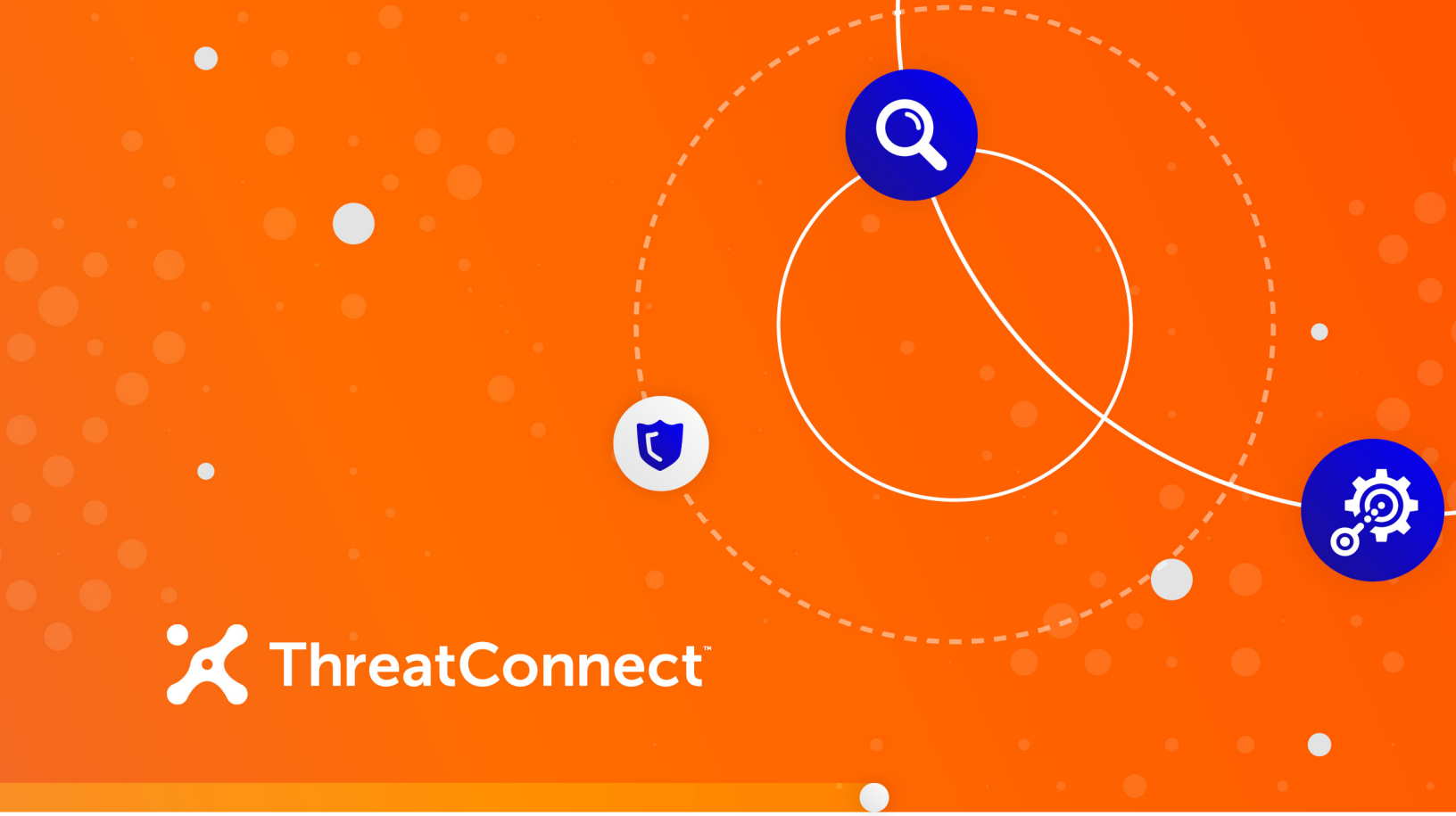

ThreatConnect™

System Administration

User Guide

Software Version 6.1

February 24, 2021

10013-13 EN Rev. A

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

P: 1.800.965.2708 | F: 1.703.229.4489
www.ThreatConnect.com

Table of Contents

System Administration

Getting Started

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 section explains many of the tasks requiring system privileges.

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.

System Account Familiarization

Log in with a System Administrator account, and on the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2).

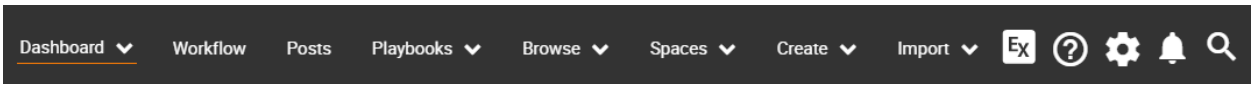

Figure 1

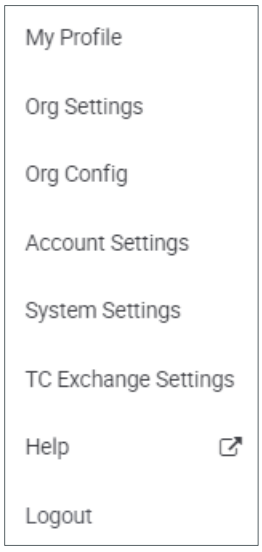

Figure 2

Table 1 provides an overview of the **Settings** menu options.

Table 1

Setting Types	Description
My Profile	Use this option to configure basic user settings for this account, including password changes.
Org Settings	Use this option to create and configure other user accounts within the Organization. Typically, these are other System Administrator accounts.
Org Config	Use this option to modify Attributes, Indicator Exclusion Lists, Security Labels, and Deprecation for a given Organization.
Account Settings	Use this option to create, configure, and manage all Organizations and accounts within an On Premises Instance.
System Settings	Use this option to configure System-wide properties for On Premises Instance.
TC Exchange™ Settings	Use this option to view loaded apps, to install apps, and to configure System Jobs, among other features.
Help	Use this option to access the ThreatConnect Knowledge Base in a new window.
Logout	Use this option to log out of ThreatConnect.

This section focuses on the system-wide tasks that are performed primarily in **System Settings**. For further information on tasks performed in **Account Settings**, refer to the *ThreatConnect Account Administration User Guide*.

System-Level Accounts

Creating System-Level User Accounts

Follow these steps to create system-level user accounts:

1. Log in with a System Administrator Account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings**  icon and the **Settings** menu will appear (Figure 2).

3. Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).

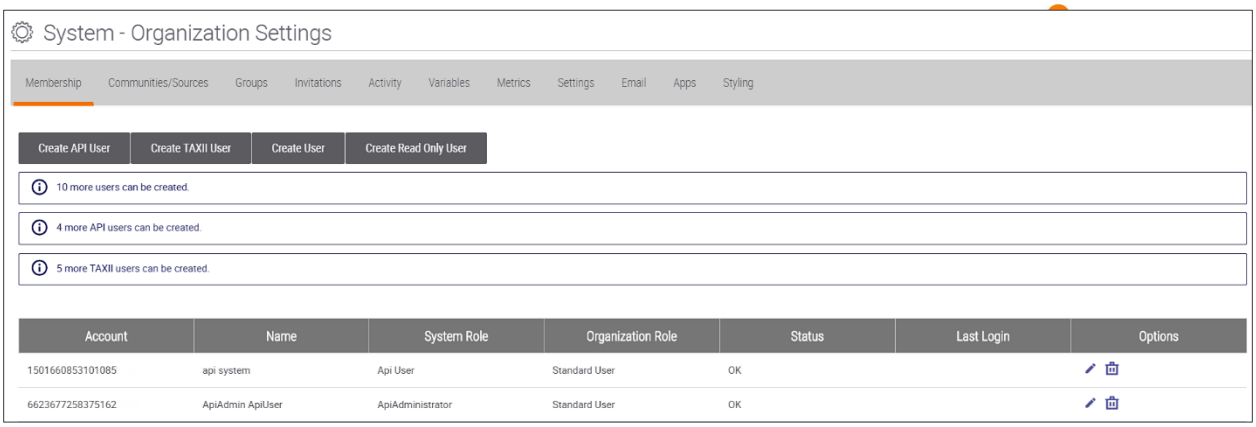

Figure 3

4. Click the **Create User** button, and the **User Administration** pop-up screen will appear (Figure 4).

NOTE: Above the Account table, the Organization Settings screen displays how many more users can be added by the Organization account.

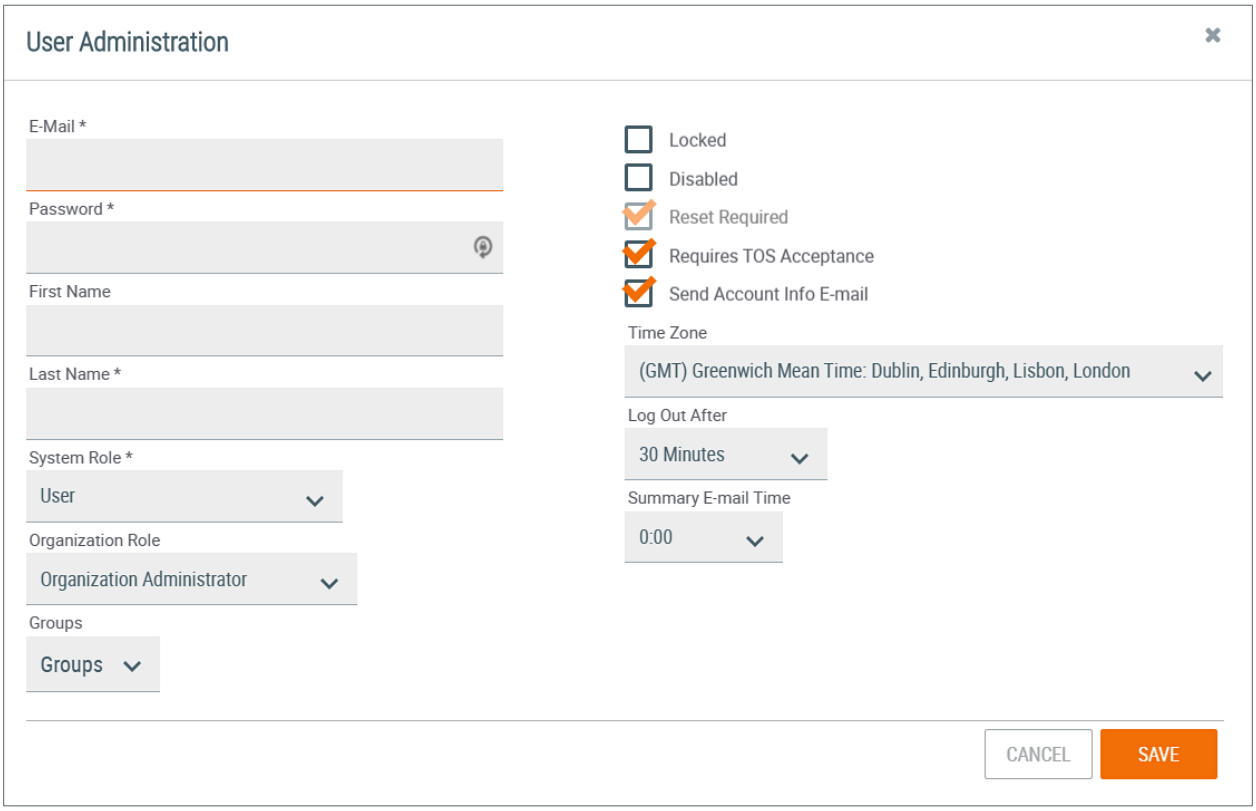

Figure 4

5. Fill in the required fields in order to create and configure the user account.
    a. **E-Mail**: Click in the box to enter an email address that will also be the name of the user account.
    b. **Password**: Click in the box to set the initial user password in this field, which is subject to the ThreatConnect password policy defined within the system settings.
    c. **First Name**: Click in the box to 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.
    d. **Last Name**: Click in the box to 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.
    e. **System Role**: Click on the drop-down menu to select one of the following System roles—Read Only User, Community Leader, Accounts Administrator, User, Operations Administrator, ApiAdministrator, or Administrator.
    f. **Organization Role**: Click on the drop-down menu to select one of the following roles—Organization Administrator, Read Only User, App Developer, Standard User, Sharing User, or Read Only Commenter.
    g. **Groups**: Click the drop-down menu to enter a Group for which to search.
    h. **Locked**: Click on the box if it is checked in order to unlock a user account that has been locked by ThreatConnect.
    i. **Disabled**: Click the checkbox to disable a user account, which is typically done when a user no longer requires ThreatConnect access and the Administrator wishes to retain log integrity.
    j. **Reset Required**: Click the checkbox to force a user to change the account password upon next login. This box is checked by default upon account creation, and it is unchecked once the password has been changed.

        NOTE: When initially creating the account, the Reset Required box cannot be unchecked. To uncheck the box, first create the account, edit it, and uncheck the setting, which enforces tighter security.
    k. **Requires TOS Acceptance**: Click the checkbox to reset the "terms of service" flag, so the user is presented with the terms of service again.

        NOTE: This setting must be set to "true" in the System Settings screen in order for the checkbox to appear.
    l. **Send Account Info E-mail**: Click the checkbox to send an email with the account information to the specified email address.
    m. **Time Zone**: Click on the drop-down menu to select the appropriate time zone.
    n. **Log Out After**: Click on the drop-down menu to select a time interval upon which a user will be logged out after a corresponding period of inactivity.

o. **Summary E-mail Time**: Click on the drop-down menu to set the time at which a user account will receive daily summary emails of followed items, or other notifications, from ThreatConnect.

6. Click the **SAVE** button to create the User account.

To create **Read-Only** user accounts, follow the preceding steps, but click the **Create Read Only User** button in Step 4. Note that the Organization Role is locked, and such users that join a Community or Source will have read-only permissions. A benefit to creating Read-Only Users is that they do not count against Organization limits.

Modifying Account Settings

Follow these steps to administer or change settings of an existing Organization user account:

1. Log in with a System Administrator Account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2).
3. Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
4. Click the **Edit** icon to the right of an entry in the table, and the **User Administration** screen will appear (Figure 5).

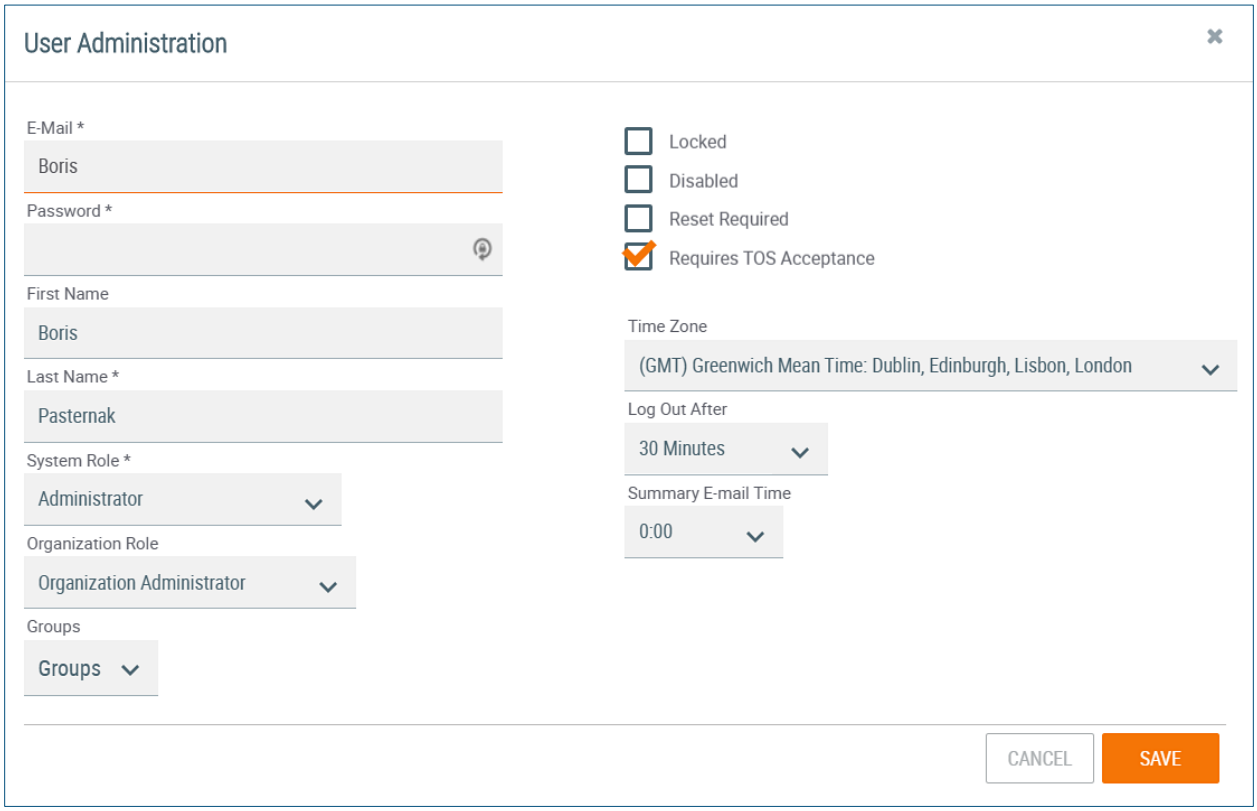

Figure 5

5. Modify any of the desired fields and click the **SAVE** button.

Editing User Profiles

Follow these steps to edit any field on an account's User Profile:

1. Log in with a System Administrator Account.
2. On the top navigation bar (Figure 1), place the cursor on the` **Settings** icon and the **Settings** menu will appear (Figure 2).
3. Select **Org Settings**, and the **Organization Settings** screen will appear (Figure 3).
4. Click on an account name in the table, and the **User Profile** screen will appear (Figure 6).

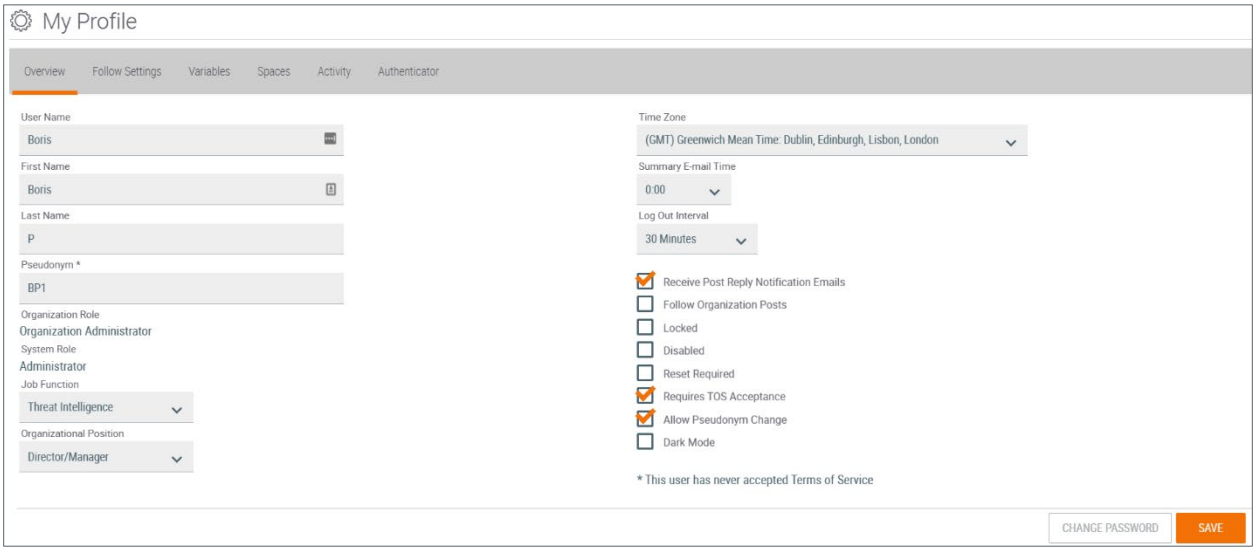

Figure 6

5. Edit any of the desired fields and click the **SAVE** button.

System Settings

Viewing and Modifying System Settings

Follow these steps to view and modify System Settings:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).

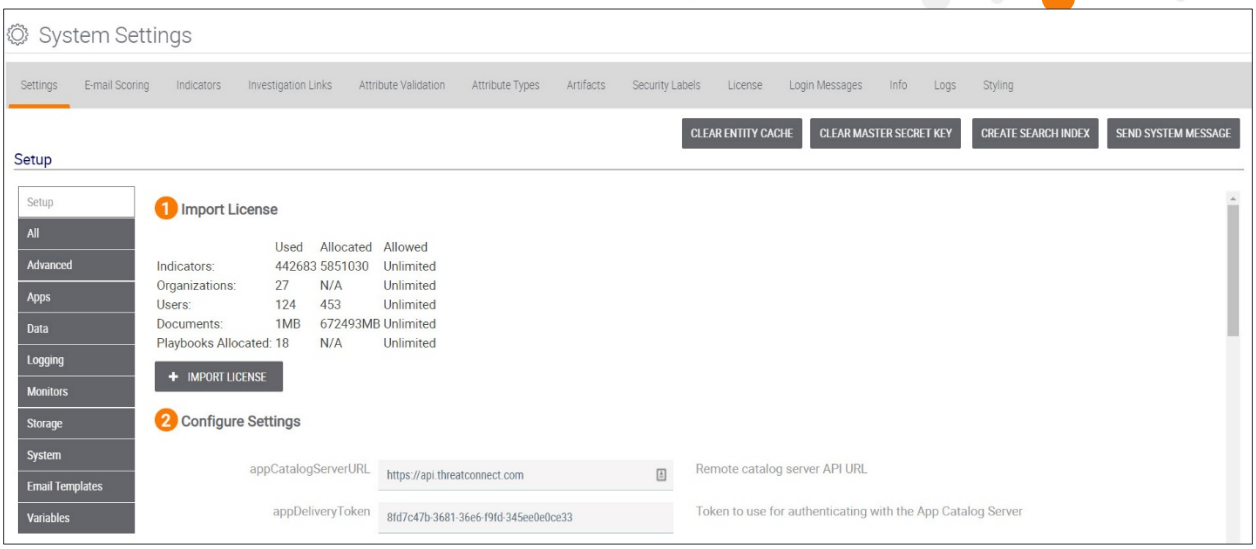

Figure 7

3. On the left-hand menu, click on the **ALL** button, and a list of settings, by category, will appear. Enter the required information in the pertinent fields to modify the setting.

Setting Descriptions

Provided as follows is a description of each system setting or group of settings:

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.

Acceptable Values: Boolean (true, false)

alertExpirationInterval

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

Acceptable Values: Positive whole numbers

alertRetentionTime

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

Acceptable Values: Positive whole numbers

allowUIErrorCollection

This setting determines whether or not UI error logs are sent to ThreatConnect.

allowOrganizationPublish

This setting determines whether or not an Organizations can create Publications (typically limited to Communities and Sources only).

appBuilderFileLimitMb

This setting specifies the maximum size allowed to store a single file in an app development project (Mb).

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.

Acceptable Values: Positive whole numbers

appMessageBrokerHost

This setting signifies the messaging broker host and port.

appsApiTokenKeepAliveOffsetSeconds

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

Acceptable Values: Positive whole numbers

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**).

NOTE: 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® 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. It is only used in Linux® installs.

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.

Acceptable Values: Boolean (true, false)

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.

Acceptable Values: Boolean (true, false)

bulkIndicatorOnDemandEnabled

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

Acceptable Values: Boolean (true, false)

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 Collective Analytics Layer (CAL), a feature that constantly monitors a user's interaction with the platform's native Indicators. The four CAL settings must be turned on to enable this feature.

CALHost

This setting identifies the hostname or IP address of the Collective Analysis Layer server.

CALMonitorEnabled

This setting enables the Collective Analysis Layer integration monitor.

caseResolutionList

[Containment Achieved, Deferred/Delayed, Escalated, False Positive, In Progress/Investigating, Not Specified, Rejected. Restoration Achieved]

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

componentForkPoolSize

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

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 (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 inodes threshold factor is reached.

diskSpaceMonitorInodeFileSystem

This setting indicates the filesystem where inodes are checked.

diskSpaceMonitor DaysToKeepDeleteFactor

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).

Acceptable Values: Positive whole numbers

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.

Acceptable Values: Boolean (true, false)

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.

Acceptable Values: Boolean (true, false)

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.

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 ID (e.g., A**CLBMQG9NSOILNSOIH8D**)

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: **[AP_NORTHEAST_1, AP_SOUTHEAST_1, AP_SOUTHEAST_2, CN_NORTH_1, EU_CENTRAL_1, EU_WEST_1, GovCloud, SA_EAST_1, US_EAST_1, US_WEST_1, US_WEST_2].**

documentAwsSecretKey

This setting determines the Secret Key used to authenticate to AWS for document storage.

Acceptable Values: Valid AWS Access ID

documentStorageFileLimit

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

Acceptable Values: Whole integers (e.g., 30 for 30 megabytes)

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, what type of storage to use (i.e., local or AWS).

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

elasticSearchCluster

This setting specifies the Elasticsearch cluster name. It must match the one specified in elasticsearch.yml.

elasticSearchEnabled

This setting determines whether the Elasticsearch® service is enabled.

Acceptable Values: Boolean (true, false)

elasticSearchUrl

This setting determines the URL for the Elasticsearch server.

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

emailEnabled

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

Acceptable Values: Boolean (true, false)

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.”

Acceptable Values: Positive whole numbers

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**

esBackupHour

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

escapeExternalLinks

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

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, placing the limit too high may result in failed import attempts.

Acceptable Values: Positive whole numbers

importLimitIndicatorFileSize

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

Acceptable Values: Positive whole numbers

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, placing the limit too high may result in failed import attempts.

Acceptable Values: Positive whole numbers

importSignatureTypes

This setting specifies the Signature file types allowed in the Signature upload.

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.

Acceptable Values: Boolean (true, false)

WARNING: 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 days to retain Indicator delete history.

indicatorExportLimit

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

Acceptable Values: Positive whole numbers

NOTE: 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.

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: Text value (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.

Acceptable Values: Positive whole numbers

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)

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.

Acceptable Values: Positive integer

loggingMaxFileSize

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

Acceptable Values: Positive integer

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.

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

logToElasticSearch

This setting turns on logging to Elasticsearch.

Acceptable Values: Boolean (true, false)

logToFile

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

Acceptable Values: Boolean (true, false)

logToSyslog

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

Acceptable Values: Boolean (true, false)

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.

mailInboundDomain

This setting specifies the mail domain for inbound email.

Acceptable Values: A valid host (e.g., **localhost**)

mailInboundEnabled

This setting enables the email-ingestion capability.

Acceptable Values: Boolean (true, false)

mailInboundEnableTLS

This setting determines whether or not TLS is enabled on inbound mail. If the **Enabled** box is checked, 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 or not TLS is required on inbound mail. If the Enabled box is checked, only inbound emails that come from SMTPS connections will be allowed.

managementAPISubscriberInterval Seconds

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.

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.

Acceptable Values: Boolean (true, false)

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.

Acceptable Values: Positive whole number

passwordLower

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

Acceptable Values: Positive whole number or zero

passwordMinimum

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

Acceptable Values: Positive whole number or zero

passwordNumber

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

Acceptable Values: Positive whole number or zero

passwordSpecial

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

Acceptable Values: Positive whole number or zero

passwordUpper

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

Acceptable Values: Positive whole number or zero

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.

playbookForkPoolSize

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

playbookVersionArchiveLimit

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

playbooksCompletedSessionDaysToKeep

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

playbooksDbHost

This setting specifies the Playbooks Redis DB host.

playbooksDbPort

This setting specifies the Playbooks Redis DB port.

playbooksDefaultRoiDollarsPerHour

This setting specifies the default ROI dollars per hour.

playbooksDefaultRoiMinutes

This setting specifies the default ROI minutes.

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 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 (TRACE, DEBUG, INFO, WARN, ERROR, or 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.

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.

Acceptable Values: Boolean (true, false)

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: Text value (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.

Acceptable Values: Boolean (true, false)

reverseWhoisInterval

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

Acceptable Values: Positive whole number

reverseWhoisMonitorConcurrency

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

Acceptable Values: Positive whole number, typically 1

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.

Acceptable Values: 0–24

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: Text (should be the desired System's URL)

sourceFeedMonitorEnabled

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

Acceptable Values: Boolean (true, false)

sourceFeedMonitorInterval

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

Acceptable Values: Positive whole numbers

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.

Acceptable Values: Positive whole numbers

synchronousBatchSaveLimit

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

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.

Acceptable Values: Text

systemEmailAddressAccount

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

Acceptable Values: Text (should be a valid email address)

systemEmailAddressNotification

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

Acceptable Values: Text (should be a valid email address)

systemSubjectName

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

Acceptable Values: Text

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 **Public Cloud Instance** of ThreatConnect.

Acceptable Values: Text (should be a valid URL)

taskEmailMonitorEnabled

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

Acceptable Values: Boolean (true, false)

taskEmailMonitorInterval

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

Acceptable Values: Positive whole numbers

taxiiExchangeMonitorEnabled

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

Acceptable Values: Boolean (true, false)

taxiiExchangeMonitorInterval

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

Acceptable Values: Positive whole numbers

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.

Acceptable Values: Positive whole number

termsOfServiceRequireNewUserToAccept

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

threatAssessIntervalCount

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

Acceptable Values: Positive whole numbers

threatAssessMonitorEnabled

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

Acceptable Values: Boolean (true, false)

threatAssessMonitorInterval

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

Acceptable Values: Positive whole number

threatAssessRefreshInterval

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

Acceptable Values: Positive whole number

threatDeprecationMonitorEnabled

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

Acceptable Values: Boolean (true, false)

threatDeprecationMonitorInterval

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

Acceptable Values: Positive whole number

v3ApiCreateLimit

This setting specifies the maximum number of items that can be created at a time using the V3 API.

v3ApiBulkDeleteAllowed

When enabled, this setting determines whether or not bulk delete operations are available using the V3 API.

v3ApiReadLimit

This setting specifies the maximum number of items that can be read at a time using the V3 API.

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: Text (should be 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.

Acceptable Values: Boolean (true, false)

whoisMonitorInterval

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

Acceptable Values: Positive whole numbers

whoisRefreshInterval

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

Acceptable Values: Positive whole numbers

xpackAdminPassword

This setting specifies the X-Pack admin password.

xpackAdminUsername

This setting specifies the X-Pack admin username.

xpackSecurityEnabled

This setting turns On or Off X-Pack security for Elasticsearch on system.

Email Templates

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

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

Customizing Emails

Follow these steps to customize an email:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. On the left-hand menu, click the **EMAIL TEMPLATES** button, and the **Email Templates** screen will appear (Figure 8).

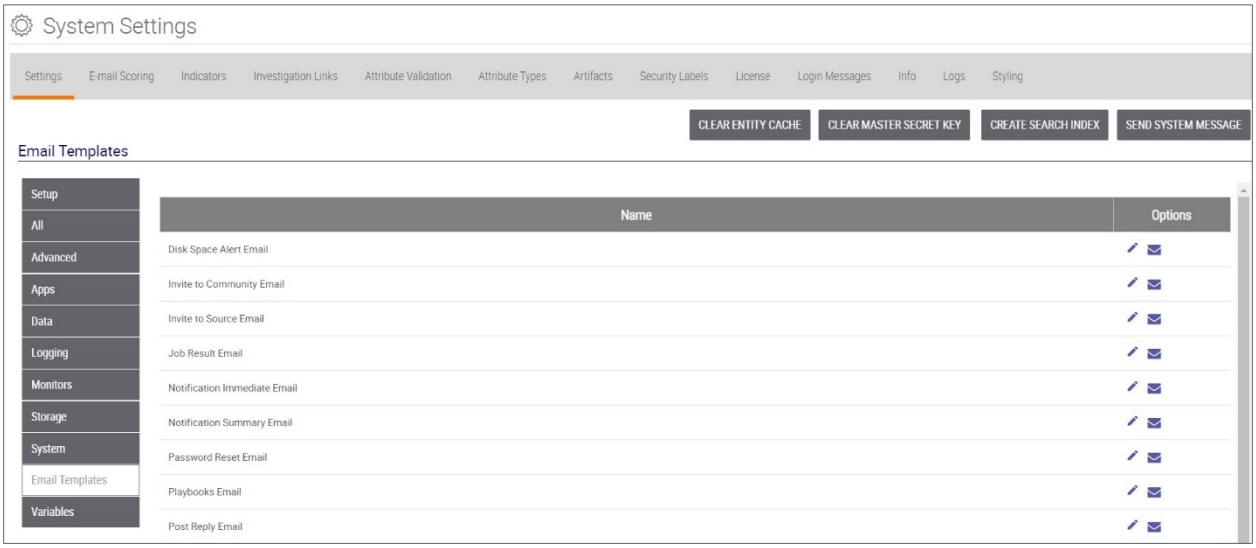

Figure 8

4. Select one of the Email Templates from the list (**Invite to Community Email** template is used in this example), and click on the **Edit** icon. The **Invite to Community Email** pop-up screen will appear (Figure 9).

