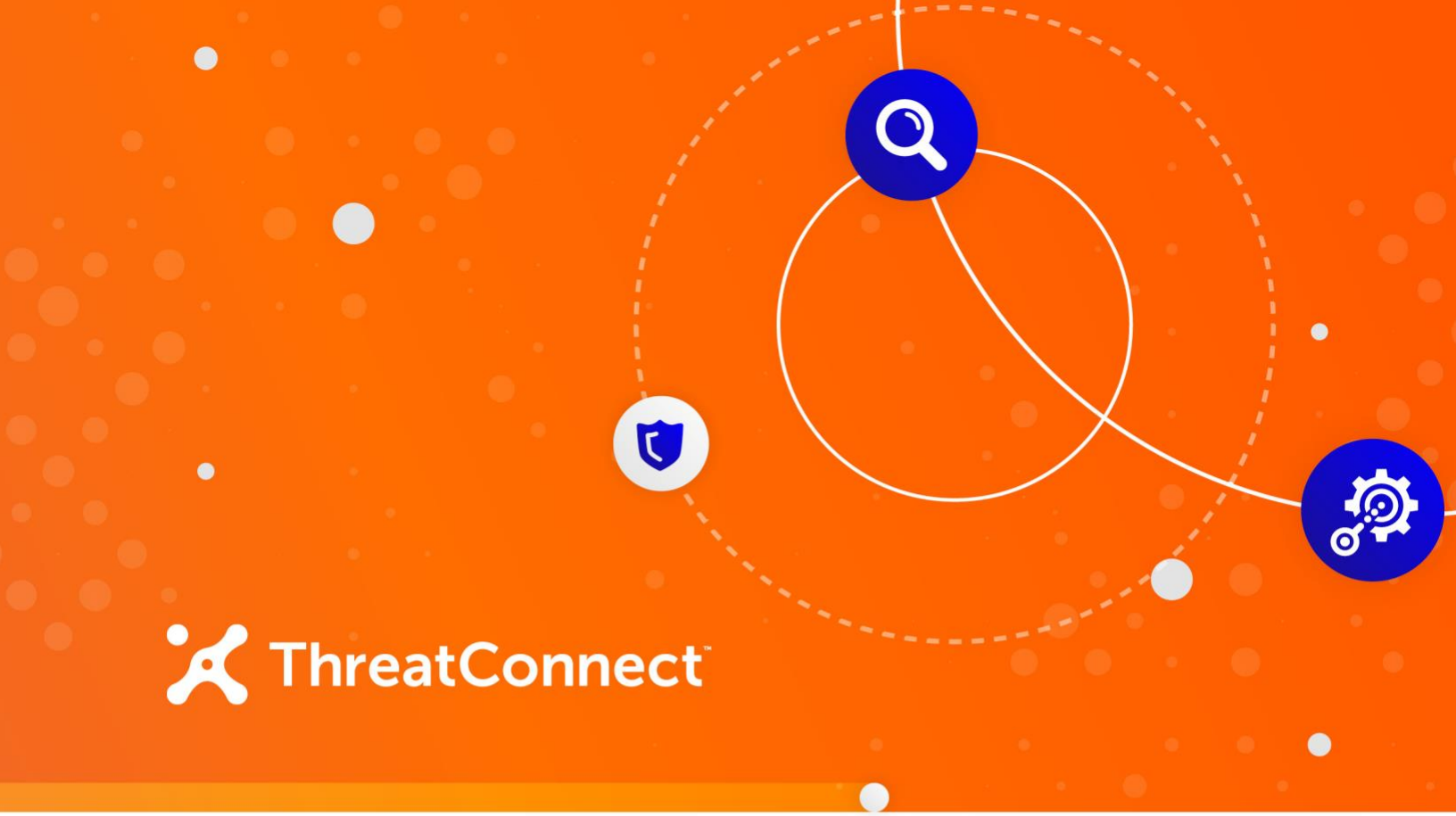

System Administration

User Guide

Software Version 6.2

June 21, 2021

10013-14 FN 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

©2021 ThreatConnect, Inc.

ThreatConnect® is a registered trademark of ThreatConnect, Inc.
CAL™ and TC Exchange™ are trademarks of ThreatConnect, Inc.
Amazon Web Services® is a registered trademark of Amazon Web Services, Inc.
FreeMarker™ is a trademark of the Apache Software Foundation.
OpenDNS® is a registered trademark of Cisco Systems, Inc.
Elasticsearch® is a registered trademark of Elasticsearch BV.
ArcSight™ is a trademark of Micro Focus.
Lastline® is a registered trademark of Lastline, Inc.
Linux® is a registered trademark of Linus Torvalds.
Excel® and Microsoft® are registered trademarks of the Microsoft Corporation.
MITRE ATT&CK™, STIX™, and TAXII™ are trademarks of the MITRE Corporation.
Java® is a registered trademark of the Oracle Corporation.
Python® is a registered trademark of the Python Software Foundation.

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 be displayed (Figure 2).

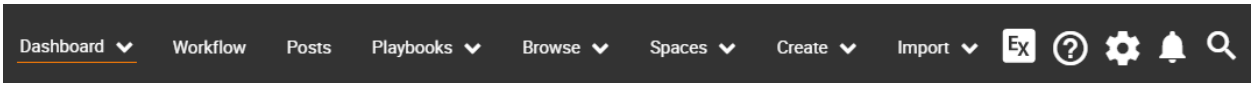

Figure 1

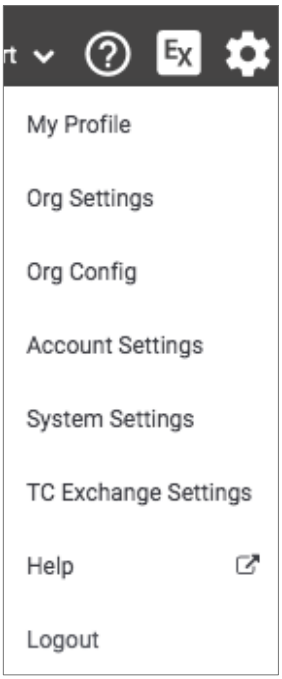

Figure 2

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 an 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 be displayed (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will be displayed (Figure 3).

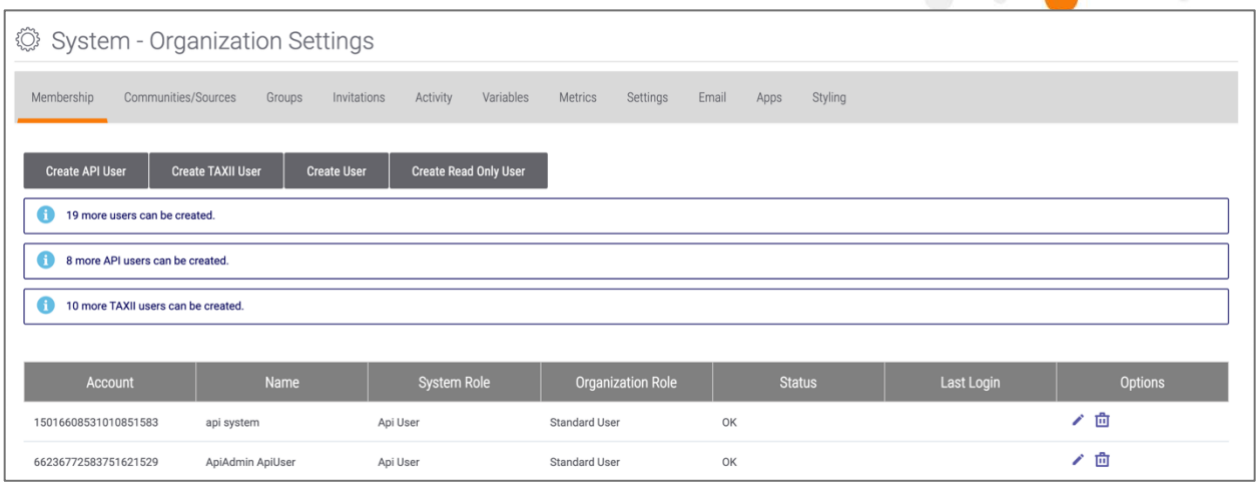

Figure 3

3. Click the **Create User** button, and the **User Administration** window will be displayed (Figure 4).

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

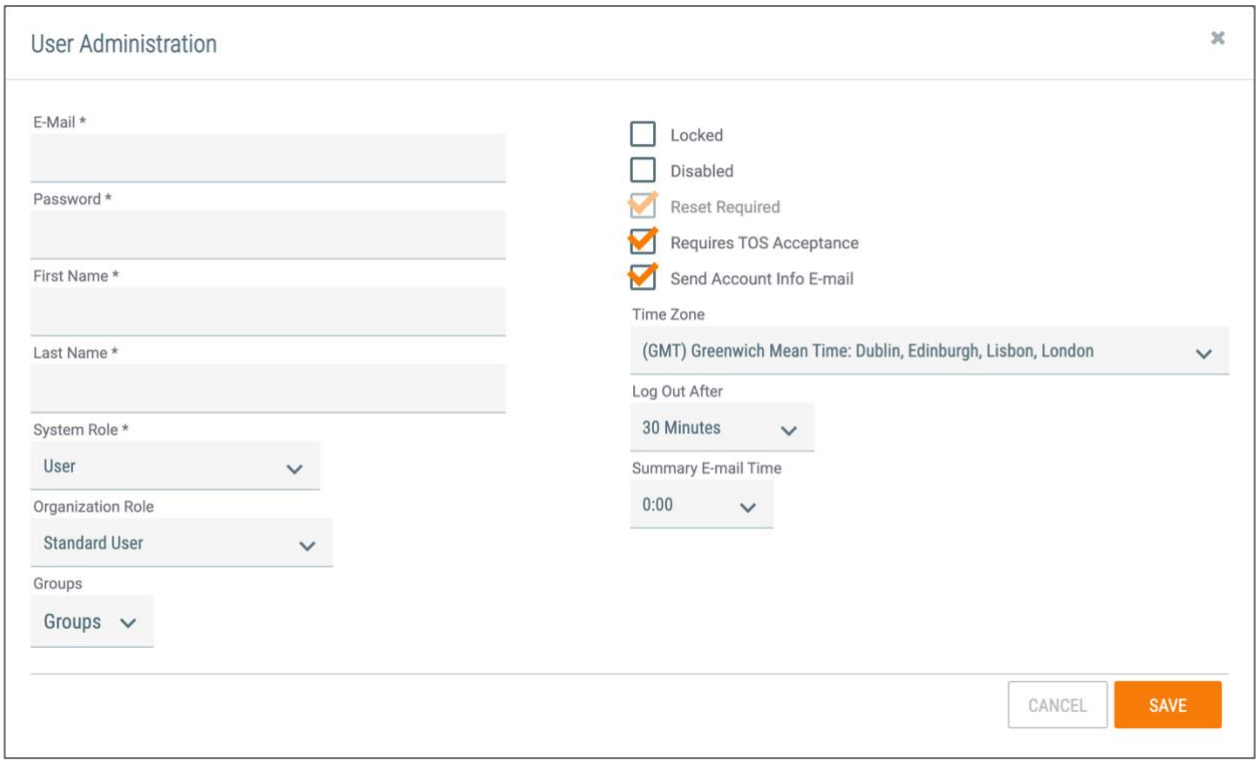

Figure 4

4. Fill in the required fields in order to create and configure the user account.
   - **E-Mail**: Enter an email address that will also be the name of the user account.
   - **Password**: Enter the initial user password, which is subject to the ThreatConnect password policy defined within the system settings.
   - **First Name**: Enter the user's first name, which, along with the last name, is what other user accounts see when the user posts within the Organization or in a full-profile Community.
   - **Last Name**: Enter the user's last name, which, along with the first name, is what other user accounts see when the user posts within the Organization or in a full-profile Community.
   - **System Role**: Use the dropdown menu to select one of the following System roles: Read Only User, Community Leader, Accounts Administrator, User, Operations Administrator, or Administrator. See *ThreatConnect System Roles and Permissions* for more information.
   - **Organization Role**: Use the dropdown menu to select one of the following roles: Organization Administrator, Read Only User, App Developer, Standard User, Sharing User, or Read Only Commenter. See *ThreatConnect Owner Roles and Permissions* for more information
   - **Groups**: Use the dropdown menu to select a user group to which to add the user, if desired.
   - **Locked**: Select the checkbox to lock a user account. Deselect the checkbox to unlock a user account that has been locked by ThreatConnect.
   - **Disabled**: Select 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.
   - **Reset Required**: Select the checkbox to force a user to change the account password upon next login. This checkbox is selected by default upon account creation, and it is cleared once the password has been changed.

