayed on menus and on the **Details** screen for Indicators and Groups.
- **Description**: Enter a description of the System Attribute Type as seen by users when inputting a value for the Attribute Type or when viewing it from the **Details** screen.
- **Error Message**: Enter the message presented when users try to input a value that does not meet the System Attribute Type's Validation Rules.
- **Validation Rule**: Select the schema that determines whether a user's input is valid when logging an Attribute Type for an Indicator or Group. ThreatConnect is preloaded with a variety of Validation Rules, such as for IP Addresses, Dates, Country Codes, etc. System, Community, and Organization Administrators can define their own System Attribute Type Validation Rules as needed.
- **Max Length**: Enter the maximum size, in number of characters, of the System Attribute Type, if applicable, based on the Attribute Type's assigned Validation Rule. The maximum size can also be entered using the plus and minus buttons to add or subtract increments of 1, respectively.

- **Allow Markdown**: Select this checkbox to allow Markdown to be used when configuring an Attribute Type.

  > **Note**: Markdown is a plaintext formatting language that can be used to add formatting elements to a number of Attribute Types, including Description and Source. See the "Enabling and Using Markdown in Attributes" section of *Attributes* for more information.

- **Enable in GroupBy**: Select this checkbox to allow the Attribute Type to be grouped or queried by dashboard cards.

  > **Important**: If an Attribute Type's maximum length is greater than 500 characters, the **Enable in GroupBy** checkbox will be disabled.

- **Mapping**:
  - **Indicators**: Click the dropdown to display a scrollable multi-select list of Indicators, and select the checkboxes to specify the types of Indicators to which the Attribute Type can apply. For example, it may make sense to track a "work-hours" Attribute Type against an Incident or File, but not against a URL.
  - **Groups**: Click the dropdown to display a scrollable multi-select list of Groups, and select the checkboxes to specify the types of Groups to which the Attribute Type can apply.
  - **Case**: Select this checkbox if the Attribute Type should apply to a Case.
  - **Max Allowed**: If the **Case** checkbox is selected, the **Max Allowed** option will become enabled. Enter the maximum number of times that the Attribute Type can be added to a single Case, or use the plus and minus buttons to add or subtract increments of 1, respectively.

    > **Note**: If a user tries to add an Attribute to a Case when the Attribute Type's **Max Allowed** limit has been reached, an error message will be displayed stating that the maximum allowed for the Attribute Type has been exceeded on the current Case, and the user will be directed to select an alternative Attribute Type or remove an existing Attribute of the maxed-out Attribute Type from the Case.

- **Victim**: Select this checkbox if the Attribute Type should apply to a Victim.
- Click the **SAVE** button to create the custom Attribute Type.

Figure 28 shows an example of a custom System Attribute Type that uses the **System Country Validation Rule** to track the suspected nationalities of those responsible for the

given Groups and Indicators. If custom Indicators have been added, they will be displayed in the **Indicators** section as well.

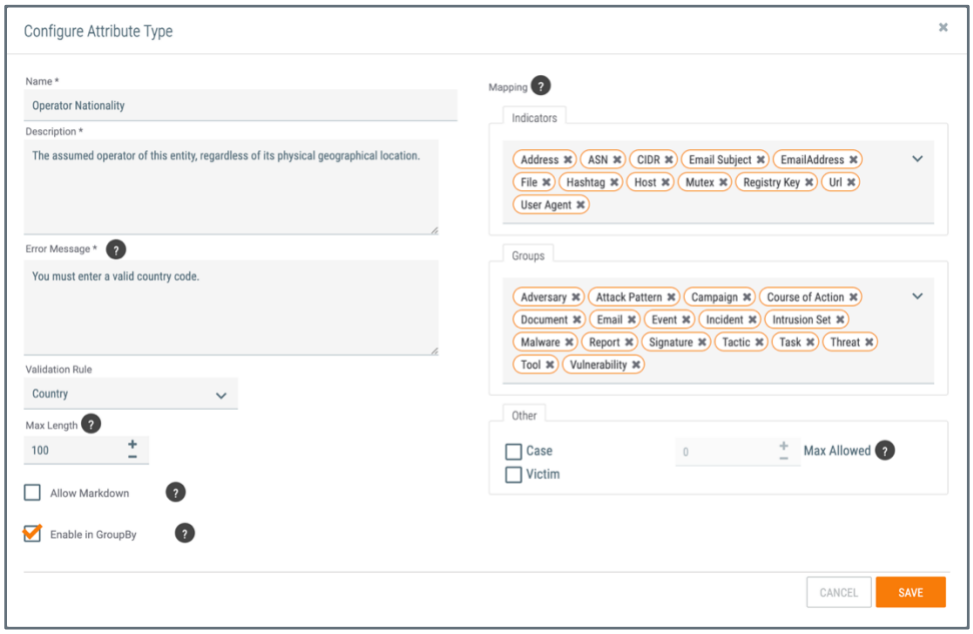

Figure 28

Upload System Attribute Types

1. Click the **UPLOAD** button on the **Attribute Types** screen (Figure 26). The **Upload Attributes** window will be displayed (Figure 29).

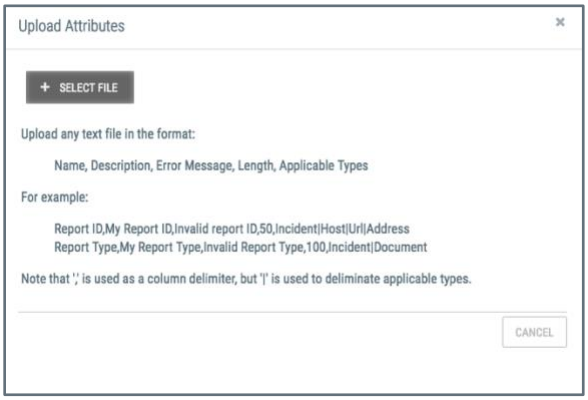

Figure 29

2. Click the **+ SELECT FILE** button to locate and select a file to upload.
3. Click the **SAVE** button.

System Attribute Types can be uploaded in a text or JavaScript Object Notation (JSON) file. If uploading a System Attribute Type via a text file, use the following format: **Name**, **Description**, **Error Message**, **Length**, **Applicable Types**.

> **Note**: In text files, columns are delimited by the comma character (,). Applicable Types are delimited by the pipe character (|).

If uploading a System Attribute Type via a JSON file, refer to Table 4 for the fields that can be included in the file.

Table 4

Field	Required	Type
allowMarkdown	FALSE	Boolean
description	TRUE	String
errorMessage	TRUE	String
groups	FALSE	String
indicators	FALSE	String
maxLength	TRUE	Integer
name	TRUE	String
version	FALSE	Integer

> **Note**: Upon creation of a new System Attribute Type, the `version` field is automatically assigned a value of `1`.

> **Note**: To update an existing System Attribute Type, the value for the `name` field must equal the name of the System Attribute Type being updated, and the value for the `version` field must be incremented from the previous value by at least 1.

The following is an example JSON file format used to upload a System Attribute Type:

```
{
    "types": [
        {
            "allowMarkdown": true,
            "description": "Description of System Attribute Type",
            "errorMessage": "Enter a valid value",
            "groups": [
                "Adversary",
                "Campaign",
                "Course of Action",
                "Document",
                "Email",
                "Incident",
                "Malware",
                "Threat"
            ],
            "indicators": [
                "Address",
                "EmailAddress",
                "File",
                "Host",
                "Url"
            ],
            "maxLength": 100,
            "name": "System Attribute Type Name",
            "system": false,
            "version": 2
        }
    ]
}
```

Edit System Attribute Types

1. Click **Edit** for the Attribute to be edited in the **Options** column of the **Attribute Types** screen (Figure 26). The **Configure Attribute Type** window will be displayed with pre-entered values for the selected Attribute Type.
2. Make any desired changes to the Attribute Type, and click the **SAVE** button.

Artifacts

Artifacts are integral components of ThreatConnect's Workflow feature. Artifacts are typed, like Indicators and Groups, and a set of supported Artifact types is preconfigured in ThreatConnect. This set includes all ThreatConnect Indicator types.

Types

Create Artifact Types

ThreatConnect is preloaded with a set of Artifact types, but System Administrators can create new Artifact types.

1. Click the **Artifacts** tab on the **System Settings** screen (Figure 1). The **Artifacts** screen will be displayed, showing all existing Artifact types (Figure 30).

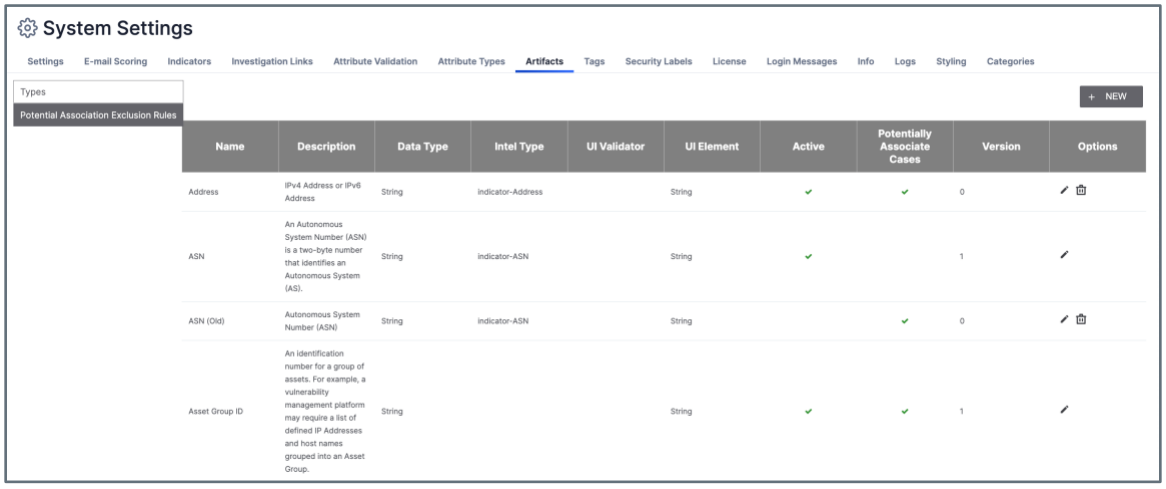

Figure 30

2. Click the **+ NEW** button. The **Configure Artifact Type** window will be displayed (Figure 31).

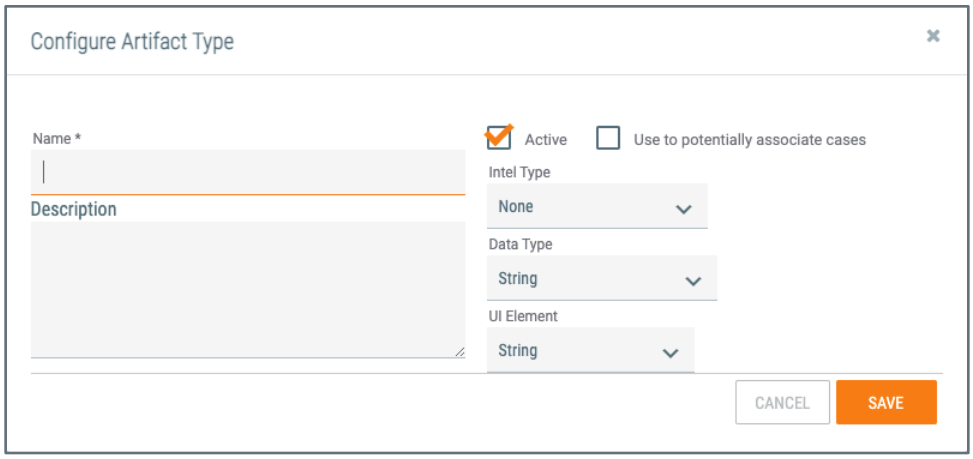

Figure 31

- **Name**: Enter the name of the Artifact type as it will be displayed in the **Artifact Types** table.
- **Description**: Enter a description of the Artifact type.
- **Active**: Select the checkbox to make this Artifact type active.
- **Use to potentially associate cases**: If this checkbox is selected, the **Use to potentially associate cases.** checkbox of the **Add Artifact** drawer will be selected automatically when a user creates an Artifact of this type in a Case.
- **Intel Type**: Select a ThreatConnect Indicator type to map to the Artifact type.
- **Data Type**: Select the data type for the Artifact type.
- **UI Element**: Select the UI element into which the user will enter data for Artifacts of this type.
- Click the **SAVE** button to create the Artifact Type.