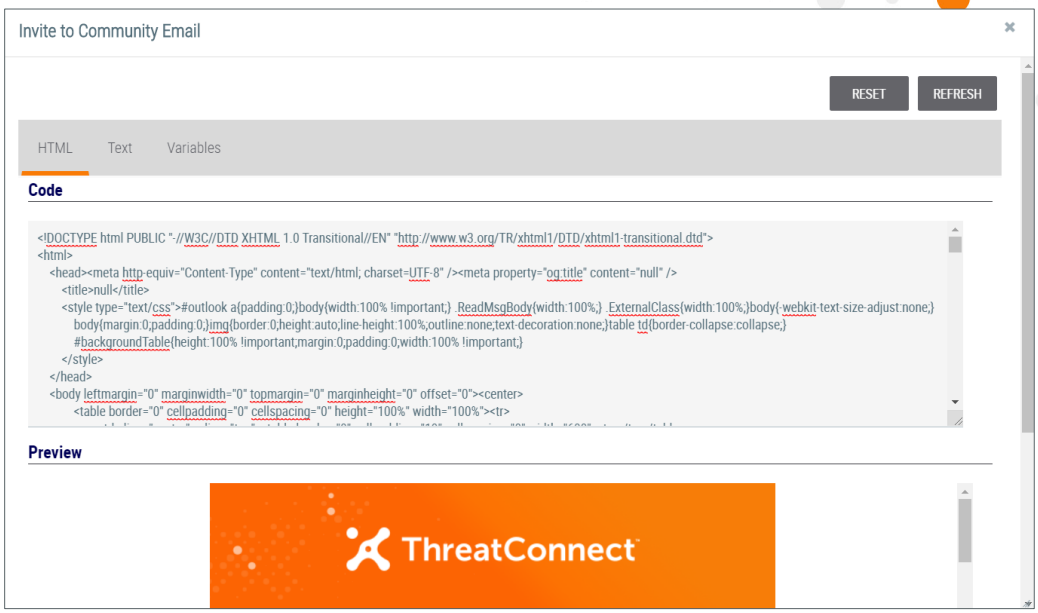

Figure 9

5. Click the **HTML** or the **Text** tab (for HTML- or text-supported emails), and enter the changes into the **Code** window.
6. Click the **Variables** tab to see a list of predefined variables. These variables are not configurable, but the **image 1-4** options allow the user to upload images that can be inserted into the email.
7. Return to the **HTML** or **Text** screen, and click the **REFRESH** button. The modified email will appear in the **Preview** or **Text Preview** window.
8. If satisfied with the changes, click the **SAVE** button. Otherwise, click the **RESET** button and the original text will appear.
9. To receive a system-generated email for review, click the **Test Email**  icon next to any of the Email Template choices, and the **Send Test Email** pop-up screen will appear (Figure 10).

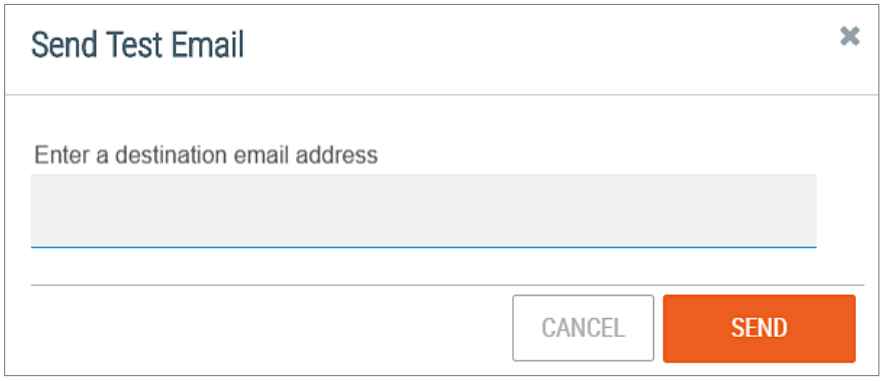

Figure 10

10. 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**.

Adding New Variables

Follow these steps to add a new variable:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. On the left-hand menu, click the **VARIABLES** button, and the **Variables** screen will appear (Figure 11).

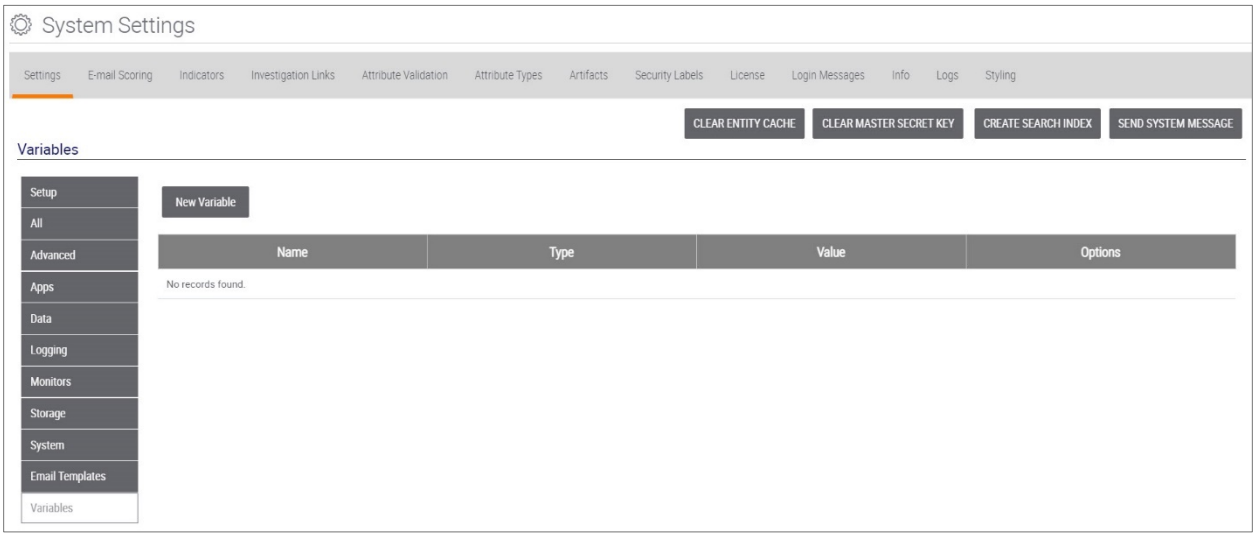

Figure 11

4. Click the **NEW VARIABLE** button, and the **Property** pop-up screen will appear (Figure 12).

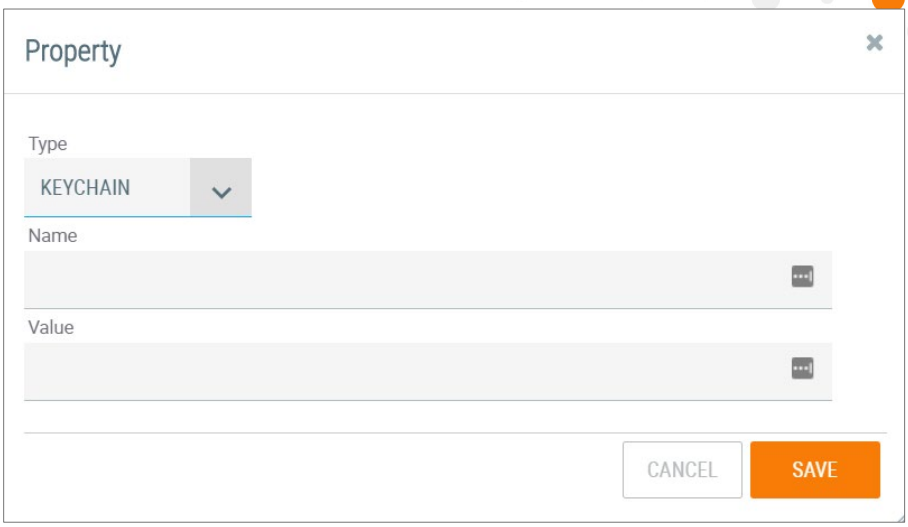

Figure 12

5. Enter the required information in the pertinent fields, and click the **SAVE** button.

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 **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.

Creating an Email-Scoring Rule

Follow these steps to create an email-scoring rule:

1. Log in with a System Administrator account.

2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).

3. Click the **E-mail Scoring** tab, and the **E-mail Scoring** screen will appear (Figure 13).

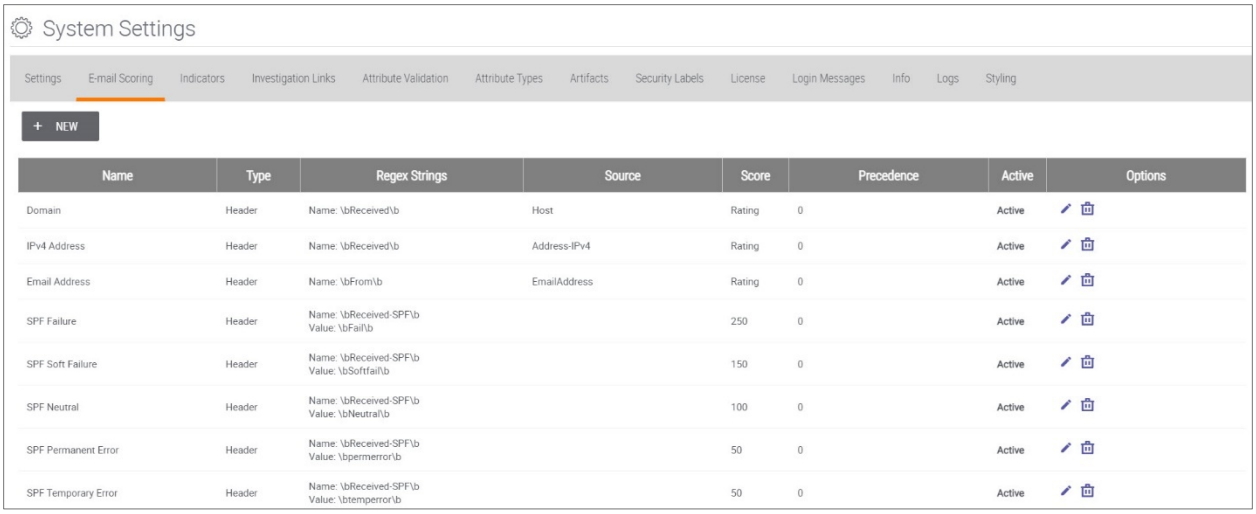

Figure 13

4. Click the **+ NEW** button, and the **E-mail Scoring Rule** pop-up screen will appear (Figure 14).

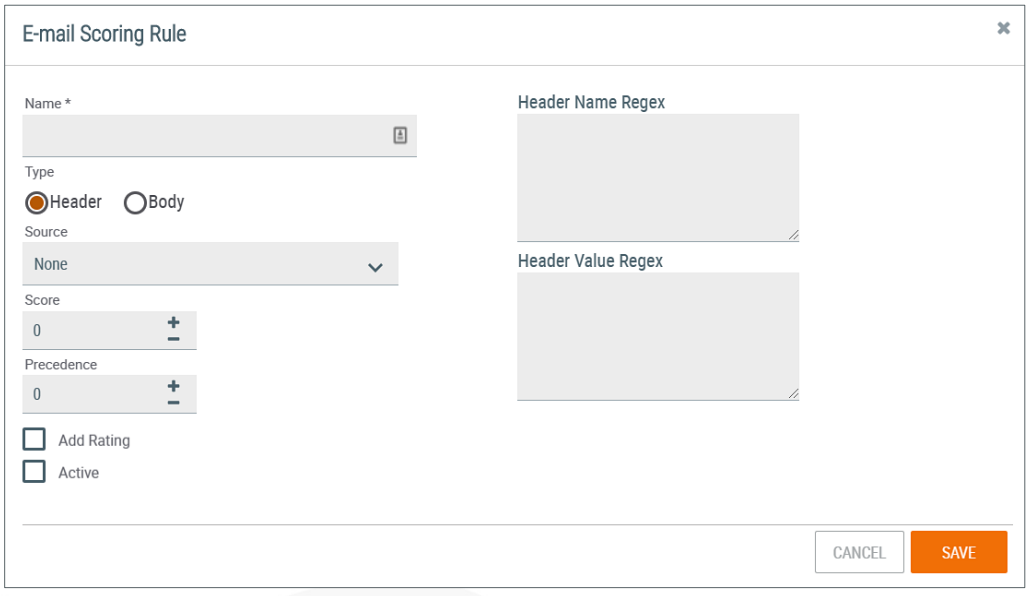

Figure 14

a. **Name**: Click in the box to set the name of the rule.

b. **Type**: Click on the **Header** or **Body** radio button to select the email component.

c. **Source**: Click on the drop-down menu to select an Indicator as the source of a rule's score, if this is a rule that will match on an Indicator string. If this is a rule that will match on a non-Indicator string, leave this field as **None**.

d. **Score**: Click in the box (or use the plus and minus signs) to manually enter a base score for the email if there is a match on the rule. Points may be added to the rule if the rule is matching on an Indicator and the Add Rating checkbox is selected.

e. **Precedence**: Click in the box (or use the plus and minus signs) to manually enter the Precedence value, which is used if two rules exist for different Indicator types. 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.

f. **Add Rating**: Click 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.

g. **Active**: Click the checkbox to specify whether the rule is active. If this box is unchecked, the rule will not be included in the Email-Scoring Engine.

h. **Header Name Regex (Header Only)**: Click in the box to input a Java-compatible regular expression that defines the email header field in which the header value will be found.

i. **Header Value Regex or Body Value Regex**: Click in the box to input a Java-compatible regular expression that defines the email header or body value that will result in a match for the rule.

5. Click the **SAVE** button to create the rule.

Editing an Email-Scoring Rule

Follow these steps to edit an email-scoring rule:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings**  icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **E-mail Scoring** tab, and the **E-mail Scoring** screen will appear (Figure 13).
4. Click on the **Edit**  icon for the rule that is to be edited, and the **E-mail Scoring Rule** pop-up screen will appear (Figure 14).
5. Configure the fields as appropriate.
6. Click the **SAVE** button to save any changes to the rule.

Indicator Validation

All Indicator-matching rules use Java-compatible regular expressions for pattern matching on Indicator creation and import. In ThreatConnect, there are currently twelve native Indicator types: Address, ASN, CIDR, Email Address, Email Subject, File (MD5, SHA1, SHA256), Hashtag, Host, Mutex, Registry Key, URL, and User Agent. 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.

Creating an Indicator Import Rule

Follow these steps to create an Indicator import rule:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Indicators** tab, and the **Indicators** screen will appear (Figure 15).

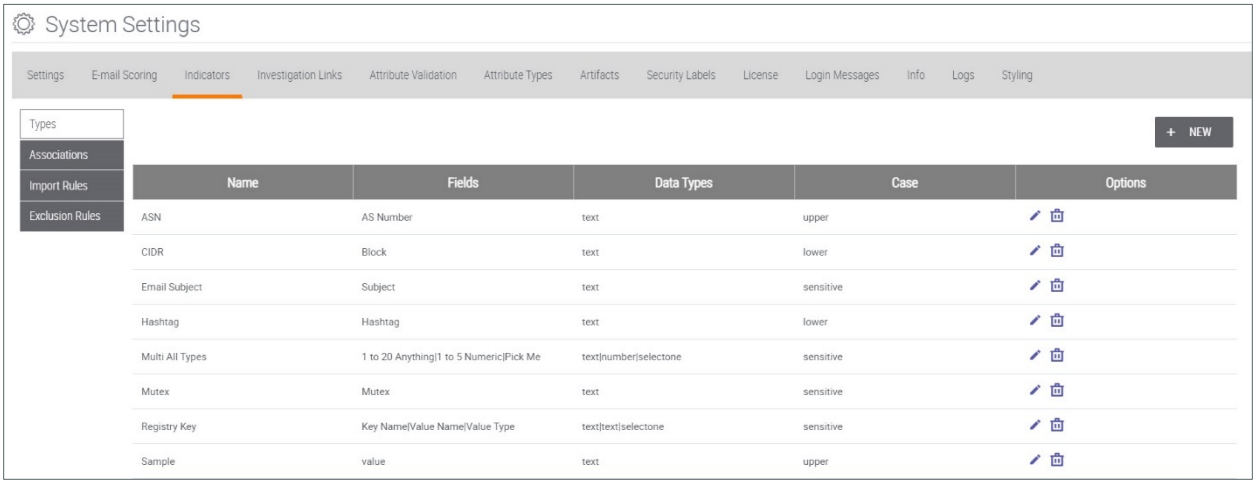

Figure 15

4. On the left-hand menu, click the **IMPORT RULES** button, and the **Import Rules** screen will appear (Figure 16).

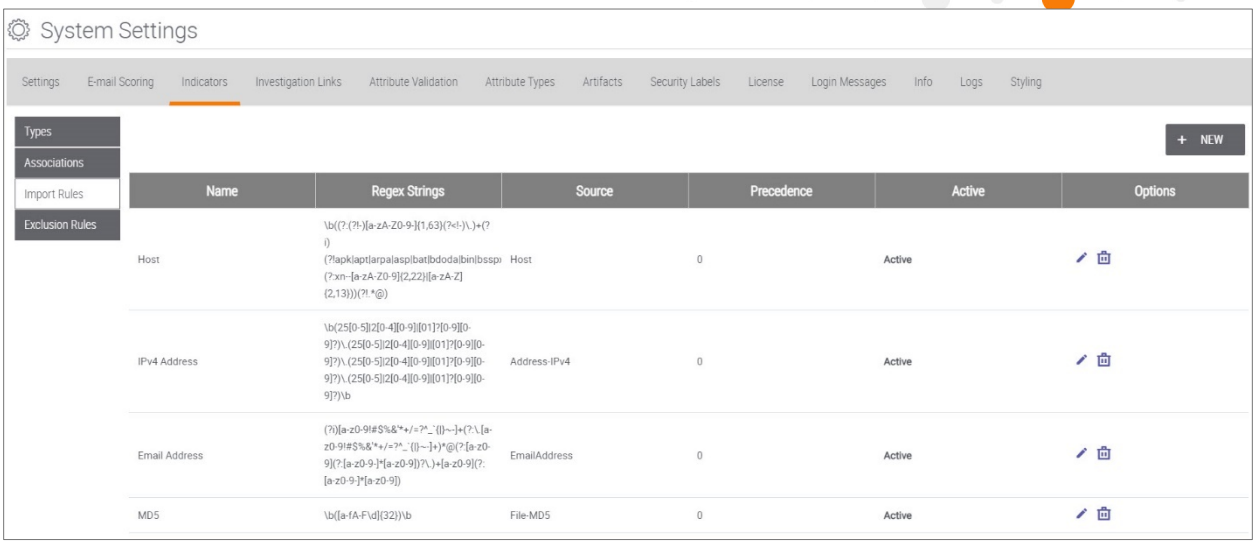

Figure 16

5. Click the**+ NEW** button, and the **Create Indicator Import Rule** pop-up screen will appear (Figure 17).

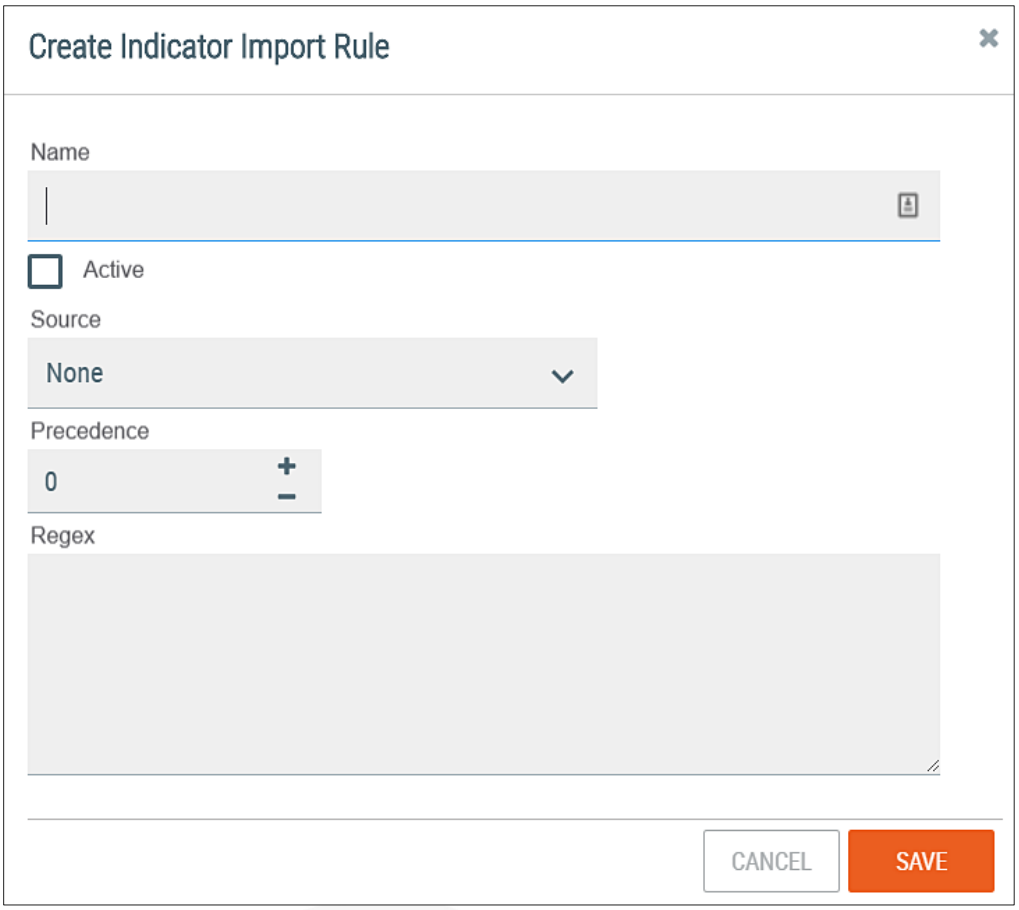

Figure 17

a. **Name**: Click in the box to enter the name of the rule.

b. **Active**: Click the checkbox to designate the rule as active. If unchecked, the rule will not be included for Indicator validation.

c. **Source**: Click on the drop-down menu to select the Indicator type on which the rule will match.

d. **Precedence**: Click in the box (or use the plus and minus signs) to manually 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. A rule with a higher Precedence value will be counted instead of a rule with a lower Precedence value.

e. **Regex**: Click in the box to input a Java-compatible regular expression to define the Indicator that will result in a match for the rule.

6. Click the **SAVE** button to create the rule.

Editing an Indicator Import Rule

Follow these steps to edit an Indicator import rule:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings**  icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Indicators** tab, and the **Indicators** screen will appear (Figure 15).
4. On the left-hand menu, click the **IMPORT RULES** button, and the **Import Rules** screen will appear (Figure 16).
5. Click on the **Edit**  icon for the rule to be edited. The **Create Indicator Import Rule** pop-up screen will appear, with pre-entered values for the given rule (Figure 18).

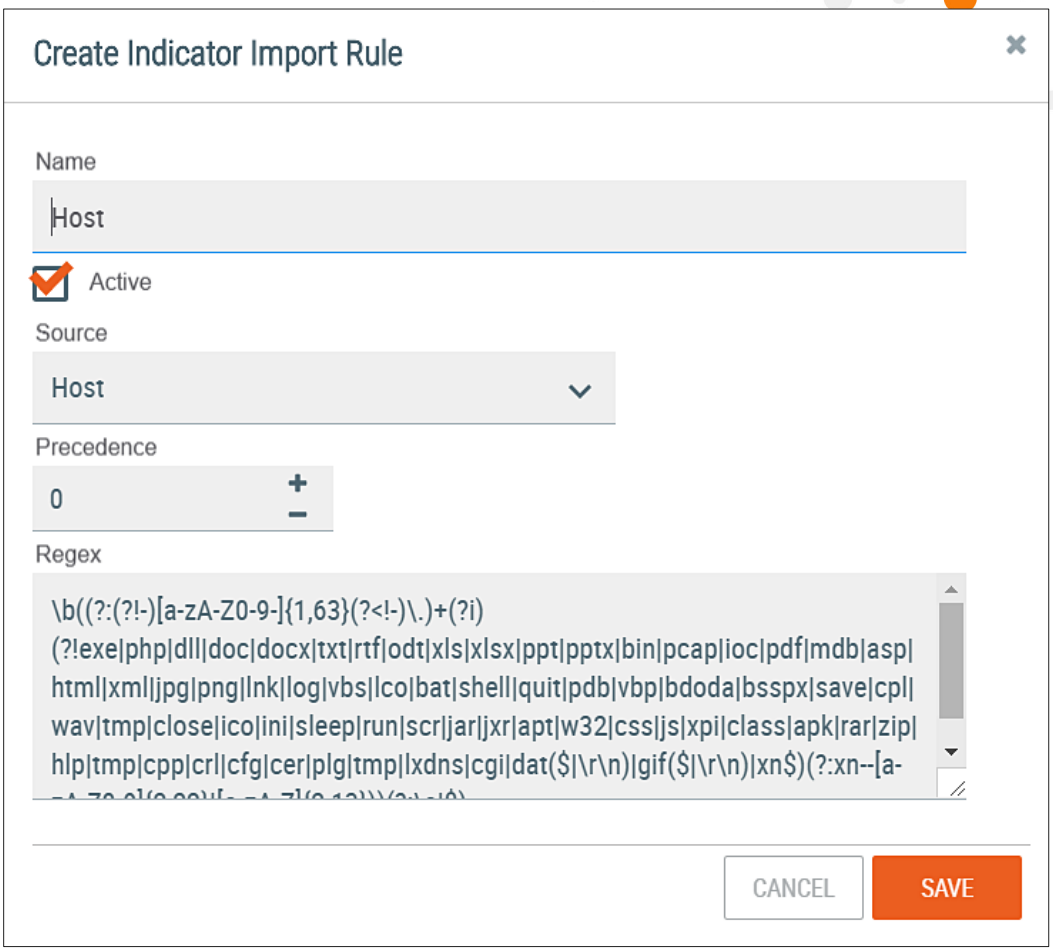

Figure 18

6. Configure the fields as appropriate.
7. Click the **SAVE** button to save any changes to the rule.

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. The ThreatConnect platform 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 2 displays a list of what is and is not blocked by an Indicator Exclusion list.

Table 2

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		✓

Creating System-Level Indicator Exclusion Lists

Follow these steps to create a System-level Indicator Exclusion list:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Indicators** tab, and the **Indicators** screen will appear (Figure 15).
4. On the left-hand menu, click the **EXCLUSION RULES** button, and the **Exclusion Rules** screen will appear (Figure 19).

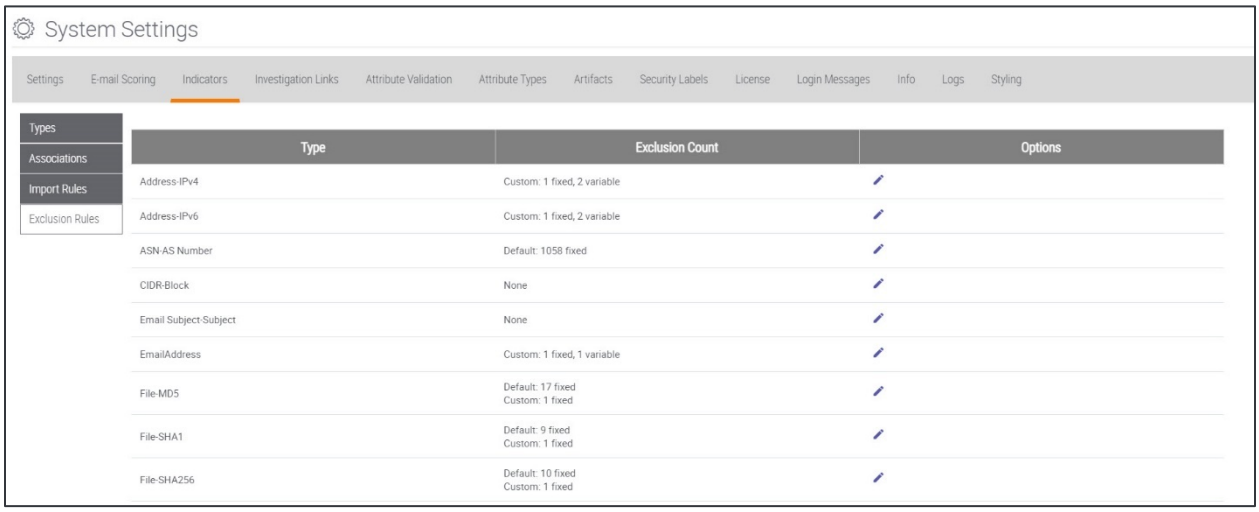

Figure 19

5. Click on the **Edit** icon for an Indicator from the **Type** column (Address-IPv6 for this example), and the **Exclusion Details** pop-up screen will appear (Figure 20).

Figure 20

6. If the toggle button on the upper right of the screen displays **Active**, then the **Default** Exclusion list on the left side of the screen will be used, in addition to any Indicators that have been added to the **Custom** Exclusion list on the right. If the toggle button is set to **Inactive**, then only the list on the **Custom** side will be used. Note that the list on the **Default** side cannot be modified.
7. When creating a new Exclusion List, enter the information directly into the **Custom** text box, and click the **SAVE** button.
8. Otherwise, click the **+ UPLOAD FILE** button to navigate to the appropriate directory. 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**.
9. Select the desired file, and the Exclusion list will be uploaded.
10. Click the **SAVE** button.
11. To modify an existing Exclusion list, edit it directly from the **Custom** text box. Otherwise, click the **DOWNLOAD** button to download and edit a file, and then click the **+ UPLOAD FILE** button to upload the edited file.
12. Click the **SAVE** button.

    NOTE: When trying to create an Indicator that has been placed on an Exclusion list, a message will appear in the Create pop-up screen warning that the Indicator is contained on a System-wide Exclusion list.
13. To remove an existing **Custom** Exclusion list, click the **CLEAR** button, and the **Remove Exclusions** pop-up screen will appear (Figure 21).

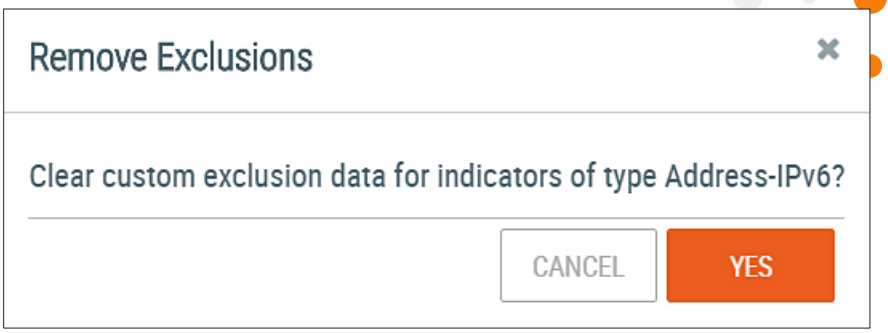

Figure 21

14. Click the **YES** button followed by the **SAVE** button.

Custom Indicator Types

For ThreatConnect users with a **Dedicated** or **On-Premise** 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 appear in menus and lists along with built-in Indicator types, and 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 User Agent strings generated by malicious binaries in HTTP traffic, they could create a User Agent custom Indicator type to store strings they may wish to filter and alert on in their Environment.

NOTE: 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.

NOTE: Also because of database constraints, custom Indicator regexes that do not constrain total character length are incompatible with custom Indicators.

NOTE: Custom Indicators may be edited or deleted by a System Administrator at any time.

Creating Custom Indicators

Follow these steps to create a custom Indicator:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Indicators** tab, and the **Indicators** screen will appear (Figure 15). The **TYPES** button will already be highlighted.
4. Click the **+ NEW** button, and the **Create Custom Indicator Type** pop-up screen will appear (Figure 22).

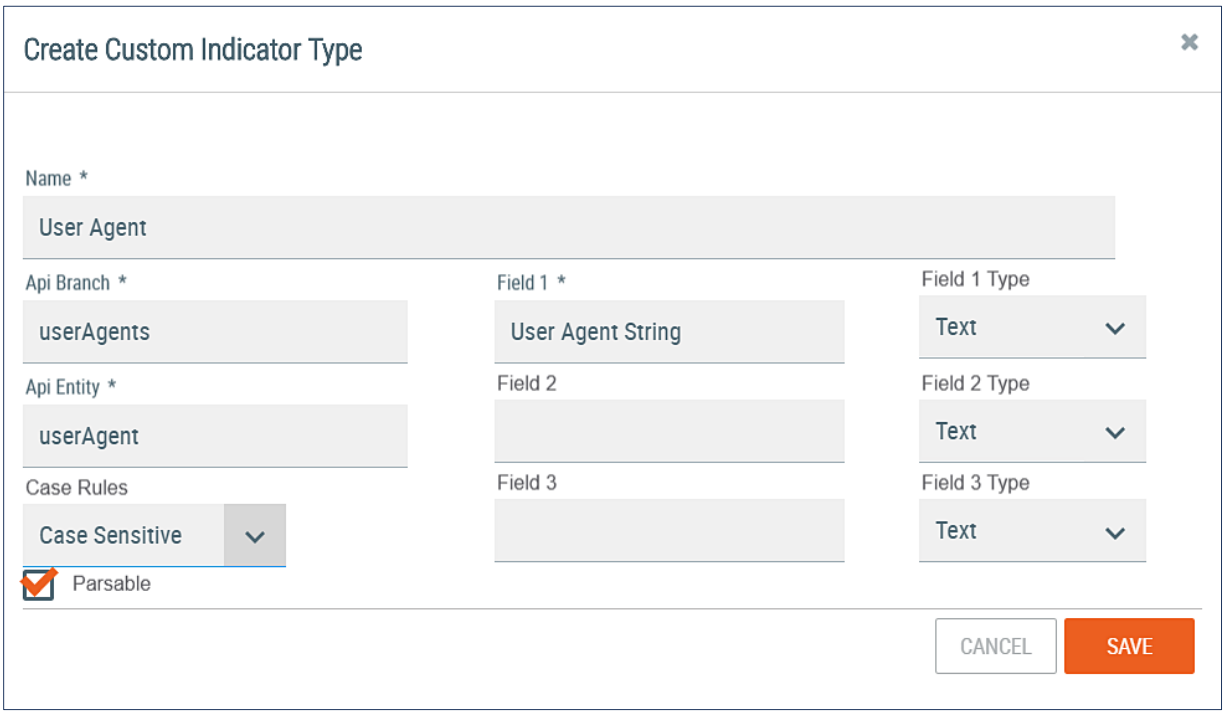

Figure 22

a. **Name**: Enter a name for the custom Indicator (e.g., **User Agent**). Once a custom Indicator has been created, its name may not be changed.

b. **Api Branch**: Set this parameter to the mapped API field in ThreatConnect, (e.g., **userAgents**).

c. **Api Entity**: Set this parameter to the mapped entity fields in ThreatConnect. In this case, the entity type would be **userAgent**.

d. **Case Rules**: Set the case rule for text fields, specifying whether the 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.

e. **Parsable**: Check this box to select whether 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.

f. **Field 1**: Set a label for the primary field (e.g., **User Agent String**).

g. **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 appear below the **Field 1 Type** box. Items entered into this box should be separated by semicolons.