     NOTE: When initially creating the account, the** Reset Required **checkbox cannot be deselected. To deselect the checkbox, first create the account, edit it, and then clear the setting, which enforces tighter security.
   - **Requires TOS Acceptance**: Select 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 be displayed in this window.
   - **Send Account Info E-mail**: Select the checkbox to send an email with the account information to the specified email address.
   - **Time Zone**: Use the dropdown menu to select the appropriate time zone.
   - **Log Out After**: Use the dropdown menu to select a time interval upon which a user will be logged out after a corresponding period of inactivity.
   - **Summary E-mail Time**: Use the dropdown menu to set the time at which a user account will receive daily summary emails of followed items or other notifications from ThreatConnect.

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

To create Read Only User accounts (including Read Only Commenters), follow the preceding steps, but click the **Create Read Only User** button in Step 4. Note that only **Read Only User** and **Read Only Commenter** are available in the **Organization Role** menu. Users of these types that join a Community or Source will have read-only permissions in that owner as well.

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

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 be displayed (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will be displayed (Figure 3).

3. Click the **Edit** icon to the right of an entry in the table. The **User Administration** screen will be displayed (Figure 5).

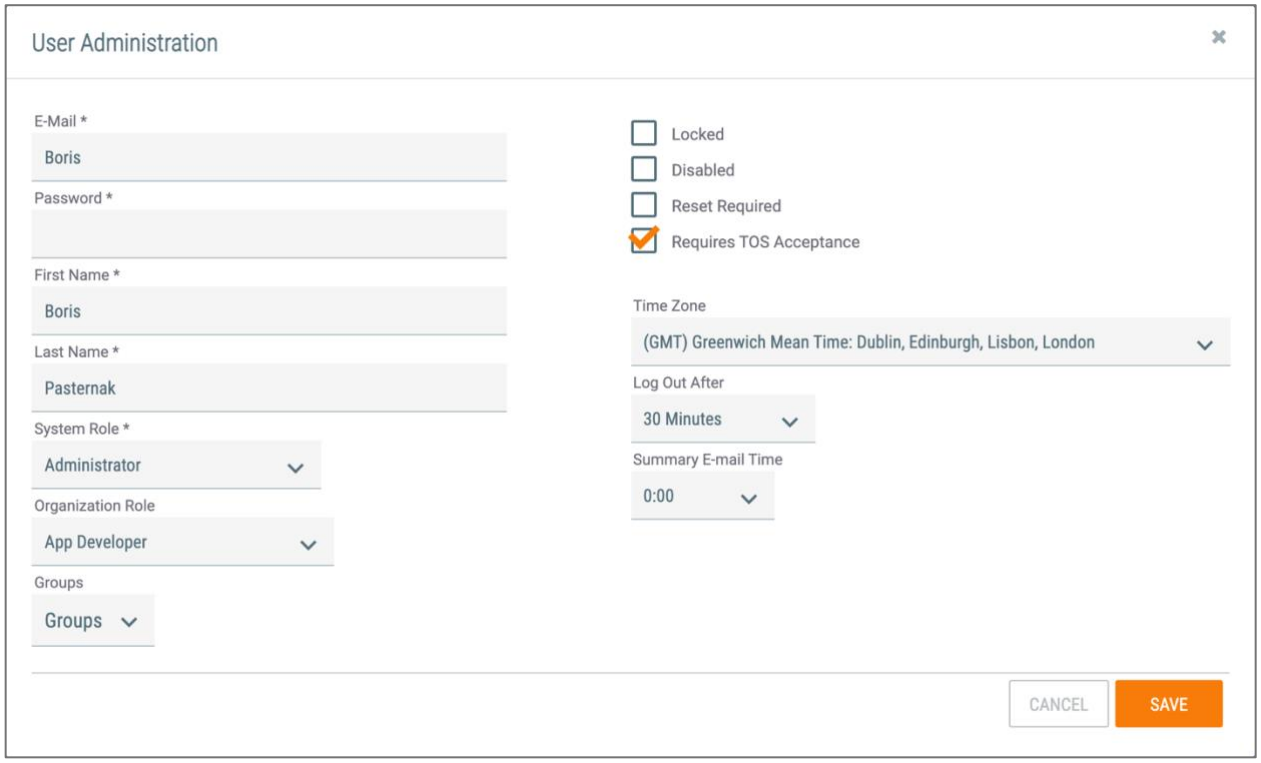

Figure 5

4. After modifying the fields, 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 be displayed (Figure 2). Select **Org Settings**, and the **Organization Settings** screen will be displayed (Figure 3).
3. Click on an account name in the table. The **User Profile** screen will be displayed (Figure 6).

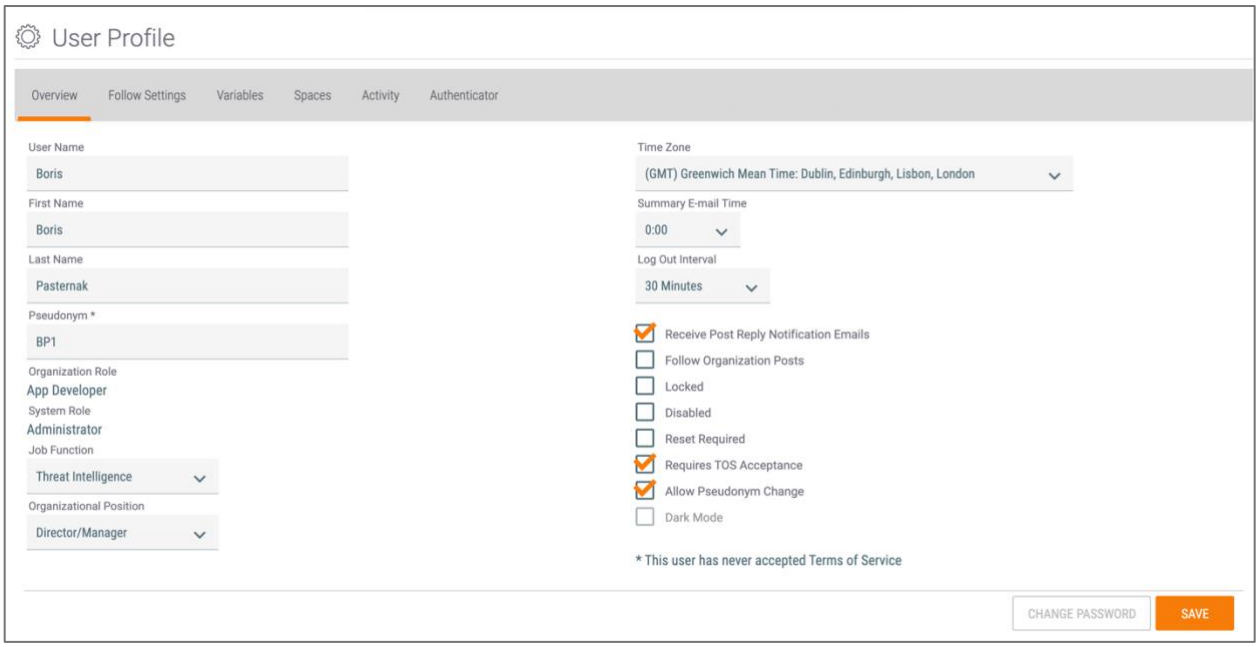

Figure 6

4. After editing the fields, 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).

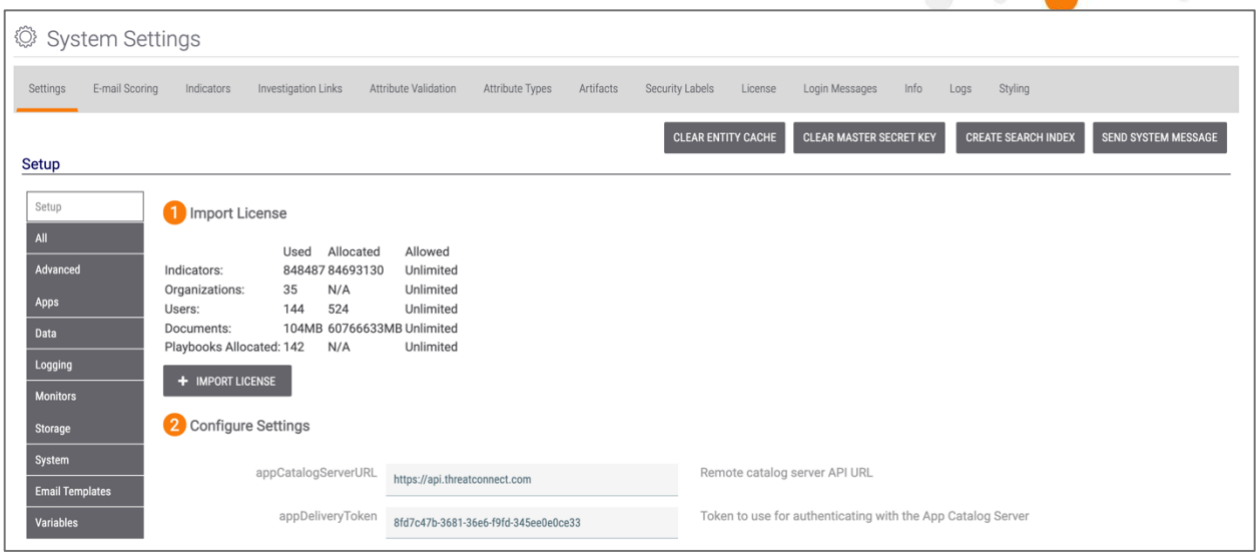

Figure 7

3. On the left-hand menu, click the **All** button to view a list of settings grouped by category. Modify the settings as desired.

Setting Descriptions

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

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 UI error logs are sent to ThreatConnect.

allowOrganizationPublish

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

appBuilderFileLimitMb

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

appCatalogServer

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

appCatalogServerURL

This setting corresponds to the remote Catalog Server API URL.

appDeliveryToken

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

appExecutionDBDaysToKeep

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

Acceptable Values: Positive whole numbers

appMessageBrokerHost

This setting signifies the messaging broker host and port.

appSharedPlaybookExpirationDays

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

appSharingServer

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

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

appSharingServerURLs

This setting corresponds to the App Sharing Server API URL.

appsApiTokenKeepAliveOffsetSeconds

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

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 used only 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 ThreatConnect's 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 (in minutes).

diskSpaceMonitorThresholdFactor

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

diskSpaceMonitorInodeFactor

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

diskSpaceMonitorAlertFactor

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

diskSpaceMonitorAlertEmail

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

diskSpaceMonitorInodeHoursToKeep

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

diskSpaceMonitorIntodeFileSystem

This setting indicates the filesystem where inodes are checked.

diskSpaceMonitorDaysToKeepDeleteFactor

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

dnsBounceDailyLimit

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

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, the 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)

NOTE: This setting must be set to true ***to enable ThreatConnect to use the DataStore. See the "DataStore" section of*** The Playbook Designer ***for more information.***

elasticSearchUrl

This setting determines the URL for the Elasticsearch server.

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

NOTE: This setting must be defined to enable ThreatConnect to use the DataStore. See the "DataStore" section of The Playbook Designer ***for more information.***

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

mailInboundKeyStore

This setting indicates the path to the Java Keystore.

mailInboundKeyStorePassword

This setting specifies the password for the Java Keystore.

mailInboundPort

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

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

mailInboundRequireTLS

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

managementAPISubscriberIntervalSeconds

This setting specifies the minimum interval for triggering alerts.

managementApiSubscriberMaxHourlyAlerts

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

maxDailyNotificationsPerPlaybook

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

mediumPriorityNotificationLimit

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

organizationStatusMonitorEnabled

This setting turns on the Organization Status Monitor.

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.

playbookFailedInteractiveSessionCount

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

playbookForkPoolSize

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

playbookVersionArchiveLimit

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

playbookWebHookPathByOrg

This setting determines if WebHook URLs are isolated per Organization.

playbooksCompletedSessionDaysToKeep

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

playbooksDbHost

This setting specifies the Playbooks Redis DB host.

playbooksDbPort

This setting specifies the Playbooks Redis DB port.

playbooksDefaultRoiDollarsPerHour

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

playbooksDefaultRoiMinutes

This setting specifies the default Playbooks ROI minutes.

playbooksDisplayFailureNotifications

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

playbooksEnabled

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

NOTE: A System Administrator can run Playbooks in Cloud for an Organization that cannot activate this feature. Furthermore, a System Administrator can see any Playbook (using 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 **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 Trusted Automated eXchange of Indicator Information (TAXII™) 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 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 using the corresponding template. A list of Email Templates is located 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. On the left-hand menu, click the **Email Templates** button. The **Email Templates** screen will be displayed (Figure 8).