Edit Artifact Types

1. Click **Edit** for the Artifact type to be edited. The **Configure Artifact Type** window will be displayed with pre-entered values for the selected Artifact type.
2. Make any desired changes to the Artifact type, and click the **SAVE** button.

Potential Association Exclusion Rules

Potential Association Exclusion Rules are not included by default, but users can add them. They prevent Artifacts from creating potential associations between Cases if the Artifacts' types are on the Exclusion List.

1. Click **Potential Association Exclusion Rules** in the menu on the left side of the **Artifacts** screen (Figure 30). The **Potential Association Exclusion Rules** screen will be displayed (Figure 32).

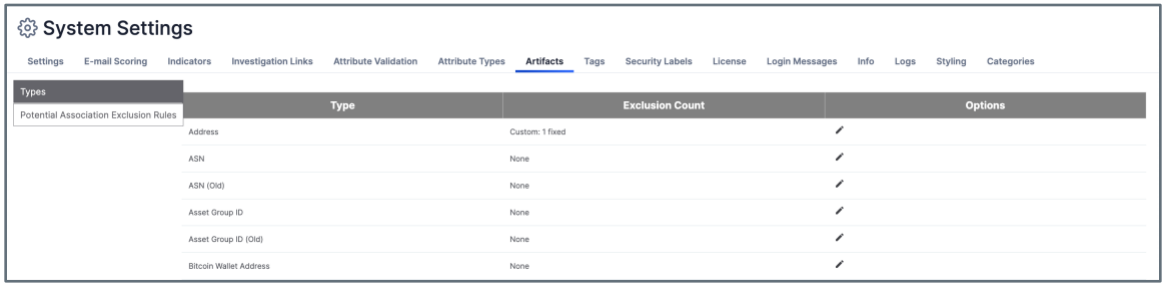

Figure 32

2. Click **Edit** for the entry to be edited. The **Exclusion Details** window will be displayed (Figure 33).

Figure 33

3. Enter the custom exclusion details manually, or click the **+ UPLOAD FILE** button to select a file to upload.
4. Click the **SAVE** button.

Tags

Tags are data objects in ThreatConnect® that can be applied to Indicators, Groups, Victims, and Workflow Cases. They create associations between the data to which they are applied, as well as a path from one intelligence item to another.

Normalization

On the **Normalization** section of the **Tags** screen (Figure 34), System Administrators can create and manage Tag normalization rules that convert one or more synonymous Tags to a main Tag. When a Tag normalization rule is enabled, existing Tags in all owners on the ThreatConnect instance that match one of the rule's synonymous Tags are converted to the main Tag, and new Tags created on the ThreatConnect instance that match one of the rule's synonymous Tags are converted to the main Tag whenever they are applied to Indicators, Groups, Victims, and Workflow Cases.

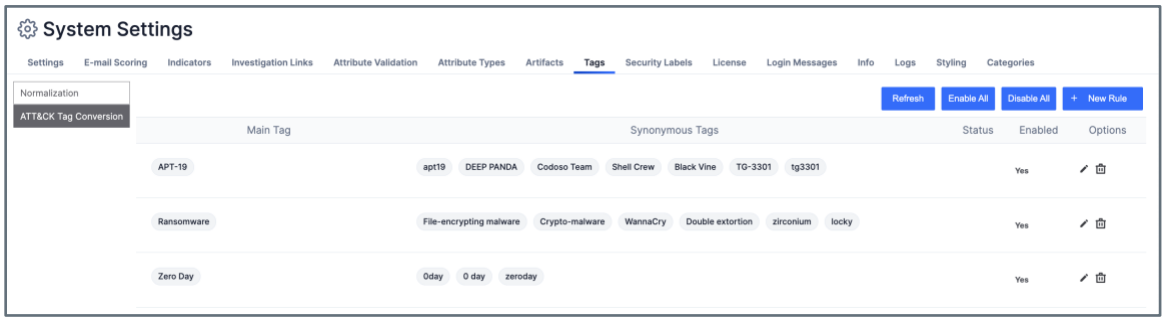

Figure 34

See *Tag Normalization* for instructions on creating and managing Tag normalization rules.

ATT&CK Tag Conversion

On the **ATT&CK Tag Conversion** section of the **Tags** screen (Figure 35), System Administrators can use pre-configured rules to convert standard Tags to ATT&CK® Tags based on whether they exactly or approximately match a specific ATT&CK Tag. This ensures that all users on a ThreatConnect instance use ATT&CK Tags when identifying the MITRE ATT&CK® Enterprise techniques and sub-techniques associated with a particular object.

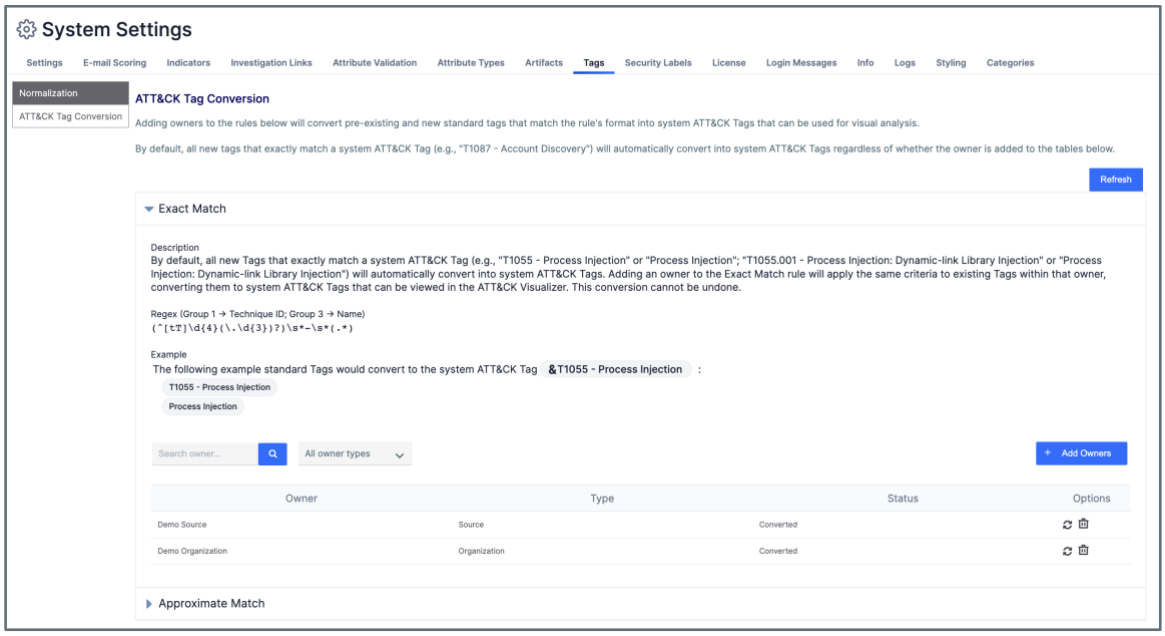

Figure 35

See the "Converting Standard Tags to ATT&CK Tags" section of *ATT&CK Tags* for instructions on adding an owner to the **Exact Match** or **Approximate Match** rules on this screen.

Security Labels

Purpose of System Security Labels

Directors can define Security Labels for use by all member Organizations. Security Labels are a good way to designate how information should be treated. ThreatConnect uses the Traffic Light Protocol (TLP) system published by the Forum of Incident Response and Security Teams™ (FIRST). Administrators can define their own Security Labels based on their needs and policies.

ThreatConnect also includes a migration tool that allows users to take an owner-specific security label and migrate it to a System label, so that every possible variation of the TLP naming convention (e.g., TLP: RED vs. TLP Red vs. TLPred) is accounted for. To view more information on creating and using owner-level Security Labels in Organizations, Communities, and Sources, refer to *ThreatConnect Organization Administration Guide* and *ThreatConnect Community and Source Administration Guide*.

Create System Security Labels

1. Click the **Security Labels** tab on the **System Settings** screen (Figure 1). The **Security Labels** screen will be displayed with a list of the standard Security Labels (Figure 36).

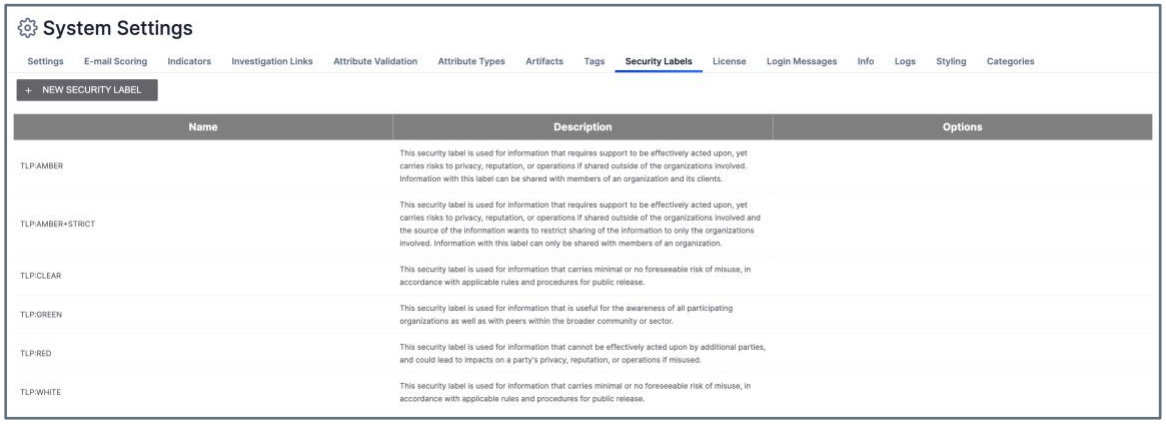

Figure 36

2. Click the **+ NEW SECURITY LABEL** button. The **Create Security Label** window will be displayed (Figure 37).

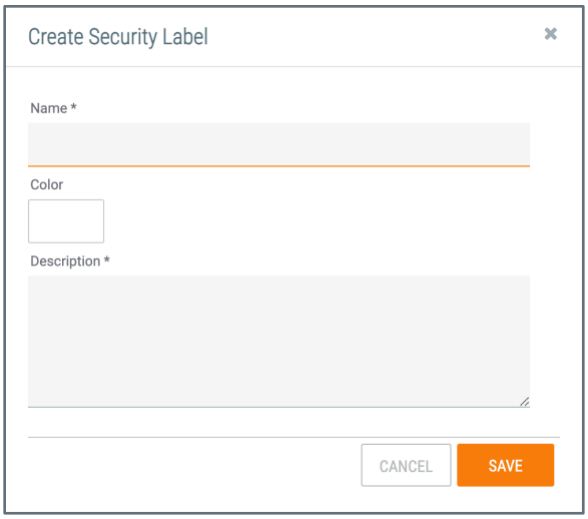

Figure 37

- **Name**: Enter a name for the Security Label.
- **Color**: Click in the box to select a color using the color picker, or enter a color code in RGB or hexadecimal format.
- **Description**: Enter a description for the Security Label.

> **Note**: These fields are provided solely for user and administrator readability, as no policy enforcement is derived from this screen.