NOTE: In this example, the User Agent String field would require the Type to be Text, while a credit card number would require the Type to be Number.

h. Optionally, configure secondary fields in the same manner as any of the primary fields. Secondary fields will be concatenated with the primary field, with the resulting value 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.

5. 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".

NOTE: For the "User Agent" example, it would make sense for Indicators with different capitalization to be treated as distinct Indicators.

Import Rules for Custom Indicator Types

Use the steps in the *Creating an Indicator Import Rule* 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 click 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 of the System Administrator's creation. The details of these associations are found on the **Browse** screen. Table 3 displays the built-in custom Associations provided by ThreatConnect.

Table 3

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

Creating Custom Associations

Follow these steps to create a custom Association:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Indicators** tab, and the **Indicators** screen will appear (Figure 15).
4. On the left-hand menu, click the **ASSOCIATIONS** button, and the **Associations** screen will appear (Figure 23).

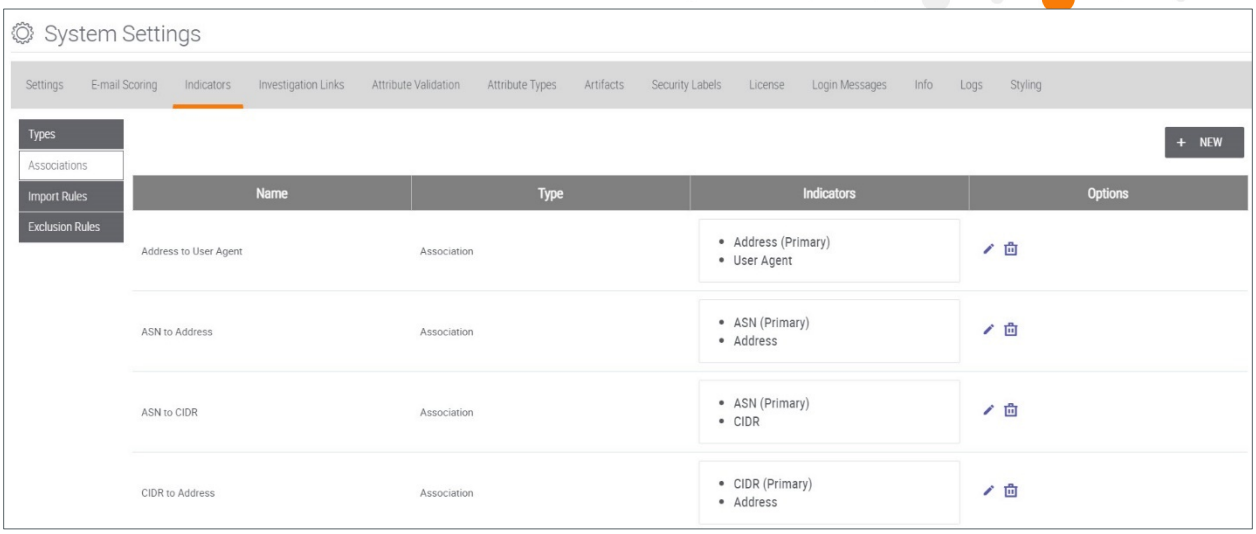

Figure 23

5. Click the **+NEW** button, and the **Create Custom Indicator Association** pop-up screen will appear with the **Association** radio button selected (Figure 24).

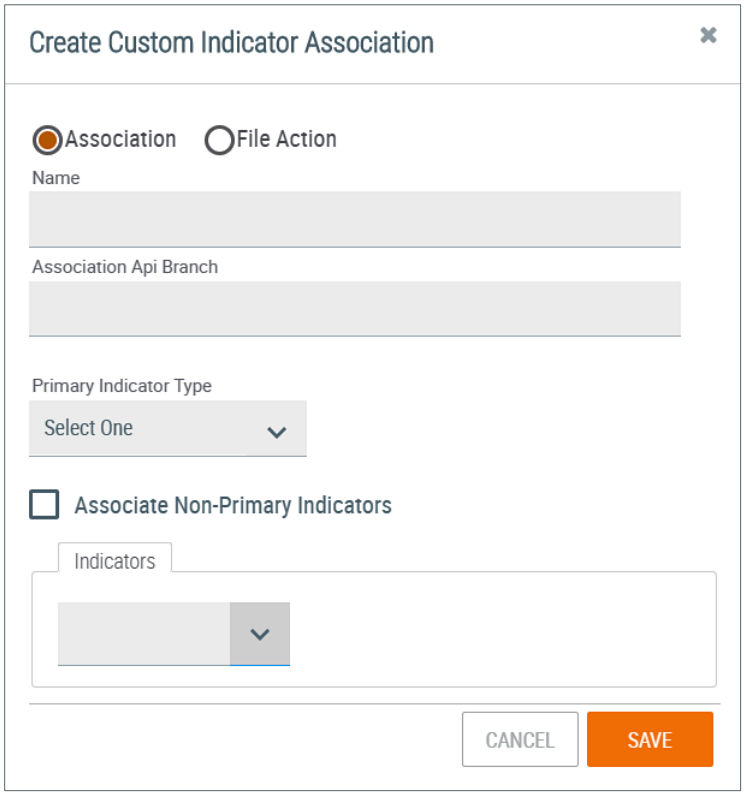

Figure 24

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

b. **Association Api Branch**: Set this parameter to the mapped API field in ThreatConnect, (e.g., **addressToCidr**).

c. **Primary Indicator Type**: Select the primary Indicator type.

d. **Associate Non-Primary Indicators**: Click this checkbox to allow non-primary Indicators that are associated with the primary Indicator to be associated with each other.

NOTE: If this box is not checked, 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 box is checked, non-primary Indicators of a given Indicator are also associated with each other.

e. **Indicators**: Click the drop-down menu to select one or more Indicators to associate with the primary Indicator type.

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

File Actions

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**.

Follow these steps to create a File Action:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings**  icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Indicators** tab, and the **Indicators** screen will appear (Figure 15).
4. Click the **ASSOCIATIONS** button, and the **Associations** screen will appear (Figure 23).
5. Click the **+NEW** button, and the **Create Custom Indicator Association** pop-up screen will appear with the **Association** radio button selected (Figure 24). Select the **File Action** radio button (Figure 25).

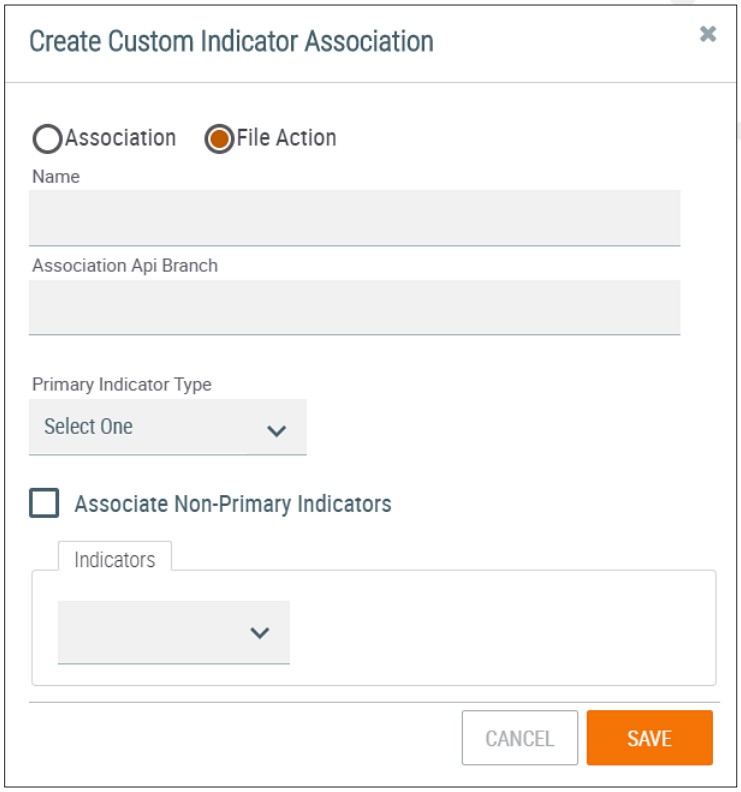

Figure 25

a. **Name**: Enter a name for the custom Association (e.g., **File CIDR**).

b. **Association API Branch**: Set this parameter to the mapped API field in ThreatConnect, (e.g., **cidr**).

c. **Indicators**: Click the drop-down menu to select one or more Indicators to associate with the File.

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

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.

Follow these steps to add a custom source to an Indicator type:

1. Log in with a System Administrator account.

2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).

3. Click the **Investigation Links** tab, and the **Investigation Links** screen will appear (Figure 26).

Figure 26

4. Click the **+ NEW** button, and the **Create External Link** pop-up screen will appear (Figure 27).

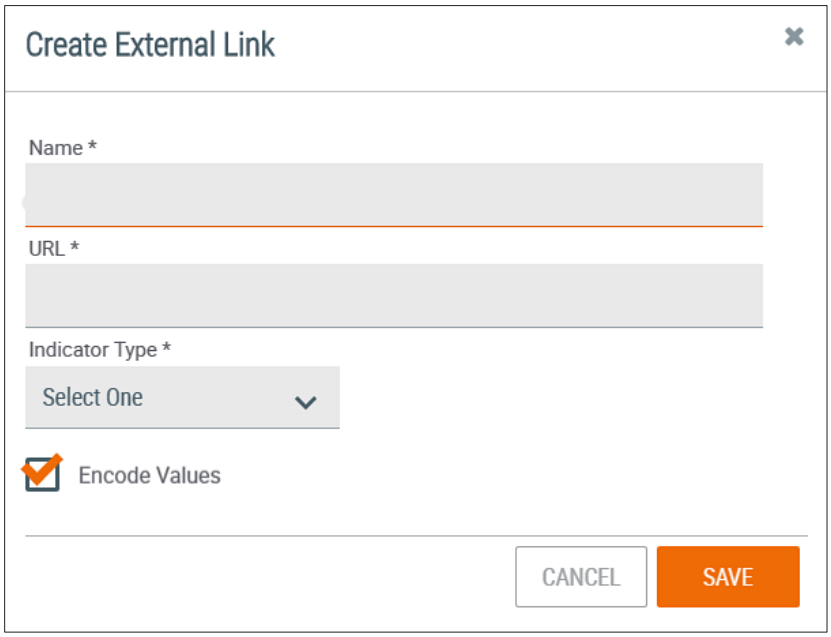

Figure 27

5. Fill in the pertinent fields and click the **SAVE** button.

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

System 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 Attributes Types to make them available to the entire user base.

Creating System Attribute Type Validation Rules

ThreatConnect is preloaded with a variety of Validation Rules to ensure that Attribute Types 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.

Follow these steps to create a System Attribute Validation Rule:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Attribute Validation** tab, and the **Attribute Validation** screen will appear (Figure 28).

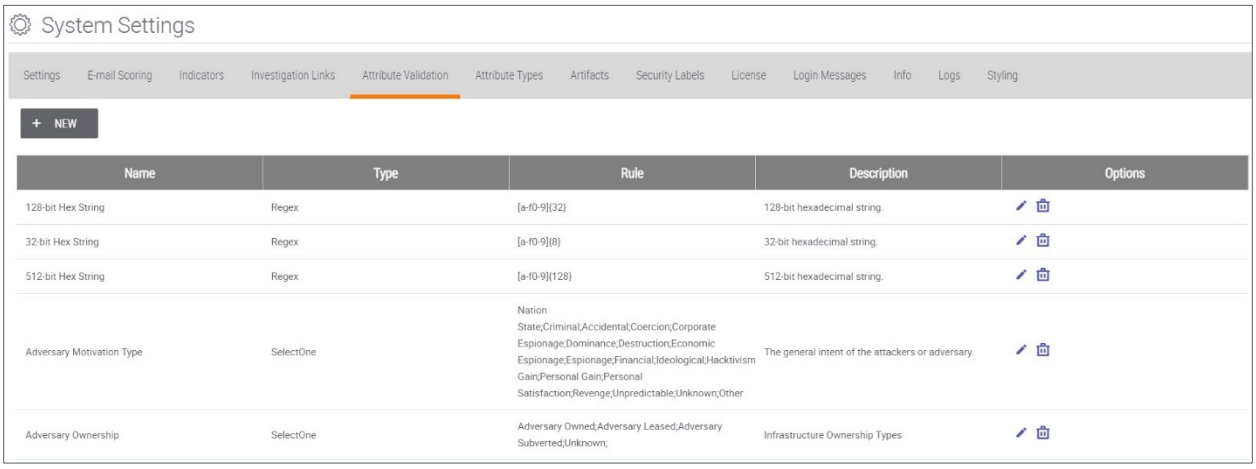

Figure 28

4. The **Attribute Validation** screen displays the existing System Attribute Validation Rules. Click the **+ NEW** button, and the **Create Attribute Validation Rule** pop-up screen will appear (Figure 29).

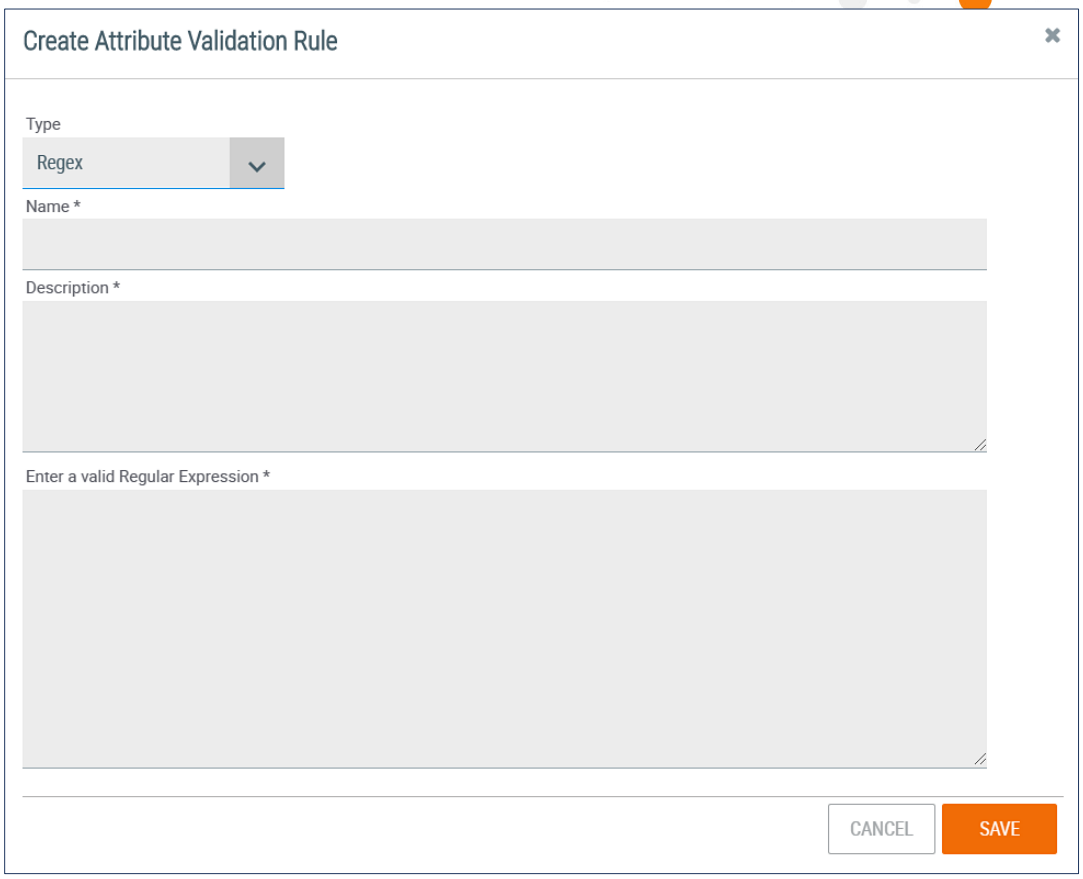

Figure 29

a. **Name**: Click in the box to enter the name of the Validation Rule as it will appear in the Validation Rules table of the Attribute Validation screen.

b. **Type**: Click on the drop-down menu to select the schema for the Validation Rule. Each option offers the flexibility to determine the valid domain for each Attribute Type:

c. **Regex**: a regular expression that considers only matching inputs to be valid (e.g., an IP address or email address on a certain domain)

d. **Xsd**: an XML Schema Definition used to validate input (useful for attaching logs from a vendor product)

e. **Select One Picklist**: presented as a drop-down menu of options—after the Administrator defines the options in the right-hand text box—from which users may only select one value (e.g., high, medium, or low priorities)

f. **Select One Radio**: similar to **Select One Picklist**, but presented as a series of radio buttons

g. **Date**

h. **Date/Time**

i. **Integer**: a whole number, valid in the range specified in the right-hand text box (e.g., 0:1440 for "minutes worked")

j. **Description**: Click in the box to enter a general description of the Validation Rule.

k. **Enter a Valid Regular Expression**: If applicable, click in the text box to enter the parameters for a Validation Rule as defined previously.

5. Click the **SAVE** button to save and use the new **System Attribute Validation Rule**. Note that it will have to be attached to an actual Attribute Type to validate user input.

Editing System Attribute Validation Rules

Follow these steps to edit a System Attribute Validation Rule:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Attribute Validation** tab, and the **Attribute Validation** screen will appear **(**Figure 28).
4. Click on the **Edit** icon for the Validation Rule to be edited. The **Create Attribute Validation Rule** pop-up screen will appear (Figure 30).

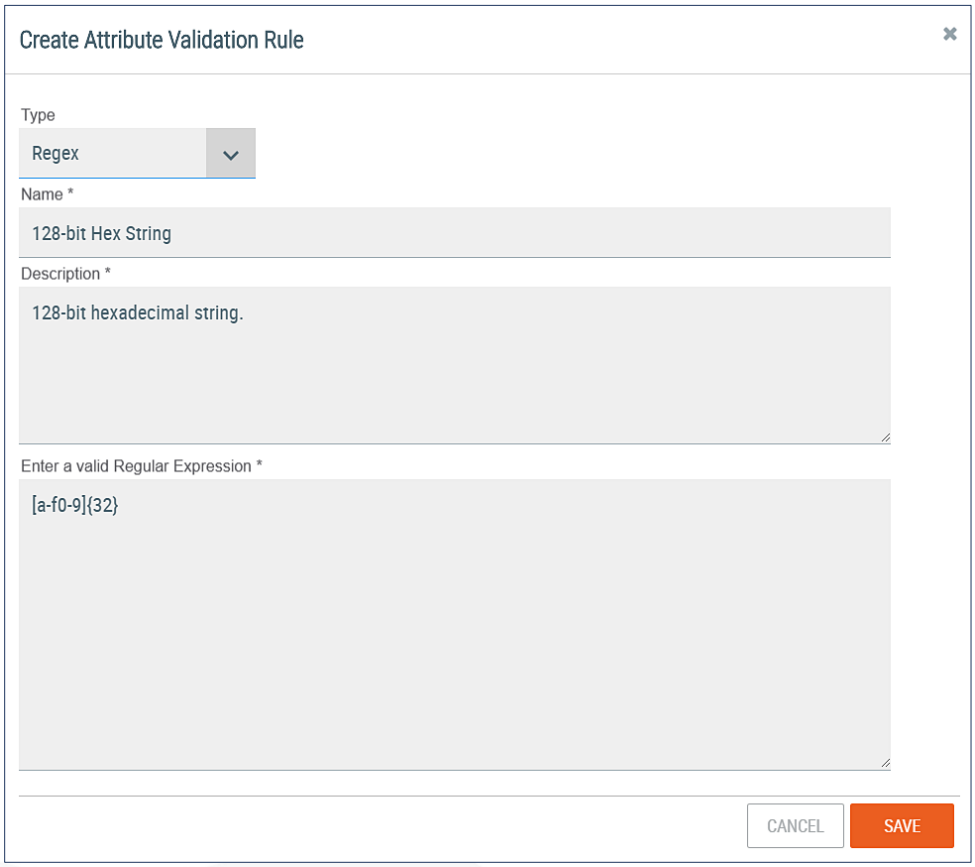

Figure 30

5. Configure the fields as appropriate.
6. Click the **SAVE** button to save any changes to the rule.

Viewing System Attribute Types

Follow these steps to view System Attributes:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Attribute Types** tab, and the **Attribute Types** screen will appear (Figure 31).

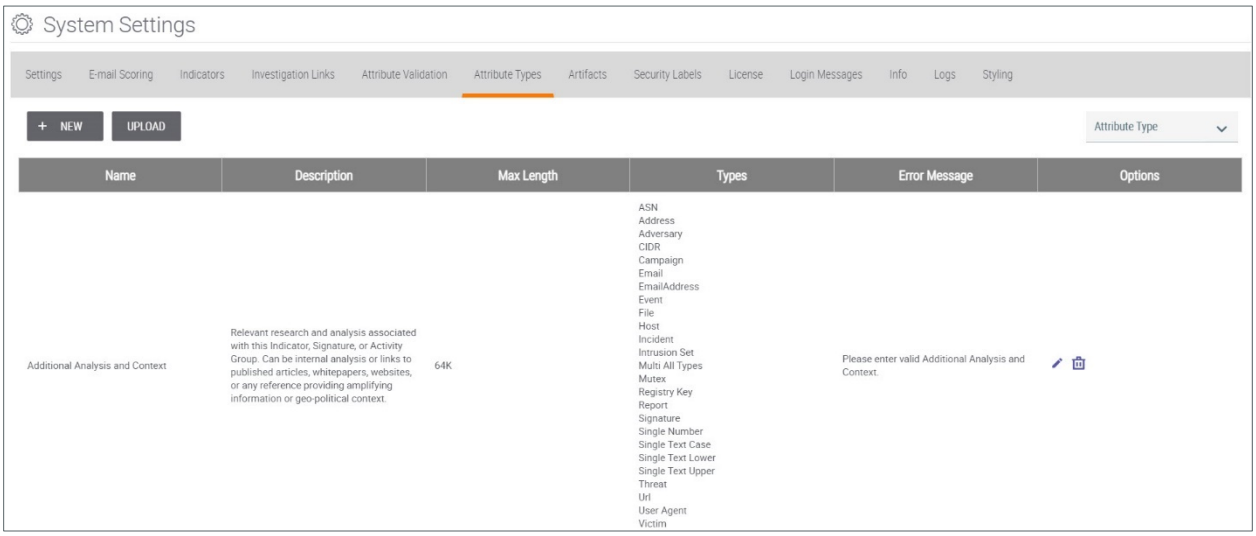

Figure 31

Creating System Attribute Types

Follow these steps to create a new System Attribute:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Attribute Types** tab, and the **Attribute Types** screen will appear (Figure 31).
4. To create a new, custom System Attribute, click the **+ NEW** button, and the **Configure Attribute Type** pop-up screen will appear (Figure 32).

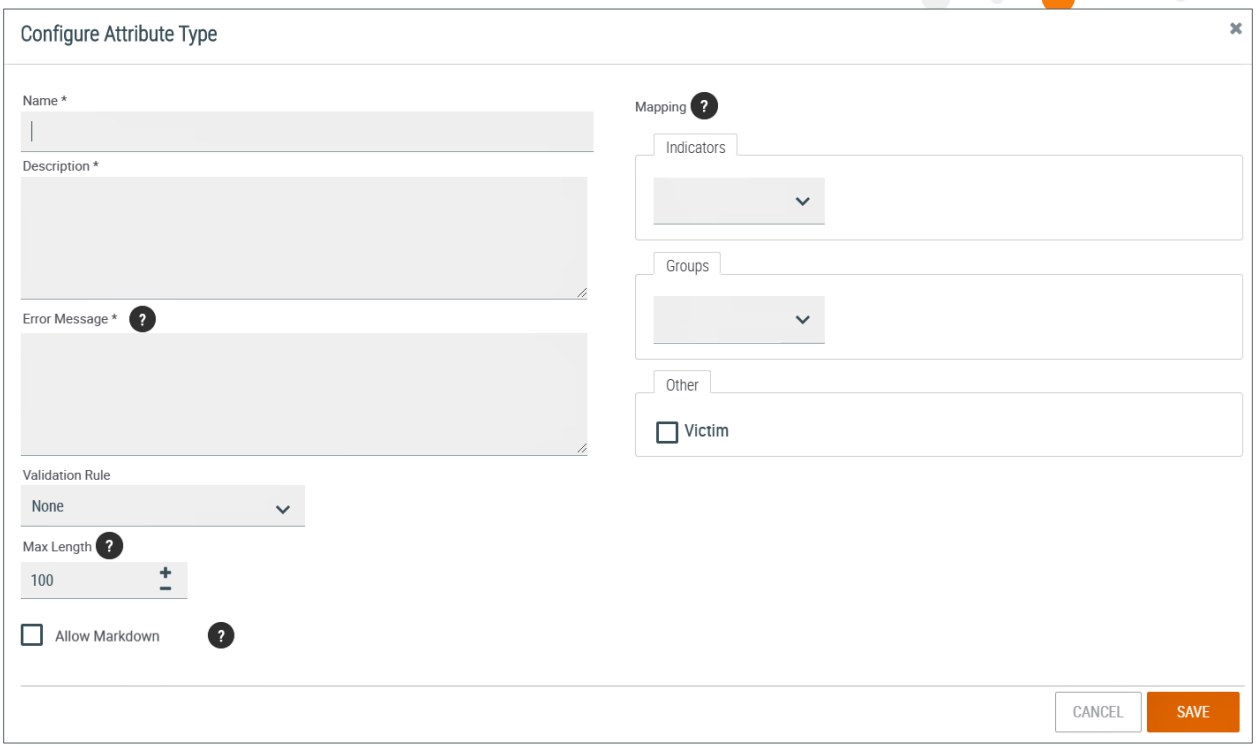

Figure 32

a. **Name**: Click in the box to enter the name of the System Attribute Type as it will appear on menus and on the **Details** screen for Indicators and Groups.

b. **Description**: Click in the box to 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.

c. **Error Message**: Click in the box to enter the message presented when users try to input a value that does not meet the System Attribute Type's Validation Rules.

d. **Validation Rule**: Click on the drop-down menu to 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 are able to define their own System Attribute Validation Rules as needed.

e. **Max Length**: Click in the box (or use the plus and minus signs) to manually enter the maximum size, in characters, of the System Attribute Type, if applicable, based on the Attribute's assigned Validation Rule.

f. **Allow Markdown**: Click this checkbox to allow the Markdown language to be used when configuring an Attribute Type.

NOTE: Markdown is a markup language used to transform text into HTML for the purpose of formatting. ThreatConnect supports the use of Markdown with several Attribute Types, including Description and Source.

g. **Mapping**: Click the drop-down arrows for Indicators or Groups, and then click on the desired checkboxes to specify the types of entities to which this 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.

5. Click the **SAVE** button to create the custom Attribute Type.

Figure 33 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 appropriate Groups and Indicators. If custom Indicators have been added, they will be displayed in the **Indicators** section as well.

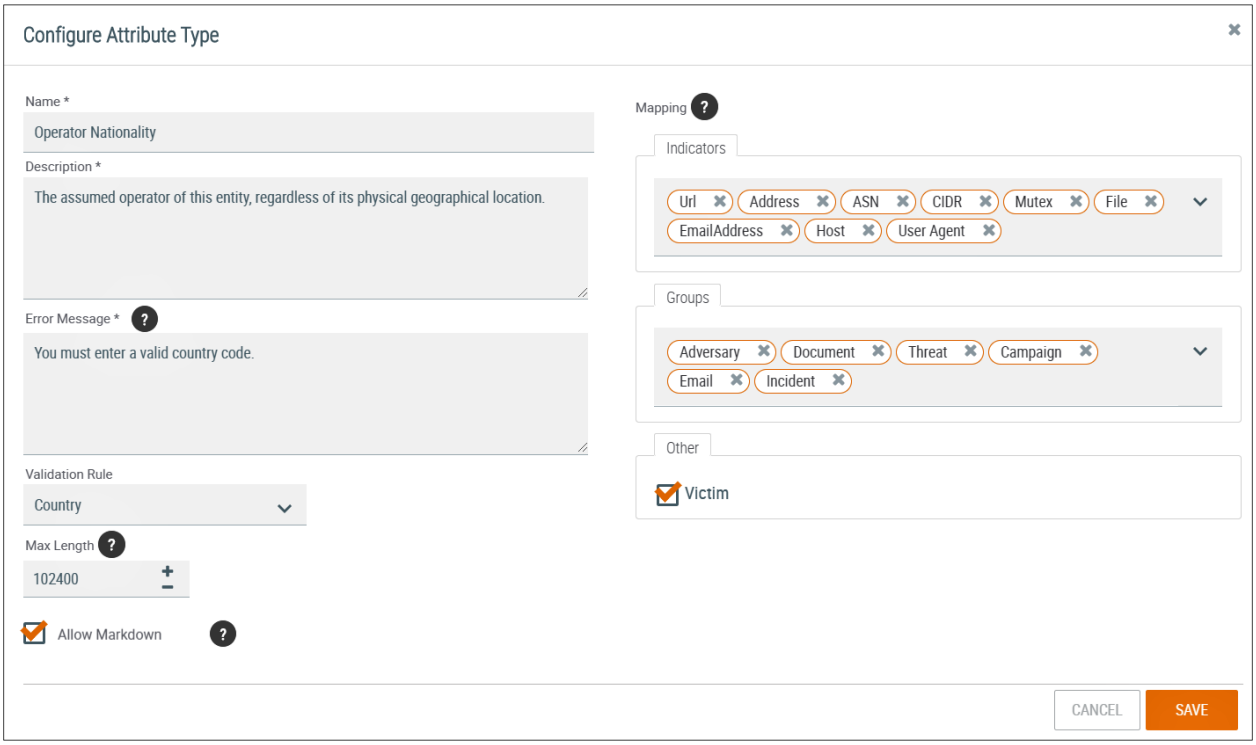

Figure 33

Uploading a System Attribute Type

Follow these steps to upload a System Attribute:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Attribute Types** tab, and the **Attribute Types** screen will appear (Figure 31).
4. Click the **UPLOAD** button, and the **Upload Attributes** pop-up screen will appear (Figure 34).

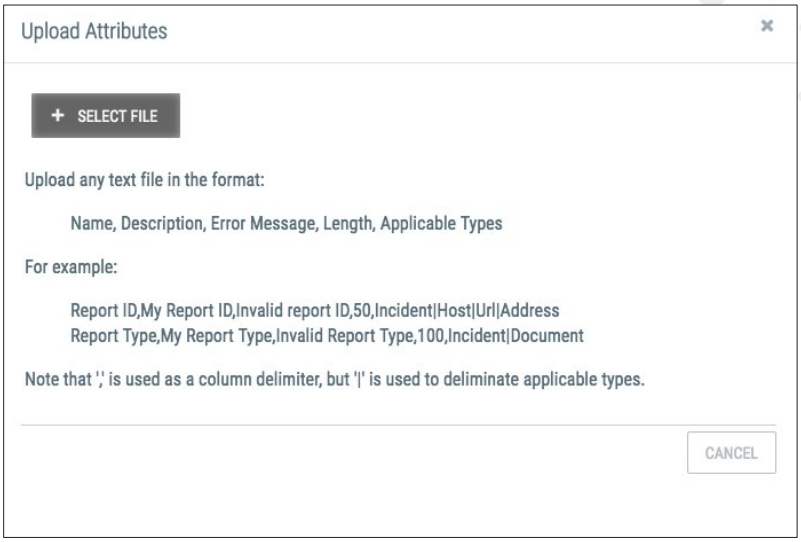

Figure 34

5. Click the **+ SELECT FILE** button, navigate to the desired directory, select a file, and click the **SAVE** button.

Editing System Attribute Types

Follow these steps to edit a System Attribute Type:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Attribute Types** tab, and the **Attribute Types** screen will appear (Figure 31).
4. Click on the **Edit** icon for the Attribute Type to be edited. The **Configure Attribute Type** pop-up screen will appear (Figure 32).
5. Configure the fields as appropriate.
6. Click the **SAVE** button to save any changes to the Attribute Type.

Artifact Types

Artifacts are integral components of ThreatConnect's Workflow and Case Management features. (See the Workflow and Case Management section of this document for more information.) Artifacts are typed, like Indicators and Groups, and the supported Artifact Types are preconfigured in the system.

Creating Artifacts

ThreatConnect is preloaded with certain Artifact Types, but the user can create new ones.

Follow these steps to create an Artifact Type:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Artifacts** tab, and the **Artifact Types** screen will appear (Figure 35).

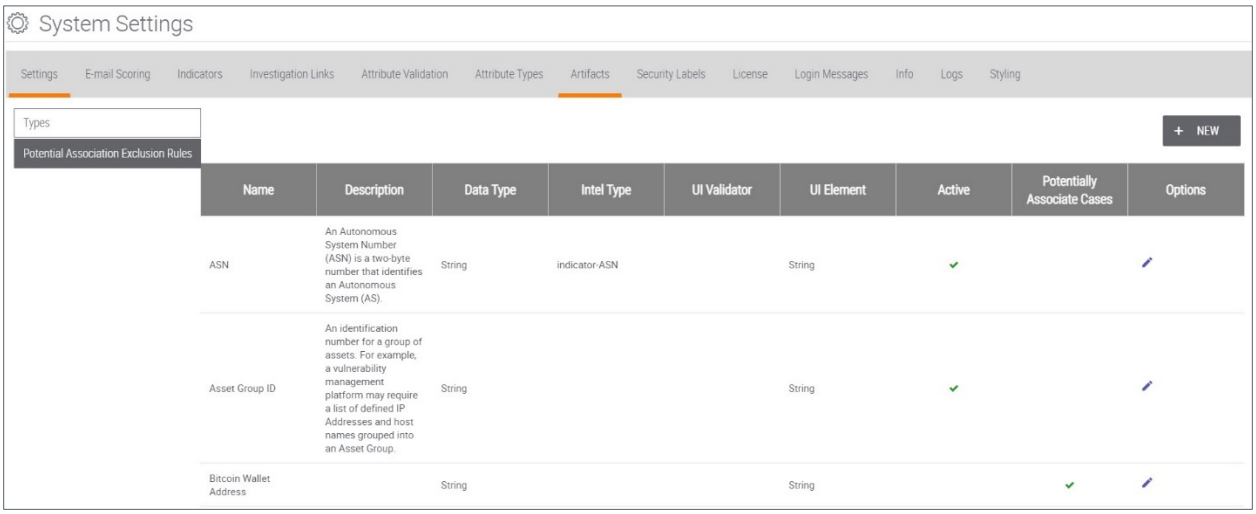

Figure 35

4. The **Artifact Types** screen displays the existing Artifact Types. Click the **+ NEW** button, and the **Configure Artifact Type** pop-up screen will appear (Figure 36).