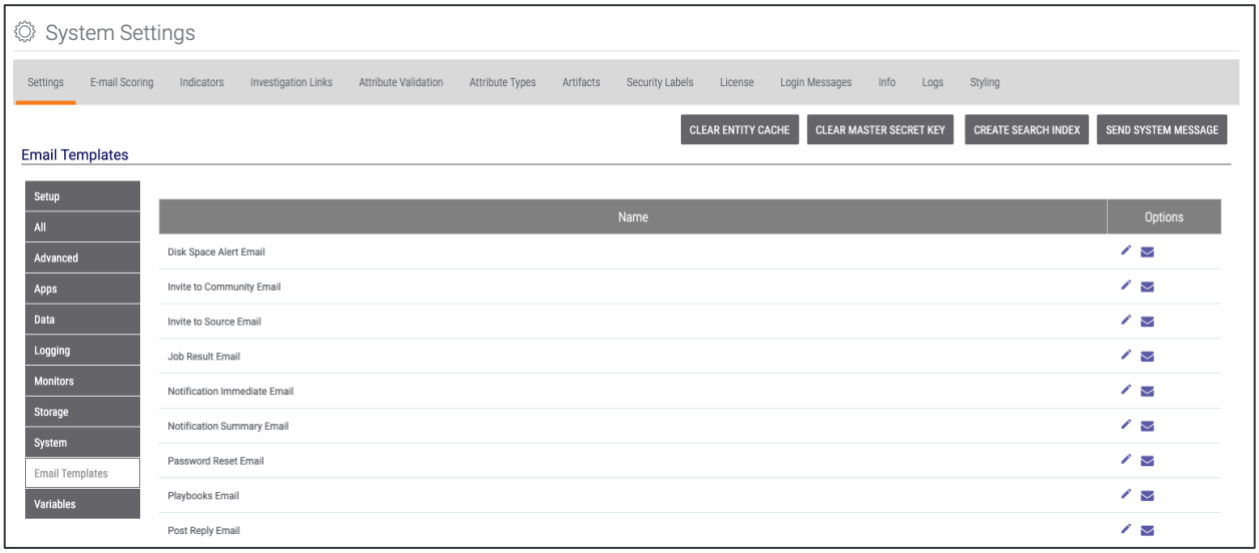

Figure 8

4. Select an email template from the list (the **Invite to Community Email** template is used in this example) and click the **Edit** icon. The **Invite to Community Email** window will be displayed (Figure 9).

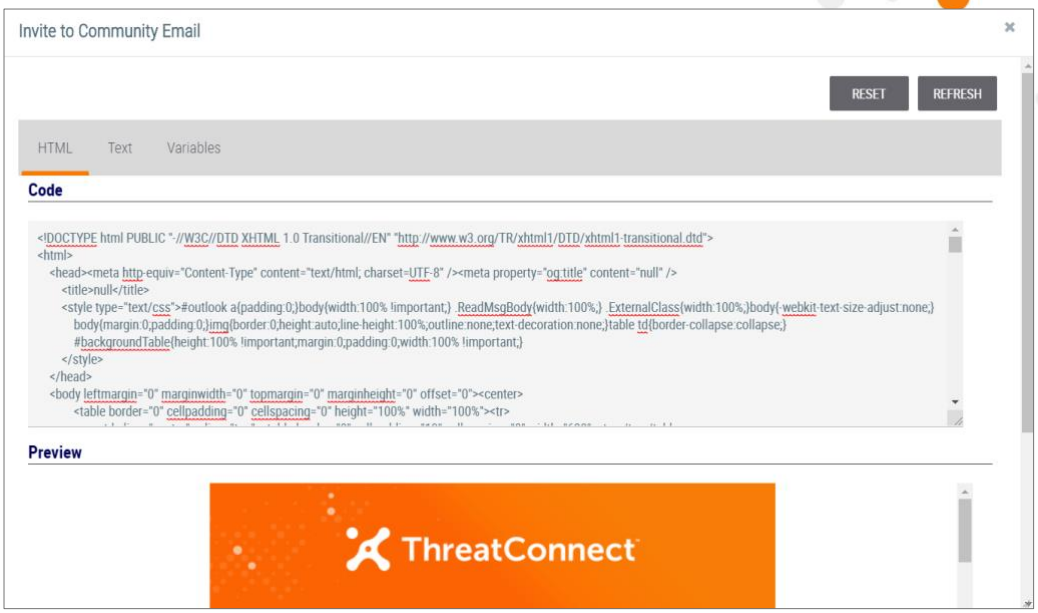

Figure 9

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 **image1-4** options allow a 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 be displayed 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 be displayed.
9. To receive a system-generated email for review, click the **Test Email**  icon next to any of the Email Template choices. The **Send Test Email** window will be displayed (Figure 10).

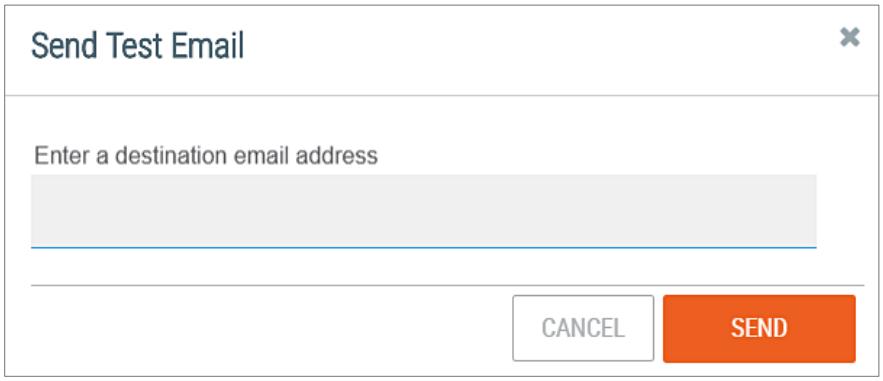

Figure 10

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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. On the left-hand menu, click the **Variables** button. The **Variables** screen will be displayed (Figure 11).

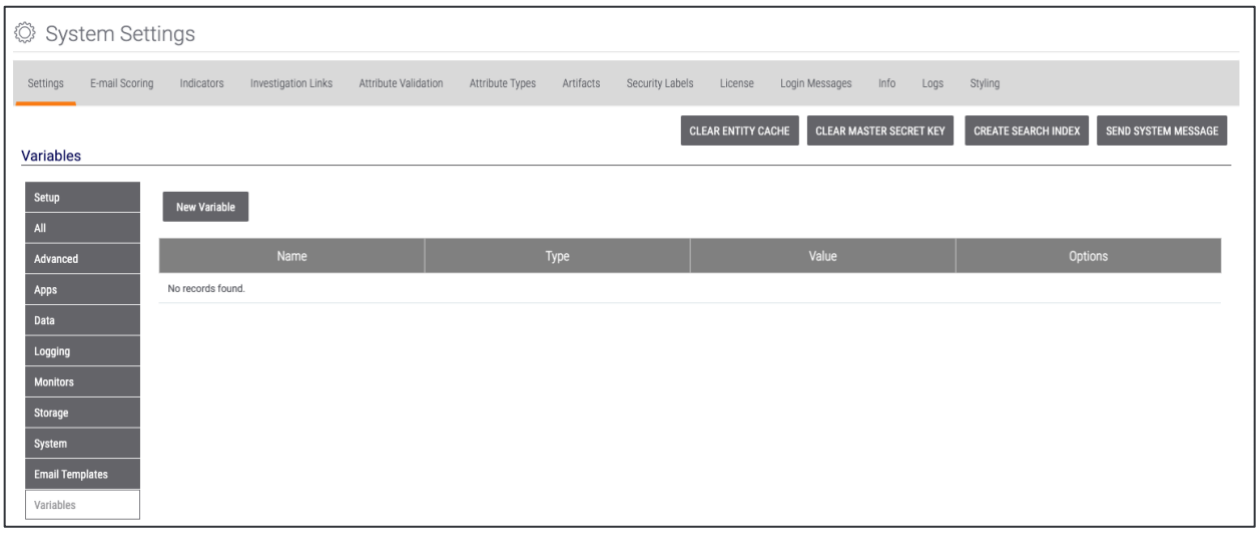

Figure 11

4. Click the **New Variable** button. The **Property** window will be displayed (Figure 12).

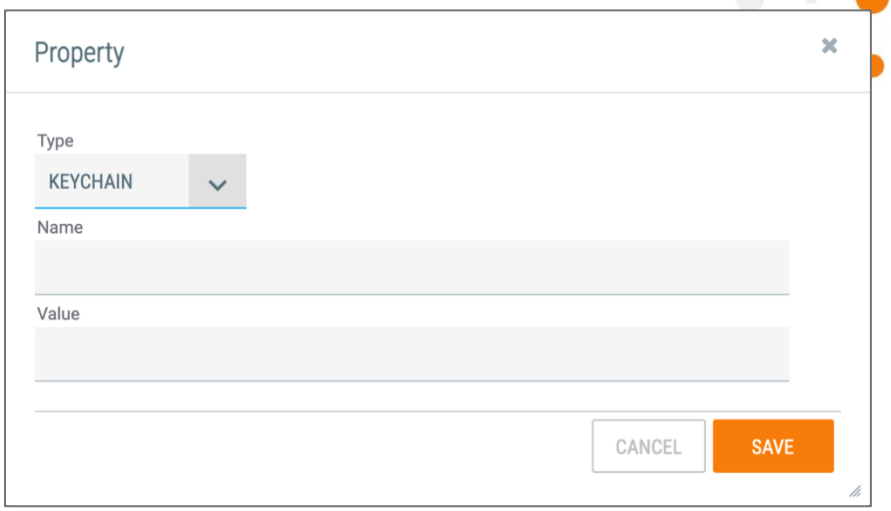

Figure 12

- **Type**: Use the dropdown menu to select the variable's type. Available options include **KEYCHAIN**, **TEXT**, and **FILE**.
- **Name**: Enter a name for the variable.
- **Value**: Enter a value for the variable.

5. Click the **SAVE** button to create the new variable.

Email-Scoring Rules

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

How the Scoring Engine Works

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

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

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

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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).