- Click the **SAVE** button.

Using System Security Labels

Security Labels are most effective when users share or contribute information within ThreatConnect. This approach enables users to withhold and divulge information with respect to their Organization's policies, based on the Security Label applied to each piece of data.

Security Labels are applied not just to Groups and Indicators, but also to their Attribute Types. For example, an IP Address Indicator may be considered TLP:GREEN (i.e., peers and partner Organizations may see it). However, its Source Attribute Type may be a sensitive system log that pinpoints a system vulnerability and thus may be considered TLP:RED (i.e., not to be shared).

License

View and Manage the System License

Click the **License** tab of the **System Settings** screen (Figure 1). The **License** screen will be displayed with the **License Config** subtab selected (Figure 38).

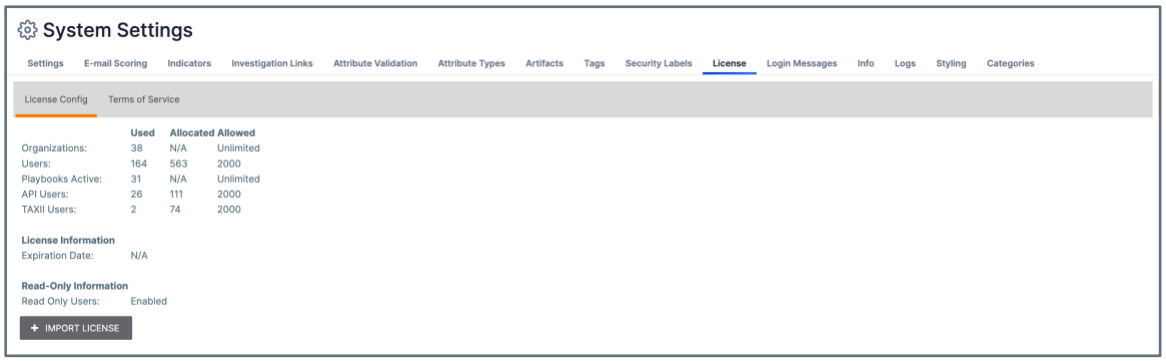

Figure 38

This screen displays the following information for Organizations, Users, Playbooks, API Users, and TAXII Users:

- **Used**: The number or amount of licensed uses for the object.
- **Allocated**: The number or amount of licensed uses allocated for the object.
- **Allowed**: The maximum number or amount of licensed uses for the object. If no value is set within the instance's license, a value of **Unlimited** will be displayed.

In addition, this screen also displays the expiration date for the instance's license and whether Read Only Users are enabled on the instance.

From this screen, the user can also import a license by clicking the **+ IMPORT LICENSE** button, which will open a file browser window to locate and select a license file.

View and Manage the Terms of Service

Click the **Terms of Service** subtab of the **License** screen (Figure 38) to display the **Terms of Service** screen (Figure 39). From this screen, the user can view, import, and delete the Terms of Service, as well as reset user acceptance.

Figure 39

Login Messages

From the **Login Messages** screen, users can add message text for display on their ThreatConnect **Login** screen or view the messages already displayed there.

Create Login Messages

1. Click the **Login Messages** tab of the **System Settings** screen (Figure 1). The **Login Messages** screen will be displayed (Figure 40).

Figure 40

2. Click the **+ NEW** button. The **Create Login Message** window will be displayed (Figure 41).

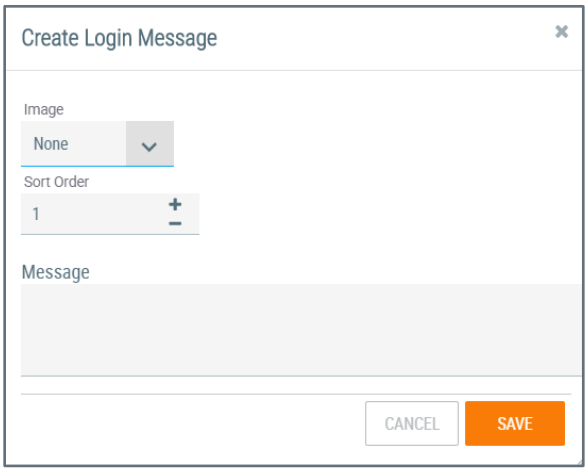

Figure 41

- **Image:** Select an icon to add next to the message.
  - **None:** No icon
  - **Vote:** Checkmark icon
  - **Feature:** Notebook icon

- **Sort Orde**r: Enter the value for the position in which the icon will be displayed on the screen next to the text, or use the plus and minus buttons to add or subtract increments of 1, respectively.
- **Message:** Enter the login message.
- Click the **SAVE** button.

Info

View Hardware and Virtualization Information

Click the **Info** tab of the **System Settings** screen (Figure 1). The **Info** screen will be displayed with the **Information** subtab selected (Figure 42). This screen displays current system hardware, software, and application database status information. For more information on determining which version and build of ThreatConnect is running on the instance, see *ThreatConnect Versioning*.

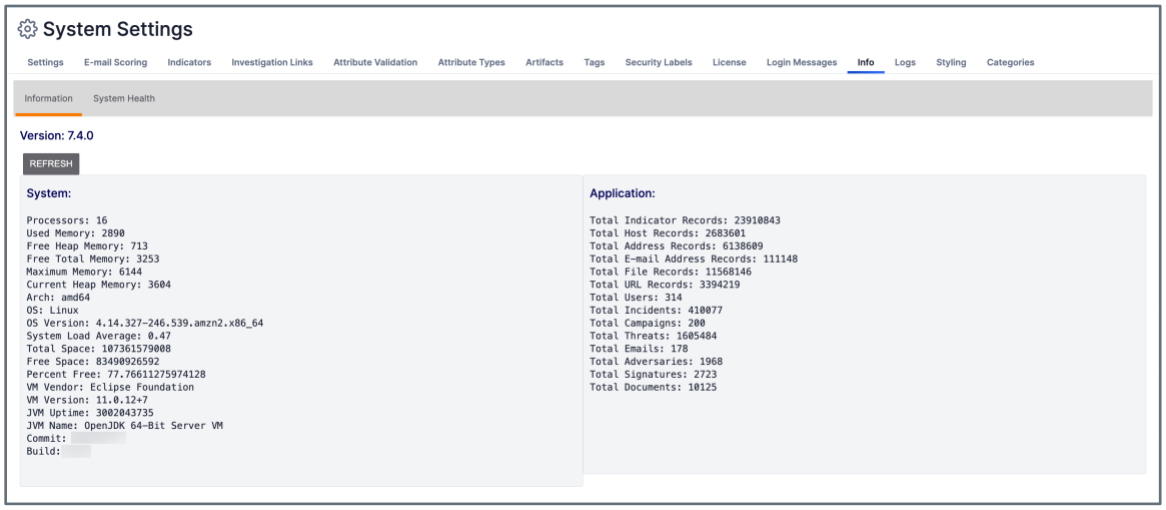

Figure 42

View System Health Information

1. Click the **System Health** tab of the **Info** screen (Figure 42) to display the **System Health** screen (Figure 43). This screen shows whether certain system processes and settings are configured and operating properly. If a component is operating properly, a green checkmark ✔ will be displayed in the **Passed** column. If a component needs attention, an orange warning sign ⚠ will be displayed in the same column.

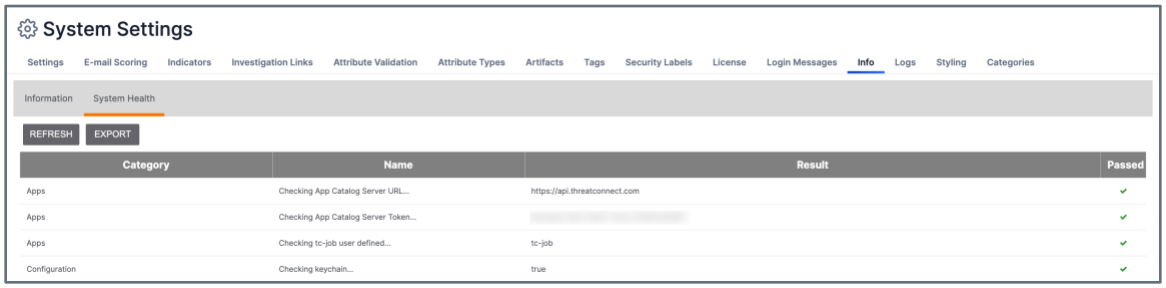

Figure 43

2. Click the **REFRESH** button to refresh the table or the **EXPORT** button to download an Excel® file displaying the system diagnostics.

The health of the ThreatConnect instance can also be retrieved via the status servlet by submitting an HTTP request in the following format:

```
GET https://{baseURL}/status
```

Refer to Table 5 for a list of headers that can be included in this request and example JSON responses.

Table 5

Header	Response Code	Example JSON Response
None	200–OK 500–System Unhealthy	

statuskey={incorrectValue}	200–OK
	500–System Unhealthy
		{
		"Message": "Invalid access key!"
		}

statuskey={correctValue}	200–OK
	500–System Unhealthy
		{
		"Product Version": "7.3.0",
		"DB Status": "OK",
		"HTTP Status": "OK",
		"Filesystem status (JBoss Server Log) ": "OK 139871MB remaining)",
		"Filesystem status (Bulk Reports)": "OK (139871MB remaining)",
		"Filesystem status (Local Storage)": "OK (139871MB remaining)",
		"Filesystem status (TC Server Log)": "N/A",
		"Current Time": "2023-10-04T12:52:09.430-0500",
		"Message": "System OK."
		}

Important: The **statuskey** value cannot be retrieved in the ThreatConnect UI. For more information about obtaining the **statuskey** value, see *ThreatConnect Management API User Guide*.

Logs

The **Logs** tab allows users to retrieve App and server logs that are saved to the **loggingLocation** directory, which is specified in the **System Settings**.

View Logs

1. Click the **Logs** tab of the **System Settings** screen (Figure 1). The **Logs** screen will be displayed with the **View** subtab selected (Figure 44). To narrow the display of table entries, enter text on which to filter in the **Source Class**, **Level**, or **Message** boxes.