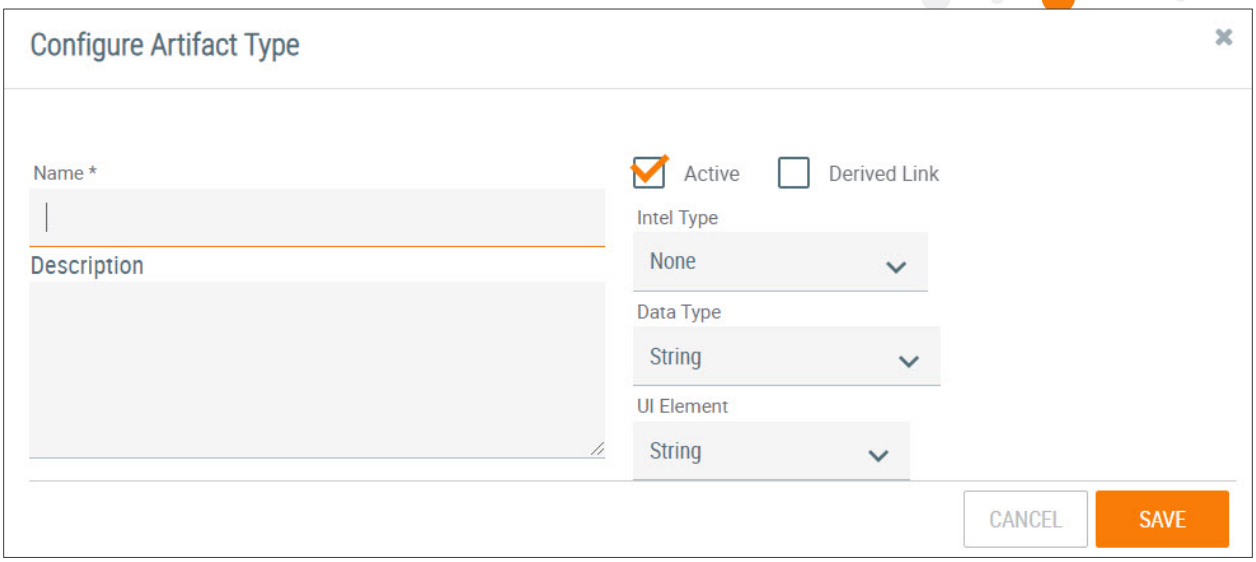

Figure 36

a. **Name**: Click in the box to enter the name of the Artifact Type as it will appear in the **Artifact Types** table.

b. **Description**: Click in the box to enter a description of the Artifact Type.

c. **Active Checkbox**: Click the checkbox to make this Artifact Type active.

d. **Intel Type**: Click on the dropdown menu to select the appropriate Indicator Intel Type, to which the Artifact Type can map.

e. **Data Type**: Click on the dropdown menu to select the appropriate Data Type, either a string or a file.

f. **UI Element**: Click on the dropdown menu to select the appropriate UI Element.

Editing Artifact Types

Follow these steps to edit an Artifact Type:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).
3. Click the **Artifact Types** tab, and the **Artifact Types** screen will appear (Figure 35).
4. Click on the **Edit** icon for the Artifact Type to be edited (Address in this example). The **Configure Artifact Type** pop-up screen will appear (Figure 37).

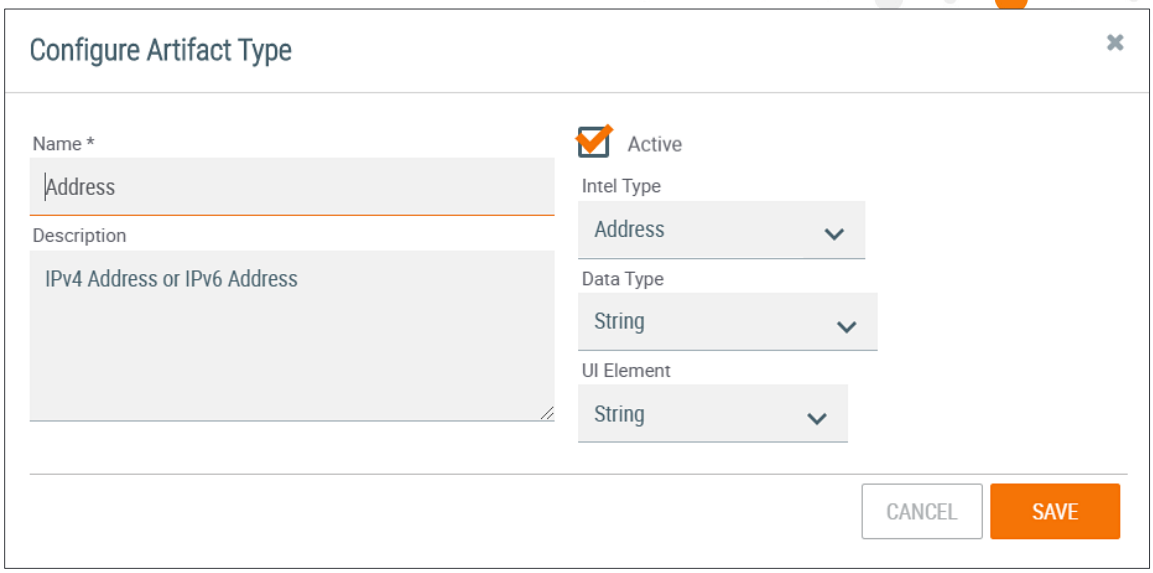

Figure 37

5. Configure the fields as appropriate (IP Address in this example).
6. Click the **SAVE** button to save any changes to the Artifact Type.

Potential Association Exclusion Rules

In the **Artifacts** tab screen, click the **Potential Association Exclusion Rules** tab on the left to display the **Exclusion Rules** screen (Figure 38). These rules are not included by default, but users can add them. They prevent artifacts from creating potential associations between cases if the artifacts are on the Exclusion List.

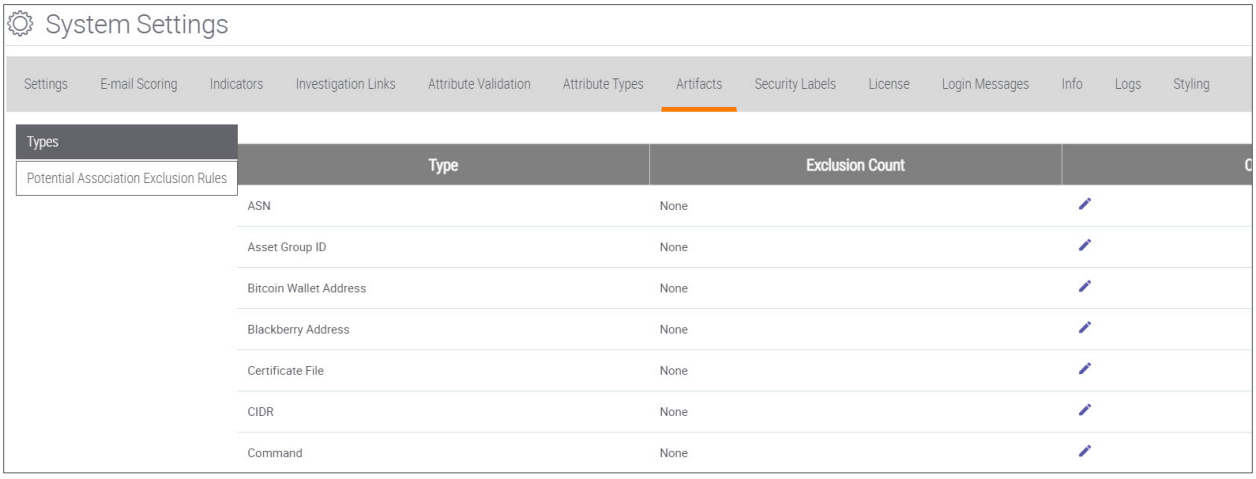

Figure 38

To edit or modify am Exclusion Rule, click the Edit icon to the right of an entry, and the **Exclusion Details** pop-up screen (Figure 39) will appear (ASN Type in this example). Enter the custom exclusion details manually, or click the **+ UPLOAD FILE** button to navigate to a directory. When done, click the **SAVE** button.

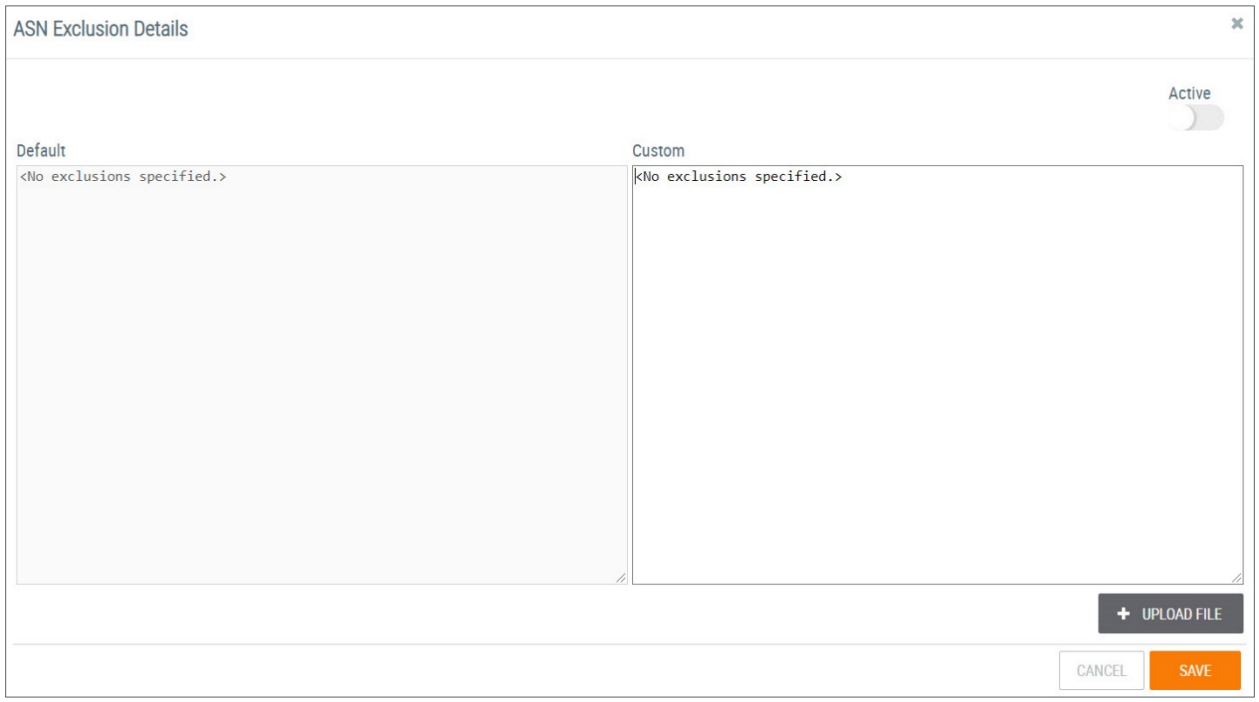

Figure 39

System 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 developed by the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT). Administrators can define their own Security Labels based on their needs and policies.

The platform also includes a migration tool that allows users to take an Owner-specific security label and migrate it to a System one, 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, or Sources, refer to the *ThreatConnect Community and Source Administration User Guide* and the *ThreatConnect Organization Administration User Guide*.

Creating System Security Labels

Follow these steps to create a custom System Security Label:

1. Log in with a System Administrator account.

2. On the top navigation bar (Figure 1), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 2). Select **System Settings** and the **System Settings** screen will appear (Figure 7).

3. Click the **Security Labels** tab, and the **Security Labels** screen will appear (Figure 40), displaying a list of the standard Security Labels.

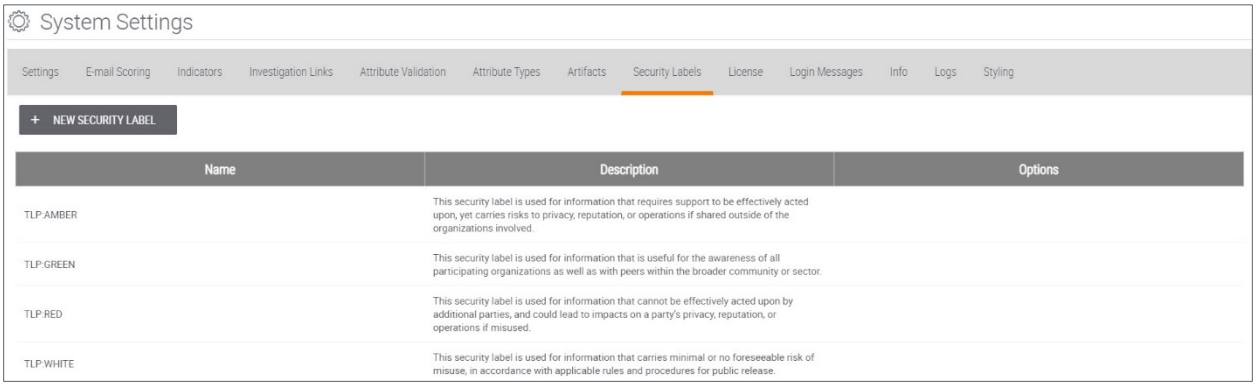

Figure 40

4. To create a new System Security Label, click the **+ NEW SECURITY LABEL** button, and the **Create Security Label** pop-up screen will appear (Figure 41).

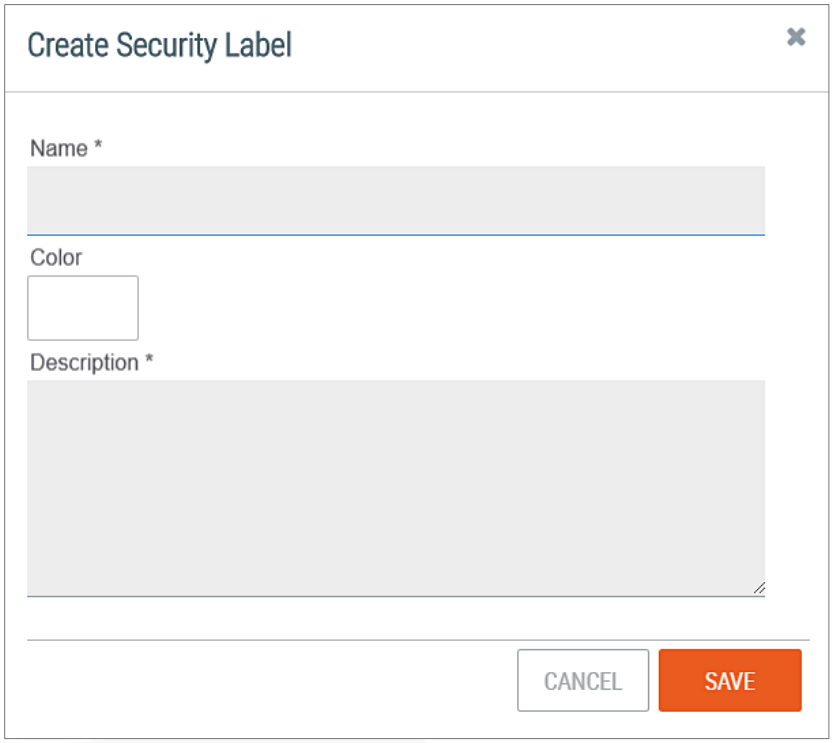

Figure 41

5. Click in the boxes to enter a **Name**, **Color**, and a **Description** for the Security Label. These fields are provided solely for user and Administrator readability, as no policy enforcement is derived from this screen.
6. Click the **SAVE** button to save the System Security Label.

Using System Security Labels

Security Labels are most effective when users share or contribute information within ThreatConnect—which allows them 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).

The System License

Viewing the System License

Follow these steps to view the System License:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 42), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 43). Select **System Settings** and the **System Settings** screen will appear (Figure 44).

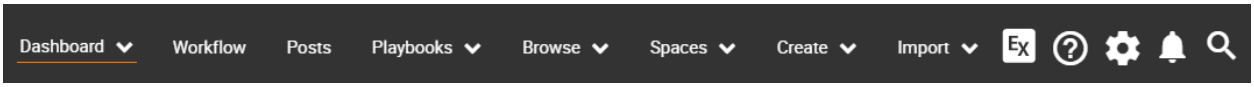

Figure 42

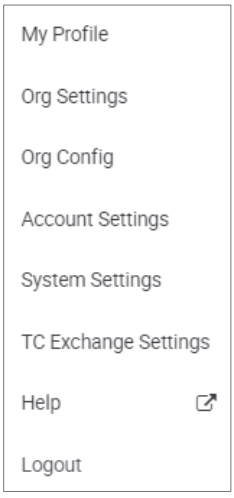

Figure 43

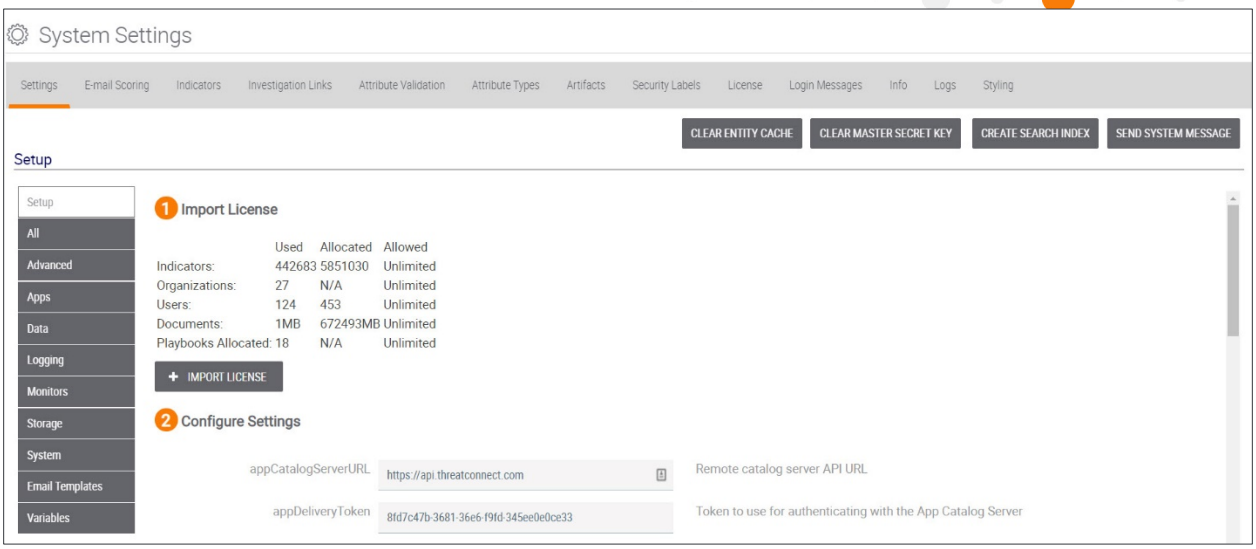

Figure 44

3. Click the **License tab**, and the **License** screen will appear with the **License Config** subtab highlighted (Figure 45), displaying the current allocations of Indicators, Organizations, Users, Documents, and Playbooks allocated. From this screen, the user can also import a license by clicking the **+ IMPORT LICENSE** button, and an **Open** screen will appear from which to select the appropriate file.

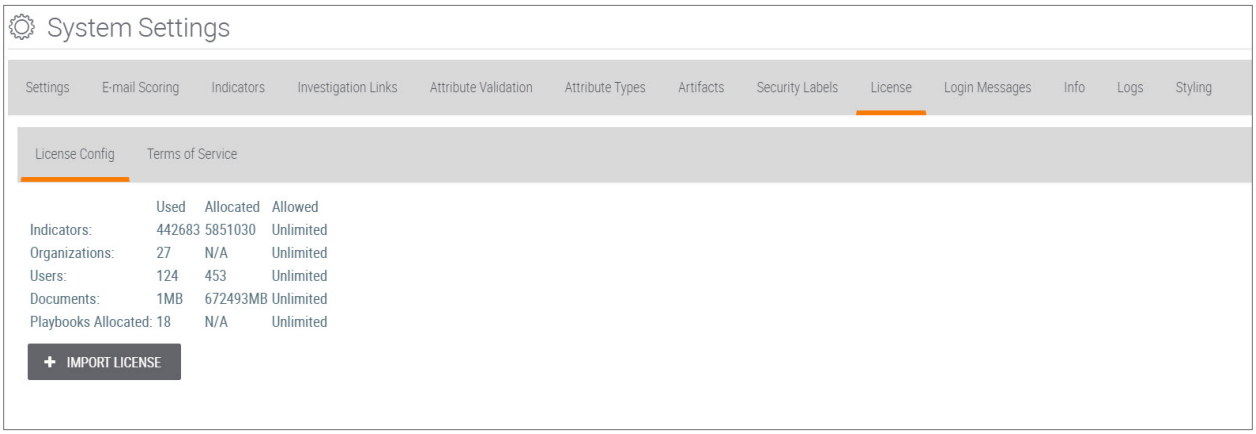

Figure 45

4. Click the **Terms of Service** subtab, and the **Terms of Service** screen will appear (Figure 46). From this screen, the user can view, import, and delete the Terms of Service, as well as reset user acceptance.

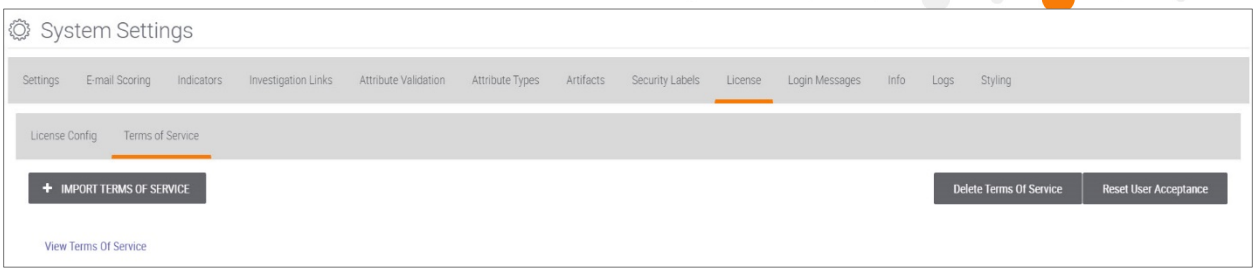

Figure 46

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.

Adding Login Messages

Follow these steps to add a login message:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 42), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 43). Select **System Settings** and the **System Settings** screen will appear (Figure 44).
3. Click the **Login Messages** tab, and the **Login Messages** screen will appear (Figure 47).

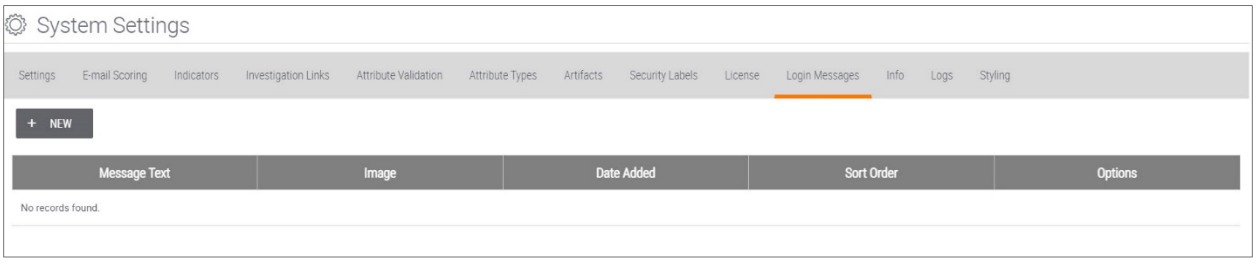

Figure 47

4. Click the **+ NEW** button, and the **Create Login Message** pop-up screen will appear (Figure 48).

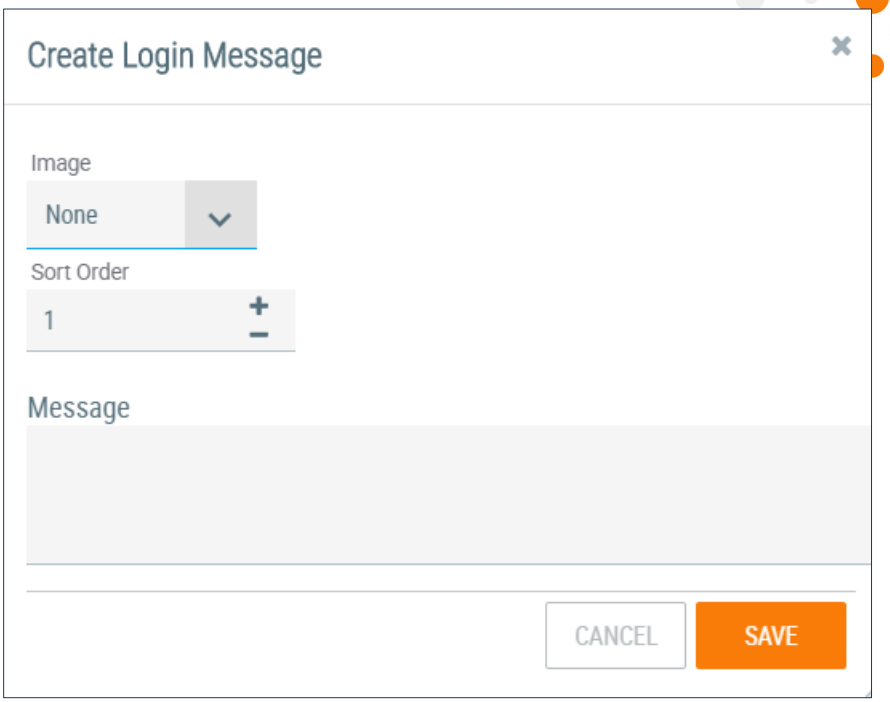

Figure 48

5. Click the **Image** drop-down menu to add an icon next to the message.
   - **None**: No icon
   - **Vote**: Checkmark icon
   - **Feature**: Notebook icon
6. For **Sort Order**, click the plus and minus signs to change the position in which the icon will appear on the screen next to the text.
7. In the text box, enter the desired message.
8. Click the **SAVE** button, and the icon and text will appear on the **Login** screen.

Hardware and Virtualization

Viewing Hardware and Virtualization Information

Follow these steps to view hardware and virtualization information:

1. Log in with a System Administrator account.

2. On the top navigation bar (Figure 42), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 43). Select **System Settings** and the **System Settings** screen will appear (Figure 44).

3. Click on the **Info** tab, and the **Info** screen will appear with the **Information** subtab highlighted (Figure 49). This screen displays current system hardware, software, and application database status information.

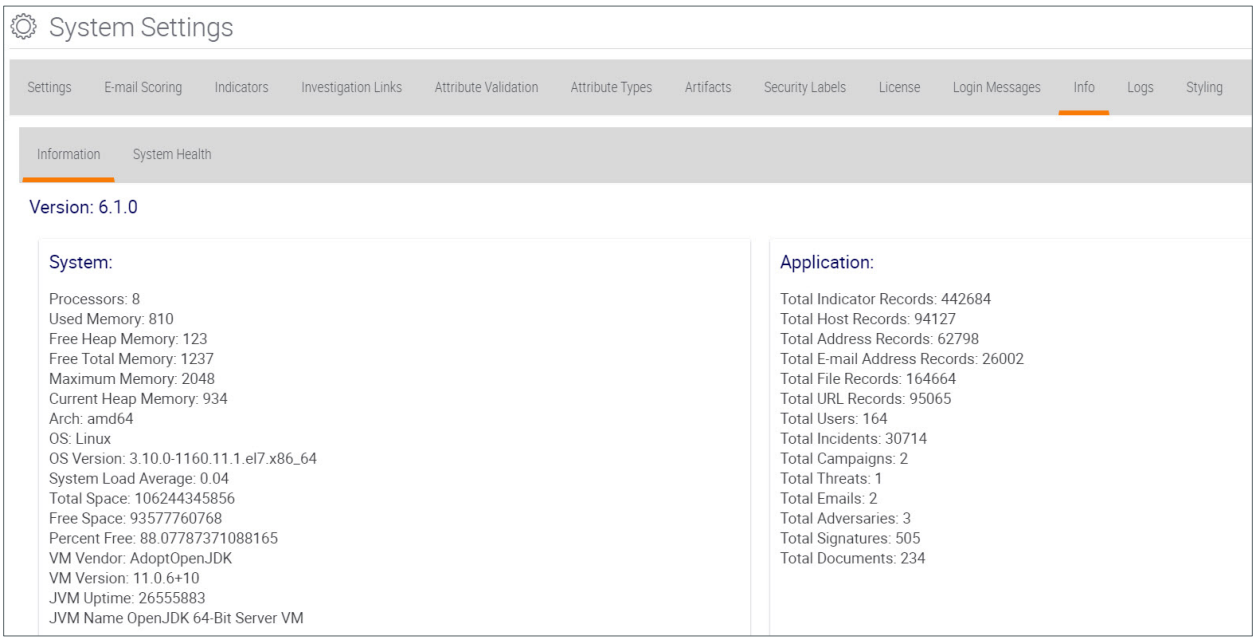

Figure 49

4. Click on the **System Health** tab and the **System Health** screen will appear (Figure 50). This screen displays if certain system processes and settings are configured and operating properly. If a component is operating smoothly, it will be indicated by a checkmark in the **Passed** column. If a component needs attention, a triangular warning sign will be displayed in the same column.

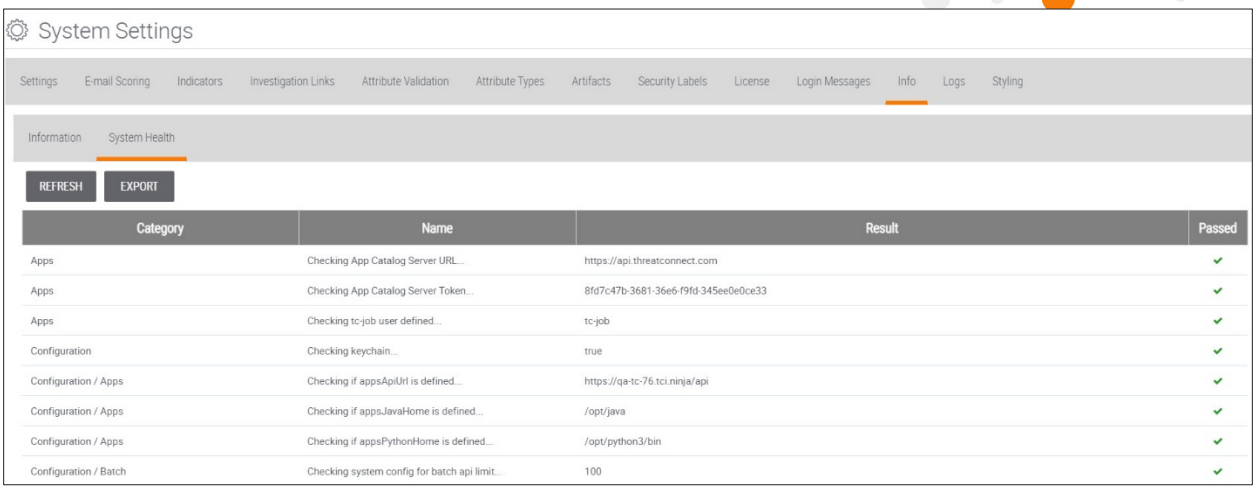

Figure 50

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

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.

Retrieving Logs

Follow these steps to retrieve a log:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 42), place the cursor on the **Settings**  icon and the **Settings** menu will appear (Figure 43). Select **System Settings** and the **System Settings** screen will appear (Figure 44).
3. Click the **Logs** tab, and the **Logs** screen will appear with the **View** subtab highlighted (Figure 51).
4. Click in one of the boxes—**Source Class**, **Level**, or **Message**—and enter the appropriate information that will narrow the table entries.