3. Click the **E-mail Scoring** tab. The **E-mail Scoring** screen will be displayed (Figure 13).

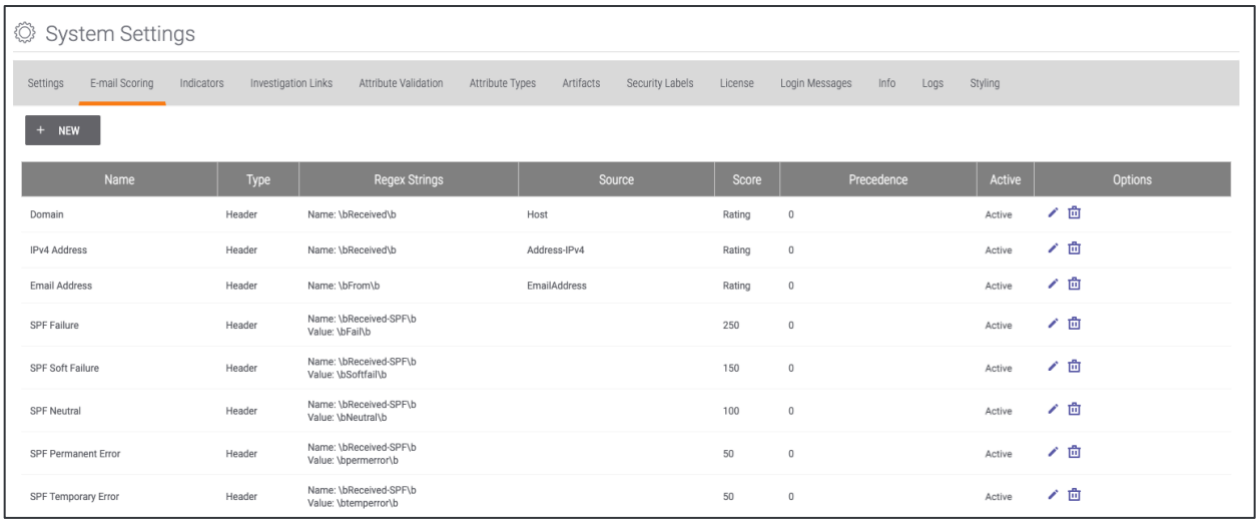

Figure 13

4. Click the **+ NEW** button. The **E-mail Scoring Rule** window will be displayed (Figure 14).

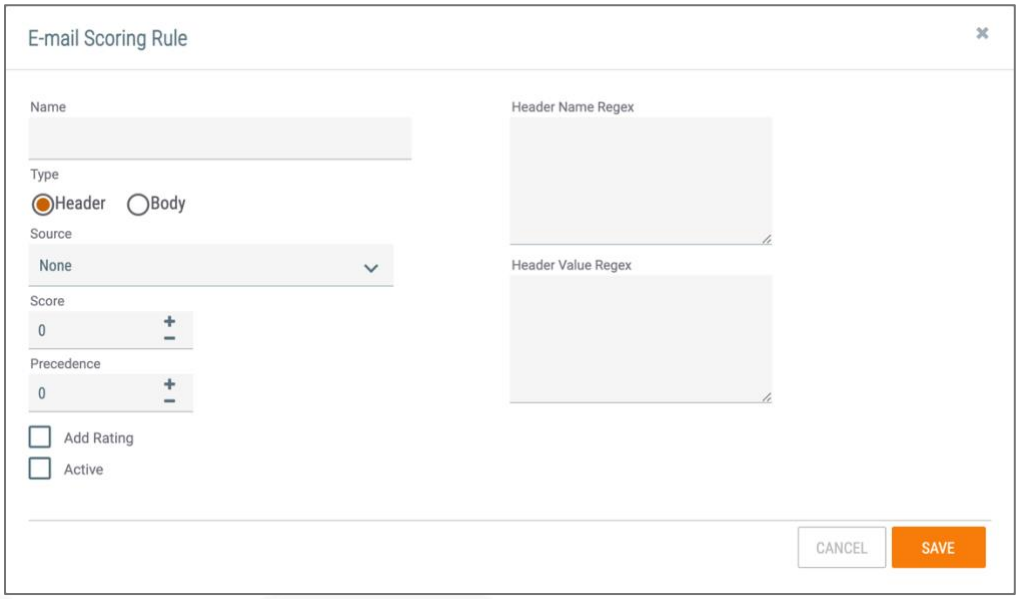

Figure 14

- **Name**: Enter the name of the rule.
- **Type**: Select either the **Header** or **Body** email component.
- **Source**: Use the dropdown menu to select an Indicator as the source of a rule's score, if this rule will match on an Indicator string. If this rule will match on a non-Indicator string, leave this field set to **None**.
- **Score**: Enter a base score for the email if there is a match on the rule in the **Score** field, or use the up and down arrows to add or subtract increments of 1, respectively. Points may be added to the rule if the rule is matching on an Indicator and the **Add Rating** checkbox is selected.
- **Precedence**: Enter the Precedence value, which is used if two rules exist for different Indicator types, or use the up and down arrows to add or subtract increments of 1, respectively. A rule with a higher Precedence value will be counted instead of a rule with a lower Precedence value that matches on the same header value. If the rules match on Indicators of different types, the rule with the higher Precedence value will determine the type.
- **Add Rating**: Select the checkbox to add an Indicator's Threat Rating (i.e., number of skulls) to the score's value when a match occurs. This feature is applicable only for rules that match on an Indicator.
- **Active**: Select the checkbox to specify whether the rule is active. The rule will not be included in the Email-Scoring Engine unless this checkbox is selected.
- **Header Name Regex (Header Only)**: Enter a Java-compatible regular expression that defines the email header field in which the header value will be found.
- **Header Value Regex or Body Value Regex**: Enter a Java-compatible regular expression that defines the email header or body value that will result in a match for the rule.

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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **E-mail Scoring** tab. The **E-mail Scoring** screen will be displayed (Figure 13).
4. Click on the **Edit** icon for the rule that is to be edited. The **E-mail Scoring Rule** window will be displayed (Figure 14).
5. Configure the fields as desired.

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 12 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Indicators** tab. The **Indicators** screen will be displayed (Figure 15).

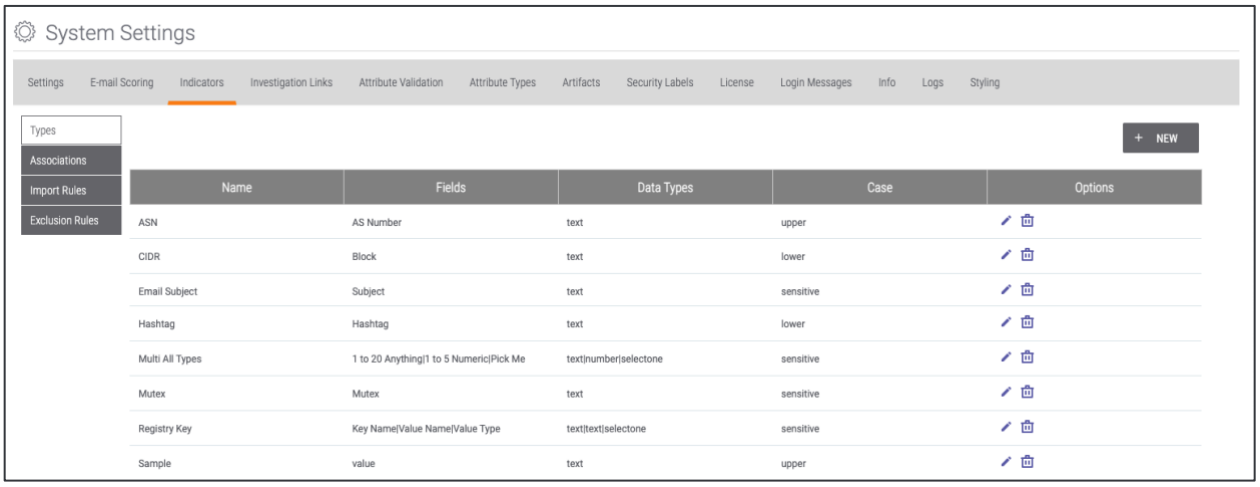

Figure 15

4. On the left-hand menu, click the **Import Rules** button. The **Import Rules** screen will be displayed (Figure 16).

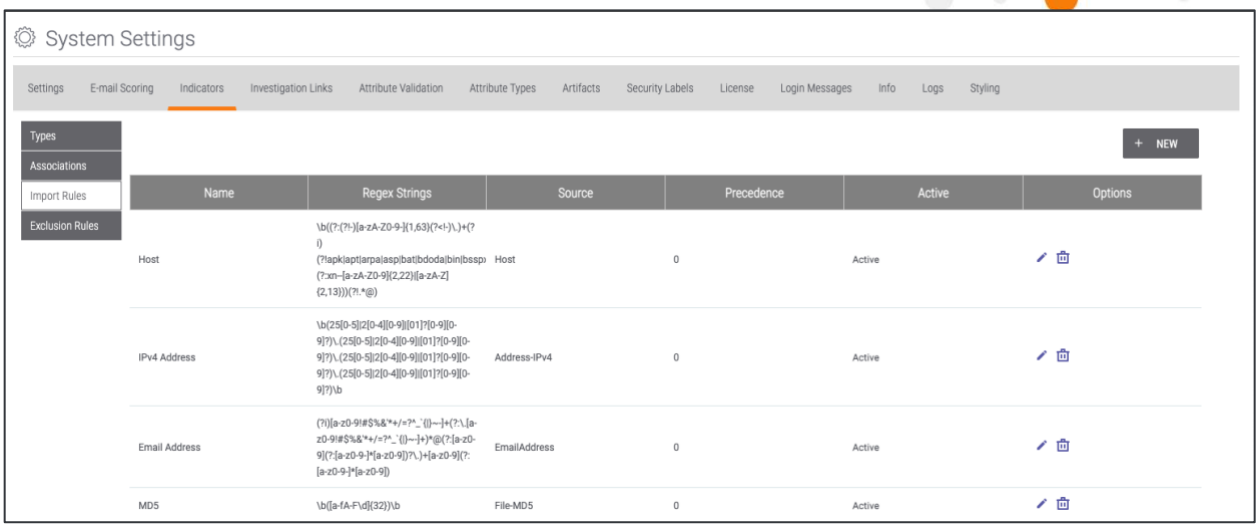

Figure 16

5. Click the **+ NEW** button. The **Create Indicator Import Rule** window will be displayed (Figure 17).

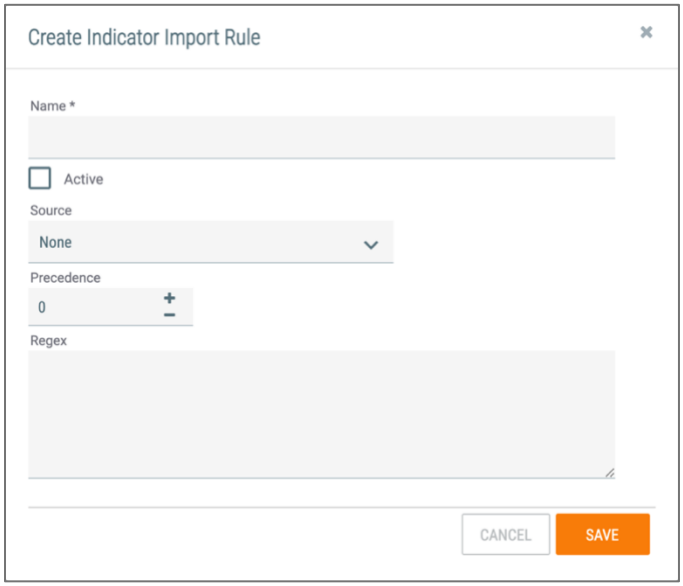

Figure 17

- **Name**: Enter the name of the rule.
- **Active**: Select the checkbox to designate the rule as active. The rule will not be included for Indicator validation unless this checkbox is selected.
- **Source**: Use the dropdown menu to select the Indicator type on which the rule will match.
- **Precedence**: Enter the Precedence value, which is used if two rules exist for different Indicator types and if the regular expressions both match on the import content, or use the

up and down arrows to add or subtract increments of 1, respectively. A rule with a higher Precedence value will be counted instead of a rule with a lower Precedence value.

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

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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Indicators** tab. The **Indicators** screen will be displayed (Figure 15).
4. On the left-hand menu, click the **Import Rules** button. The **Import Rules** screen will be displayed (Figure 16).
5. Click the **Edit** icon for the rule to be edited. The **Create Indicator Import Rule** window will be displayed with pre-entered values for the given rule (Figure 18).

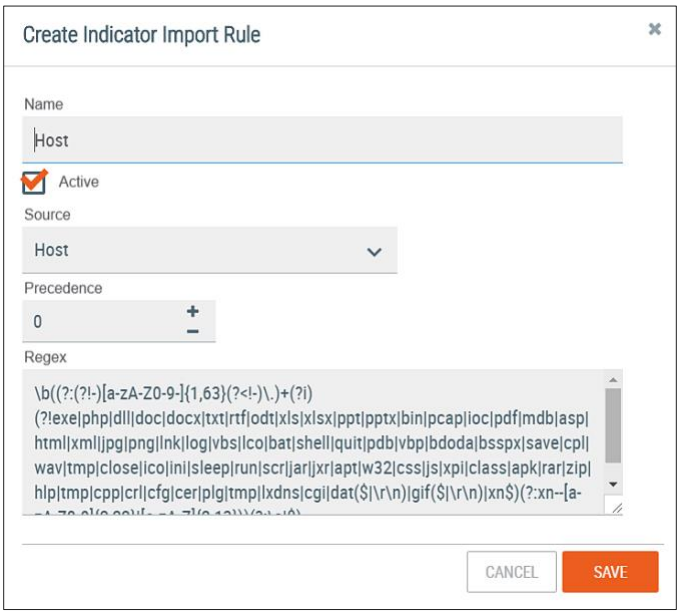

Figure 18

6. Configure the fields as desired.
7. Click the **SAVE** button.

Indicator Exclusion Lists: System Level

The purpose of creating an Indicator Exclusion List is to prevent the importation of Indicators that may be deemed legitimate or non-hostile by an Administrator. ThreatConnect is prepopulated with default Indicator Exclusion Lists, but the system allows users to create custom Exclusion Lists at the System, Organization, Community, or Source level. The System-level List is configured through the **System Settings** screen by a System Administrator.

Table 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Indicators** tab. The **Indicators** screen will be displayed (Figure 15).
4. On the left-hand menu, click the **Exclusion Rules** button. The **Exclusion Rules** screen will be displayed (Figure 19).