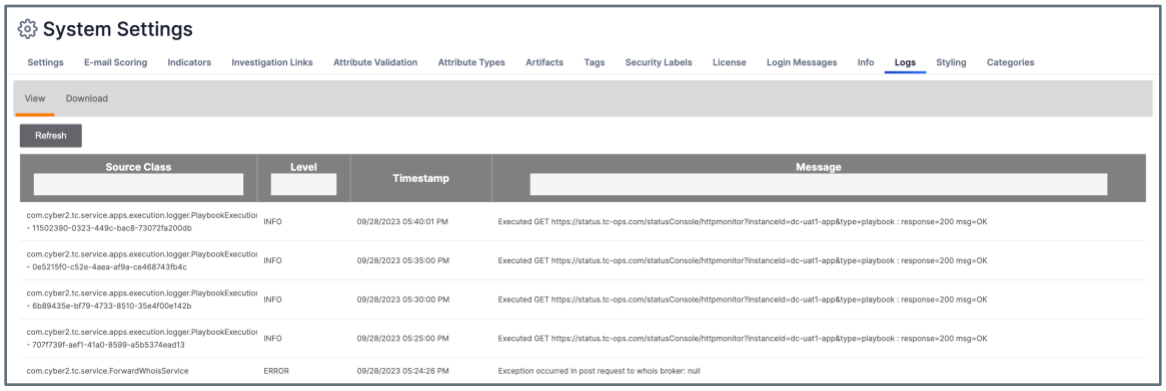

Figure 44

2. Select an entry to display its **Log Details** window (Figure 45).

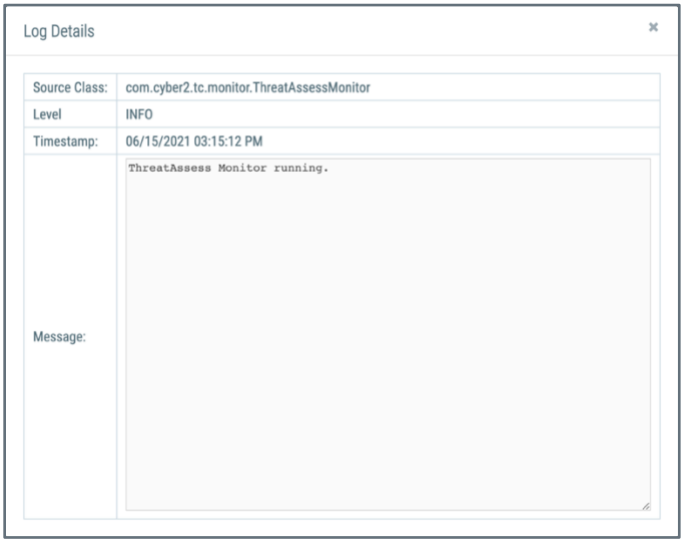

Figure 45

Download Logs

1. Click the **Download** subtab of the **Logs** screen (Figure 44) to display the **Download** screen (Figure 46).

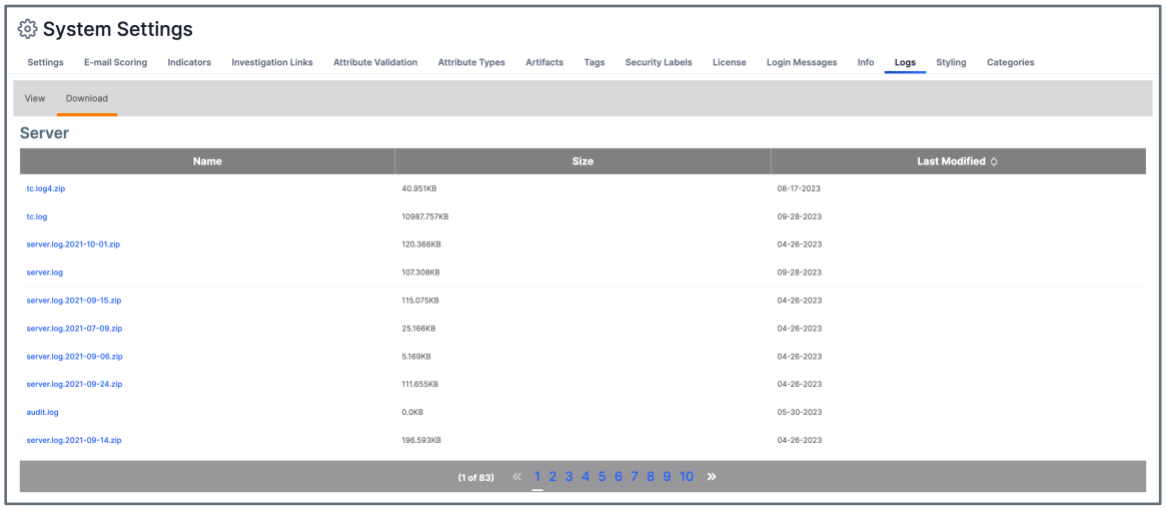

Figure 46

2. Click on an entry's name in the **Name** column to download its log file to the computer's **Downloads** folder.

Styling

When downloading a PDF that describes an Adversary, Incident, or Threat, a user may want to include a custom header on the PDF. A user may also wish to style the ThreatConnect site with a custom header or footer.

Style a PDF Header and a Site Header or Footer

1. Click the **Styling** tab of the **System Settings** screen (Figure 1). The **Styling** screen will be displayed (Figure 47). This screen shows the default ThreatConnect headers and footer that will be used if no other images are uploaded.

   Note: Hover over the question-mark symbols for image-size requirements.

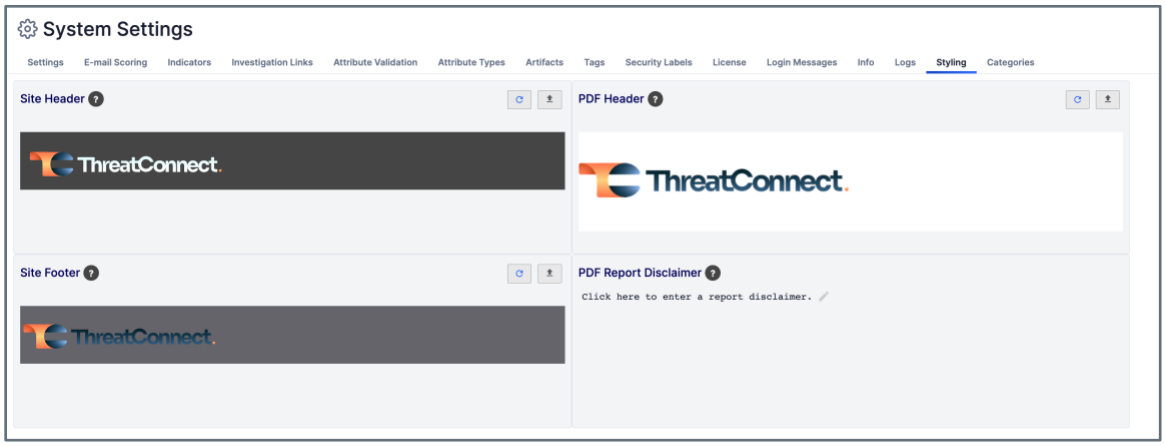

Figure 47

2. Click the **Upload** button In the upper-right corner of the **Site Header**, **Site Footer**, or **PDF Header** cards to select a JPEG or PNG image file. The selected image will now be displayed in the appropriate header or footer box. It will also be displayed as a header for downloaded PDFs or as a header or footer for the user's ThreatConnect site.

3. Click **Edit** in the **PDF Report Disclaimer** card to add a disclaimer, such as "Demo," to a PDF.

Categories

The **Categories** tab (Figure 48) allows System Administrators to view, create, edit, and delete Intelligence Requirement (IR) categories. IR categories provide users with greater control over how they organize their IRs. For example, they can use categories to organize IRs based on different stakeholder groups (e.g., SecOps, HR, Finance) or threat actor types (e.g., Nation State, Hacktivist).

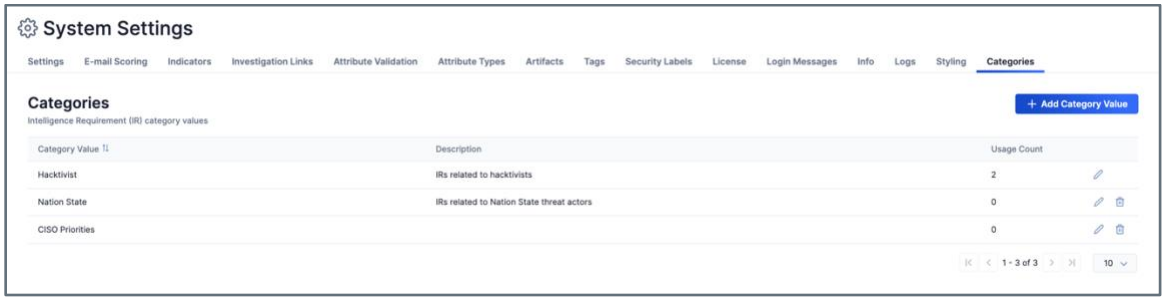

Figure 48

TC Exchange Settings Screen

ThreatConnect is integrated with many third-party applications and services, such as Lastline®, OpenDNS®, and ArcSight™, which allow ThreatConnect users to employ these product integrations as Apps via TC Exchange™ to further augment their analytic capabilities.

Access the TC Exchange Settings Screen

1. Log into ThreatConnect with a System Administrator account.
2. On the top navigation bar, hover the cursor over **Settings** and select **TC Exchange Settings**. The **Installed** tab of the **TC Exchange Settings** screen will be displayed (Figure 49). This screen displays all installed Apps.

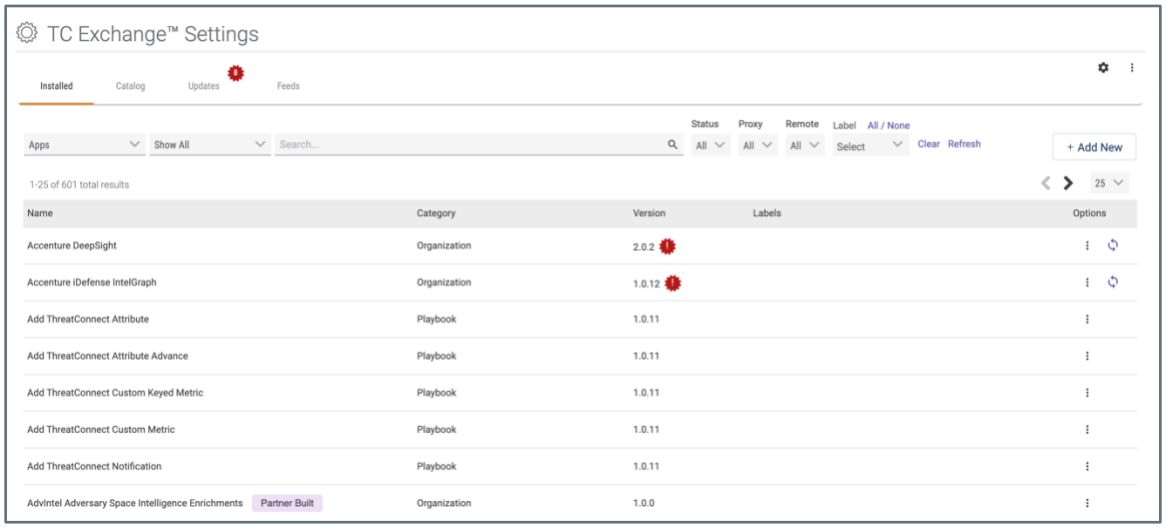

Figure 49

Note: A purple box containing the text "Partner Built" displayed in the **Name** column denotes a partner-built App. When working with partner-built Apps, contact the company that built the App for support and to provide feedback about the App.

- **Type**: Select whether to display installed Apps, Playbook Templates, or Workflow Templates. By default, **Apps** is selected.
- **App Type**: Select which type of installed Apps to display. By default, **Show All** is selected. Note that this dropdown menu is displayed only when viewing Apps.

- **Search…**: Enter the name of an installed App, Playbook Template, or Workflow Template into the search bar. The displayed Apps or Templates will be filtered as text is entered into the search bar. To remove the filter, highlight and delete the text entered into the search bar.
- **Status**: Use this dropdown to filter installed Apps by status (**Active** or **Deprecated**).
- **Proxy**: Use this dropdown to filter installed Apps based on whether they use an external proxy.
- **Remote**: Use this dropdown to filter installed Apps based on whether they allow remote execution.
- **Label**: Use this dropdown to filter installed Apps, Playbook Templates, or Workflow Templates based on the label(s) applied to them. Clicking the **All** or **None** displayed above the dropdown will select or clear the checkboxes for all labels, respectively.
- **Clear**: Click this option to clear any filters applied on the **Installed** tab of the **TC Exchange Settings** screen.
- **Refresh**: Click this option to refresh the list of installed Apps, Playbook Templates, or Workflow Templates.

> **Note**: The **Type**, **App Type**, and **Search…** filter options are also available on the **Catalog** tab of the **TC Exchange Settings** screen.

Installed

View Installed Items

1. To view installed items by category (Apps, Content Packs, Playbook Templates, and Workflow Templates), select a category from the dropdown menu located below the **Installed** tab. To search for an installed item, enter a term in the search box to return all items matching the search term.
2. Items on the **Installed** tab can be sorted and filtered using the menus to the right of the search bar:
   - **Status**: Use the **Status** dropdown menu to filter installed items based on whether they are **Active** or **Deprecated**.
   - **Proxy**: Use the **Proxy** dropdown menu to filter installed items based on whether the **Use External Proxy** option is turned on or turned off.