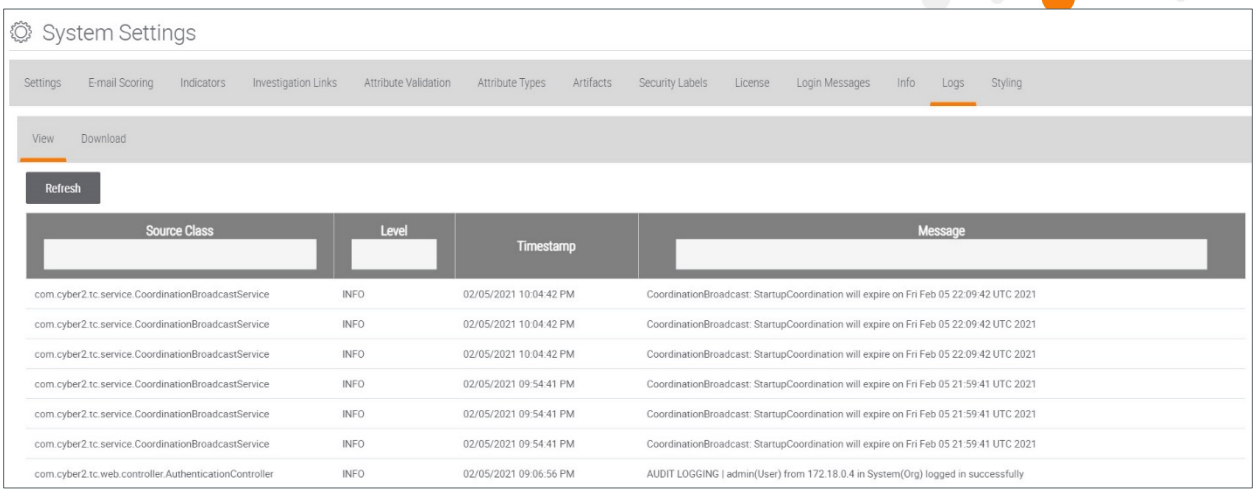

Figure 51

5. Click on an entry, and the **Log Details** pop-up screen will appear (Figure 52).

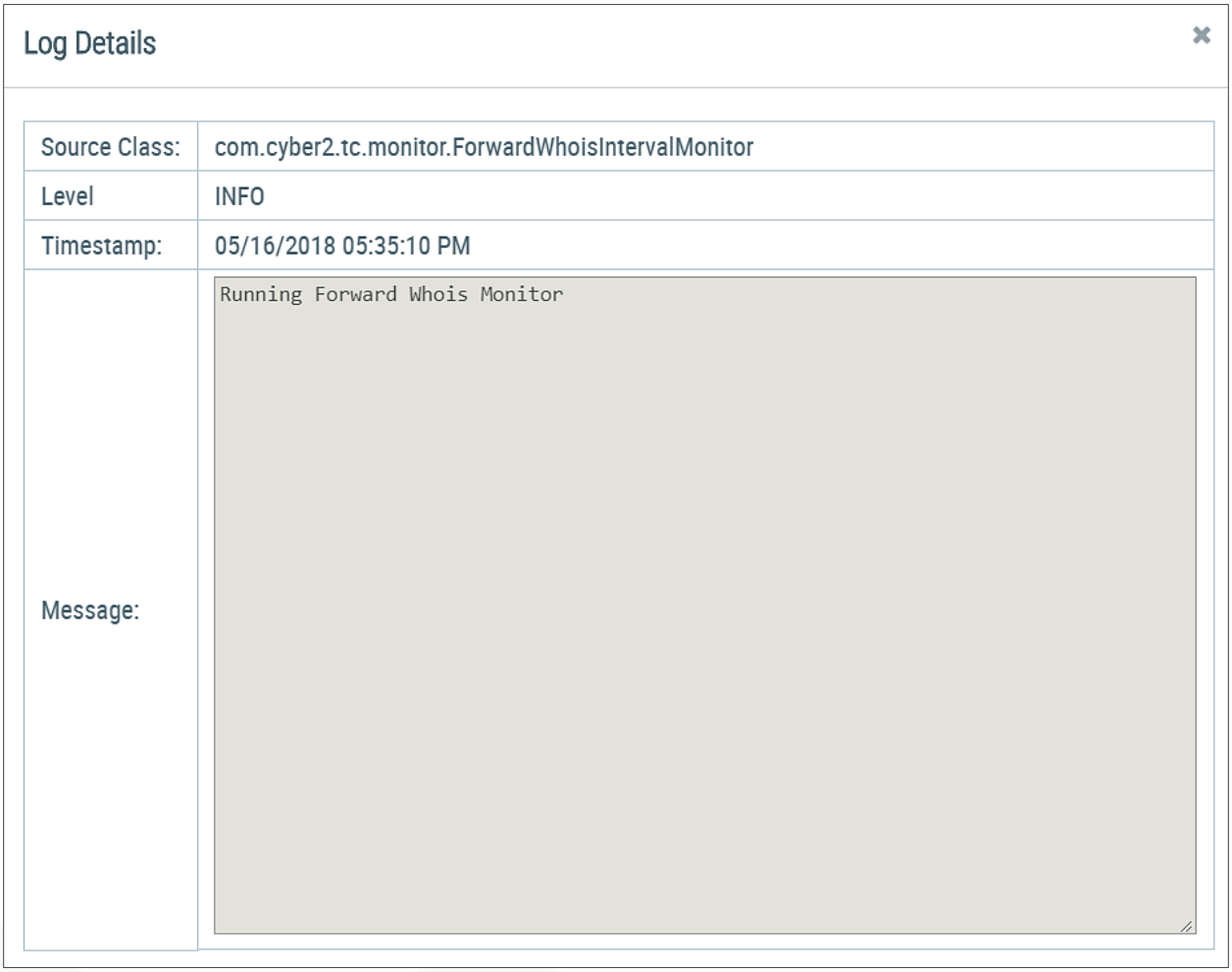

Figure 52

6. Click the **Download** subtab and the **Download** screen will appear (Figure 53).

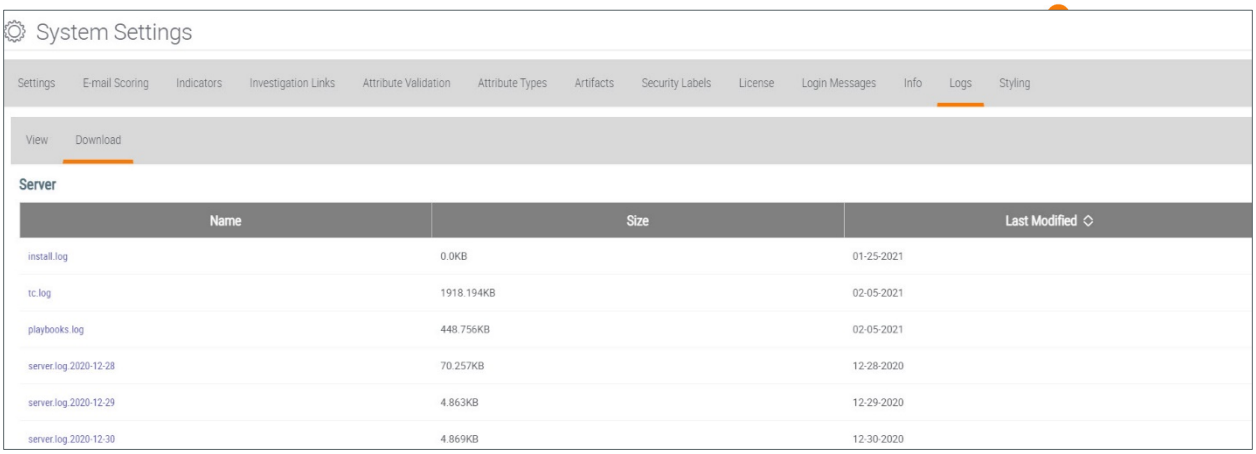

Figure 53

7. Click one of the entries to download a log file to a local directory.

Headers and Footers

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.

Styling a PDF Header and a Site Header or Footer

Follow these steps to style a PDF header and a site header or footer:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 42), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 43). Select **System Settings** and the **System Settings** screen will appear (Figure 44).
3. Click the **Styling** tab, and the **Styling** screen will appear (Figure 54), showing the default ThreatConnect headers and footer that will be used if no other images are uploaded.

   NOTE: Hover the cursor over the question mark symbols to obtain information on image-size requirements.

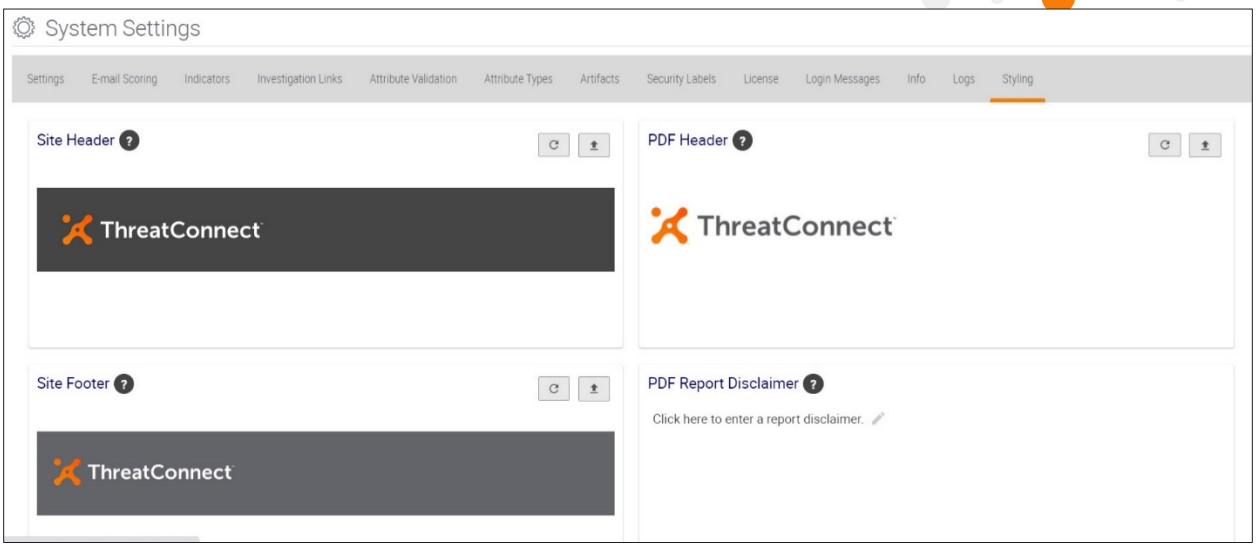

Figure 54

4. Click the **Upload**  icon next to the standard header or footer, navigate to a directory, and select a JPEG or PNG image file.

5. Click the Pencil  icon under **PDF Report Disclaimer** to add a disclaimer, such as "Demo," to a PDF.

6. The selected image will now appear in the appropriate header or footer box, and it will also appear as a header for downloaded PDFs or as a header or footer for the user's ThreatConnect site.

System Health

The health of the ThreatConnect Instance can be retrieved via the status servlet by submitting an HTTP request with the parameters defined in Figure 55.

NOTE: A System Administrator can retrieve the value of the statusKey via System Settings.

Verb	Address	Header	Response Code	Example JSON Response Content
GET	https://<tcAddress>/status	<none>	204 - all ok 500 - system unhealthy	

		statuskey=<incorrect>	200 - all ok
			500 - system unhealthy
				{
				"Message" : "Invalid access key!"
				}

		statuskey=<correct>	200 - all ok
			500 - system unhealthy
				{
				"Product Version" : "3.2.1",
				"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" : "2015-07-01T12:52:09.430-0500",
				"Message" : "System OK."
				}

Figure 55

Apps and Jobs

Installing an App

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

Follow these steps to manually install an app:

1. Log in with a System Administrator account.

2. On the top navigation bar (Figure 42), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 43). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will appear (Figure 56). The **Installed** tab will be highlighted, displaying all installed applications, or click on the drop-down menu below the tab to view the apps by category: Custom Apps, Custom Trigger, Feed Apps, Playbook, Playbook Template, REST API, Spaces, STIX, Third Party, Web Hook Trigger, and Workflow Templates. Entering a term in the search box to the right of the drop-down menu will return all applications matching the search term.

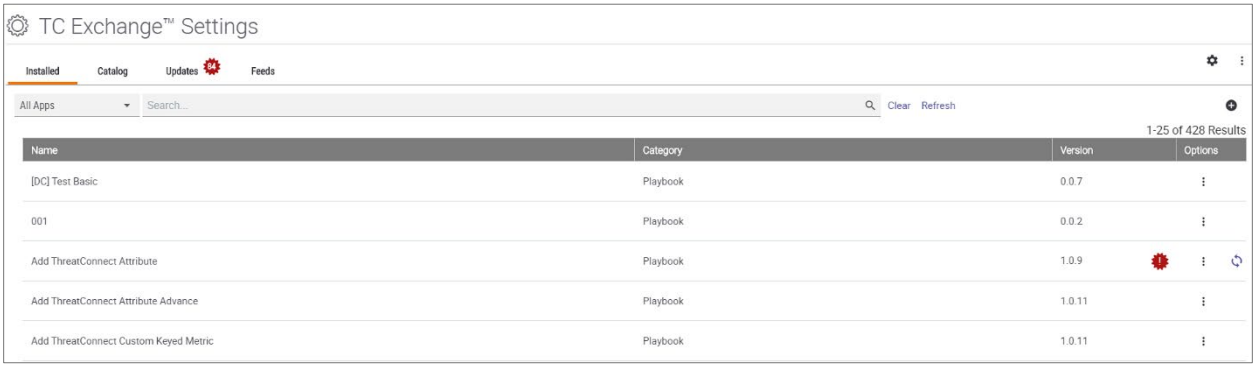

Figure 56

3. Select an app and click the vertical ellipsis in the **Options** column to bring up a pop-up menu (Figure 57).

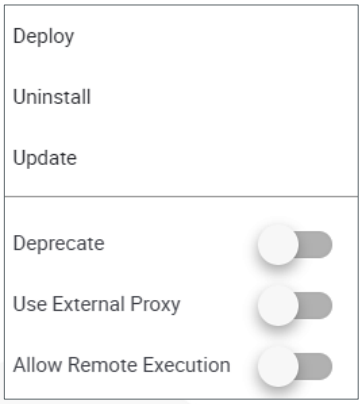

Figure 57

NOTE: Figure 57 is an Options-menu example for a specific app. More or fewer options may be available for different applications.

4. From this menu a user can do the following:
   - Deploy Feeds
   - Set Permissions to select the organizations that can run an app
   - Uninstall the app
   - Update the app
   - Deprecate the app manually (the only option available for internal apps)
   - Set the app's Proxy setting to **Active** or **Not Active**
   - Set the app's Remote-Execution setting to **Active** or **Not Active**

5. Click the **Install App** button  on the upper right of the screen, and the **Install App** pop-up screen will appear (Figure 58).

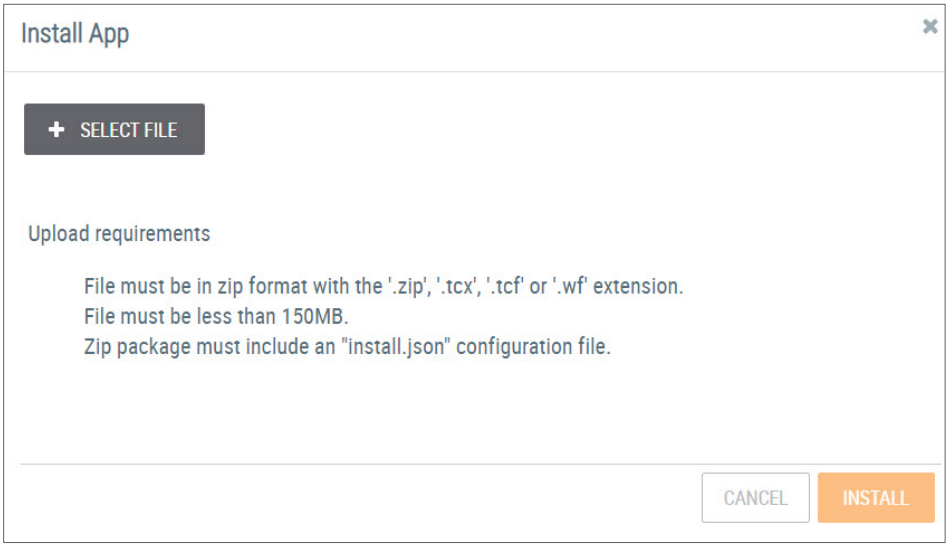

Figure 58

6. Click the + **SELECT FILE** button, and navigate to the zipped app file.

   NOTE: The file must be in a zipped format with the .zip, .tcx, .tcf, or wf extension and less than 150MB in size, and it must include an install.json configuration file.

7. Verify that the information in the **App Name, Type,** and **Version** fields is correct, and then click the **INSTALL** button.
8. The app will now appear in the **Installed Apps** list.

   NOTE: Administrators can choose to install apps in bulk. This makes it easier to install and upgrade large bundles of app.

Feed Deployment

Apps with feeds take advantage of the feed-deployment mechanism to create Sources, which then run associated jobs.

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.

Follow these steps to deploy a feed:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 42), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 43). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will appear (Figure 56).
3. Select an app and click the ellipsis in the **Options** column to bring up a pop-up menu (Figure 57).
4. Click **Deploy** and the **Feed Deployer** screen will appear, with the **Source** tab highlighted (Figure 59).

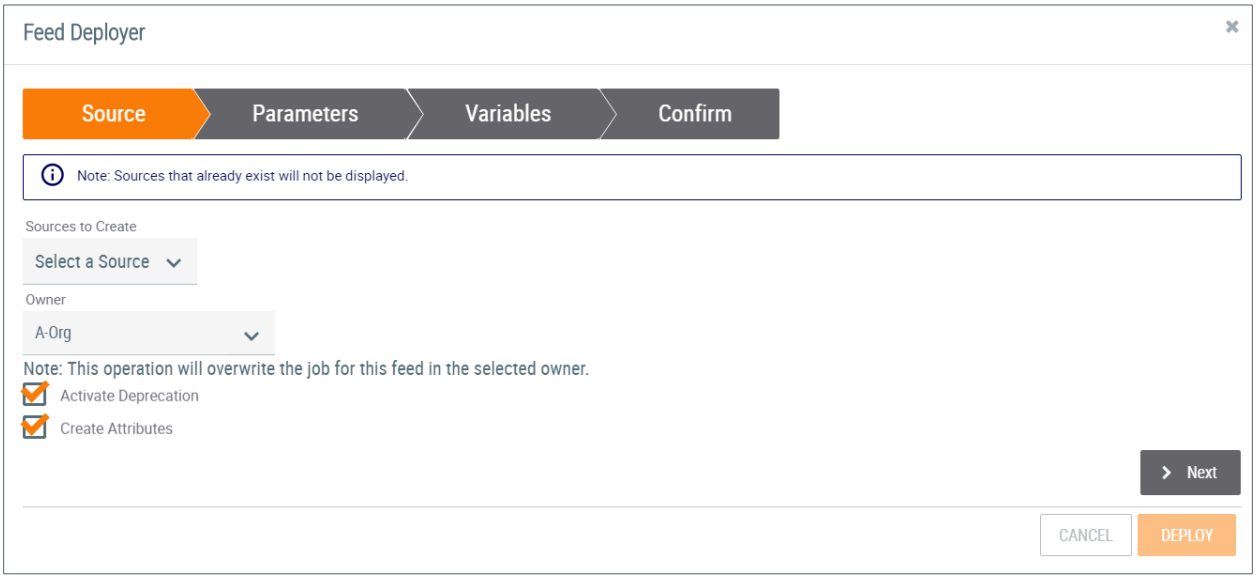

Figure 59

5. Select a **Source** (or Sources) and an **Owner**, and click the **Activate Deprecation** and the **Create Attributes** checkboxes, as warranted.
6. Click the **Next** button and the **Parameters** screen will appear (Figure 60).

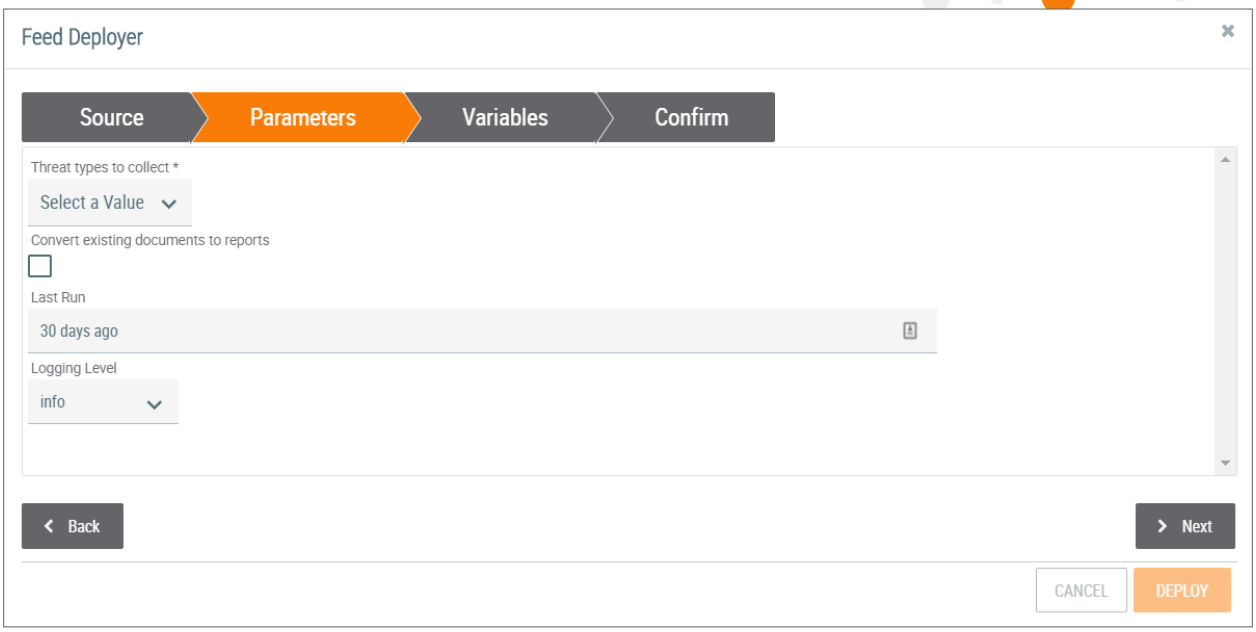

Figure 60

7. Note that parameters are customized and unique per each individual app, and the user should fill them out, if des5ired. For the app example in Figure 60, select a **Threat Type Value** and a **Logging Level**. Specify the **Last Run Date**, and check the **Convert existing documents to reports** box.
8. Click the **Next** button, and the **Variables** screen will appear (Figure 61), which will create a specified variable as part of the deployment, if required for the specified Source.

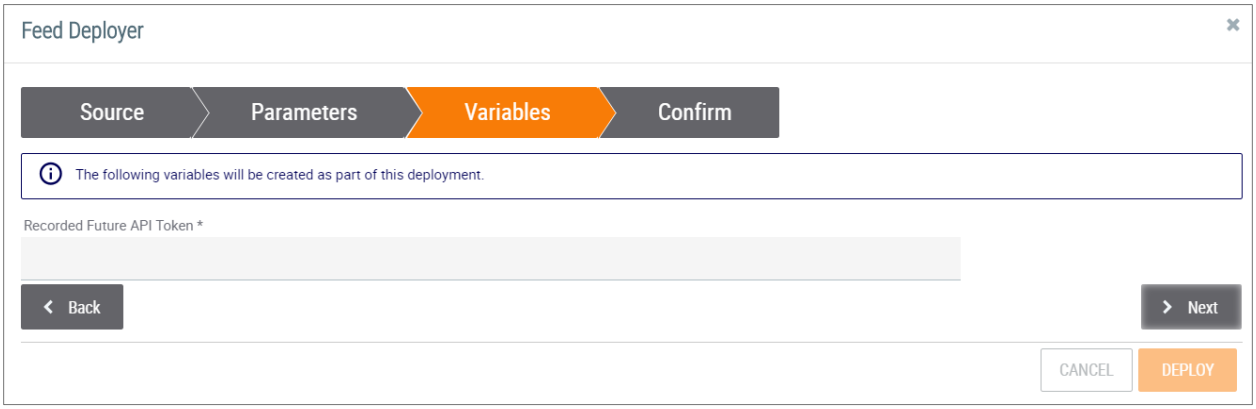

Figure 61

9. Enter the token information (for this app example only), or any other type of variable that may be required, and click the **Next** button. The **Confirm** screen will appear (Figure 62).

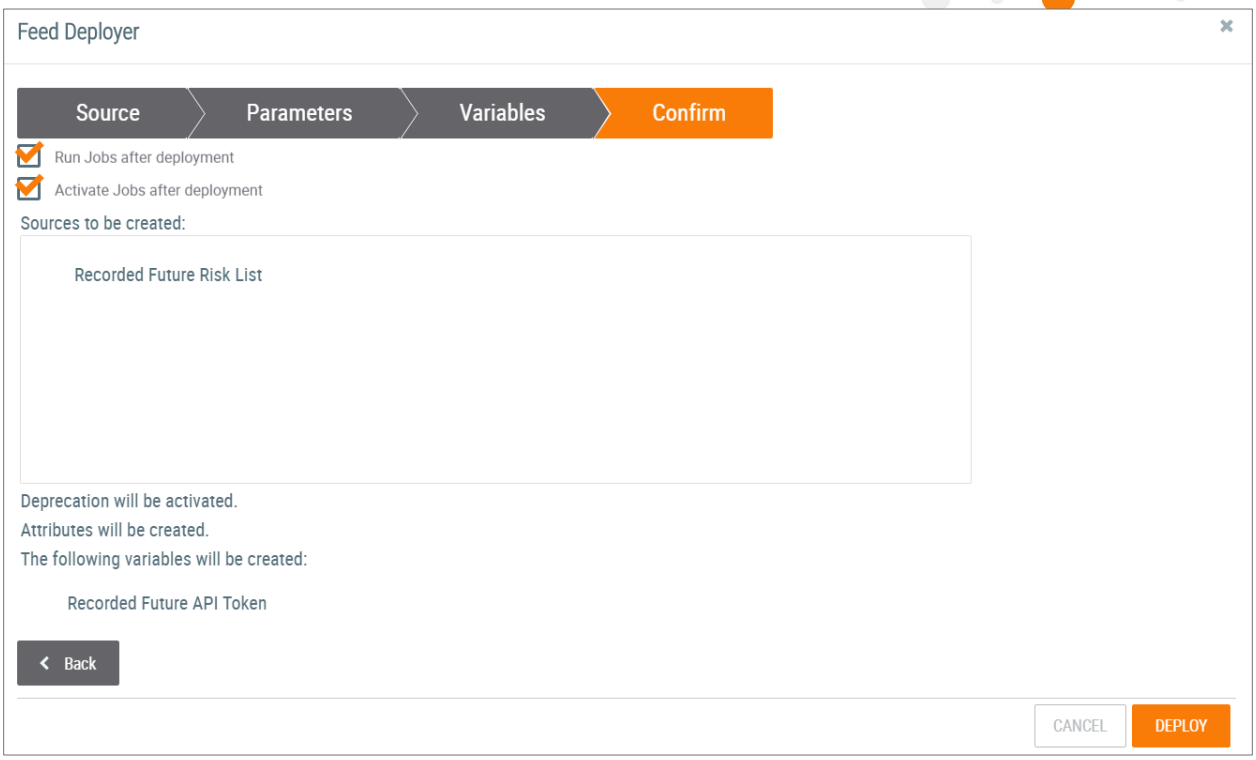

Figure 62

10. Click the **Run Jobs after deployment** and the **Activate Jobs after deployment** checkboxes, as warranted, and then click the **DEPLOY** button to deploy the Feed.

App Delivery

A ThreatConnect Instance can act as a server that will deliver any supported application 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://app.threatconnect.com.

To configure the machine acting as a server:

1. Log in with a System Administrator account.

2. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 64).

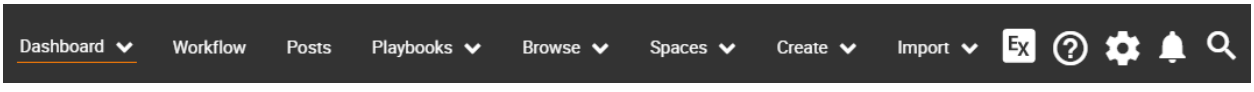

Figure 63

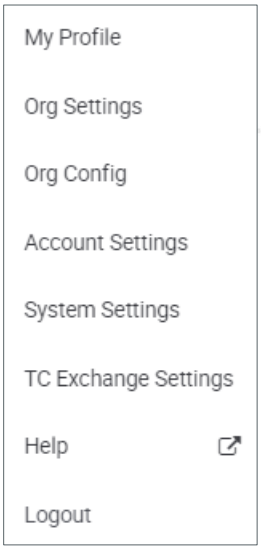

Figure 64

3. Select **System Settings** and the **System Settings** screen will appear (Figure 65).

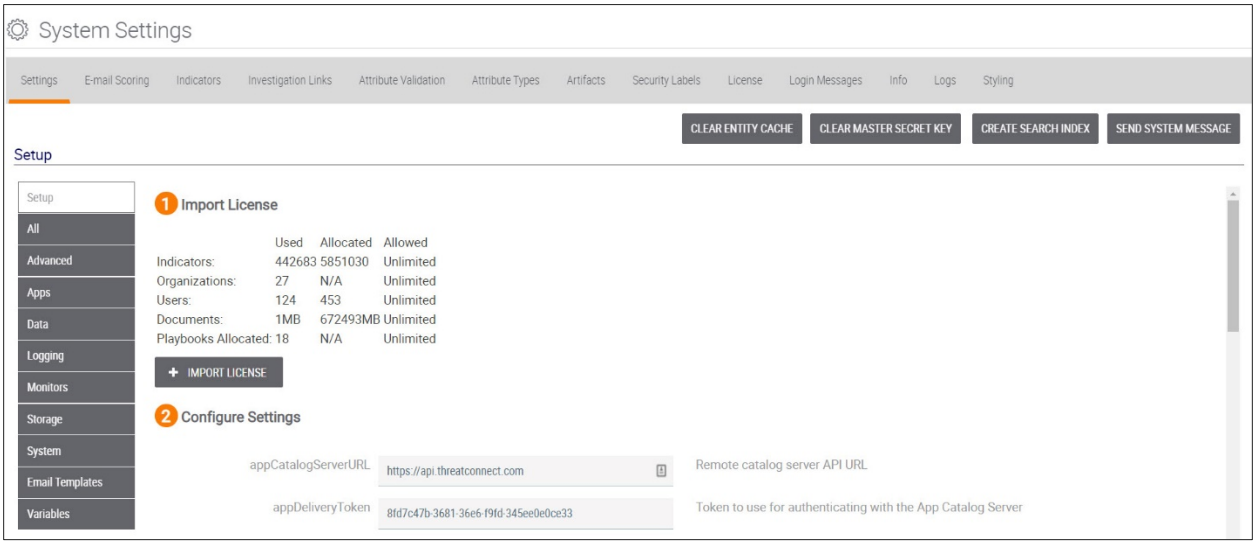

Figure 65

4. On the left-hand menu, click on the **APPS** menu option. Configure these settings as follows:
   - **appCatalogServer**: Check the **Enabled** box.
   - **appCatalogServerURL**: Leave blank to have machine act as a server.
   - **appDeliveryToken**: Leave blank to have machine act as a server.

5. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will appear (Figure 56).

6. The **Installed** tab (highlighted) displays all installed applications, or click on the drop-down menu below the tab to view the apps by category: Custom Apps, Custom Trigger, Feed Apps, Playbook, Playbook Templates, REST API, Spaces, STIX, Third Party, Web Hook Trigger, and Workflow Templates. Entering a term in the search box to the right of the drop-down menu will return all applications matching the search term.
7. The **Catalog** tab reflects the 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.
8. The **Updates** tab reflects the available app updates that can be accessed by the client. This tab is disabled when the machine is acting as a server.
9. The **Feeds** tab allows access to apps data from created feeds.

To configure the machine acting as a client:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 64). Select **System Settings** and the **System Settings** screen will appear (Figure 65).
3. On the left-hand menu, click on **APPS** menu option. Configure these settings as follows:
   - **appCatalogServer**: Uncheck the **Enabled** box.
   - **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. To obtain the token:
4. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 64). Select **Account Settings**, and the **Account Settings** screen will appear (Figure 66).

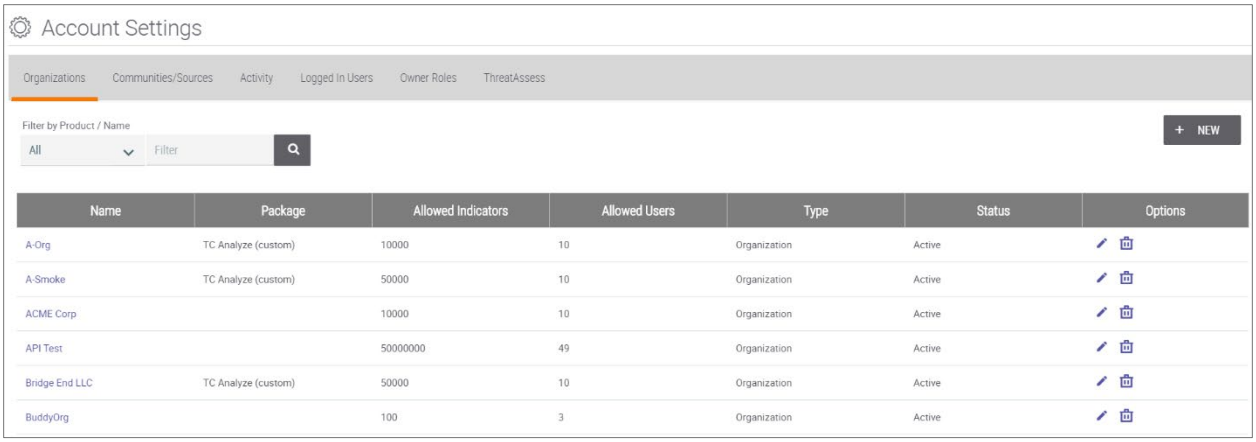

Figure 66

5. Click on an organization, and its **Organization Settings** screen will appear (Figure 67).

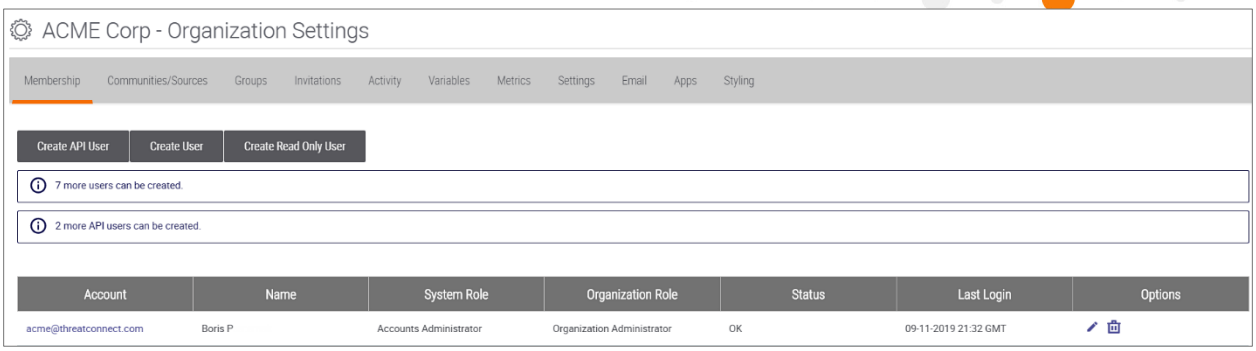

Figure 67

6. Click the **Apps** tab, and the Apps screen will appear (Figure 68).

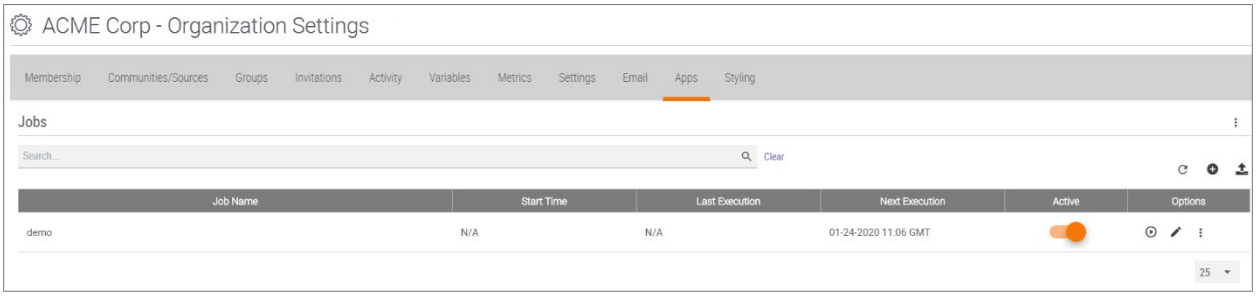

Figure 68

7. Click the **Ellipsis**  icon above the **Import Job**  icon and select **App Delivery**. The **App Delivery Token** pop-up screen will appear (Figure 69).