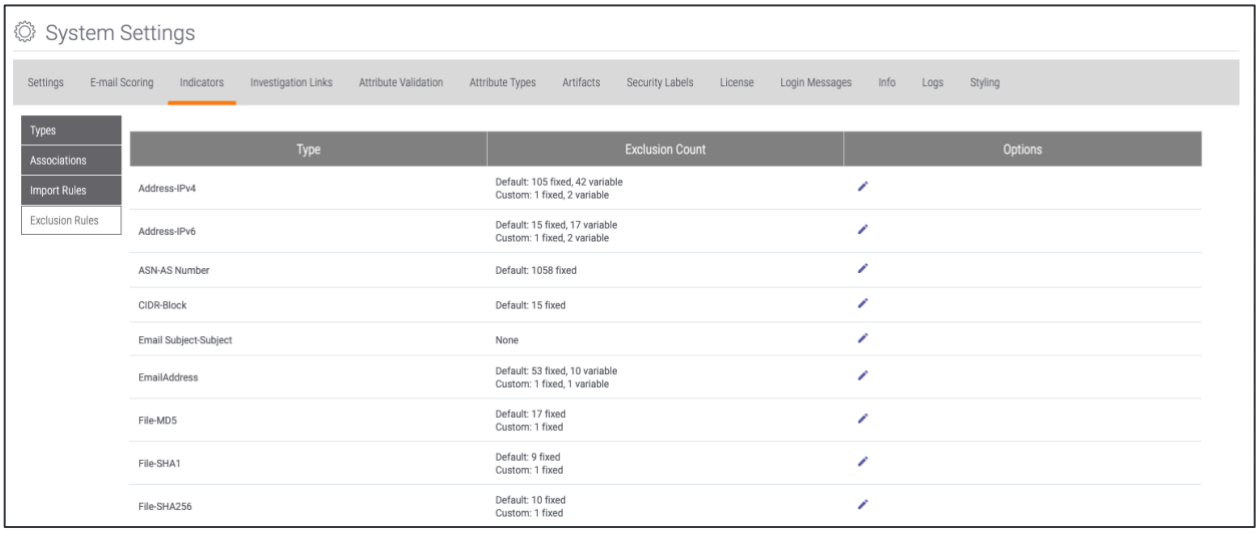

Figure 19

5. Click the **Edit** icon for an Indicator from the **Type** column (Address-IPv6 for this example). The **Exclusion Details** window will be displayed (Figure 20).

Figure 20

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

   NOTE: 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. Alternatively, click the **+ UPLOAD FILE** button to locate and select a file upload. After the file is uploaded, click the **SAVE** button.

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

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

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

9. To remove an existing **Custom** Exclusion List, click the **CLEAR** button, and the **Remove Exclusions** window will be displayed (Figure 21).

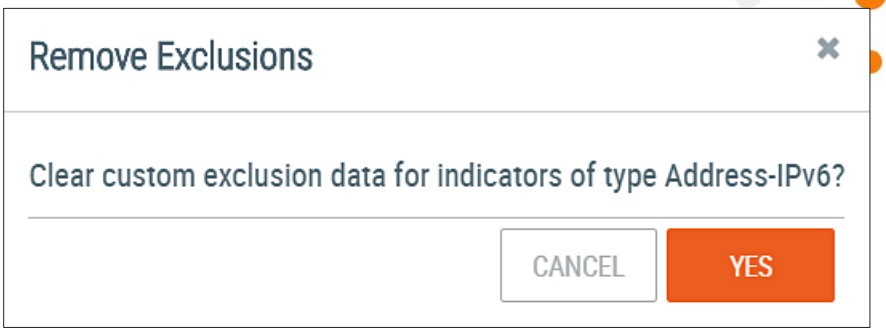

Figure 21

10. Click the **YES** button, followed by the **SAVE** button.

Custom Indicator Types

For ThreatConnect users with a **Dedicated Cloud** 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 be displayed in menus and lists along with built-in Indicator types. Users will not be able to tell the difference between a custom Indicator and a built-in Indicator.

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

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: System Administrators can edit and delete custom Indicators 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Indicators** tab. The **Indicators** screen will be displayed (Figure 15).
4. Click the **+ NEW** button. The **Create Custom Indicator Type** window will be displayed (Figure 22).

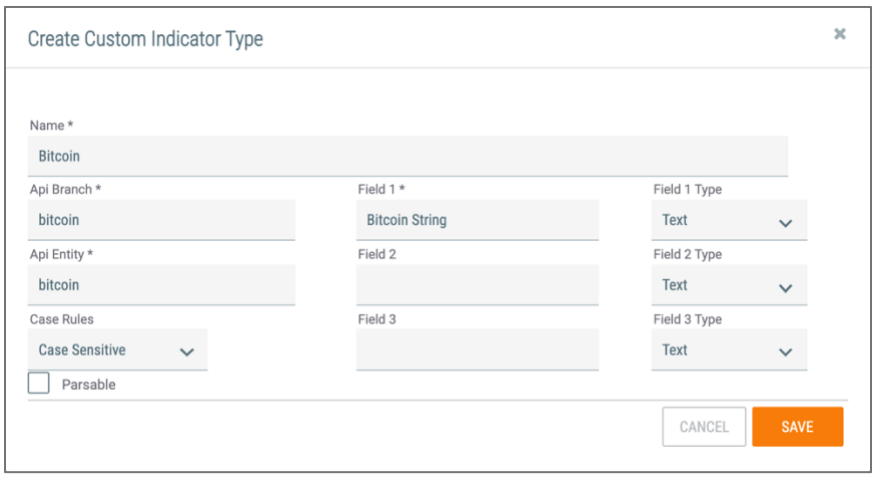

Figure 22

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

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

  NOTE: Multi-value custom Indicator types are not parsable.
- **Field 1**: Set a label for the primary field (e.g., **Bitcoin String**).

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

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

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

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

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

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**.

Import Rules for Custom Indicator Types

Follow 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 select the **Active** checkbox to designate the rule as active. It is recommended that the regular expressions be used to define the three fields of a custom Indicator so that they conform to the character-limit rules. Each field of a custom Indicator must have at least one import rule defined before Indicators of that type can be created.

Custom Associations

Custom associations allow Indicators to be associated to other Indicators. These Indicators can be native Indicators [Address, ASN, CIDR, Email Address, Email Subject, File (MD5, SHA1, SHA256), Hashtag, Host, Mutex, Registry Key, URL, and User Agent] or custom Indicators created by the System Administrator. The details of these associations are found on the **Browse** screen. Table 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Indicators** tab. The **Indicators** screen will be displayed (Figure 15).
4. On the left-hand menu, click the **Associations** button. The **Associations** screen will be displayed

(Figure 23).

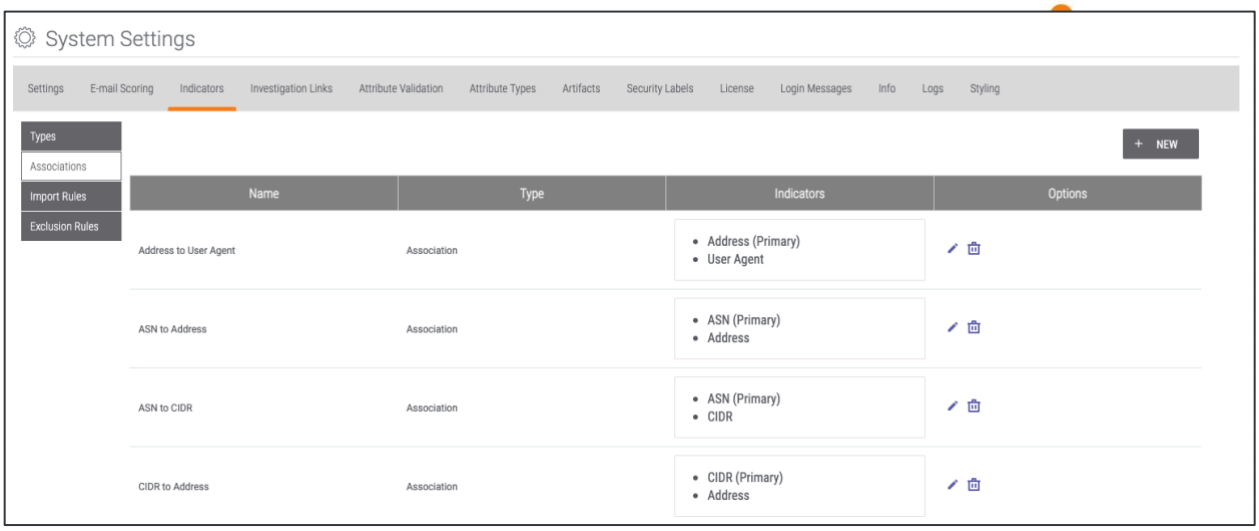

Figure 23

5. Click the **+ NEW** button. The **Create Custom Indicator Association** window will be displayed with the **Association** radio button selected (Figure 24).

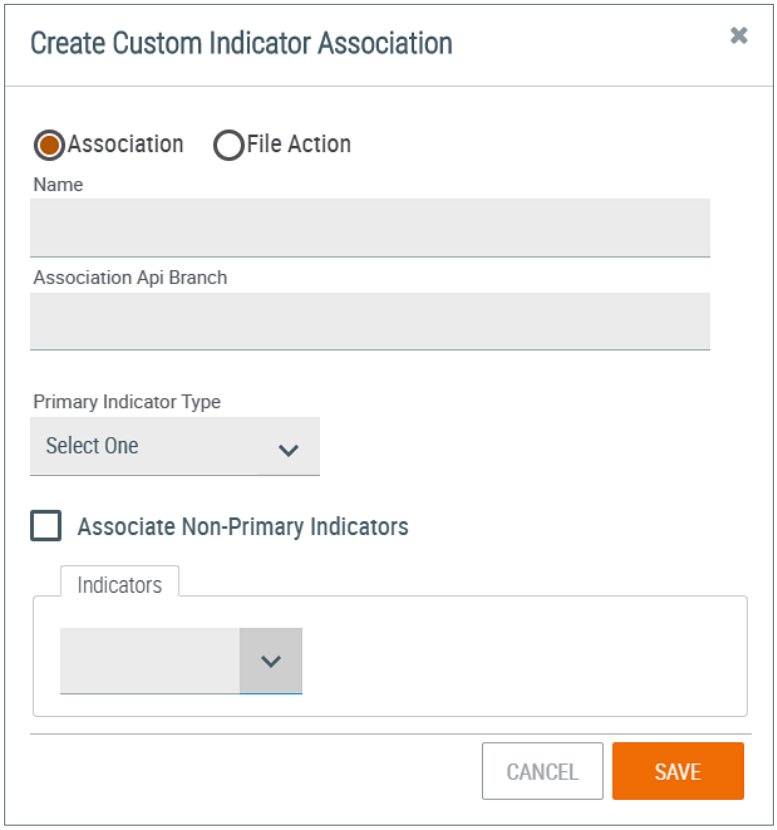

Figure 24

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

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

  NOTE: If this checkbox is not selected, an association between two Indicators is commutative. That is, the designation of primary vs. non-primary is insignificant: The association works equally in both directions, and non-primary Indicators associated with a given primary Indicator are not associated with each other. If this checkbox is selected, non-primary Indicators of a given Indicator are also associated with each other.
- **Indicators**: Use the dropdown 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Indicators** tab. The **Indicators** screen will be displayed (Figure 15).
4. Click the **Associations** button, and the **Associations** screen will be displayed (Figure 23).
5. Click the **+ NEW** button. The **Create Custom Indicator Association** window will be displayed with the **Association** radio button selected (Figure 24). Select the **File Action** radio button (Figure 25).