- **Remote**: Use the **Remote** dropdown menu to filter installed items based on whether the **Allow Remote Execution** option is turned on or turned off.
- **Label**: Use the **Label** dropdown menu to display a scrollable multi-select list of available labels. Selecting one or more labels will display only installed items with those labels applied. To select all labels, click **All** above the **Label** dropdown menu. To deselect all selected labels, click **None** above the **Label** dropdown menu.

> **Note**: Any filters and sorting preferences applied to the list view on the **Installed** tab of the **TC Exchange Settings** screen will persist if the user navigates to another tab on the **TC Exchange Settings** screen. However, if the user navigates away from the **TC Exchange Settings** screen, all filters and sorting preferences will be reset.

3. Click the vertical ellipsis ⋮ in the **Options** column for an item (an App in this example) to display its **Options** menu (Figure 50).

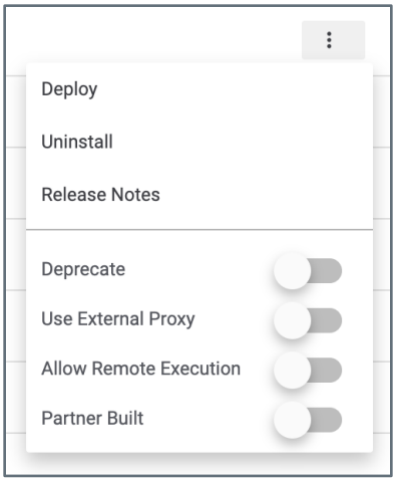

Figure 50

> **Note**: Figure 50 is an example of an **Options** menu for a specific App. The number of options available may vary for different Apps and the type of installed item (i.e., App, Content Pack, Playbook Template, or Workflow Template).

4. From the **Options** menu, a user can do the following:
   - deploy a feed for the App
   - set permissions to select the Organizations that can run an App
   - uninstall the App
   - update the App
   - view release notes for the App

- deprecate the App manually (the only option available for internal Apps)
- enable or disable use of an external proxy
- enable or disable remote execution
- indicate whether the App is a partner-built App

Install an Item From a File

1. Click the **+ Add New** button at the top right of the **Installed** tab of the **TC Exchange Settings** screen. The **Install a new file** drawer will be displayed (Figure 51).

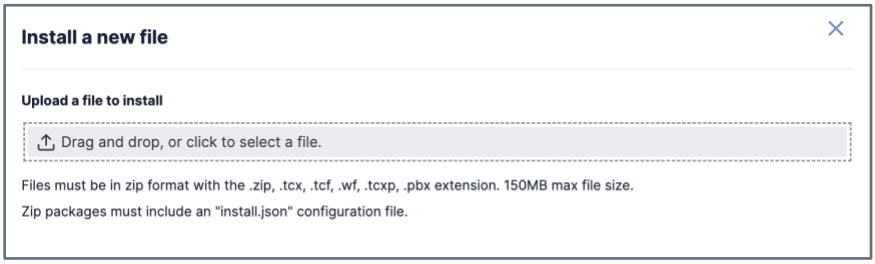

Figure 51

2. Drag and drop a file for an App, Content Pack, Playbook Template, or Workflow Template into the **Drag and drop, or click to select a file**. box, or click the box to browse for and select a file.

> **Note**: The file must be in a zipped format with the **.zip**, **.tcx**, **.tcf**, **tcxp**, **.wf**, or **.pbx** extension; be less than 150MB in size; and include an **install.json** configuration file.

3. After uploading a file (an App file in this example), information about the item will be displayed in the **Install a new file** drawer (Figure 52).

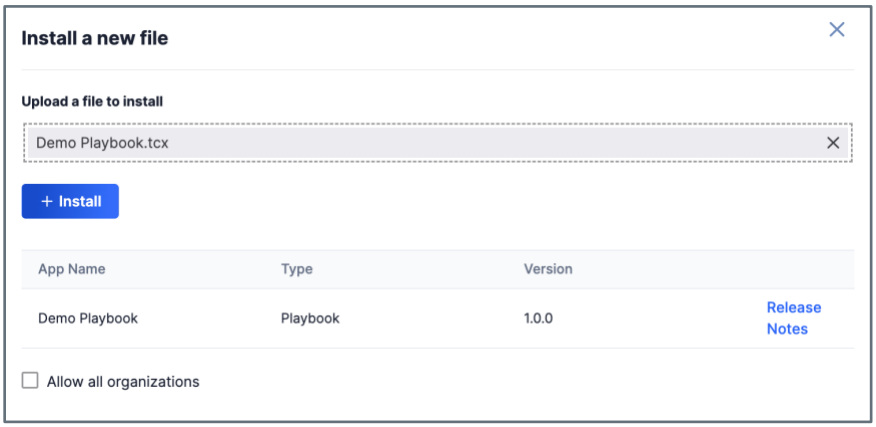

Figure 52

- Verify that the information displayed in the table is correct.
- **Release Notes**: If installing an App, this option will be displayed. Click this link to display the App's release notes.
- **Allow all organizations**: If installing an App, this option will be displayed. Select this checkbox to allow all Organizations on the ThreatConnect instance access to use the App. If installing a Service App, it does not matter whether this checkbox is selected. The Service itself, rather than the Service App, sets the permissions and access to the App.
- Click the + **Install** button to install the item.

> **Note**: If a new version of an existing item is installed, the previous version(s) are deprecated automatically.

Feed Deployment

Apps with feeds take advantage of the feed-deployment mechanism to create Sources, which then run associated Jobs (for Job Apps) or Services (for Feed API Service Apps). See *The Feed Deployer* for instructions on how to deploy a feed.

> **Note**: When the Feed Deployer creates a new Source (i.e., deploys a feed), it creates a number of other elements, such as Users, Attribute Types, Rules, etc. For this reason, using the Feed Deployer to "redeploy" feeds after the initial deployment for testing or other purposes is not supported at this time.

App Delivery

A ThreatConnect instance can act as a server that will deliver any supported App to a client's system. Thus, QA servers can be configured as App-delivery servers, allowing clients to connect to a particular machine and have Apps delivered to them. The primary catalog server for this feature is hosted at **https://api.threatconnect.com**.

Configure the Machine Acting as a Server

1. Navigate to the **System Settings** screen (Figure 1) and click **Apps** in the menu on the left side of the screen.
2. Configure the following settings:
   - **appCatalogServer**: Select the **Enabled** checkbox.
   - **appCatalogServerURL**: Leave this field blank to have the machine act as a server.
   - **appDeliveryToken**: Leave this field blank to have the machine act as a server.
3. Navigate to the **TC Exchange Settings** screen (Figure 49). Refer to the "View Installed " section for more information on how to search for and filter installed Apps.
4. The **Catalog** tab displays available Apps on the remote catalog server that may be installed for the client. This tab is disabled when the machine is acting as a server.
5. The **Updates** tab displays available App updates that can be accessed by the client. This tab is disabled when the machine is acting as a server.
6. The **Feeds** tab allows access to Apps data from created feeds.

Obtain the App Delivery Token From a Cloud Account

1. On the top navigation bar, hover the cursor over **Settings** and select **Account Settings**. The **Organizations** tab of the **Account Settings** screen will be displayed.
2. Select an organization to display the **Membership** tab of its **Organization Settings** screen (Figure 2).
3. Click the **Apps** tab. The **Apps** screen will be displayed (Figure 53).

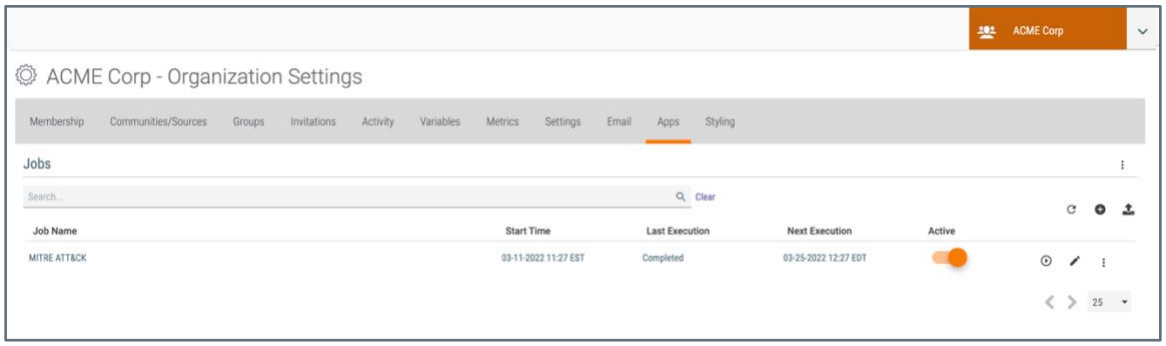

Figure 53

4. Click the vertical ellipsis ⋮ above the **Import Job** icon, and select **App Delivery**. The **App Delivery Token** window will be displayed (Figure 54).

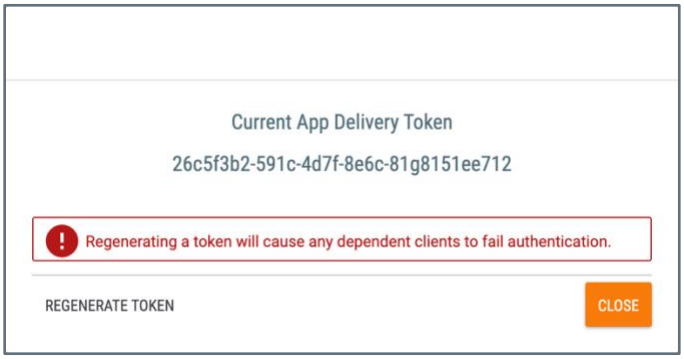

Figure 54

5. Copy the token, and then click the **CLOSE** button.

Configure the Machine Acting as a Client

1. Navigate to the **System Settings** screen (Figure 1) and click **Apps** in the menu on the left side of the screen.
2. Configure the following settings:
   - **appCatalogServer**: Deselect the **Enabled** checkbox.
   - **appCatalogServerURL**: Enter the server machine API URL.
   - **appDeliveryToken**: Enter the App Delivery Token, which allows access by a specific Organization on the server to all the Apps to which it is entitled.

Catalog

Install an App from the Catalog

1. Navigate to the **TC Exchange Settings** screen (Figure 49) and click the **Catalog** tab. The **Catalog** screen will be displayed (Figure 55). This screen displays all Apps available in the system.

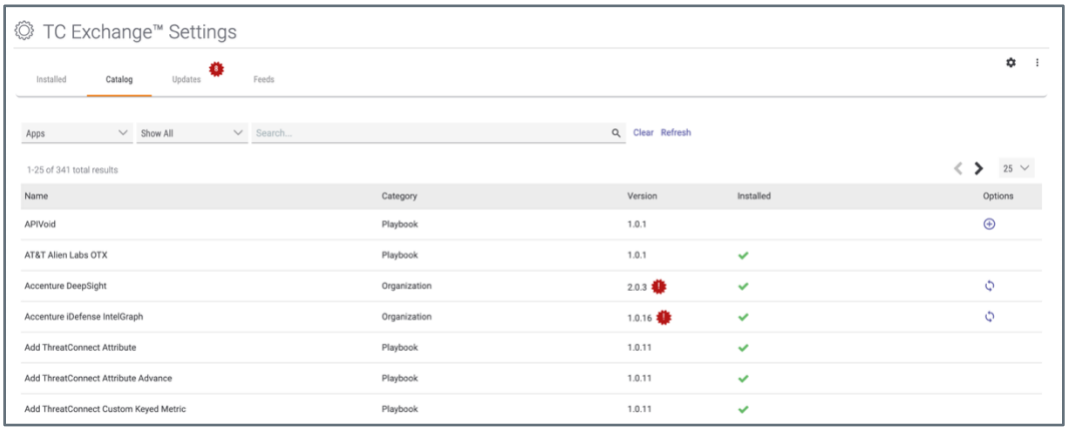

Figure 55

2. If an App is available, but has not been installed, the **Install** icon will be displayed in the **Options** column. Click this icon to install an App. The **Release Notes** window will be displayed (Figure 56).