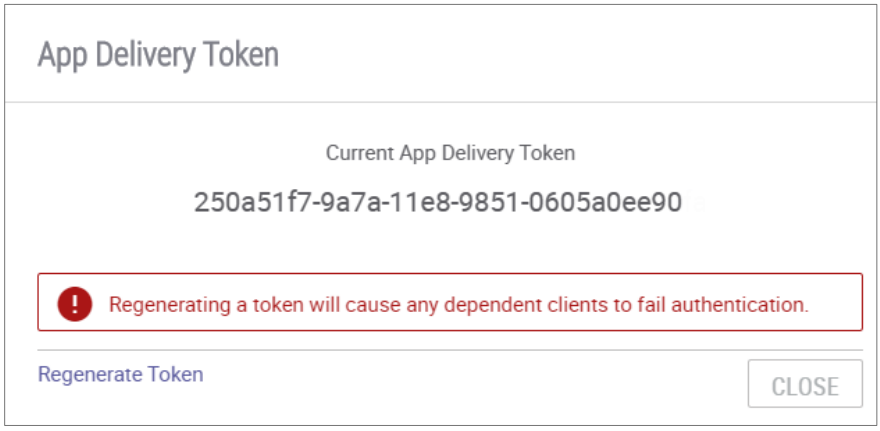

Figure 69

8. Copy the token and then click the **CLOSE** button.
9. Return to the **System Settings** screen, and enter the token in the **appDeliveryToken** text box.
10. Return to the **TC Exchange Settings** screen, and now the **Catalog** and **Updates** tabs will be enabled.

11. Click the **Catalog** tab, and the **Catalog** screen will appear (Figure 70), displaying all apps available in the system.

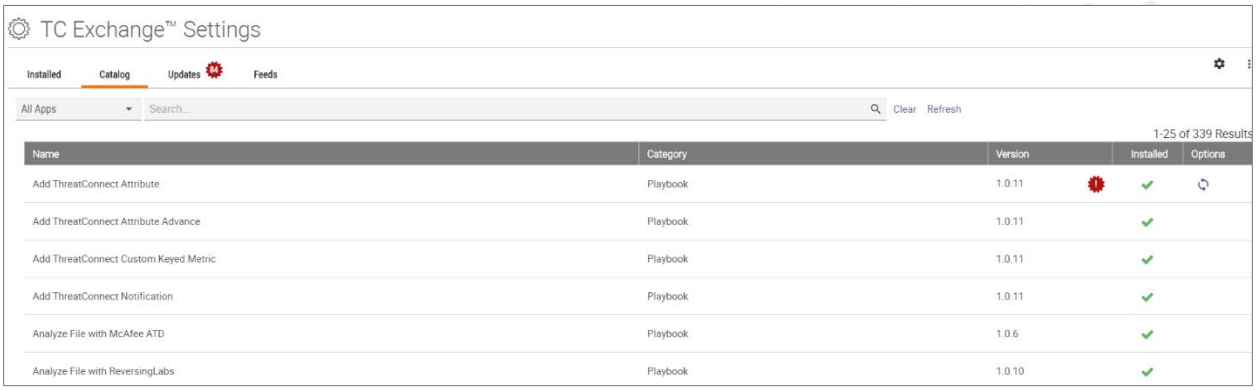

Figure 70

12. If an app is available but has not been installed, the **Install**  icon will appear in the **Options** column. Click the icon, and the **Release Notes** pop-up screen will appear (Figure 71).

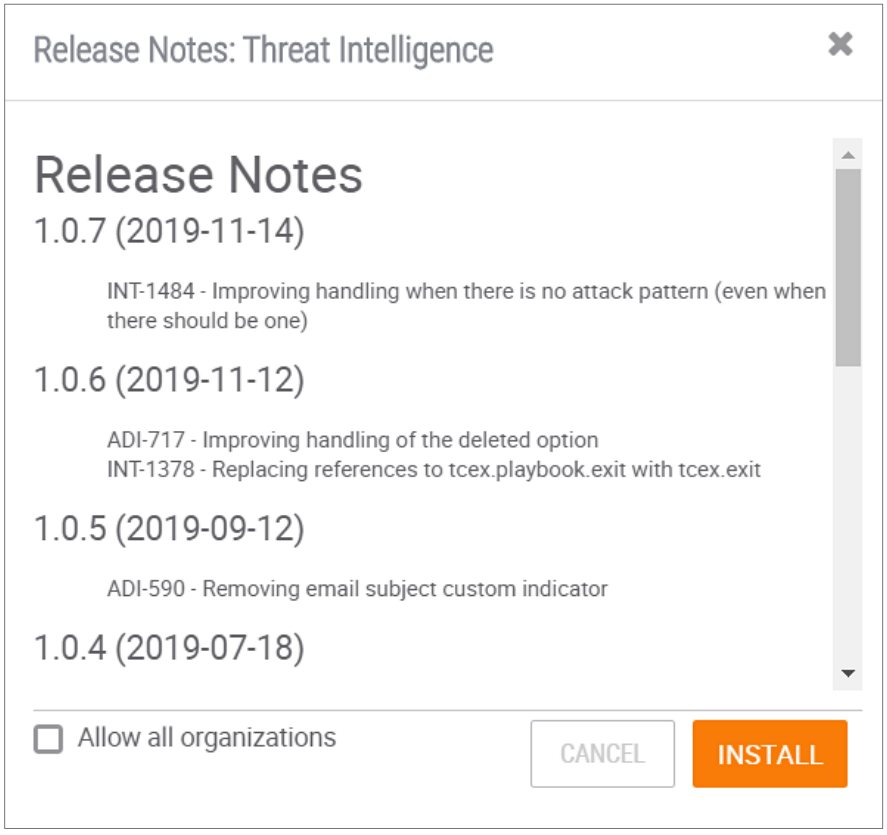

Figure 71

13. Click the **INSTALL** button to install the app. A **Success** message (Figure 72) will appear on the upper right of the screen if the app was installed. The **Feed Deployer** screen (Figure 59) will also appear. Follow the instructions in the Feed Deployment section to deploy the newly installed app.

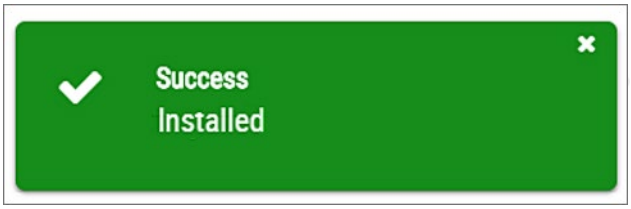

Figure 72

14. Click the **Updates** tab and the **Updates** screen will appear (Figure 73), displaying all the apps that have an update pending.

15. The **Update Available**  icon will appear on the **Updates** tab with the number of apps available for updating or next to an app in the **Catalog** table or the **Updates** table if an update is available. If there are no updates available, the **Updates** tab will not be accessible

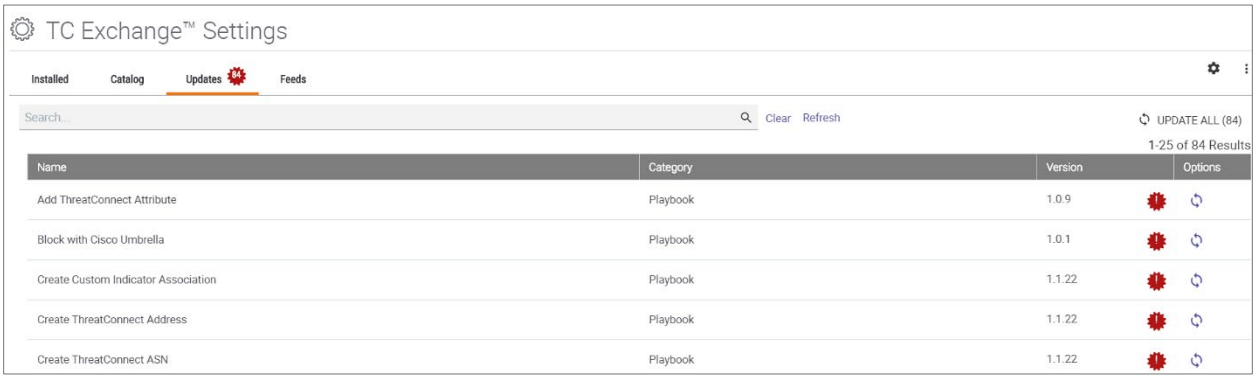

Figure 73

16. Click the **UPDATE ALL** 

button on the top right of the screen to install all available updates.

17. Or click the **Update Now**  icon in the **Options** column t update one application at a time. The **Release Notes** pop-up screen will appear (Figure 74).

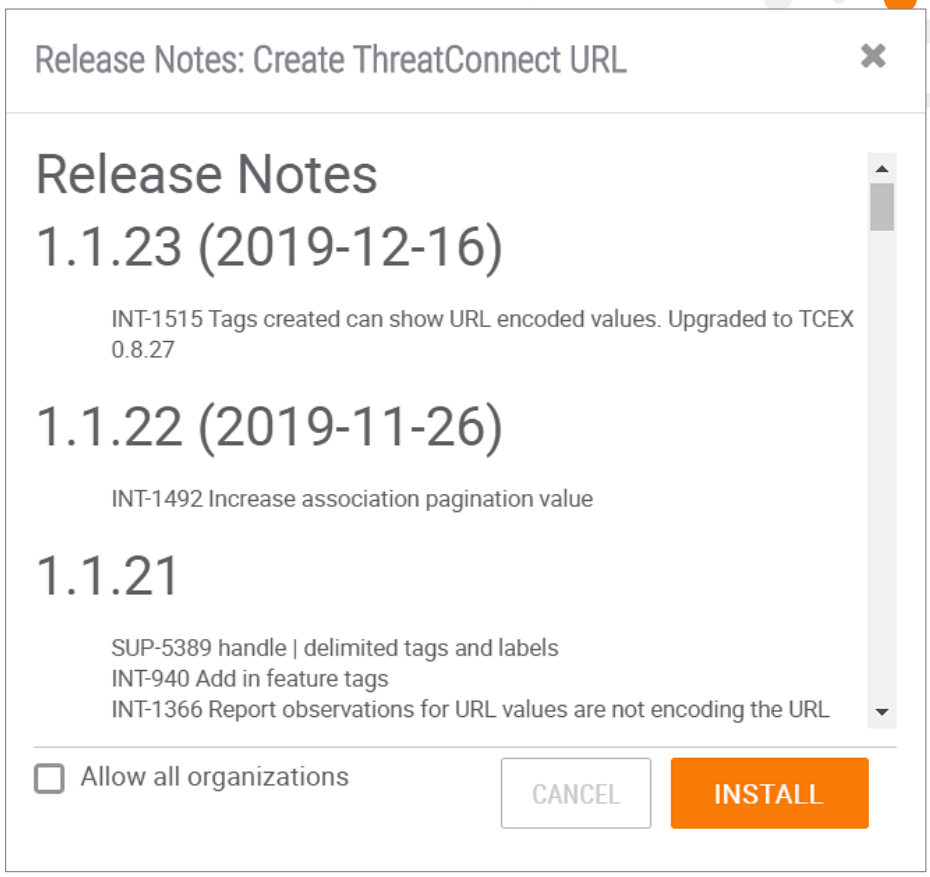

Figure 74

18. Click the **INSTALL** button to install the update.

The Feeds Tab

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.

Follow these steps to activate a Feed:

1. Log in with a System Administrator account.

2. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will appear (Figure 75).

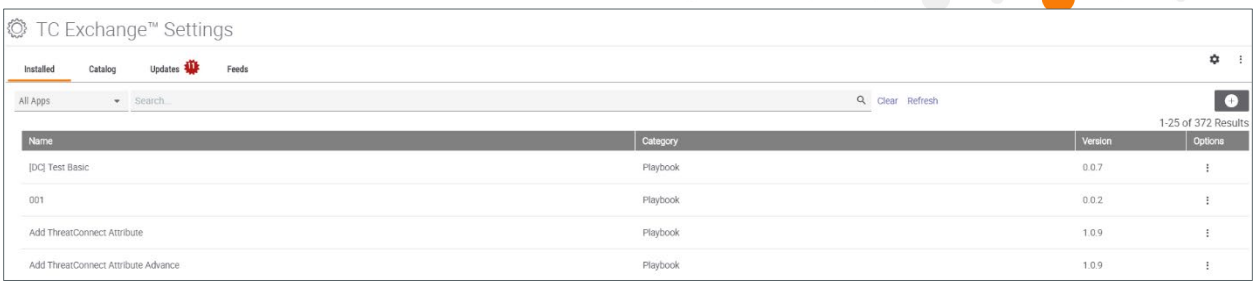

Figure 75

3. Click the **Feeds** tab and the **Feeds** screen will appear (Figure 76).

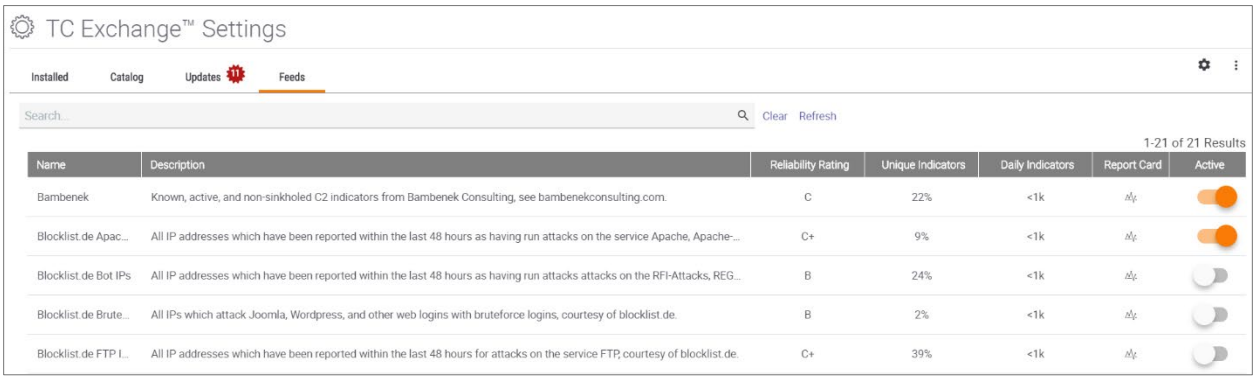

Figure 76

4. There are seven separate columns for each Feed. Columns three, four, and five—**Reliability Rating**, **Unique Indicators**, and **Daily Indicators**—represent CAL data, which offers the user criteria for activating a Feed.
5. Column six, **Report Card**, also offers additional, CAL-generated data for users to determine if they wish to activate a Feed in their system. Click the  icon, and a pop-up screen with this information will appear (Figure 77).

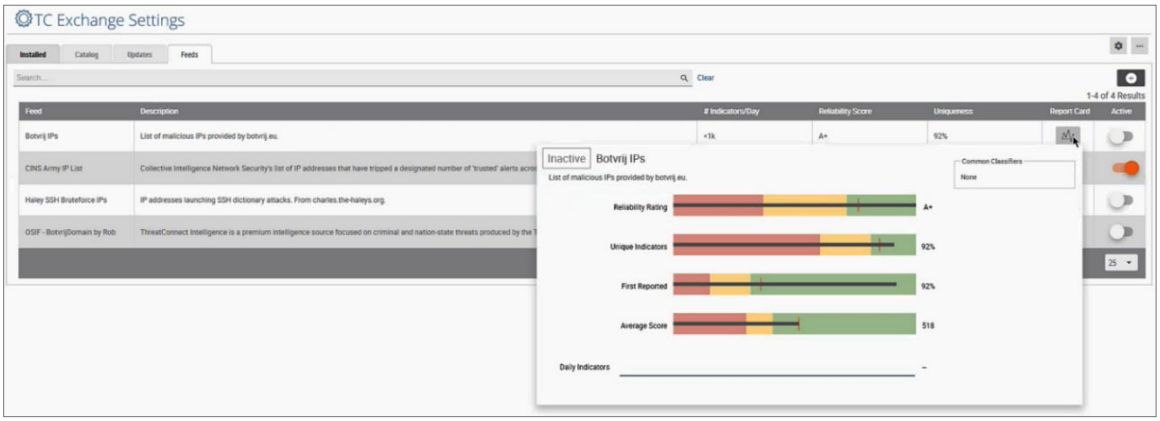

Figure 77

NOTE: 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 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 Account Settings screen, click the pencil icon for the System Organization, click on the Permissions tab of the Organization Information window, and ensure that the box for Enable CAL Data is checked.

6. Click the **Gear**  icon in the upper right, and the **App Delivery Settings** pop-up screen will appear (Figure 78). Click the drop-down menu at the bottom to select a **Default Feed Owner**.

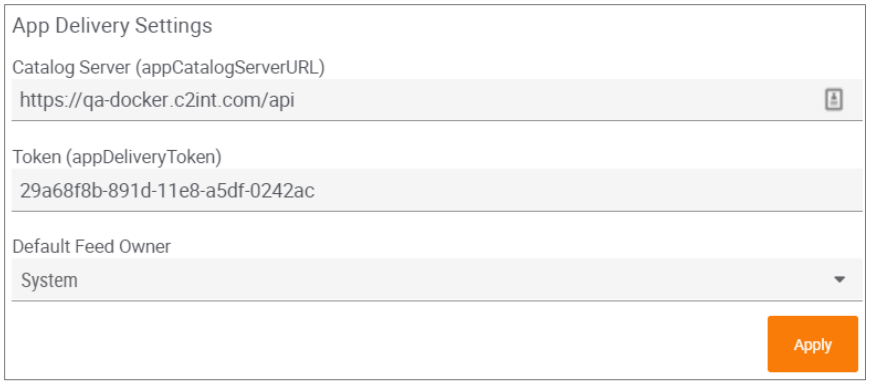

Figure 78

7. To activate a Feed, select an entry from the table and switch the gray toggle in the **Active** column to the right, and the toggle will turn orange (Figure 79). This will create a ThreatConnect Source that will access all pertinent apps data.

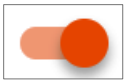

Figure 79

8. To redeploy a Feed, deactivate it by switching the toggle to the left, and then delete the job and Source in that Organization.

App Distribution

NOTE: Multi-Environment Orchestration must be configured and connected in order for the App Distribution option to appear in the menu.

To configure an app for app distribution:

1. Log in with a System Administrator account.

2. On the top navigation bar (Figure 63), place the cursor on the **Settings**  icon and the **Settings** menu will appear (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will appear (Figure 75).

3. In the **Search** bar, enter the name of an app, and after the result appears, click the vertical ellipsis in the **Options** column to bring up a pop-up menu (Figure 80).

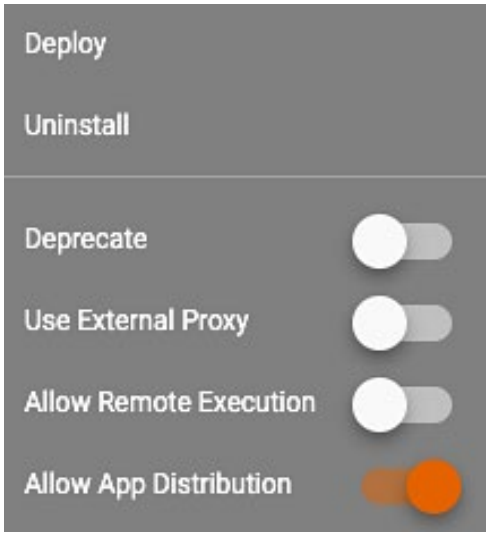

Figure 80

4. For the **Allow App Distribution** option, slide the toggle switch to the right, and it will turn from gray to orange.

The ATT&CK™ Framework

The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework is a knowledge base incorporated into the ThreatConnect platform that classifies and standardizes Adversary behavior. With the ATT&CK framework, users will be able to determine how an attack was performed by tracking Adversary techniques, which have unique IDs and multiple metadata. For further information on the uses and properties of the ATT&CK framework, refer to the MITRE ATT&CK Knowledge Base article.

A Source (Feed) named **MITRE ATT&CK** is distributed by the ThreatConnect Research Team, and users need to deploy the Feed on their ThreatConnect instance as follows:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will appear (Figure 75).
3. Click the **Feeds** tab and the **Feeds** screen will appear (Figure 76).
4. Click the **Gear** icon in the upper right, and the **App Delivery Settings** pop-up screen will appear (Figure 78). Click the drop-down menu at the bottom to select a **Default Feed Owner**.
5. In the **Source** (**Feed**) search bar, enter **MITRE ATT&CK**, and it will appear in the **Results** table (Figure 81).

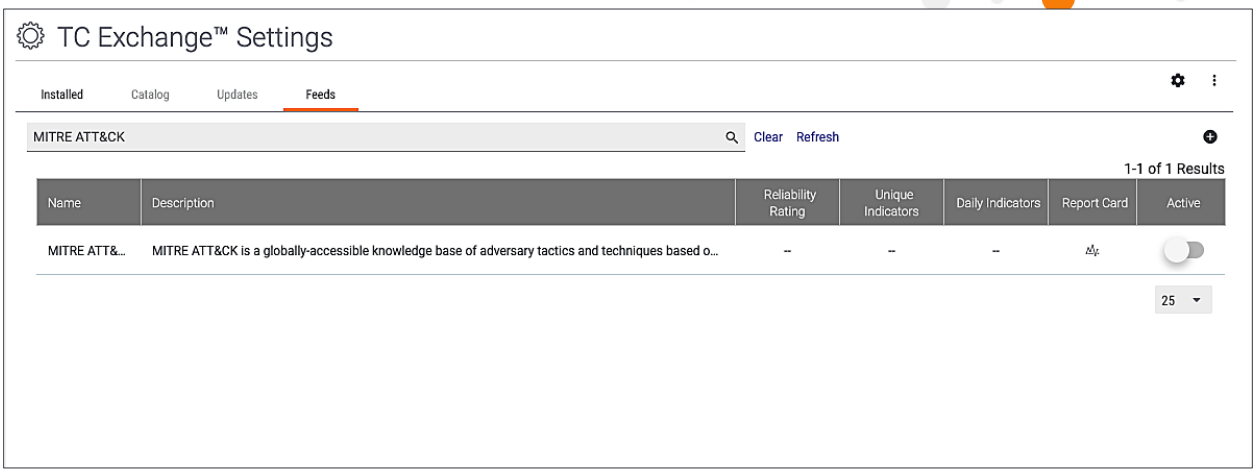

Figure 81

6. Switch the gray toggle in the **Active** column to the right. The toggle will turn orange, and a **Success** pop-up message will appear (Figure 82).

Figure 82

7. To invite users to the **MITRE ATT&CK** Source in ThreatConnect, as well as to give users rights to copy data from the Source to a private Organization, refer to the **Inviting Users to a Source** section of the *ThreatConnect Community and Source Administration Guide*.

Creating a Job

Follow these steps to create a new job:

1. Log in with a System Administrator account.

2. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will appear (Figure 75).

3. Click the **Ellipsis** icon on the upper right, and select the **System Jobs** option, and the **System Jobs** screen will appear (Figure 83).

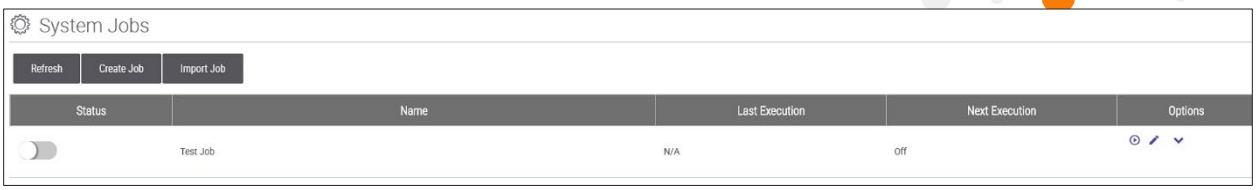

Figure 83

4. Click the **Create Job** button, and the **Configure Job** pop-up screen will appear (Figure 84).

   NOTE: Click the Refresh button to reload the list of jobs.

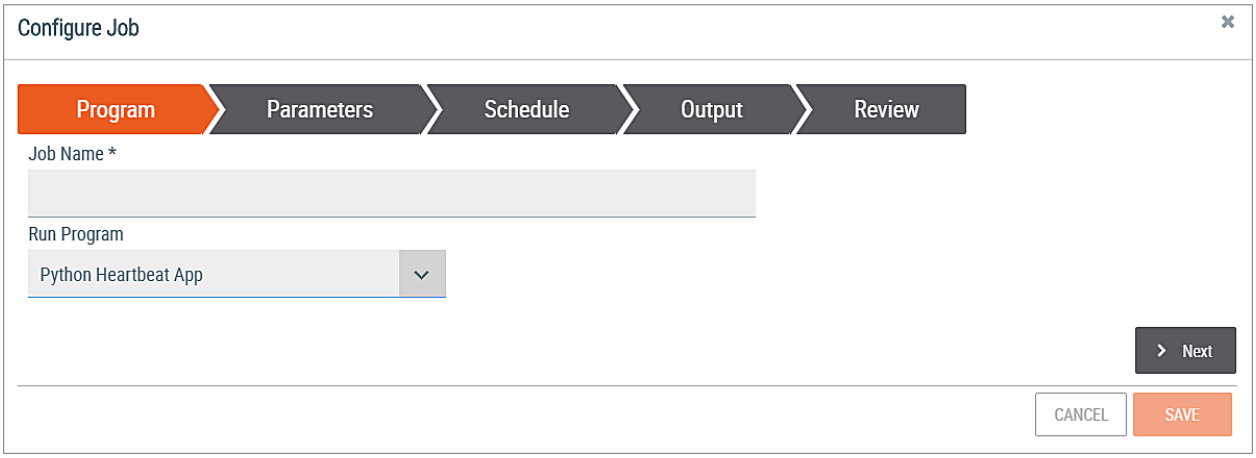

Figure 84

   a. **Job Name**: Click in the text box to enter a name.

   b. **Run Program**: Click on the drop-down menu and select a program.

5. Click the **Next** button, and the **Parameters** screen will appear (Figure 85). Enter all pertinent parameters.

   NOTE: The parameters to be entered will be different for each program selected.

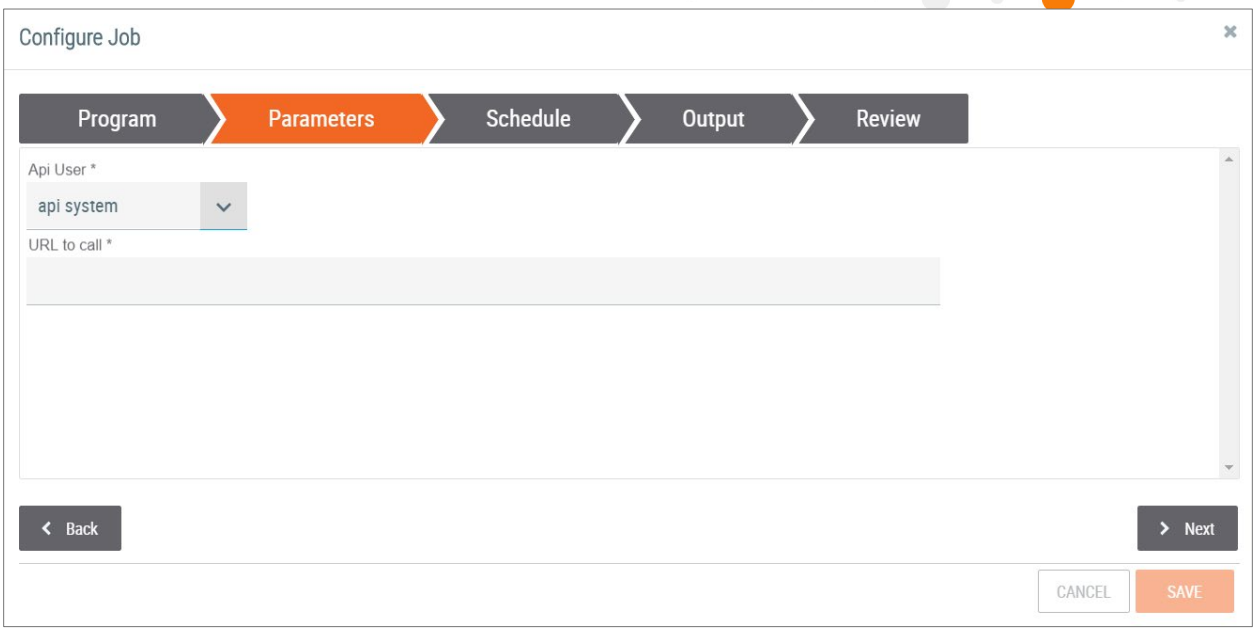

Figure 85

6. Click the **Next** button, and the **Schedule** screen will appear (Figure **86**).

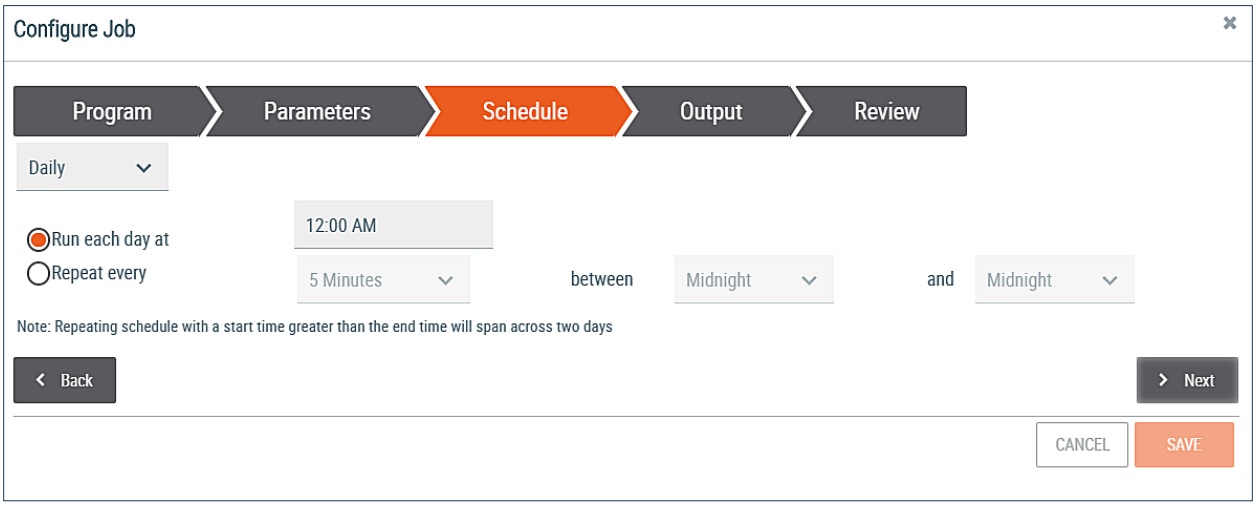

Figure 86

a. **Daily**: Click on the drop-down menu to select whether the job should run daily, weekly, or monthly.

b. **Run each day at / Repeat every**: Enter the desired time of day on which to run the job, or enter a time interval during which to repeat the job.

7. Click the **Next** button, and the **Output** screen will appear (Figure 87).

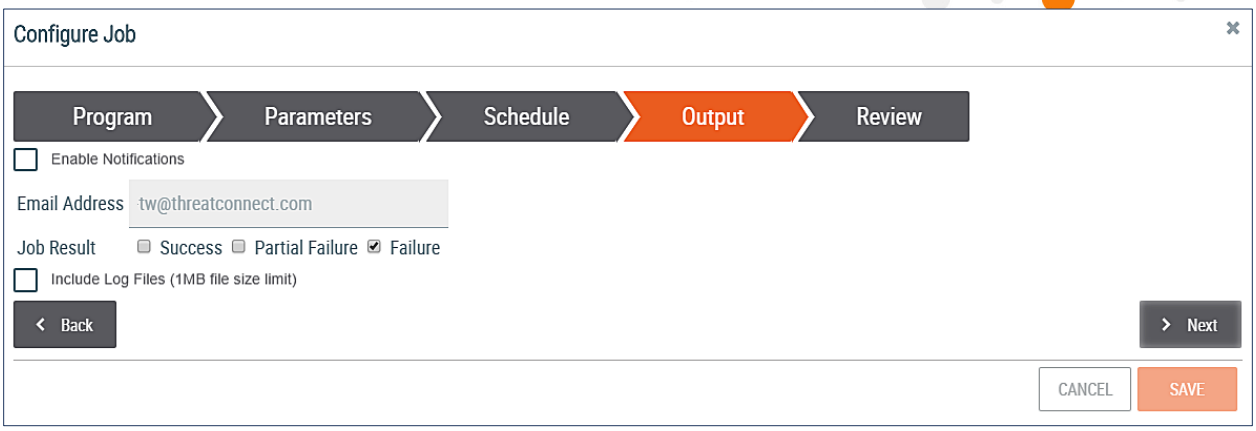

Figure 87

a. **Enable Notifications**: Click the checkbox to enable notifications.

b. **Email Address**: Enter the email address to which notifications should be sent.

c. **Job Result**: Click the box(es) for the job results for which notifications should be sent.

d. **Include Log Files**: Check the box to include log files of 1MB or less in the notification email.