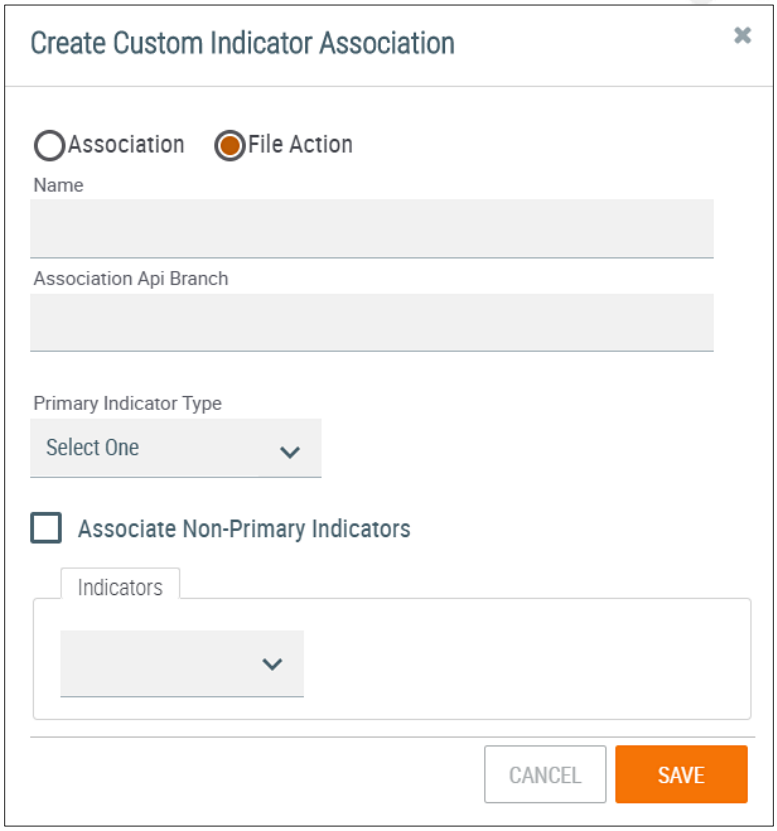

Figure 25

- **Name**: Enter a name for the custom association (e.g., **File CIDR**).
- **Association API Branch**: Set this parameter to the mapped API field in ThreatConnect (e.g., **cidr**).
- **Indicators**: Use the dropdown 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).

3. Click the **Investigation Links** tab. The **Investigation Links** screen will be displayed (Figure 26).

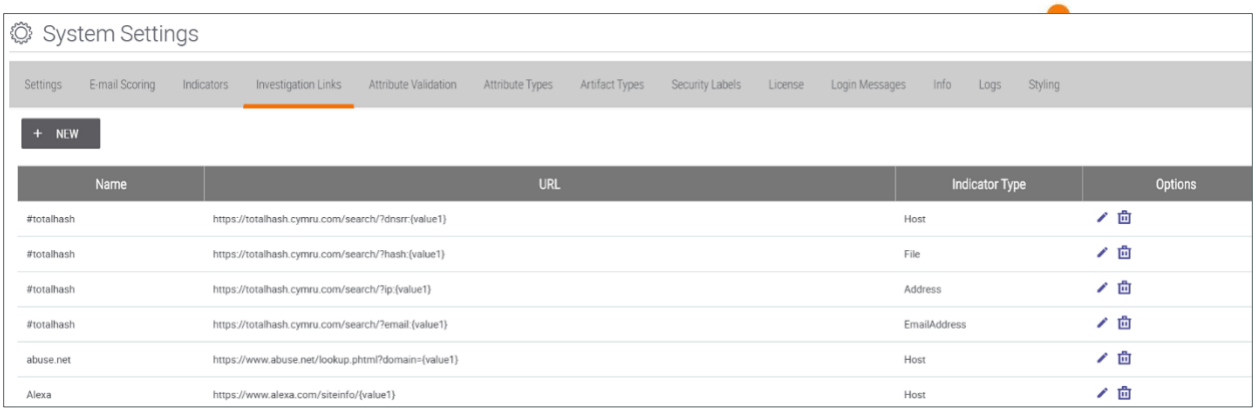

Figure 26

4. Click the **+ NEW** button. The **Create External Link** window will be displayed (Figure 27).

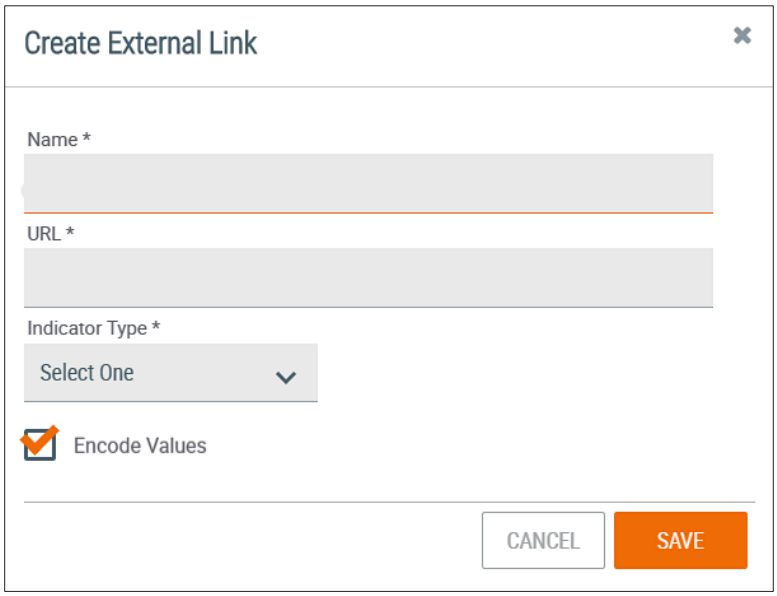

Figure 27

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

NOTE: It is best practice for System Administrators to click the *Clear Entity Cache* ***button located on the*** *Settings* ***tab 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 Attribute 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Attribute Validation** tab. The **Attribute Validation** screen will be displayed (Figure 28). The **Attribute Validation** screen displays the existing System Attribute Validation Rules.

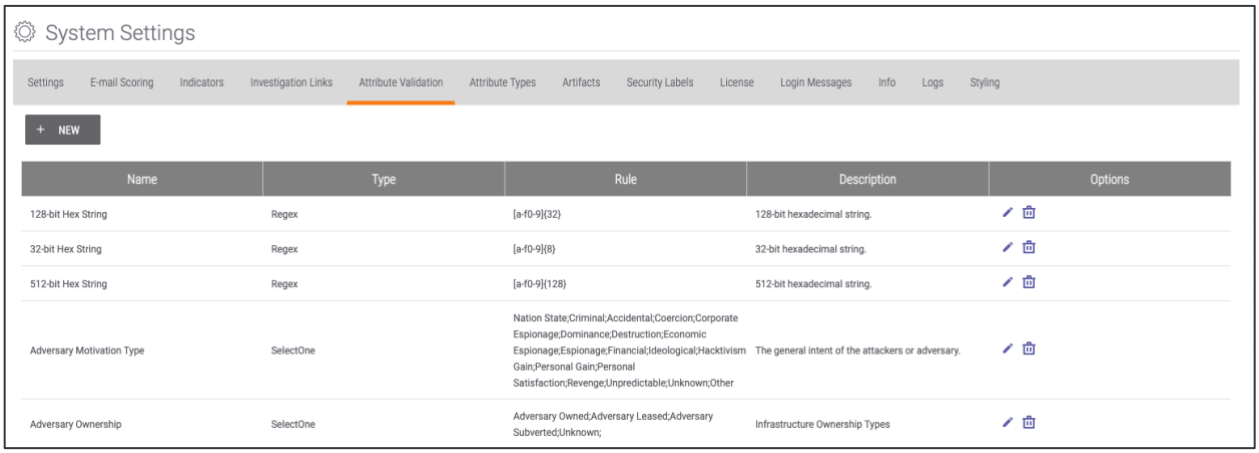

Figure 28

4. Click the **+ NEW** button. The **Create Attribute Validation Rule** window will be displayed (Figure 29).

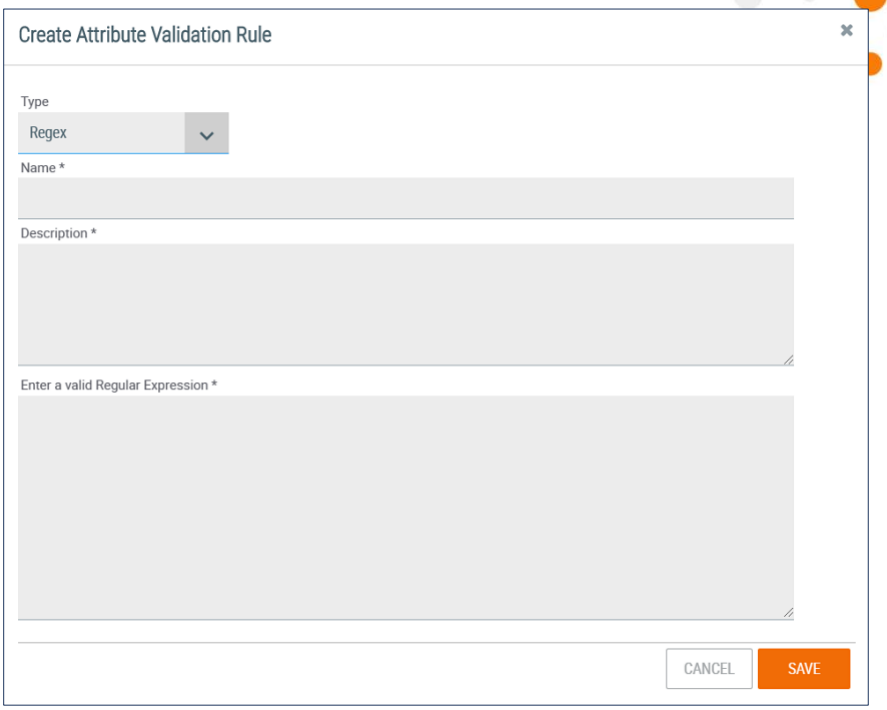

Figure 29

- **Type**: Use the dropdown menu to select the schema for the Validation Rule. Each option offers the flexibility to determine the valid domain for each Attribute Type:
  - **Regex**: A regular expression that considers only matching inputs to be valid (e.g., an IP address or email address on a certain domain)
  - **Xsd**: An XML Schema Definition used to validate input (useful for attaching logs from a vendor product)
  - **Select One Picklist**: Presented as a dropdown menu of options—after the Administrator defines the options in the text box at the bottom of the window—from which users may only select one value (e.g., high, medium, or low priorities)
  - **Select One Radio**: Similar to **Select One Picklist**, but presented as a series of radio buttons
  - **Date**
  - **Date/Time**
  - **Integer**: A whole number, valid in the range specified in the right-hand text box (e.g., 0:1440 for "minutes worked")
- **Name**: Enter the name of the Validation Rule as it will be displayed in the Validation Rules table of the Attribute Validation screen.
- **Description**: Enter a general description of the Validation Rule.
- **Enter a Valid Regular Expression**: If applicable, enter the parameters for a Validation Rule as defined previously.

5. Click the **SAVE** button to save and use the new **System Attribute Validation Rule**.

   NOTE: A System Attribution Validation Rule will need 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Attribute Validation** tab. The **Attribute Validation** screen will be displayed (Figure 28).
4. Click the **Edit** icon for the Validation Rule to be edited. The **Create Attribute Validation Rule** window will be displayed (Figure 30).

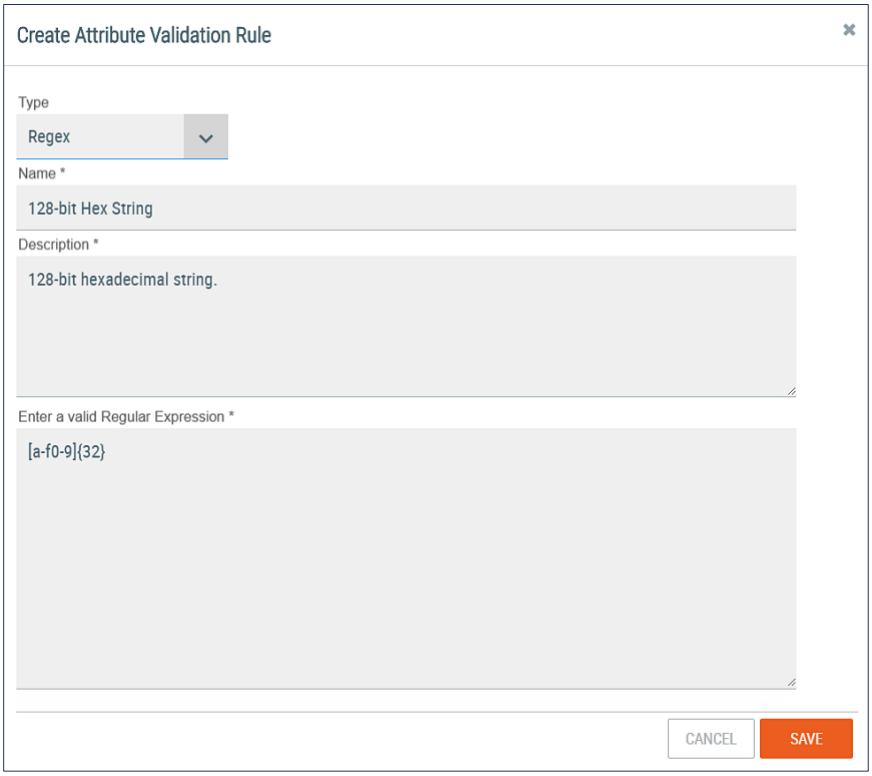

Figure 30

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 Attribute Types:

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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Attribute Types** tab. The **Attribute Types** screen will be displayed (Figure 31).