Figure 56

- **Allow all organizations:** Select this checkbox to allow all Organizations on the ThreatConnect instance to have access to the App. If installing a Service App, it does not matter whether this checkbox is selected, as the Service itself, rather than the Service App, sets the permissions and access to the App.
- Click the **INSTALL** button.

If the App was installed successfully, a confirmation message will be displayed temporarily at the lower-left corner of the screen. Depending on the type of App installed, the **Feed Deployer** screen may also be displayed. See *The Feed Deployer* for instructions on how to deploy the newly installed App.

Updates

1. Navigate to the **TC Exchange Settings** screen (Figure 49) and click the **Updates** tab. The **Updates** screen will be displayed (Figure 57). This screen displays all the Apps that have a pending update available.

   Note: If there are one or more Apps with a pending update available, a notification with the message "TC Exchange Update Available: *‹App Name›*" will be displayed in the **Notifications Center** for each App.

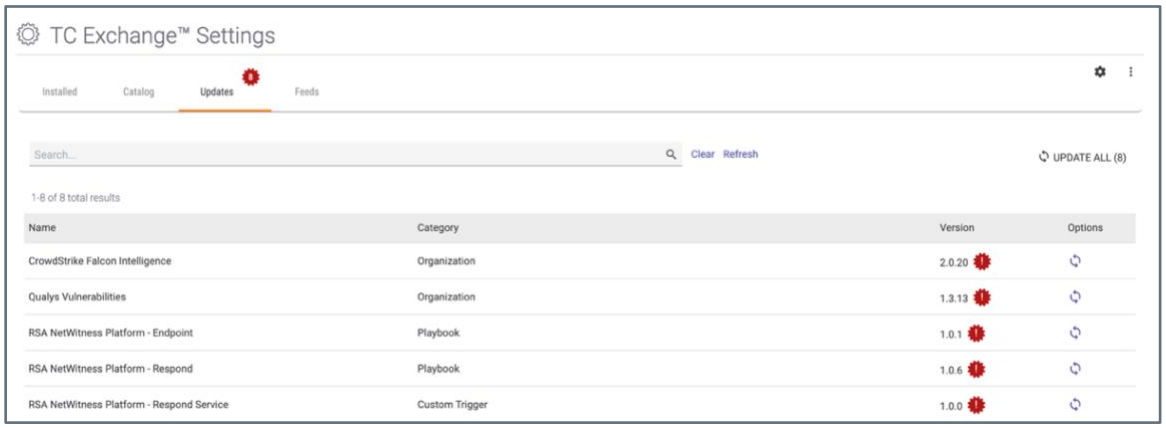

Figure 57

2. The **Update Available** icon will be displayed on the **Updates** tab for Apps with pending updates available. This icon will also be displayed next to an App in the **Catalog** table or the **Updates** table if an update is available.

   Note: If there are no updates available, the **Updates** tab will not be accessible.

3. Click the **UPDATE ALL** button at the top right of the screen to install all available updates. Alternatively, click **Update Now** in the **Options** column to update one App at a time. The **Release Notes** window will be displayed (Figure 56).
4. Click the **INSTALL** button to install the update.

Feeds

The **Feeds** tab allows access to Apps data from created feeds. As soon as the **appCatalogServer**, **appCatalogServerURL**, and **appDeliveryToken** System Settings are configured per the specifications in the "App Delivery" section, the **Feeds** tab will be populated with all available Feeds.

Activate a Feed

1. Navigate to the **TC Exchange Settings** screen (Figure 49) and click the **Feeds** tab. The **Feeds** screen will be displayed (Figure 58).

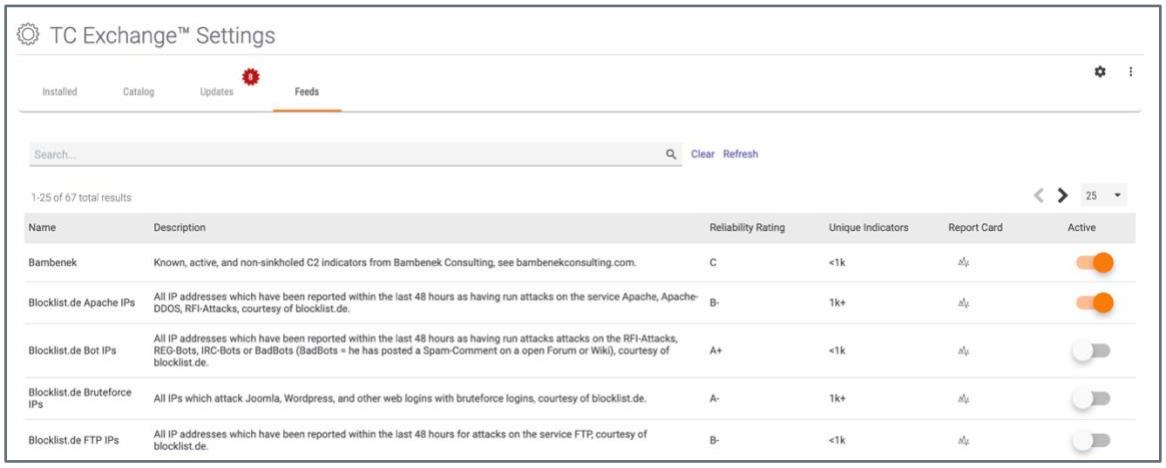

Figure 58

2. There are six columns for each feed. The **Reliability Rating** and **Unique Indicators** columns represent CAL data, which offers the user criteria for activating a feed.
3. The **Report Card** column also offers additional, CAL-generated data for users to determine whether they wish to activate a feed in their system. Click the **graph** icon, and a report card showing information containing metrics from other columns and how they compare with aggregated metrics from other feeds is displayed (Figure 59).

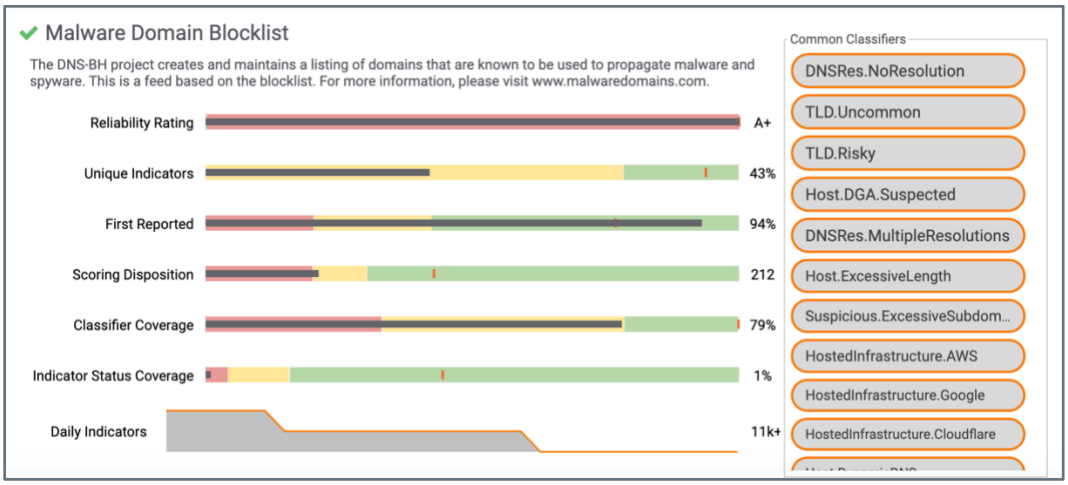

Figure 59

Important: CAL must be enabled in two places to get report card data. First, the CAL settings must be enabled in **System Settings**. (Refer to the information on CAL settings in the "Setting Descriptions" section of this guide for more information.) Second, the System Organization must be given permission to enable CAL data. To do so, navigate to the **Organizations** tab of the **Account Settings** screen, click the **pencil** icon for the System Organization, click the **Permissions** tab of the **Organization Information** window, and ensure that the checkbox for **Enable CAL Data** is selected.

4. Click the **gear** icon at the upper-right corner of the screen. The **App Delivery Settings** window will be displayed (Figure 60). Use the dropdown menu at the bottom of this window to select a **Default Feed Owner**.

Figure 60

5. To activate a feed, select an entry from the table and toggle the slider to on (orange) in the **Active** column. This action will create a ThreatConnect Source that will access all data for that feed.

6. To redeploy a feed, toggle the slider off in the **Active** column, delete the Job and Source in that Organization, and then log out and log back into ThreatConnect.

App Distribution

Important: Multi-environment orchestration must be configured and connected for the **App Distribution** option to be displayed in the menu.

1. Navigate to the **Installed** tab of the **TC Exchange Settings** screen (Figure 49) and enter the name of an App in the search bar. After the App is displayed in the search results, click the vertical ellipsis ⋮ in the **Options** column to view the App's **Options** menu.
2. Toggle the **Allow App Distribution** slider on (Figure 61).

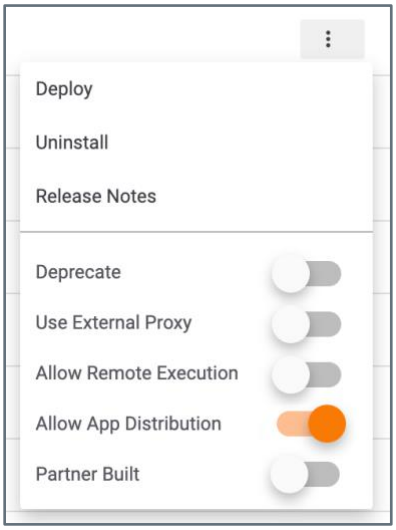

Figure 61

Jobs

Create a Job

1. Navigate to the **TC Exchange Settings** screen (Figure 49), click the vertical ellipsis ⋮ at the upper-right corner of the screen, and select **System Jobs**. The **System Jobs** screen will be displayed (Figure 62).

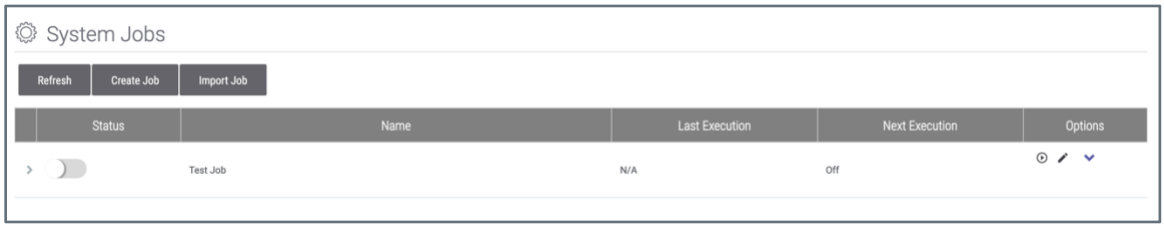

Figure 62

2. Click the **Create Job** button. The **Configure Job** window will be displayed (Figure 63).

> **Note**: Click the **Refresh** button to reload the list of Jobs.