8. Click the **Next** button, and the **Review** screen will appear (Figure 88).

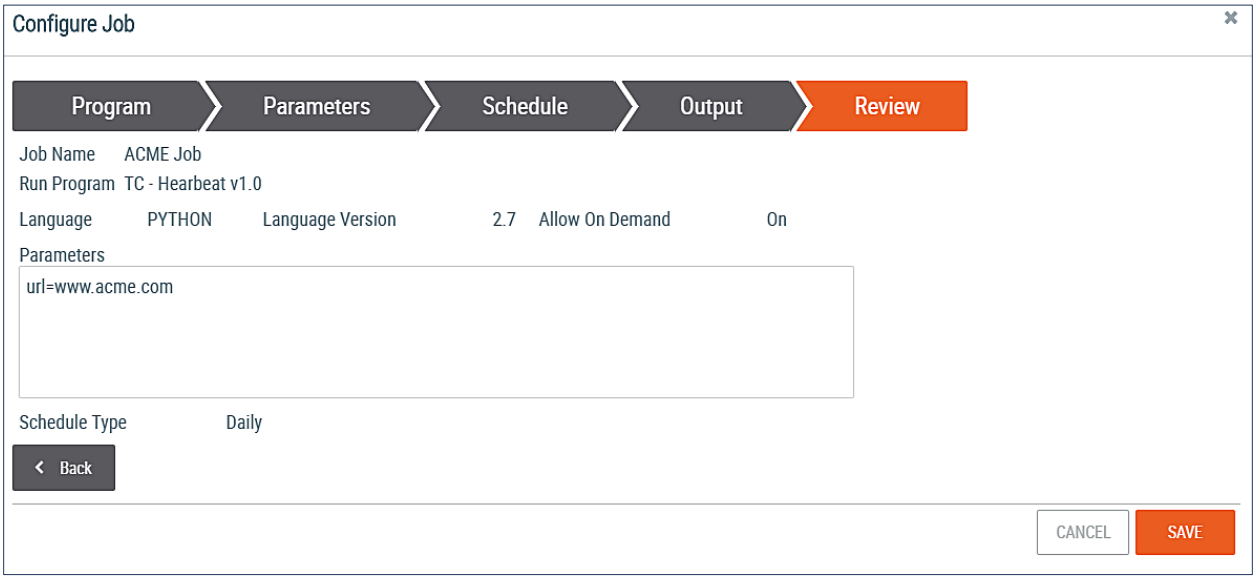

Figure 88

9. Review the Job Name, Run Program, Language, Language Version, Allow On Demand, Parameters, and Schedule Type values to ensure they are correct.

10. Click the **SAVE** button.

Editing or Running a Job

Follow these steps to edit or run a job:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will appear (Figure 75).
3. Click the **Ellipsis** icon on the upper right, and select the **SYSTEM JOBS** option, and the **System Jobs** screen will appear (Figure 83).
4. The following functions can be performed for an existing job in the **System Jobs** table:
   - Click on the **Run Now** icon 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 on the **Modify** icon to edit a job's setting.
   - Click on the **Details** icon to view a pop-up menu that provides the following options:

     Delete the job, **View Details** for a 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**, **Add Attributes**, **Published Files**, and **Export Job**.

Data Store

Data Store is a feature that allows TC Exchange apps to persist data using Elasticsearch. The app is intentionally decoupled from the data to offer a flexible data-sharing Environment while still allowing a private database for apps that require it. As such, the information provided by Data Store is essentially "read only."

Data Store is available to any Job or Spaces apps requiring persistent storage. There is no initial setup required, and the Elasticsearch resources are available as an extension of the ThreatConnect API. The app will interact with Elasticsearch exclusively through the API to enforce proper security in a multi-tenant Environment.

NOTE: To enable ThreatConnect to use Data Store, the System Settings must have "elasticSearchEnabled" set to "true," and "elasticSearchUrl" must be defined.

Follow these steps to use the Data Store feature:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will appear (Figure 75).

3. Click the **Ellipsis** icon on the upper right, and select the **Data Store** option, and the **Datastore** screen will appear (Figure 89).

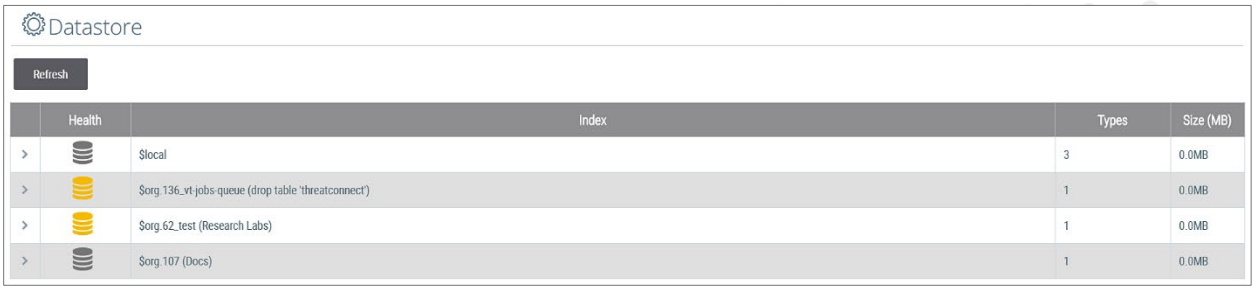

Figure 89

4. Click the **Right-Arrow**  icon on the left of the index whose data are to be viewed. A table showing an expanded view of the types within that index will appear (Figure 90).

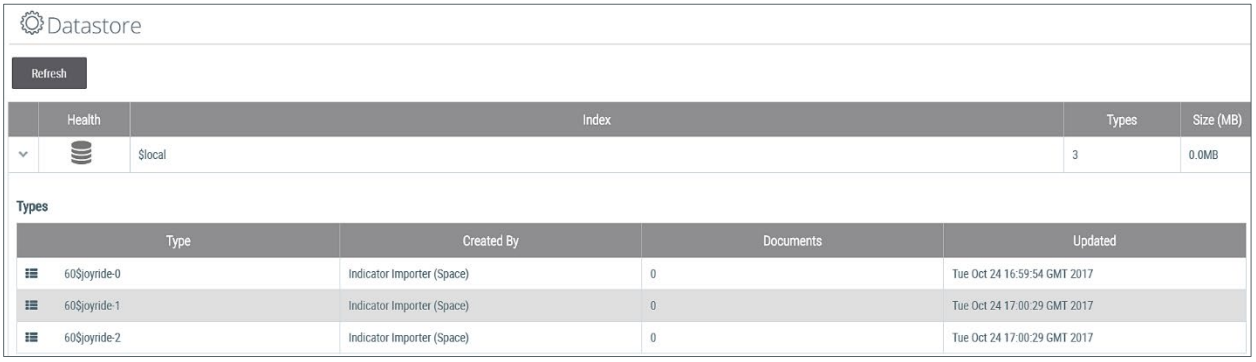

Figure 90

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. Dashboard creation an editing, as well as other functions and properties of dashboards, are not discussed in this Administration Guide, since those topics are discussed at length in the Dashboard Knowledge Base article.

Multi-Environment Orchestration

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

Configuring the ThreatConnect Instance

To configure the ThreatConnect instance:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), place the cursor on the **Settings**  icon and the **Settings** menu will appear (Figure 64). Select **System Settings** and the **System Settings** screen will appear (Figure 65).
3. Click the **Apps** tab on the left side of the screen, and configure these settings as follows:
4. **appMessageBrokerHost**: Enter this domain name, which will be the instance being used plus the number of any available port in the system.

   NOTE: If this value is not set, the** Playbooks **tab on the navigation menu will not display the** Environments **option.
5. **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.

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:

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

Overview

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
- Minimize the time it takes to assess impact
- Maximizing the amount of information that can be turned into actionable intelligence for later use

Components of Case Management

- **Case**: Contains all required elements of a notable event in a logical structure. Used to build an incident or capture key evidence to enable the security team to decide if a case should be escalated.
- **Workflow**: Used in a case to manage the sequence of tasks and guide the security team through a standardized process to uncover elements of a case. Workflows can be augmented in each case as unique challenges arise.
- **Workflow Template**: Workflow starts with the creation of Workflow templates, which are processes users define for their team. A user, for example, might create one template for phishing analysis, one for alert triage, and maybe several different ones for handling breaches. By codifying these processes in a template, users can reduce the risk of missing critical steps or artifacts during an investigation, because processes and procedures that are stored externally can be captured in ThreatConnect and tied back to threat intel.
- **Task**: Individual units of work a user must perform to complete a case. Tasks can be manual (a user performs them) or automated (a Playbook performs them).
- **Artifact**: Used in a case to collect key evidence to support the Workflow. Not all artifacts are significant and some can be loosely correlated to Threat Intelligence. Examples of artifacts include domains, email addresses, log files, email, PCAP, screen shots, SIEM event files, and malware documents.
- **Note**: The primary mechanism to capture the progress of a case in human-readable form. Notes enable a security team to journal key data findings in unstructured form.
- **Timeline:** A recording of actions performed on a Case in chronological order. Timelines enable the security team to quickly observe key events over a span of dates in a Case. They also allow users to drill down into important timeframes in the lifespan of a Case.

Accessing Workflow

Follow these steps to configure an account:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), place the cursor on the **Settings**  icon, and the **Settings** menu will appear (Figure 64).
3. Select **Account Settings**, and the **Account Settings** screen will appear (Figure 66).
4. Click the **Edit**  icon in the **Options** column of the Organization whose information is to be configured. The **Organization Information** pop-up screen will appear (Figure 91) with the **Standard Options** tab underlined.

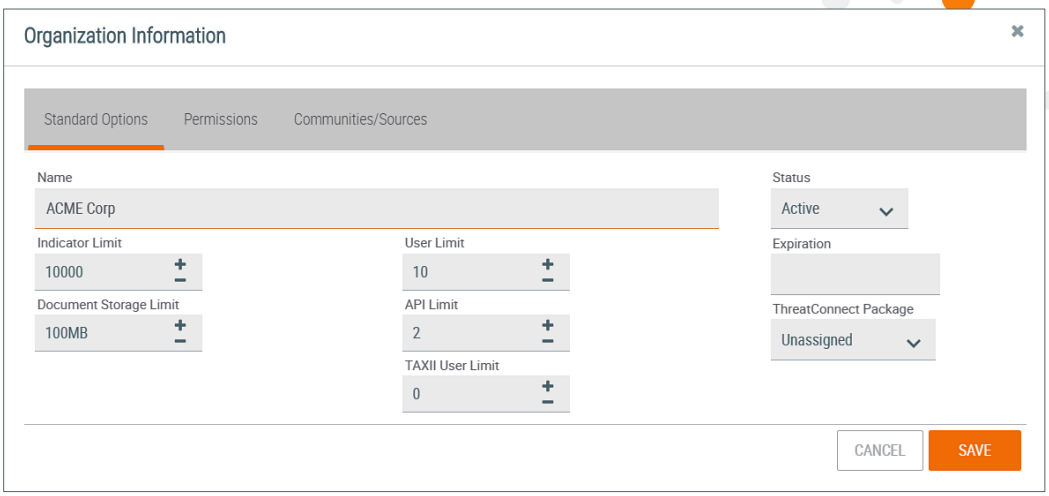

Figure 91

5. Click the **Permissions** tab to view the Permissions screen (Figure 92).

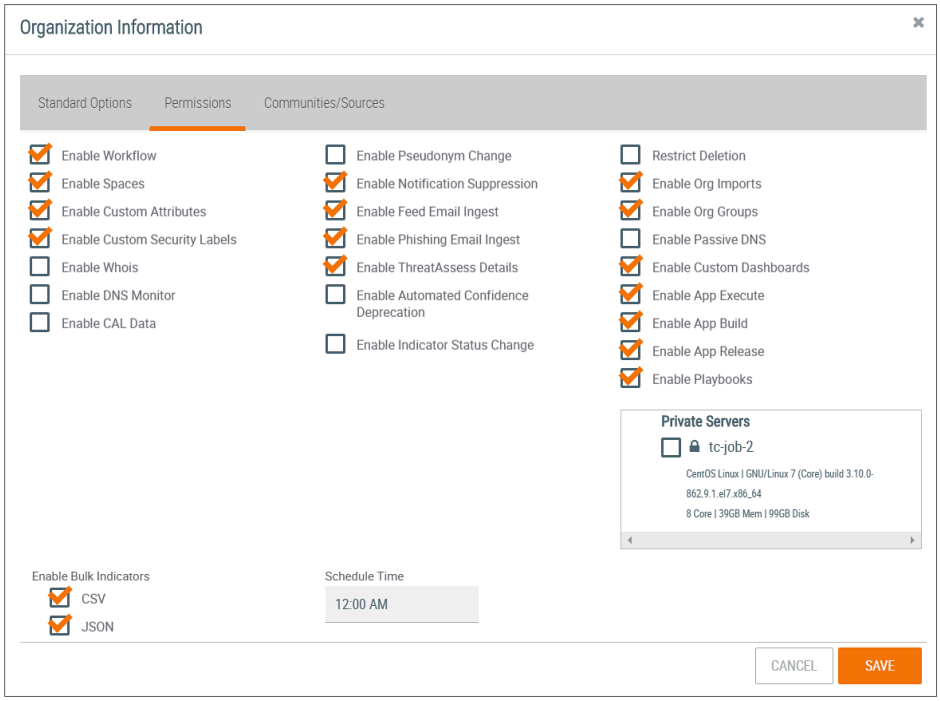

Figure 92

6. Click the Enable Workflow checkbox and then click the **SAVE** button.

The Workflow Tab

The following sections offer a general overview of the **Workflow** tab in the ThreatConnect platform and its application to Case Management. Refer to the pertinent Knowledge Base articles for additional, and more detailed, information.

To access the **Workflow** tab:

1. Log in with a System Administrator account.
2. Click the **Workflow** tab, and the **Workflow** screen will appear with the **Tasks** tab selected (Figure 93). Otherwise, hover the cursor over the **Workflow** tab to select the screen to enter (**Cases**, **Tasks**, or **Templates**).

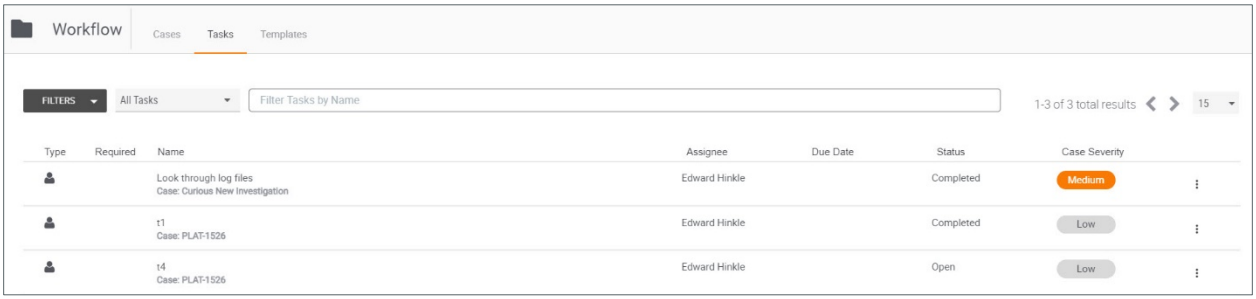

Figure 93

3. The first step in Case Management is to create a Workflow Template. Click the **Templates** tab, and the **Templates screen** will appear (Figure 94).

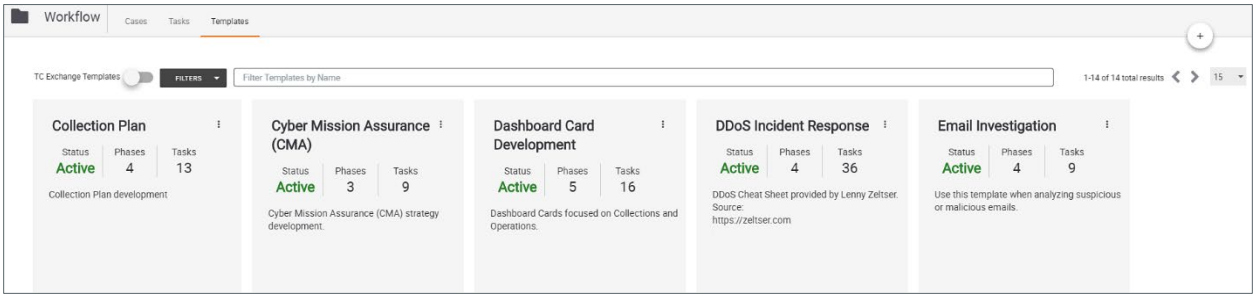

Figure 94

4. Click the **Plus**  button in the upper-right portion of the screen, and choose the **New Template** option. The **New Workflow Template** screen will appear (Figure 95).

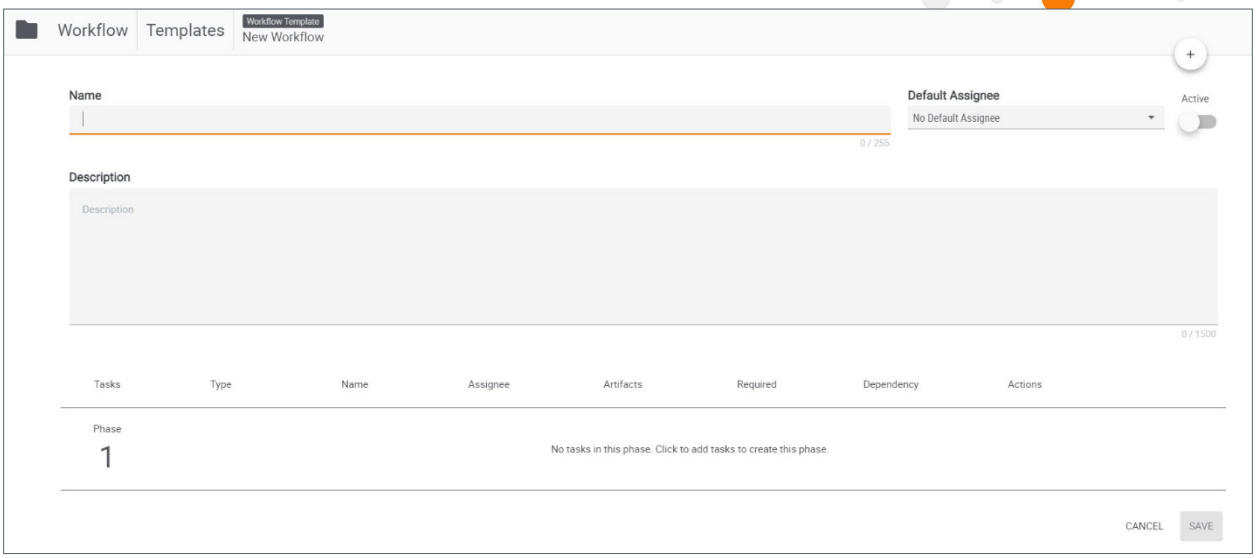

Figure 95

5. Fill in the necessary fields, and move the **Active** toggle to the right. The slide bar will turn orange once template is activated.

6. Click the **Plus**  button above the **Active** toggle, and the **Create Task** pop-up screen will appear (Figure 96).

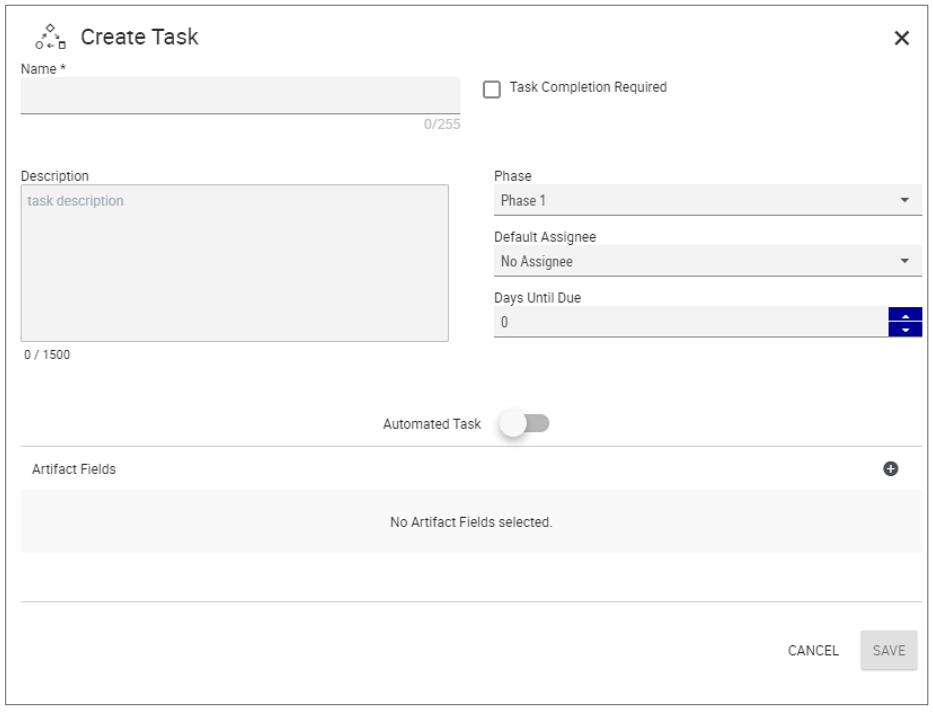

Figure 96

7. Fill in the necessary fields:
   - **Task Completion Required**: Check this box to specify if the Task is required for the Case to be completed.
   - **Phase**: A Phase is a numerical container in which to group a Task.
   - **Default Assignee (optional)**: A user or group may be specified here, to which the task will be assigned by default.
   - **Dependency**: This field will only appear once a Task has been created, so that a second Task can be dependent on the first.
   - **Automated Task**: An Automated Task is dependent on a Workflow Playbook.
   - **Artifact Fields (optional)**: Click the **Plus** button to fill in the appropriate parameters. Artifacts Fields are where information is collected as the user completes a task.
8. Click the **SAVE** button to return to the **Workflow Template** screen, and click **SAVE** button once more to save the new Template.

   NOTE: A System Administrator may also download an existing Workflow Template file from TC Exchange.
9. Click the **Cases** tab, and the **Cases** screen will appear (Figure 97).

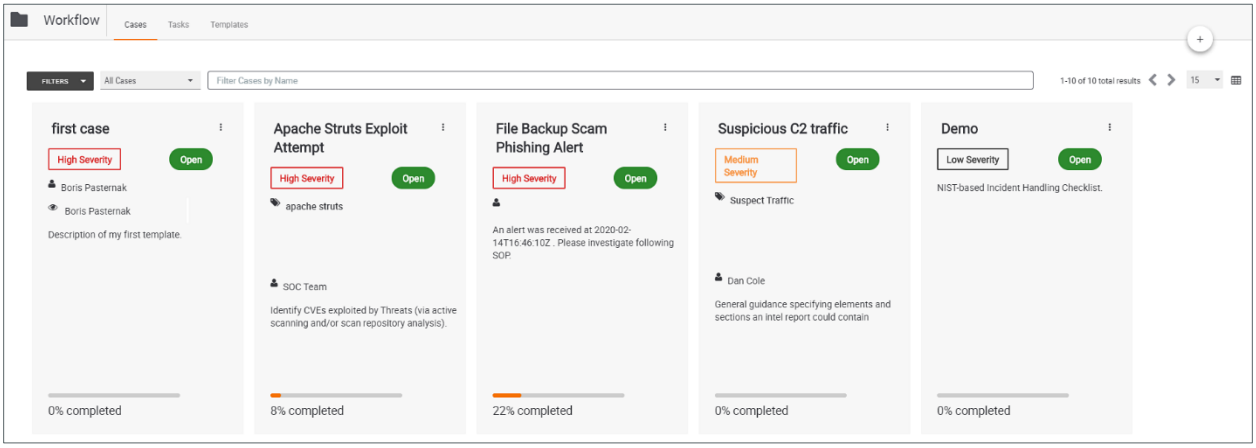

Figure 97

10. Click the drop-down button next to the **FILTERS** menu to select which Cases to display (e.g., All Cases, My Open Cases, etc.).
11. Click the **Plus** button in the upper-right portion of the screen, and the New Case pop-up screen will appear (Figure 98).

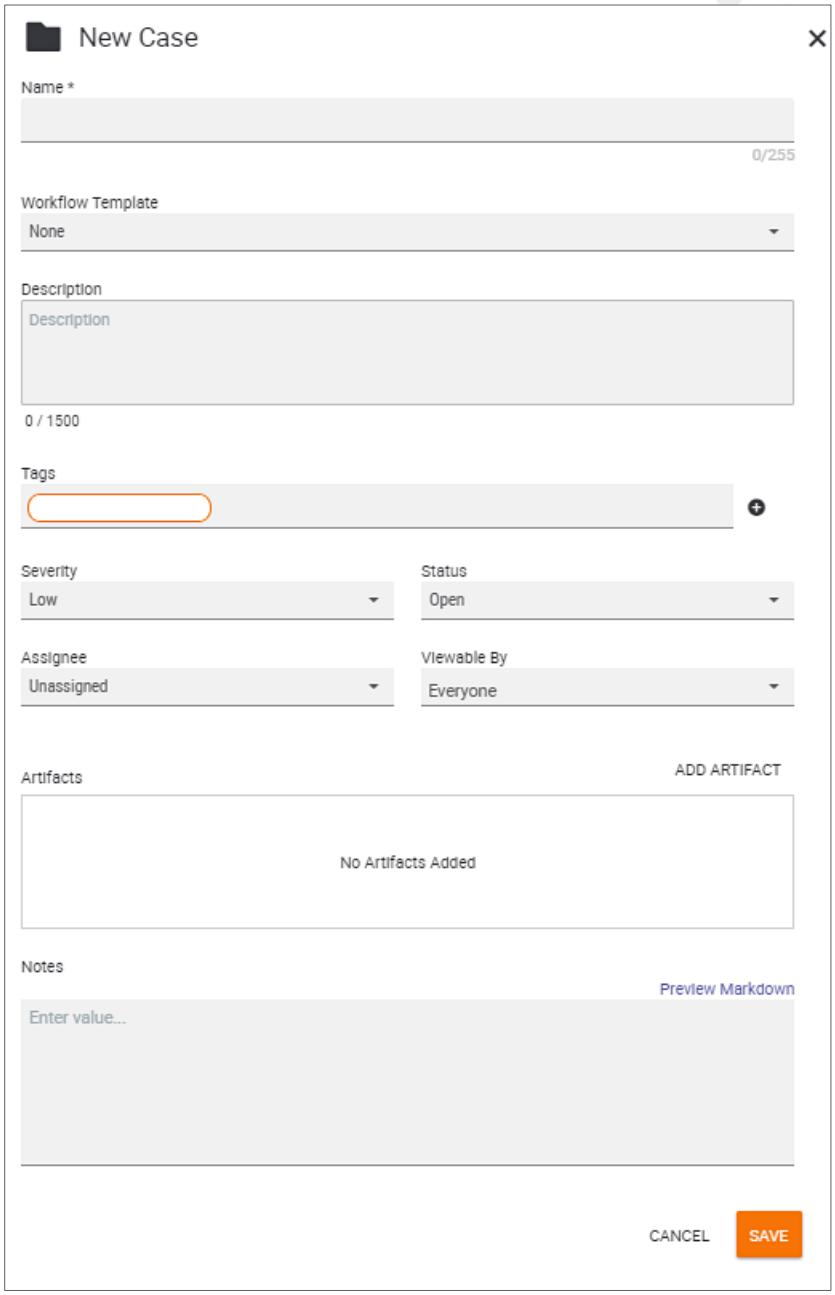

Figure 98

12. Fill in the pertinent fields and click the **SAVE** button. The new Case will appear in the **Cases** screen.
13. Click on a Case and the **Case Details** screen will appear (Figure 99).

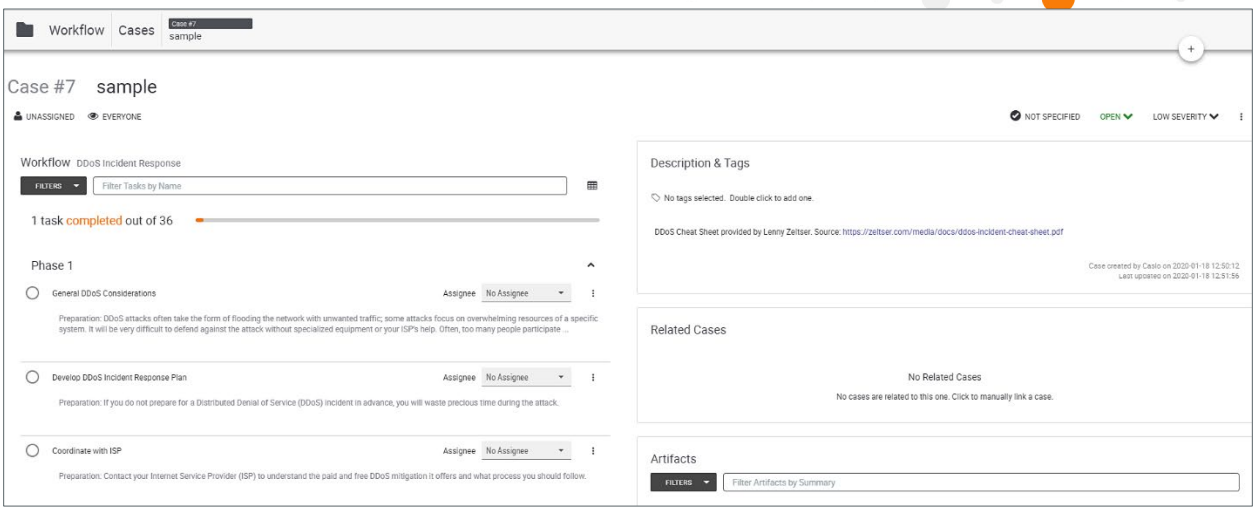

Figure 99

14. In the upper-left portion of the screen, there are options for selecting an assignee and for viewing permissions. In the upper-right portion, there are options for selecting Case status, for closing the case, for assigning severity, and for deleting the Case. The rest of the screen details Workflow properties, Phases, Description, Tags, Related Cases, Artifacts, Notes, and Timeline.
15. Click Workflow in the upper-left portion of the screen to return to the main Workflow screen, and the **Tasks** tab will be highlighted. (Figure 93). This screen allows users to filter which Tasks they want to view (e.g., All Tasks, My Open Tasks, etc.)

Playbooks System Features

Playbooks allow users to automate cyber-defense 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 following sections cover Playbook functionality that can only be executed 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, Templates, and Triggers—refer to the pertinent Knowledge Base articles.

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.

The Playbooks Queue

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

- Queue Size: number of Playbooks in the queue
- Wait Time: the estimated number of seconds a Playbook will wait for execution
- Queued Playbooks: the Playbooks that are in the queue

Additionally, the UI permits the user to manage the queue.

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), hover the cursor over **Playbooks**, and select the **Activity** option. The **Activity** screen will appear (Figure 100).

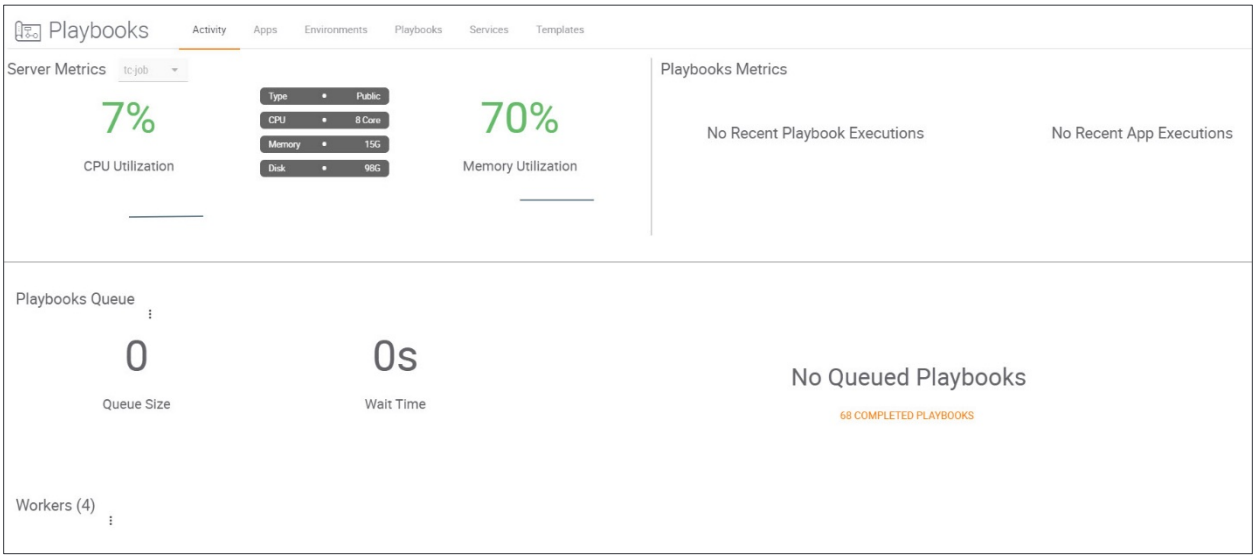

Figure 100

3. Click the vertical ellipsis next to the words **Playbooks Queue**, and the following options will be available:
   - Pause Queue: This action prevents new Playbooks executions from occurring.
   - Resume Queue: This action allows new Playbooks executions to occur.
   - Flush Queue: This action removes all messages from the queue.