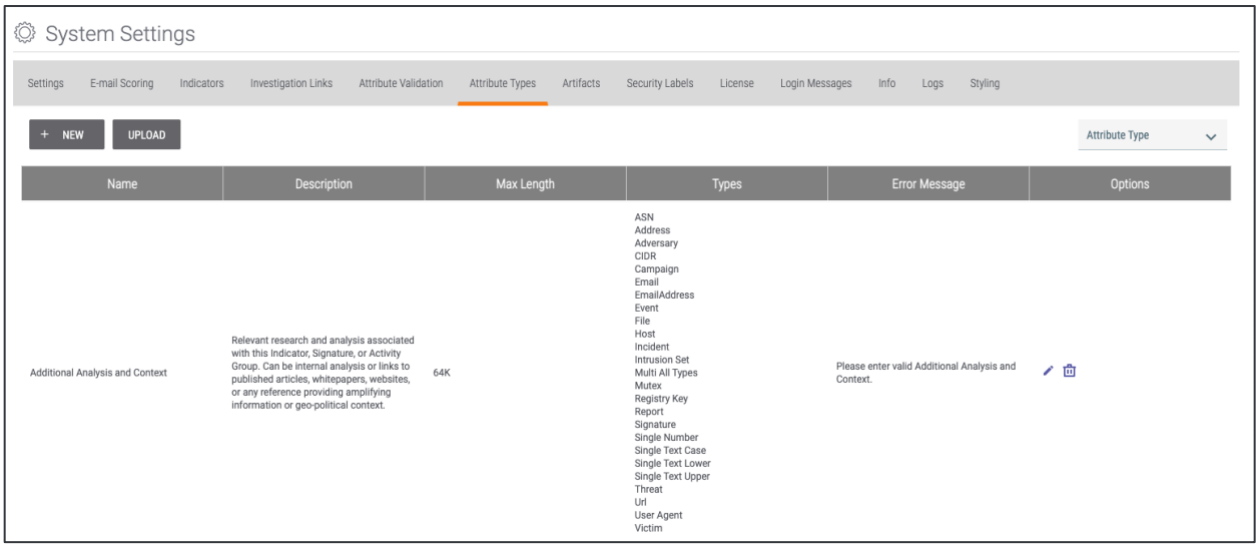

Figure 31

Creating System Attribute Types

Follow these steps to create a new 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Attribute Types** tab. The **Attribute Types** screen will be displayed (Figure 31).
4. To create a new, custom System Attribute Type, click the **+ NEW** button. The **Configure Attribute Type** window will be displayed (Figure 32).

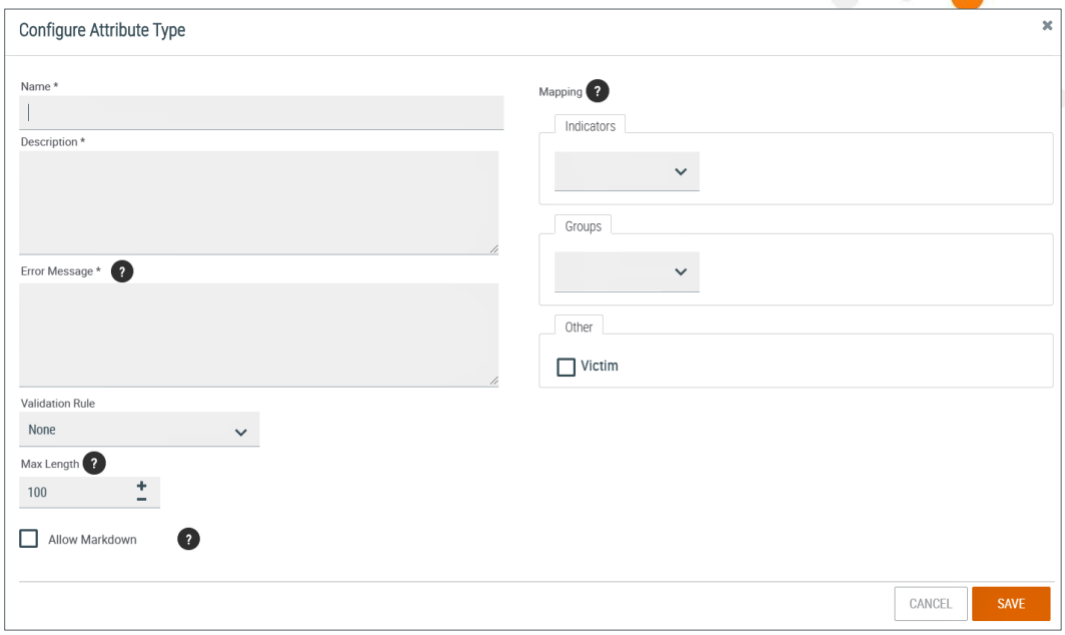

Figure 32

- **Name**: Enter the name of the System Attribute Type as it will be displayed on menus and on the **Details** screen for Indicators and Groups.
- **Description**: Enter a description of the System Attribute Type as seen by users when inputting a value for the Attribute Type or when viewing it from the **Details** screen.
- **Error Message**: Enter the message presented when users try to input a value that does not meet the System Attribute Type's Validation Rules.
- **Validation Rule**: Use the dropdown 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 can define their own System Attribute Type Validation Rules as needed.
- **Max Length**: Enter the maximum size, in number of characters, of the System Attribute Type, if applicable, based on the Attribute Type's assigned Validation Rule. The maximum size can also be entered using the plus and minus buttons to add or subtract increments of 1, respectively.
- **Allow Markdown**: Select this checkbox to allow Markdown to be used when configuring an Attribute Type.

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

- **Mapping**: Use the dropdown menus for Indicators or Groups, and then select the 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 given Groups and Indicators. If custom Indicators have been added, they will be displayed in the **Indicators** section as well.

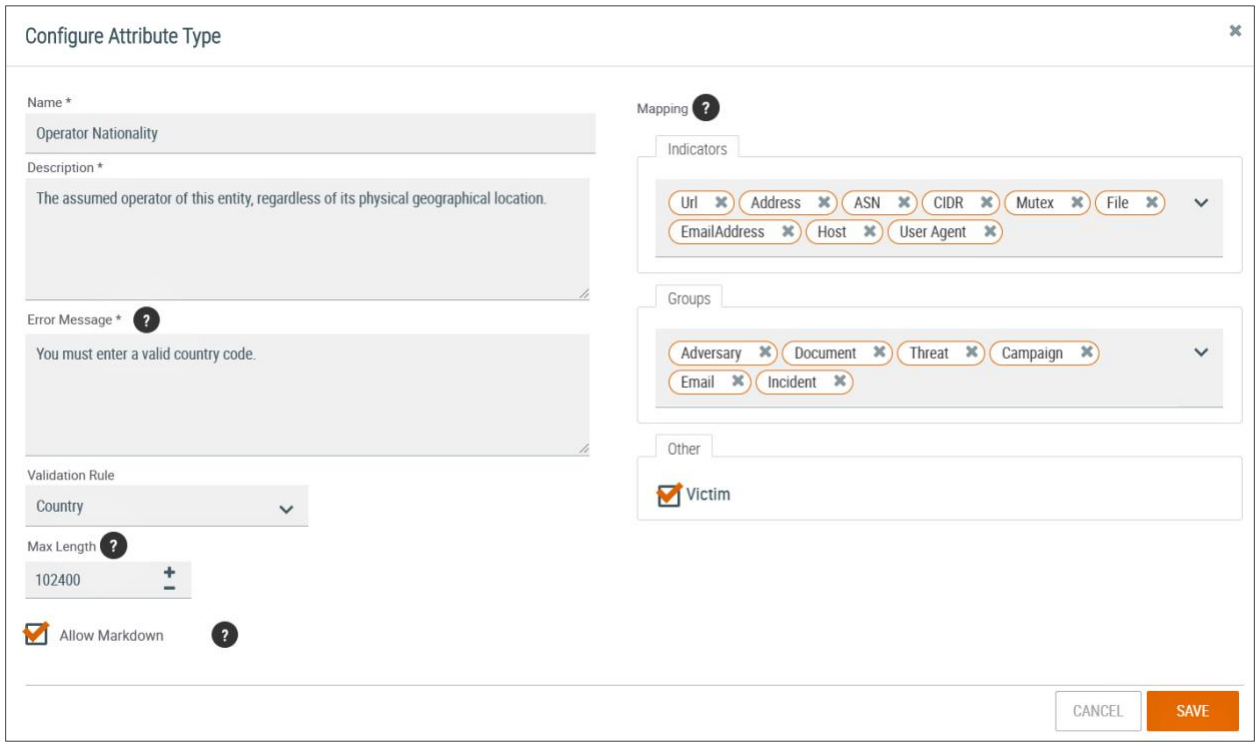

Figure 33

Uploading a System Attribute Type

Follow these steps to upload a System Attribute 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Attribute Types** tab. The **Attribute Types** screen will be displayed (Figure 31).
4. Click the **UPLOAD** button. The **Upload Attributes** window will be displayed (Figure 34).

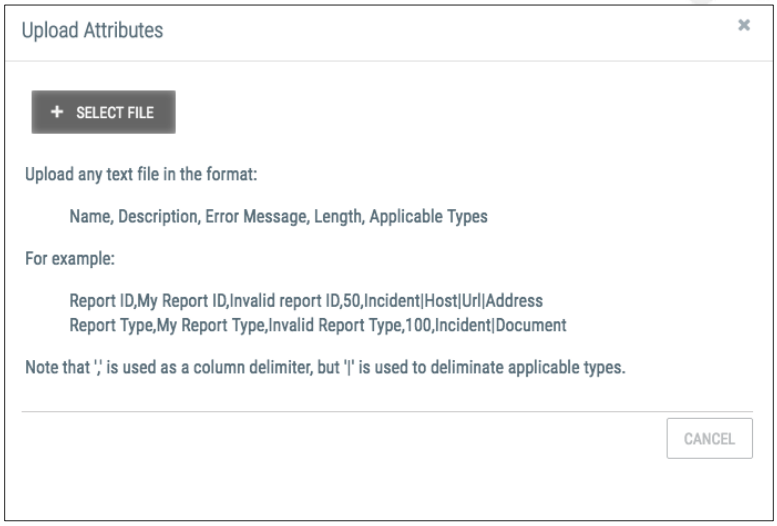

Figure 34

5. Click the **+ SELECT FILE** button, locate and select a file to upload, and click the **SAVE** button.

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

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

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

Table 4

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

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

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

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

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

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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Attribute Types** tab. The **Attribute Types** screen will be displayed (Figure 31).
4. Click the **Edit**  icon for the Attribute to be edited. The **Configure Attribute Type** window will be displayed (Figure 32).
5. Configure the fields.
6. Click the **SAVE** button.

Artifact Types

Artifacts are integral components of ThreatConnect's Workflow feature. (See the "Workflow and Case Management" section and *Workflow Overview* for more information.) Artifacts are typed, like Indicators and Groups, and a set of supported Artifact types is preconfigured in ThreatConnect. This set includes all ThreatConnect Indicator types.

Creating Artifact Types

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

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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Artifacts** tab. The **Artifact Types** screen will be displayed (Figure 35). The **Artifact Types** screen displays the existing Artifact types.