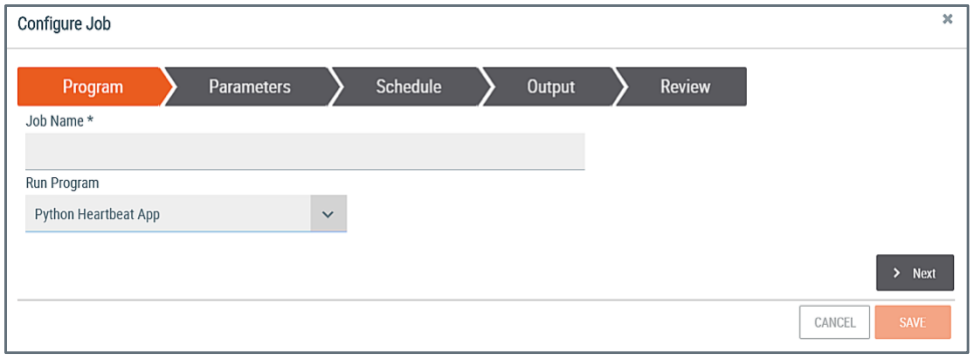

Figure 63

- **Job Name**: Enter a name for the Job.
- **Run Program**: Select a program (App).
- Click the **Next** button.

3. The **Parameters** screen will be displayed (Figure 64).

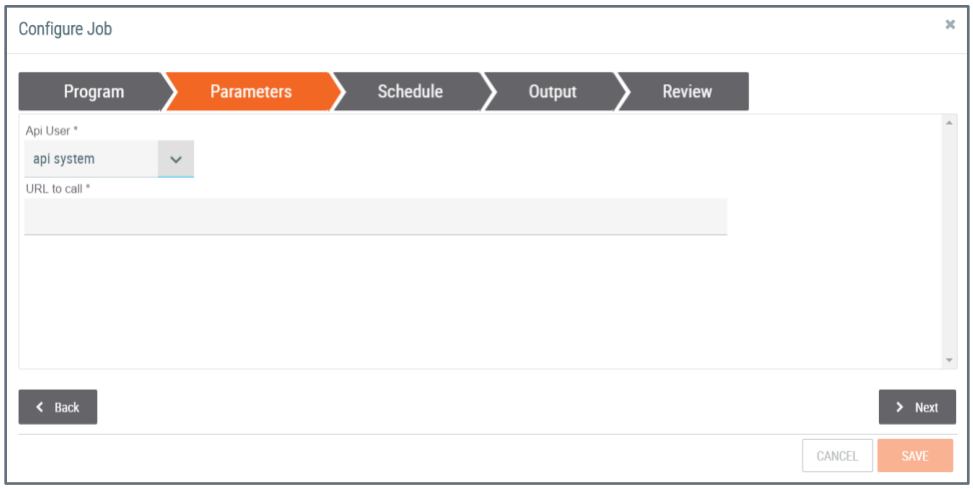

Figure 64

- Configure the parameters for the program. The parameters displayed on this screen will vary based on the program selected in Step 2.
- Click the **Next** button.

4. The **Schedule** screen will be displayed (Figure 65).

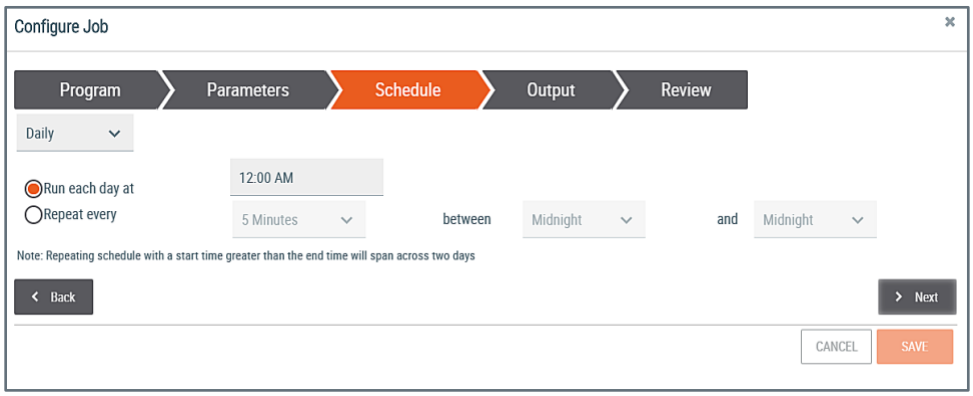

Figure 65

- **Daily**: Select whether the Job should run daily, weekly, or monthly.
- **Run each day at / Repeat every**: Enter the time of day on which to run the Job, or enter a time interval during which to repeat the Job.
- Click the **Next** button.

5. The **Output** screen will be displayed (Figure 66).

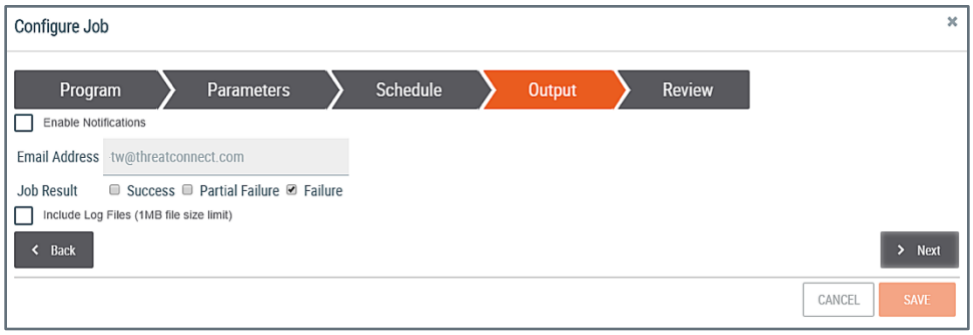

Figure 66

- **Enable Notifications**: Select the checkbox to enable notifications.
- **Email Address**: Enter the email address where notifications should be sent.
- **Job Result**: Select the Job results checkbox(es) for which notifications should be sent.
- **Include Log Files**: Check the box to include log files of 1MB or less in the notification email.
- Click the **Next** button.

6. The **Review** screen will be displayed (Figure 67).

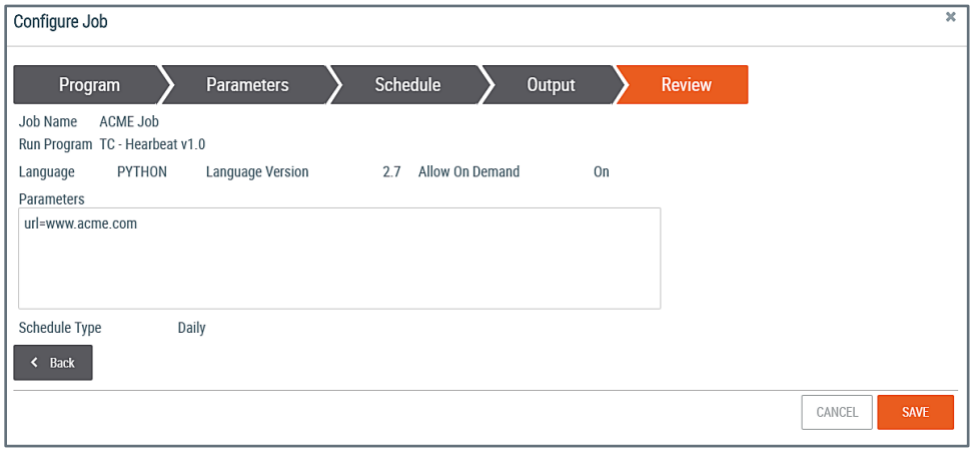

Figure 67

- Review the **Job Name**, **Run Program**, **Language**, **Language Version**, **Allow On Demand**, **Parameters**, and **Schedule Type** values to ensure they are correct.
- Click the **SAVE** button.

Edit or Run a Job

The following functions can be performed for an existing Job in the **System Jobs** table:

- Click **Run Now** to start a Job on demand.

  Note: A Job can be run On Demand only if "on demand" is enabled in the Job's configuration.

- Click **Edit** to edit a Job's setting.
- Click **Details** to view the **Details** menu with the following options:
  - **Delete**: Select this option to delete the Job.
  - **View Details**: Select this option to view the details for the Job, including the following parameters: **Program Name**, **Peak Memory** Usage, **Peak CPU** Usage, **Exit Message**, **Session Id**, **Server** Information, **Queued** Date, **Started** Date, **Completed** Date, and **Failed** Date.
  - **View Logs**: Select this option to view logs for the Job. Logs can be filtered by **Session ID**, **Level**, and **Message**.
  - **Add Attributes**: Select this option to add attributes to the Job.
  - **Published Files**: Select this option to display a list of links to files published by the Job.
  - **Export Job**: Select this option to export the Job in a JSON file format.

Dashboards

A dashboard is the control center of ThreatConnect. From a dashboard, users can view a variety of valuable data, including Recent History, Active Incidents, Open Tasks, Sources, Indicators, and Intelligence. ThreatConnect will initially be configured to display a default, System-level master dashboard, but a user can create new, customized dashboards to display any combination of data cards.

To create a System-level dashboard, log in as a System Administrator. Otherwise, a user can create a user-level dashboard, and an Organization Administrator can create an Organization-level dashboard. For more information on enabling custom dashboards in an Organization, see the "Configure an Organization Account" section of *ThreatConnect Account Administration Guide*.

Multi-Environment Orchestration

The multi-environment orchestrations feature allows users that have an Environment Server behind a firewall to use their Dedicated Cloud or Public Cloud instances to communicate with that server and run operations and applications within the firewall.

Configure the ThreatConnect Instance

1. Navigate to the **System Settings** screen (Figure 1) and click **Apps** in the menu on the left side of the screen.
2. Configure the following settings:
   - **appMessageBrokerHost**: Enter the domain name for the instance being used, plus the number of any available port in the system.

     Important: If this value is not set, the **Playbooks** menu on the top navigation bar will not display the **Environments** option.
   - **appMessageBrokerToken**: This token is used to secure the communications between the TC instance and the Environment Server. It is already set, so the user does not have to enter it.

Enable Playbooks Apps to Run in a Remote Environment

1. Navigate to the **TC Exchange Settings** screen (Figure 49), search for and select an App, and click the vertical ellipsis ⋮ in the **Options** column to view its **Options** menu (Figure 50).
2. Toggle the **Allow Remote Execution** slider on to enable remote execution for the App.

See *Multi-Environment Orchestration: Executing Playbook Apps Through a Firewall* for information on how to configure remote execution for Playbook Apps.

Workflow and Case Management

The Workflow feature in ThreatConnect allows users to combine manual and automated operations to define consistent and standardized processes for their security teams, including, but not limited to the following:

- Malware analysis
- Phishing triage
- Alert triage
- Intel requirement development
- Escalation procedures
- Breach SOP

Workflow in ThreatConnect supports the concept of Case Management, which gives users the capability to investigate and track information security threats and incidents by

- minimizing the time it takes to match a case to historical data;
- minimizing the time it takes to assess scope;
- minimizing the time it takes to assess impact;
- maximizing the amount of information that can be turned into actionable intelligence for later use.

For more information on the components of Workflow, see *Workflow Overview*.

Enable Workflow

1. Log into ThreatConnect with a System Administrator account.
2. On the top navigation bar, hover the cursor over **Settings** and select **Account Settings**. The **Organizations** tab of the **Account Settings** screen will be displayed.
3. Click **Edit** in the **Options** column of the Organization in which Workflow is to be enabled. The **Organization Information** window will be displayed (Figure 68).