Workers

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.

To change a Worker count:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), hover the cursor over **Playbooks**, and select the **Activity** option. The **Activity** screen will appear (Figure 100).
3. Click the vertical ellipsis next to the word **Workers**, and then click on **Change Worker Count**. The **Change Worker Count** pop-up screen will appear (Figure 101).

   NOTE: Users that attempt to add more Workers than their license permits will not see an increase in the Worker Count total, although no message will alert them to the fact.

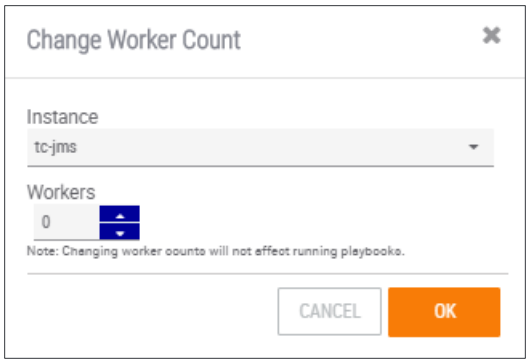

Figure 101

4. Make sure the correct instance is selected, and then use the up-and-down arrows to change the Worker count and click **OK**. The new count will be reflected next to the word **Workers** on the **Activity** screen.

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

To create an Environment:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), hover the cursor over **Playbooks**, and select the **Environments** option. The **Environments** screen will appear (Figure 102).

a. An Environment can be created but set to **Inactive** by toggling to the left the switch at the bottom.

b. An Environment can be created and set to **Active** by toggling to the right the switch at the bottom.

c. If the Environment has not been connected to an Environment Server, then **No Environment servers attached** will appear at the bottom of the screen.

d. The top part of an Environment will be green if the environment is active and configured to an Environment Server; yellow if the Environment is active, but not configured to an Environment Server; and gray if the Environment is inactive.

NOTE: Users that attempt to activate more Playbooks than their license permits will receive a message alerting them that they are not able to do so.

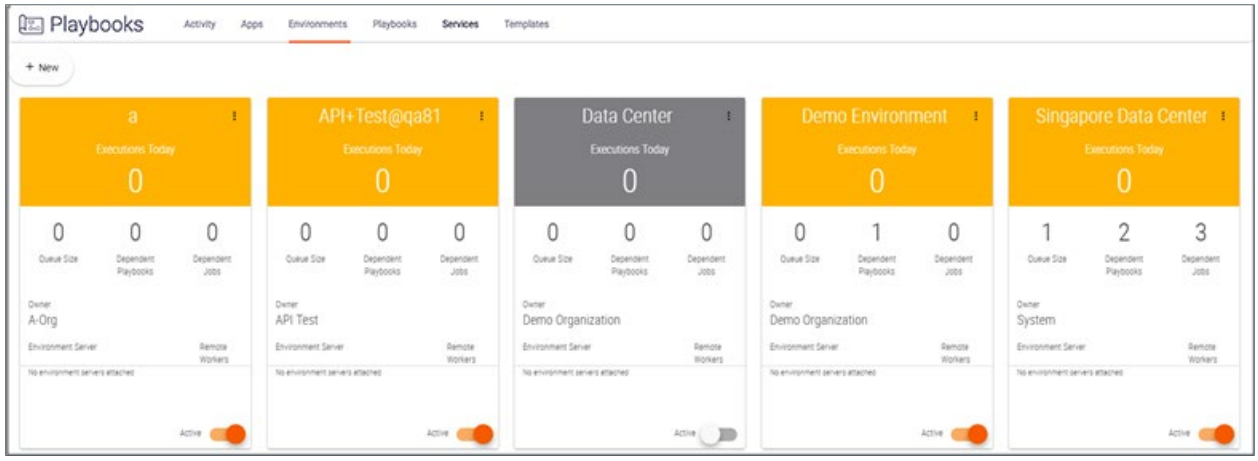

Figure 102

3. To create an Environment, click the **+ NEW** button at the upper left of the screen, and the **New Environment** screen will appear (Figure 103).

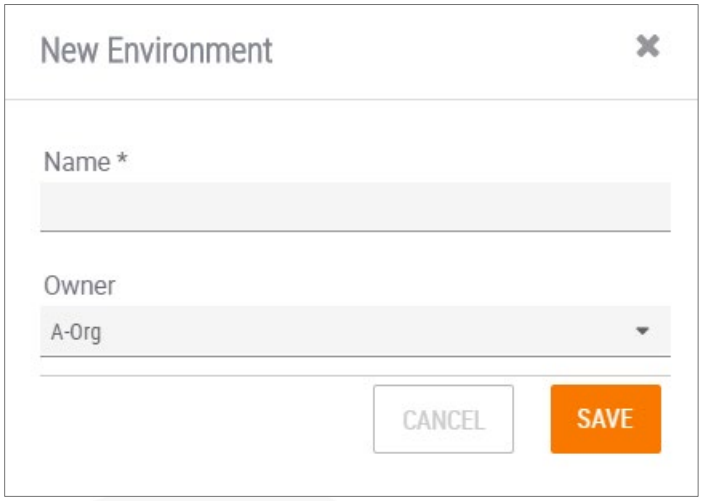

Figure 103

4. Fill in the Name field, and click on the drop-down menu to select the Environment Owner.
5. Click the **SAVE** button to create the Environment.

Running an Application in a Remote Environment

Refer to the [Playbooks Knowledge Base Article] for additional information.

To run an application in a remote Environment:

1. Log in with a System Administrator account.

2. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon and the **Settings** menu will appear (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will appear (Figure 104). The **Installed** tab will be highlighted, displaying all installed applications, or click on the drop-down menu below the tab to view the apps by category: Custom, Feed, Playbooks, Playbooks Template, Spaces, STIX, and Third Party. Entering a term in the search box to the right of the drop-down menu will return all applications matching the search term.

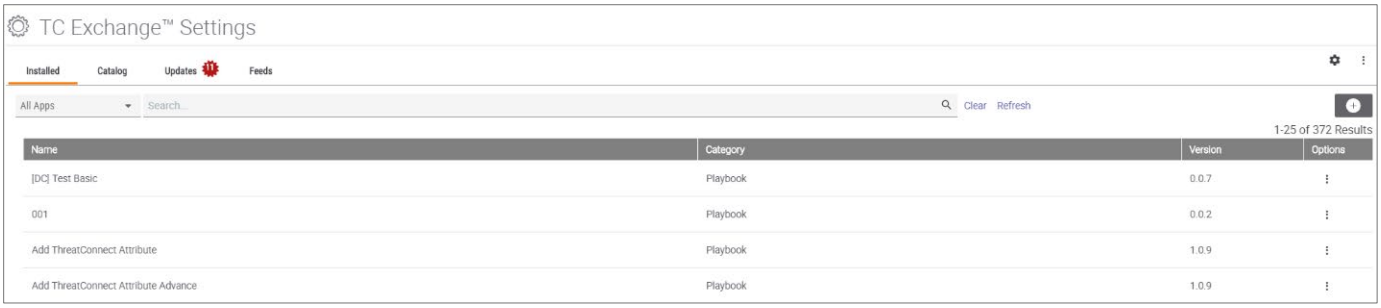

Figure 104

3. Select an app and click the vertical ellipsis in the **Options** column to bring up a pop-up menu (Figure 105).

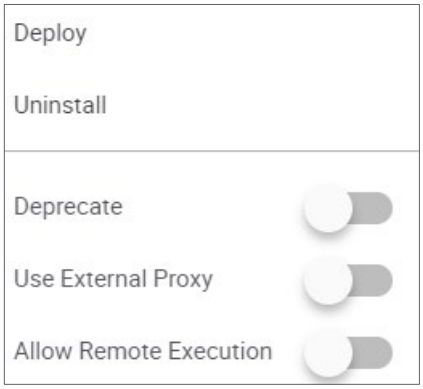

Figure 105

NOTE: Not every option listed in Figure 105 will be available for every application.

4. From this menu, a user can allow remote execution of an app by sliding the **Allow Remote Execution** toggle switch to the right. It will turn from gay to orange.

The Apps Screen

Creating a Playbook App

For detailed instructions on how to create, clone, edit, or import a Playbook app—among other topics—refer to the App Builder article in the Knowledge Base.

To create a Playbook app:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), hover the cursor over **Playbooks**, and select the **Apps** option. The **Apps** screen will appear (Figure 106Figure 100).

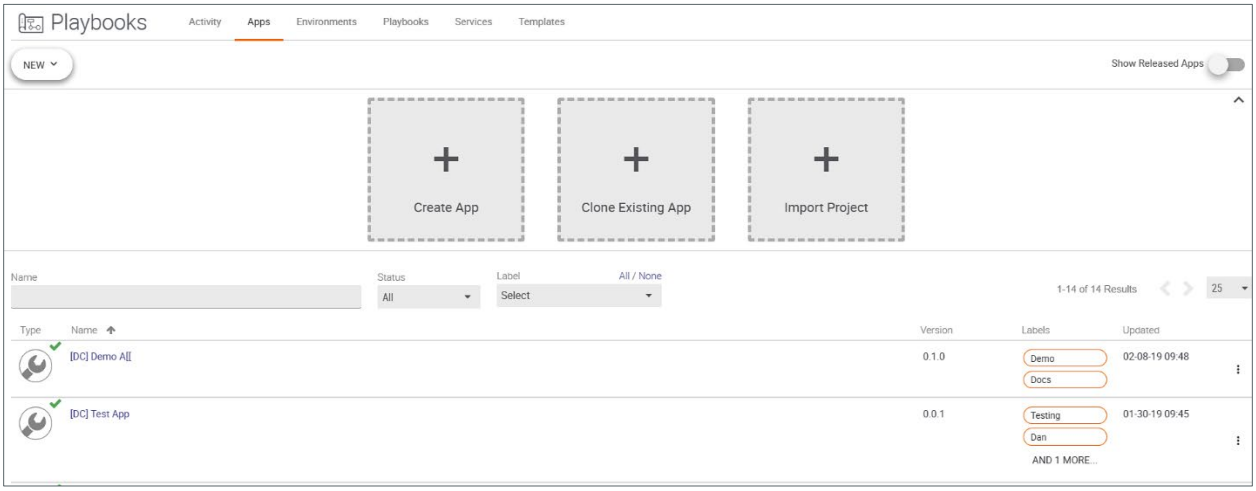

Figure 106

NOTE: The three gray squares at the top of the Apps screen will only appear if the Show Released Apps toggle bar is in the Off (gray) position.

3. Click the **Create App** gray square with the plus sign, and the **Create App** pop-up menu will appear (Figure 107). Alternatively, click the **NEW** drop-down menu at the upper-left portion of the screen, and select the **Create App** option.

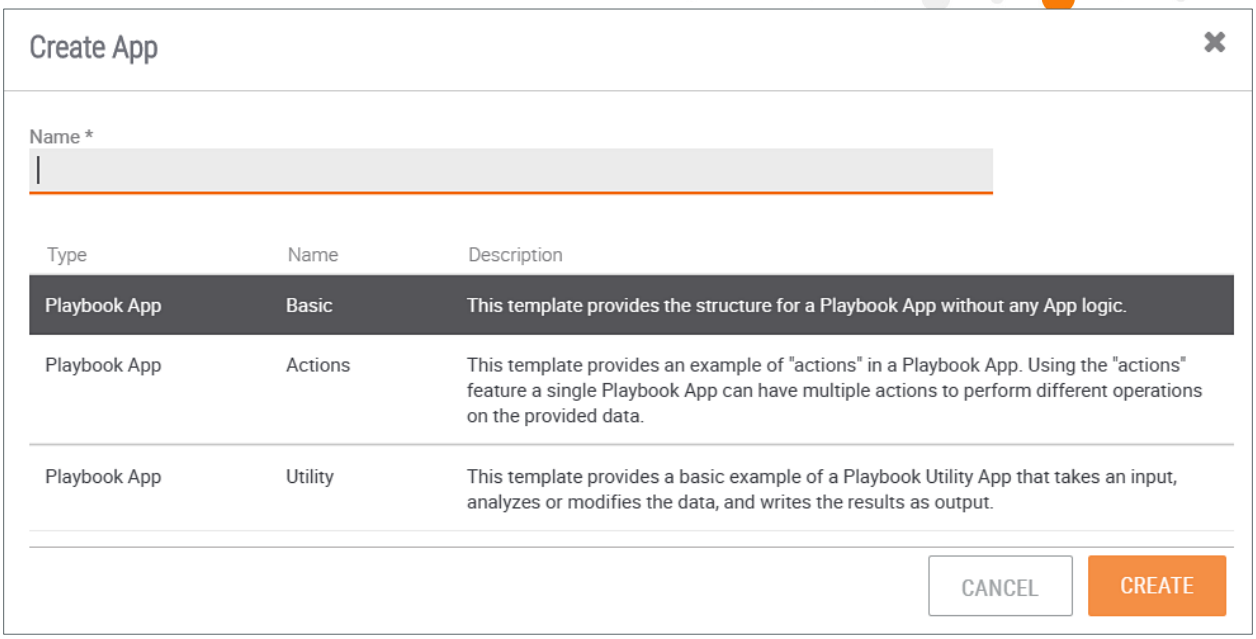

Figure 107

- **Name**: Enter a name for app.
- **Template**: Select one of the given templates for the app project.

4. Click the **CREATE** button to create the app.

Cloning a Playbook App

To create a Playbook app:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), hover the cursor over **Playbooks**, and select the **Apps** option. The **Apps** screen will appear (Figure 106).
3. Click the **Clone Existing App** gray square with the plus sign, and the **Show Released Apps** toggle bar will switch to the On (orange) position. The screen will display all apps that are on TC Exchange and available for cloning into the App Builder (Figure 108). Alternatively, click the **NEW** drop-down menu at the upper-left portion of the screen, and select the **Clone Existing App** option.

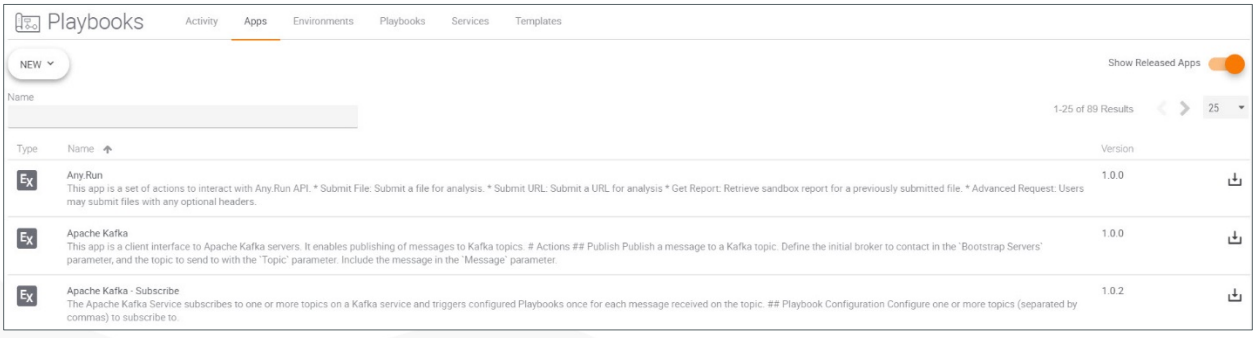

Figure 108

4. Select an app to be cloned, and click the **Clone**  icon on the right of the screen. A new version of the app will open in the App Builder.

Importing a Playbook App

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), hover the cursor over **Playbooks**, and select the **Apps** option. The **Apps** screen will appear (Figure 106Figure 100).
3. Click the **Import Project** gray square with the plus sign, and an **Open** pop-up screen will appear. Navigate to the appropriate directory and select an **.abx** file to. The file will open as a project in the **App Builder** screen. Alternatively, click the **NEW** drop-down menu at the upper-left portion of the screen, and select the **Import Project** option.

The Services Screen

Apps normally run for a specified period of time. Service apps, however, are microservices, which constantly run in the background. The two currently available Service apps are Custom Triggers and WebHook Triggers. They are installed exactly like other apps.

- Custom Trigger app: Suited for Push-type events to handle a custom protocol, raw-port access, or Pull on a configured interval
- WebHook Trigger app: Suited for Push-type events that have complex data requiring normalization, filtering or a better UX

Creating a Service App

To create a service app:

1. Log in with a System Administrator account.
2. On the top navigation bar (Figure 63), hover the cursor over **Playbooks**, and select the **Services** option. The **Services** screen will appear (Figure 109), displaying the Services apps that are installed.

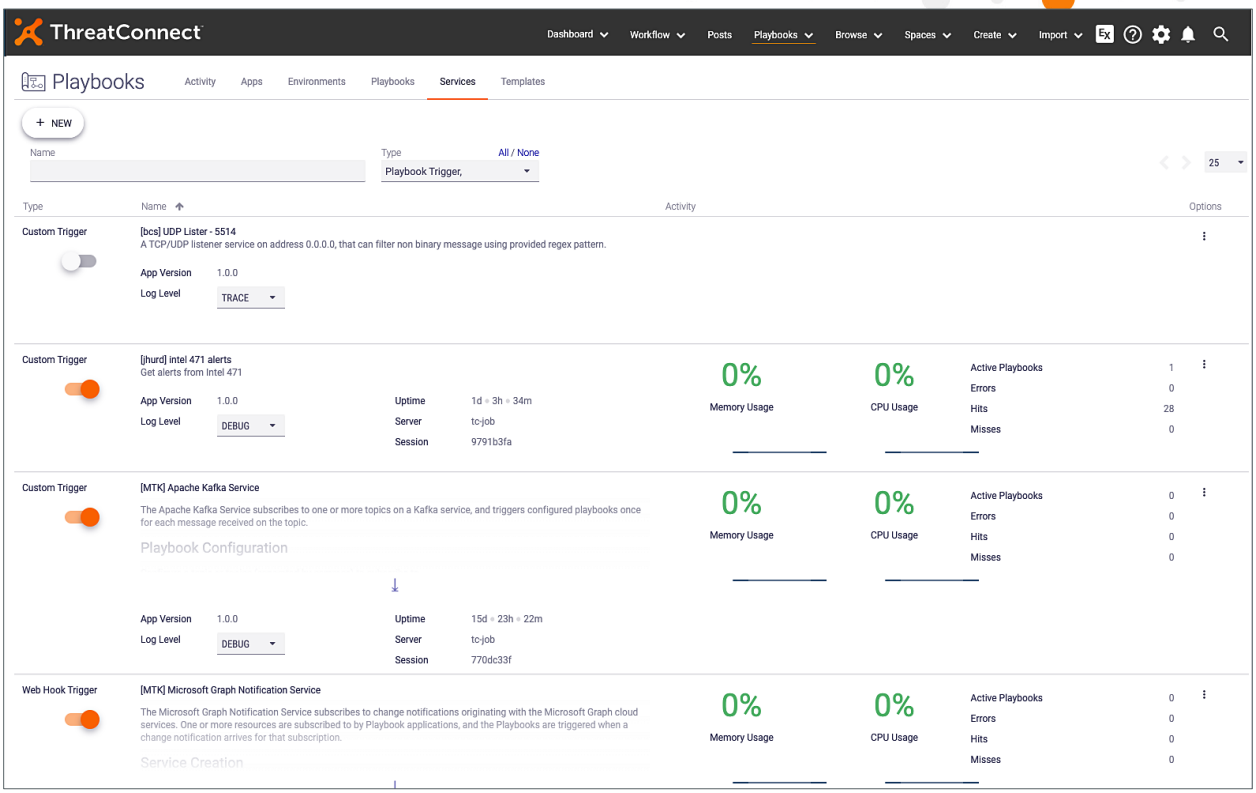
ThreatConnect
Dashboard
Workflow
Posts
Playbooks
Browse
Spaces
Create
Import
Playbooks
Activity
Apps
Environments
Playbooks
Services
Templates
NEW
Name
Type
All / None
Playbook Trigger,
25
Type
Name
Activity
Options
Custom Trigger
[bcs] UDP Lister - 5514
A TCP/UDP listener service on address 0.0.0.0, that can filter non binary message using provided regex pattern.
App Version 1.0.0
Log Level TRACE
Custom Trigger
[jhurd] intel 471 alerts
Get alerts from Intel 471
App Version 1.0.0
Log Level DEBUG
Uptime 1d • 3h • 34m
Server tc-job
Session 9791b3fa
0%
Memory Usage
0%
CPU Usage
Active Playbooks 1
Errors 0
Hits 28
Misses 0
Custom Trigger
[MTK] Apache Kafka Service
The Apache Kafka Service subscribes to one or more topics on a Kafka service, and triggers configured playbooks once for each message received on the topic.
Playbook Configuration
App Version 1.0.0
Log Level DEBUG
Uptime 15d • 23h • 22m
Server tc-job
Session 770dc33f
0%
Memory Usage
0%
CPU Usage
Active Playbooks 0
Errors 0
Hits 0
Misses 0
Web Hook Trigger
[MTK] Microsoft Graph Notification Service
The Microsoft Graph Notification Service subscribes to change notifications originating with the Microsoft Graph cloud services. One or more resources are subscribed to by Playbook applications, and the Playbooks are triggered when a change notification arrives for that subscription.
Service Creation
0%
Memory Usage
0%
CPU Usage
Active Playbooks 0
Errors 0
Hits 0
Misses 0

Figure 109

3. Click the **+ NEW** button at the upper-left portion of the screen, and the **Create Service** pop-up screen will appear (Figure 110).

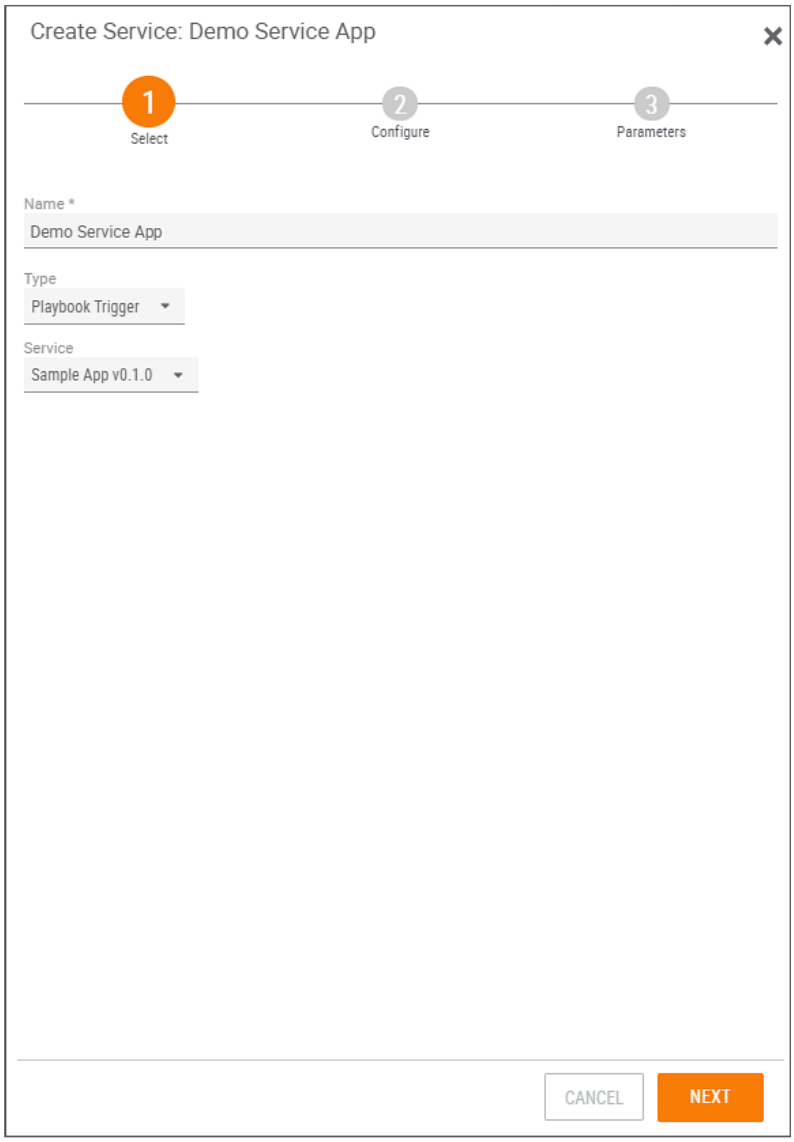

Figure 110

a. **Name**: Enter a name for the service.

   NOTE: One service can be created multiple times for different customers by using different credentials. Take that into account when naming the service.

b. **Type**: This drop-down menu should already be set to **Playbook Trigger**. Leave as is, since that option covers both Custom Trigger and WebHook Trigger apps.

c. **Service**: Pick one of the Service apps, which are installed from the App Catalog.

4. Click the **NEXT** button, and the **Configure** screen will appear (Figure 111).

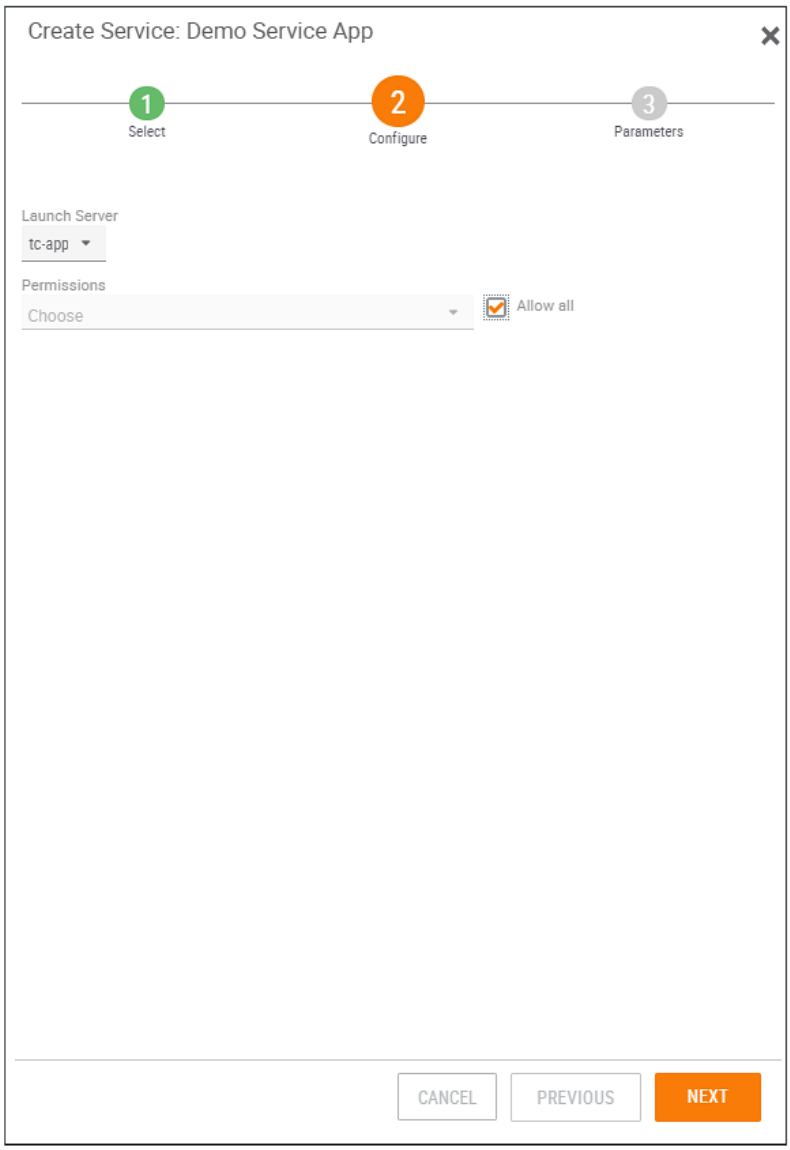

Figure 111

a. **Launch Server**: Click the drop-down menu to select from which server the Service app will launch. Typically, on multi-server environments, the app is launched on the **tc-job** server.

b. **Permissions**: Click the drop-down menu to select which Organizations will use the app. Otherwise, click the Allow all checkbox to allow all Organizations to use the app.

5. Click the **NEXT** button and the **Parameters** screen will appear (Figure 112).

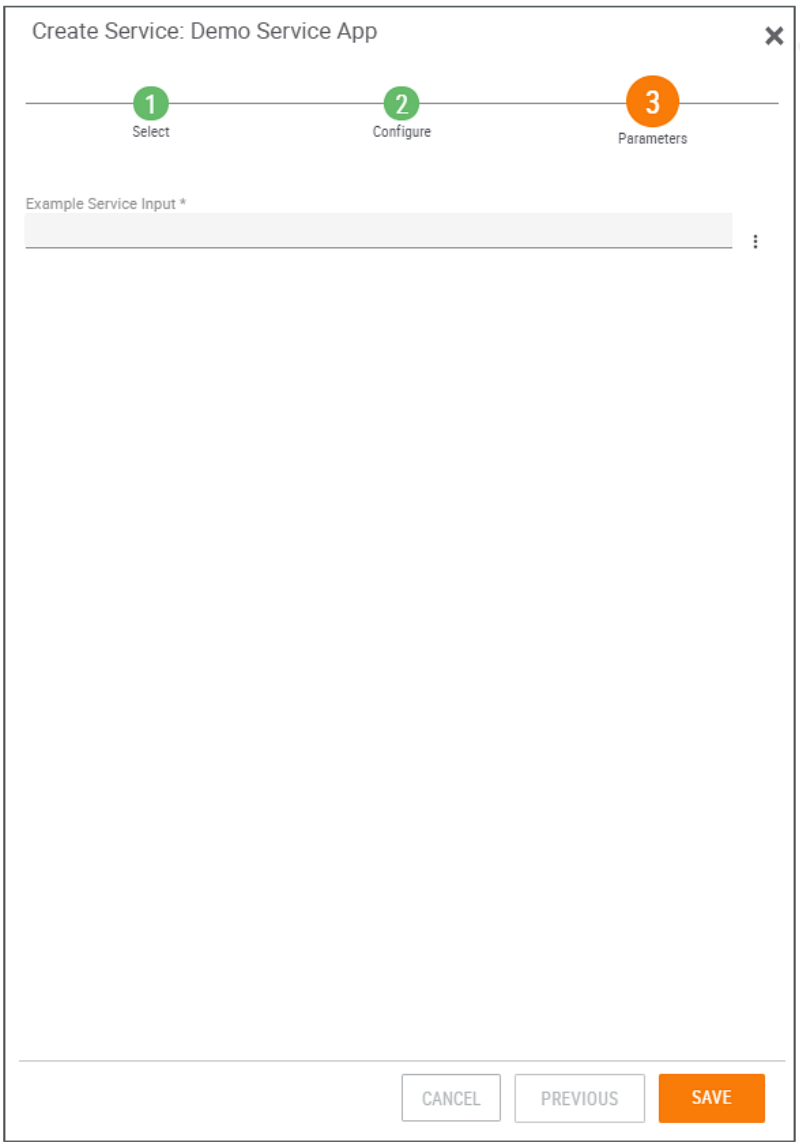

Figure 112

6. In the field, enter the configuration parameters corresponding to the Service app. Unlike Playbook apps that only have standard inputs, Service apps will have two types of inputs: Global inputs and Playbook inputs.
7. Click the **SAVE** button, and the new app will appear in the Services Apps list. Slide the **Toggle Switch** to the right to activate the Service app.

Services Screen App Components

An app included in the Services Apps list displays several components (Figure 113). The interactive components are listed below.

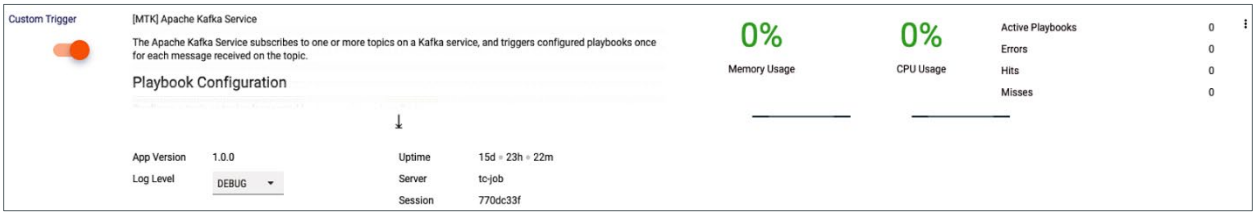

Figure 113

a. The **Name** and **Description** of the Service app are displayed at the top left of the screen, to the right of the **Toggle Switch.**

b. **Down Arrow:** Click the **Down Arrow** icon to expand this section in order to view the app notes offering detailed information.

c. **App Version**: Displays the installed version of the app.

d. **Log Level**: Click the drop-down menu to select a new Log File Level of **ERROR, WARN, INFO, DEBUG**, or **TRACE**. Whenever the level is changed, it immediately impacts the Service app.

e. **Running Service Metrics**: In the center of the screen, **Uptime**, **Server**, **Memory Usage**, and **CPU Usage** are core platform metrics.

f. **App-Based Metrics:** On the right of the screen, **Active Playbooks**, **Errors**, **Hits**, and **Misses** are metrics sent by the app to core to present in the UI.

g. **Ellipsis**: Click the vertical **Ellipsis** icon on the right to select the following options:

- **Delete**: This option deleted the Service app.
- **Edit**: This option allows the user to edit the Service app.
- **Download Logs**: Allows the user to download a truncated version of logs in .zip format.
- **Autostart**: Slide the toggle switch to the right (orange) so that if the ThreatConnect instance is off, it will restart the Service app automatically once the instance is restarted.
- **Toggle Switch**: Slide the **Toggle Switch** to the left (gray) to turn off the Service (e.g., to perform troubleshooting). Slide the toggle switch to the right (orange) to restart the Service.

For information on how to use Service apps once they are created and configured, refer to the *Playbooks* Knowledge Base article.