Figure 68

4. Click the **Permissions** tab. The **Permissions** screen will be displayed (Figure 69).

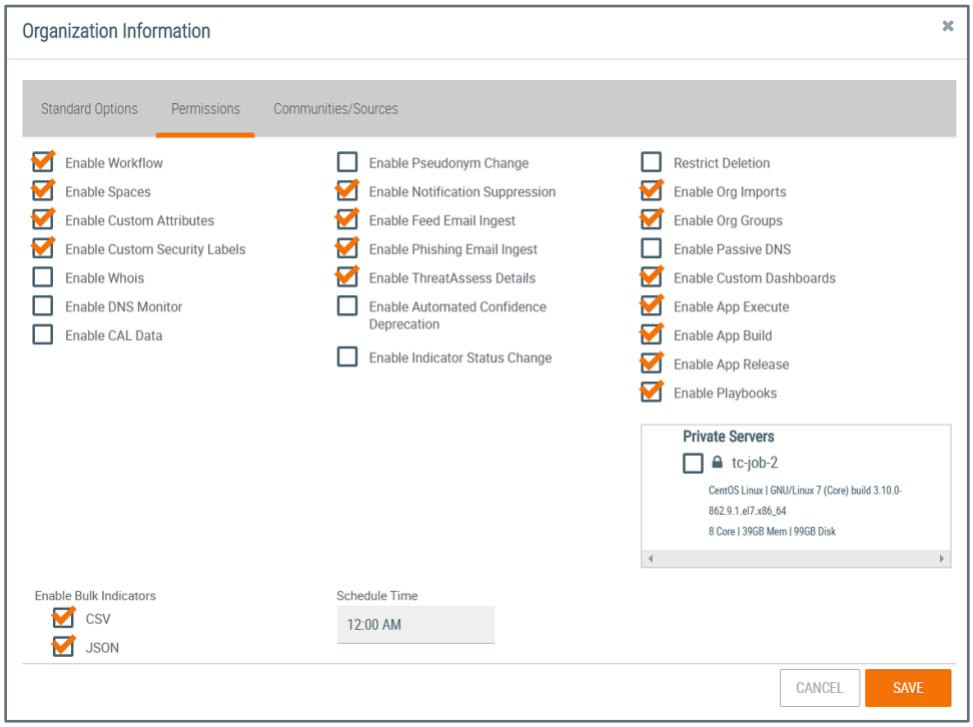

Figure 69

5. Select the **Enable Workflow** checkbox, and then click the **SAVE** button.

Import a Workflow Template

In addition to being able to install Workflow Templates via the **TC Exchange Settings** screen, System Administrators can import Templates into a ThreatConnect instance via the **Templates** screen (Figure 70). See the "Installing System-Level Templates" section of *The Templates Screen* for instructions on importing a Workflow Template.

Figure 70

Playbooks System Features

Playbooks allow users to automate cyberdefense tasks by passing data to Apps, which perform a variety of functions, including data enrichment, malware analysis, and blocking actions. Once enabled, Playbooks run in real time and provide users with detailed logs of each execution. The next set of sections covers Playbook functionality that can be executed only by a System Administrator. For additional details about Playbooks—specifically, about functionality that is not in the strict domain of a System Administrator, but can be executed by an Organization Administrator or other users, such as creating Playbooks, Workflow Playbooks, Playbook Templates, and Playbook Triggers—see *Playbooks*.

The Activity Screen

The Playbooks **Activity** screen is a control panel on which Organization Administrators and higher can monitor Playbook Server and Worker execution metrics, priorities, and processes for their instance. From this screen, current, present, and past Worker activity and allocation to Servers can be viewed and Playbook executions can be killed.

View and Manage the Playbooks Queue

The **Playbooks Queue** section of the Playbooks **Activity** screen provides the following information about the queue of Playbooks waiting for execution:

- **Queue Size:** the number of Playbooks in the queue, in real time.
- **Wait Time:** the estimated number of seconds a Playbook that just got added to the queue will wait before execution.
- **Queued Playbooks:** the Playbooks that are currently in the queue.
- **Completed Playbooks**: the number of Playbooks that have been completed.

1. Log into ThreatConnect with a System Administrator account.
2. On the top navigation bar, hover the cursor over **Playbooks** and select **Activity**. The **Activity** screen will be displayed (Figure 71).

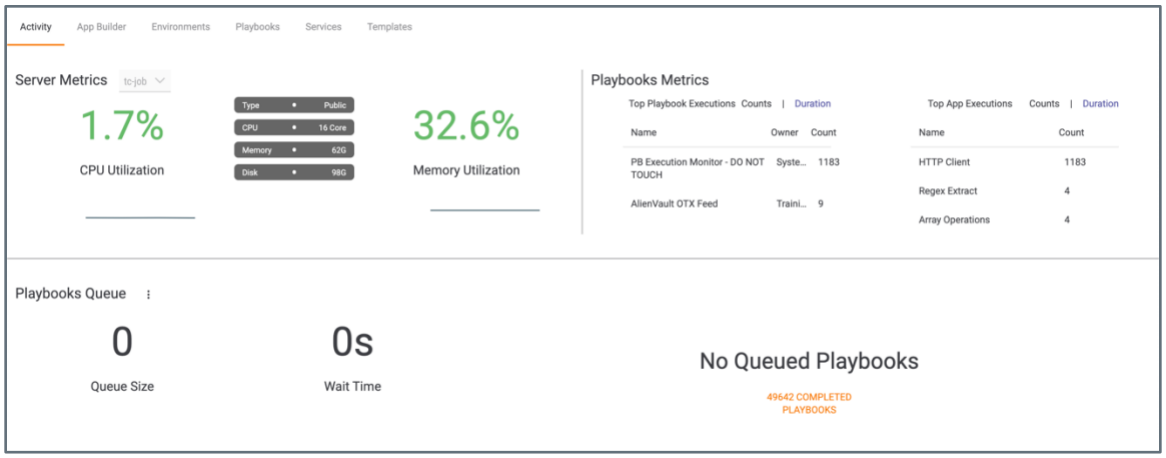

Figure 71

3. Click the vertical ellipsis ⋮ in the **Playbooks Queue** section of the screen. The following options will be available:
   - **Pause Queue:** This action prevents new Playbook executions from occurring.
   - **Resume Queue:** This action allows new Playbook executions to occur.
   - **Flush Queue:** This action removes all messages from the queue.

Change the Count for a Worker

A Playbook Worker is an embedded process in a Playbook Server responsible for executing orchestration logic in a queue. A Worker can execute only one Playbook at a time, and multiple Workers can exist inside a Playbook Server. Worker count can be changed on the Playbooks **Activity** screen by a System Administrator.

1. Log into ThreatConnect with a System Administrator account.
2. On the top navigation bar, hover the cursor over **Playbooks** and select **Activity**. The **Activity** screen will be displayed (Figure 71).
3. Click the vertical ellipsis ⋮ next to **Workers**, and then select **Change Worker Count**. The **Change Worker Count** window will be displayed (Figure 72).

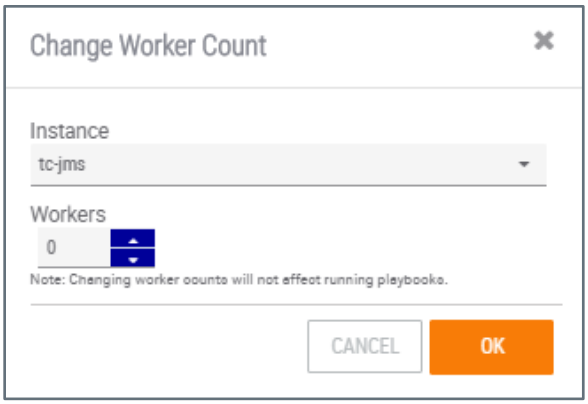

Figure 72

- **Instance**: Select the instance for which to change the Worker count.
- **Workers**: Enter the new Worker count.

  Important: If more Workers than the number permitted by the system license are added, the Worker count will not be increased. There will be no notification to this effect.

- Click the **OK** button.

The Environments Screen

The Playbooks **Environments** screen provides information to Organization Administrators and higher on the Environments available to their ThreatConnect instance and allows them to administrate the Environments from within their instance.

Creating an Environment

1. Log into ThreatConnect with a System Administrator account.
2. On the top navigation bar, hover the cursor over **Playbooks** and select **Environments**. The **Environments** screen will be displayed (Figure 73).

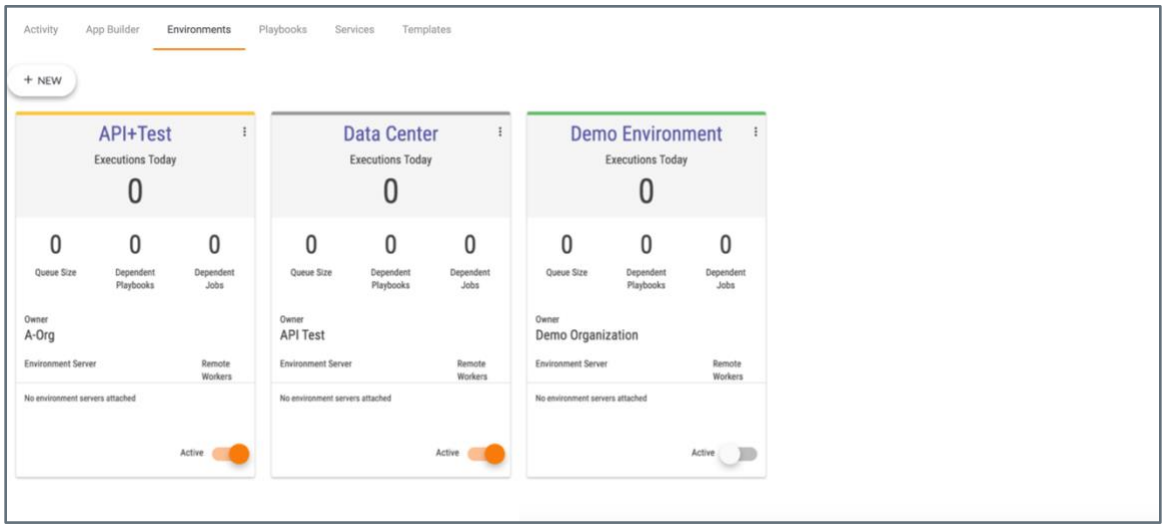

Figure 73

- An Environment can be activated by toggling the **Active** slider at the bottom left of the Environment card on.
- An Environment can be deactivated by toggling the **Active** slider at the bottom left of the Environment card off.
- If an Environment has not been connected to an Environment Server, then **No Environment servers attached** will be displayed at the bottom of the Environment card.
- The color of the top border of the Environment card reflects the following color scheme:
  - **Green:** The Environment is active and configured to an Environment Server.
  - **Yellow**: The Environment is active, but not configured to an Environment Server.
  - **Gray:** The Environment is inactive.

3. To create a new Environment, click the **+ NEW** button. The **New Environment** screen will be displayed (Figure 74).

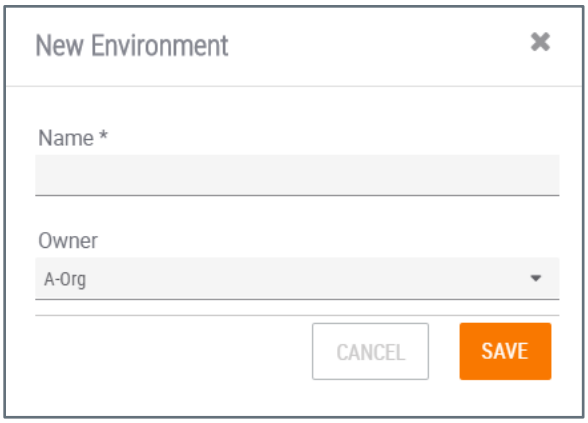

Figure 74

- **Name:** Enter a name for the Environment.
- **Owner:** Select the Organization that will own the Environment.
- Click the **SAVE** button.

Playbook Services

Apps normally run for a specified period of time. Service Apps, or Services, however, are microservices that continuously run in the background. See *Playbook Services* for instruction on how to create, administrate, and use Services.

Note: The **JS Report** REST API Service is toggled on by default and should remain that way so that users can leverage the **Preview PDF** feature when creating reports.