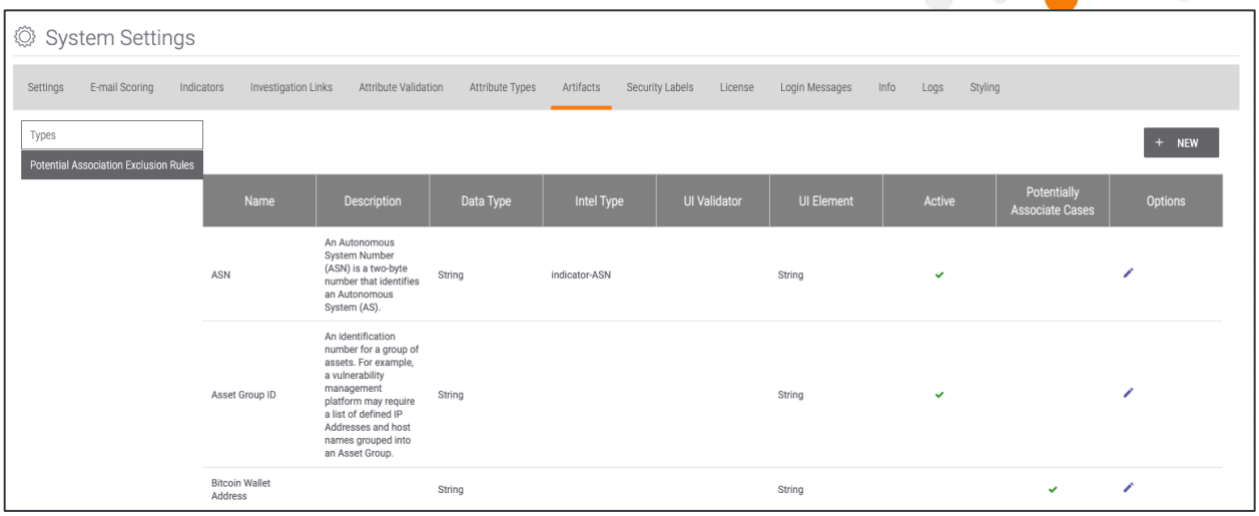

Figure 35

4. Click the **+ NEW** button. The **Configure Artifact Type** window will be displayed (Figure 36).

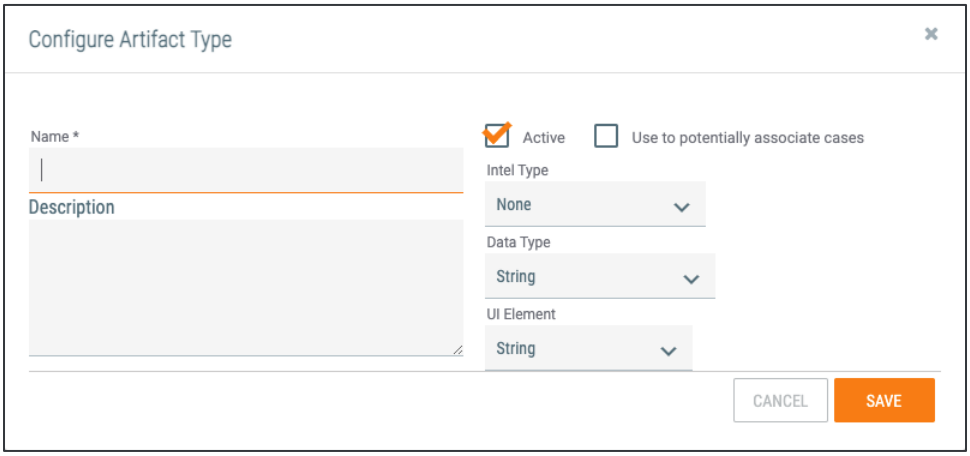

Figure 36

- **Name**: Enter the name of the Artifact type as it will be displayed in the **Artifact Types** table.
- **Description**: Enter a description of the Artifact type.
- **Active**: Select the checkbox to make this Artifact type active.
- **Intel Type**: Use the dropdown menu to select a ThreatConnect Indicator type to map to the Artifact type.
- **Data Type**: Use the dropdown menu to select the data type for the Artifact type (either String or File).
- **UI Element**: Use the dropdown menu to select the UI element into which the user will enter data for Artifacts of this type.

5. Click the **SAVE** button to create the Artifact Type.

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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Artifact Types** tab. The **Artifact Types** screen will be displayed (Figure 35).
4. Click the **Edit** icon for the Artifact Type to be edited (Address in this example). The **Configure Artifact Type** window will be displayed (Figure 37).

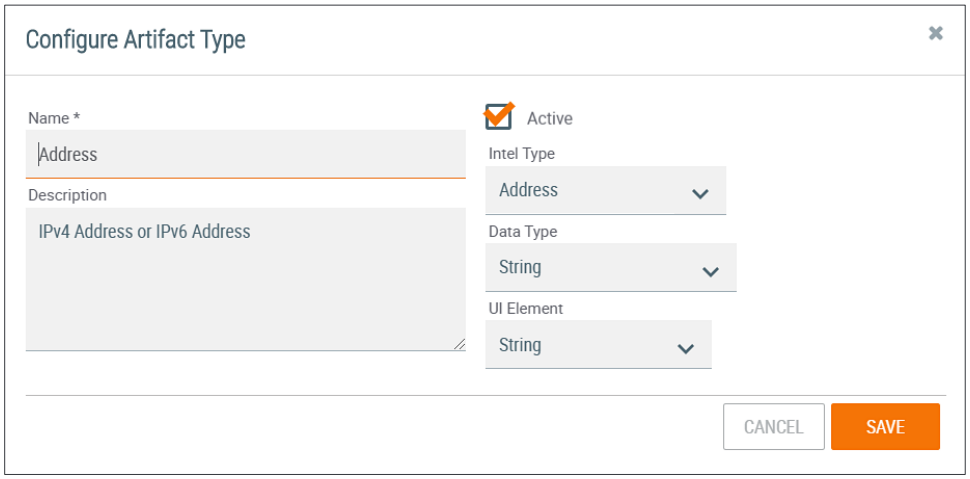

Figure 37

5. Configure the fields.
6. Click the **SAVE** button.

Potential Association Exclusion Rules

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

Follow these steps to edit an Exclusion Rule:

1. On the **Artifacts** tab of the **System Settings** screen, click the **Potential Association Exclusion Rules** button in the left-hand menu. The **Exclusion Rules** screen will be displayed (Figure 38).

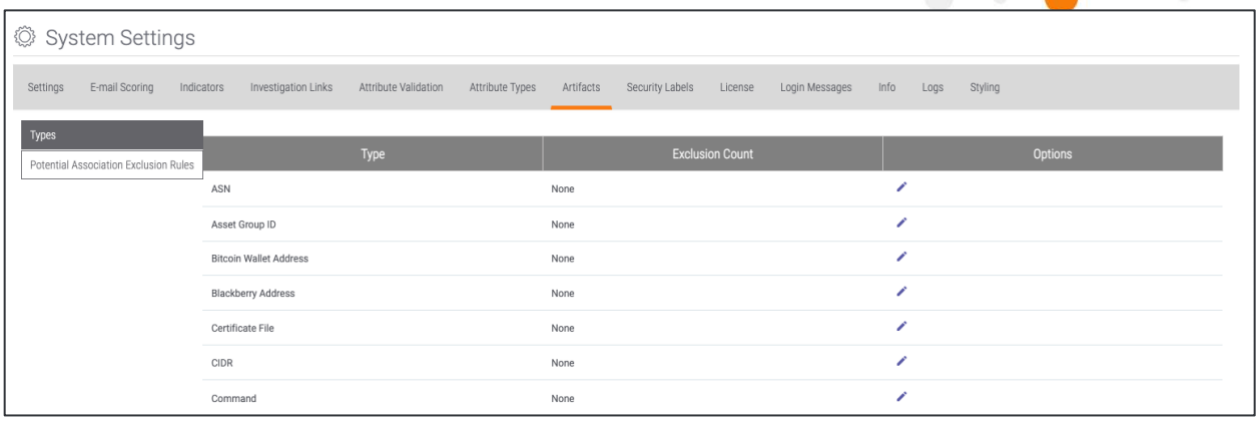

Figure 38

2. Click the **Edit**  icon to the right of an entry. The **Exclusion Details** window (Figure 39) will be displayed (ASN type in this example).

Figure 39

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

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.

ThreatConnect also includes a migration tool that allows users to take an owner-specific security label and migrate it to a System label, so that every possible variation of the TLP naming convention (e.g., TLP: RED vs. TLP Red vs. TLPred) is accounted for. To view more information on creating and using owner-level Security Labels in Organizations, Communities, and Sources, refer to 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 be displayed (Figure 2). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 7).
3. Click the **Security Labels** tab. The **Security Labels** screen will be displayed (Figure 40) with a list of the standard Security Labels.

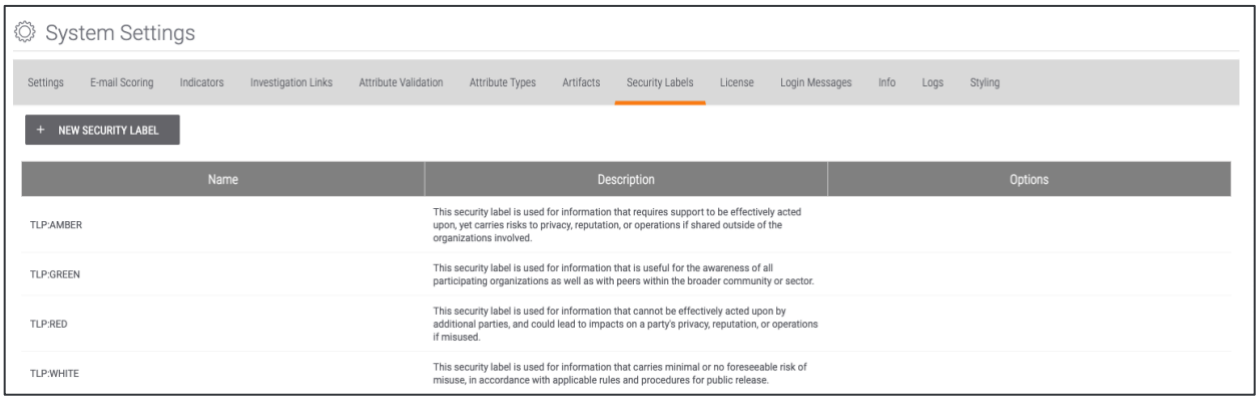

Figure 40

4. Click the **+ NEW SECURITY LABEL** button. The **Create Security Label** window will be displayed (Figure 41).

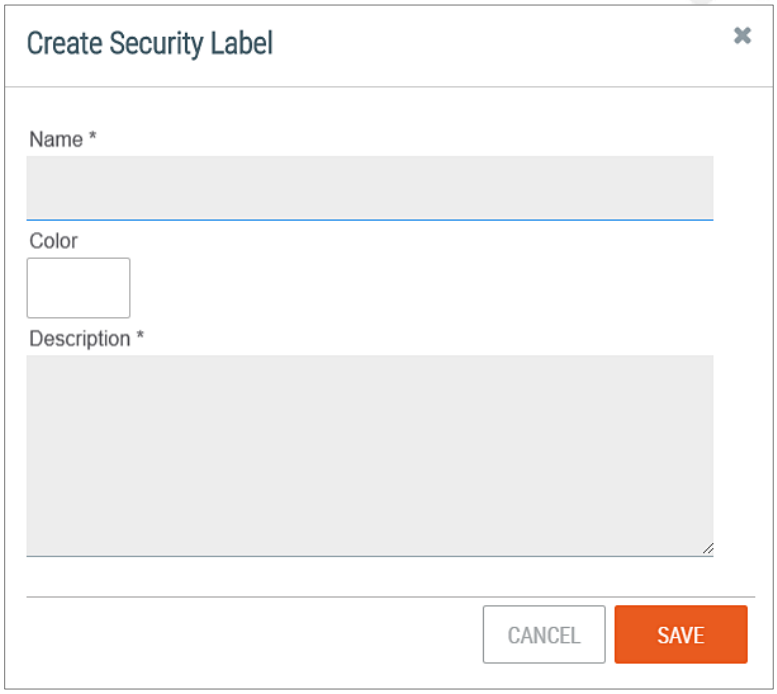

Figure 41

5. Enter a **Name**, **Color**, and **Description** for the Security Label.

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

6. Click the **SAVE** button.

Using System Security Labels

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

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

The System License

Viewing the System License and Terms of Service

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 be displayed (Figure 43). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 44).

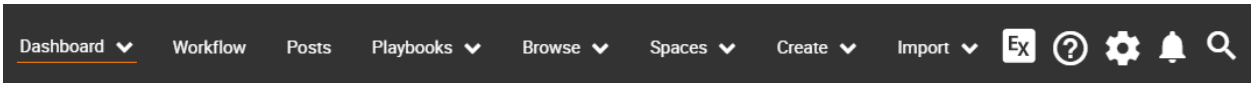

Figure 42

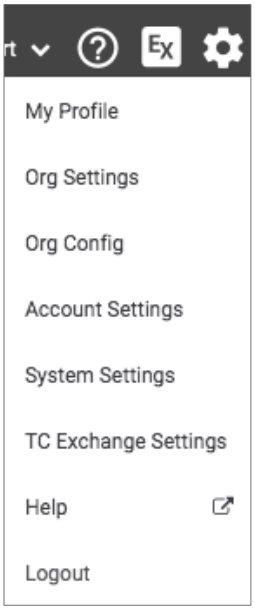

Figure 43

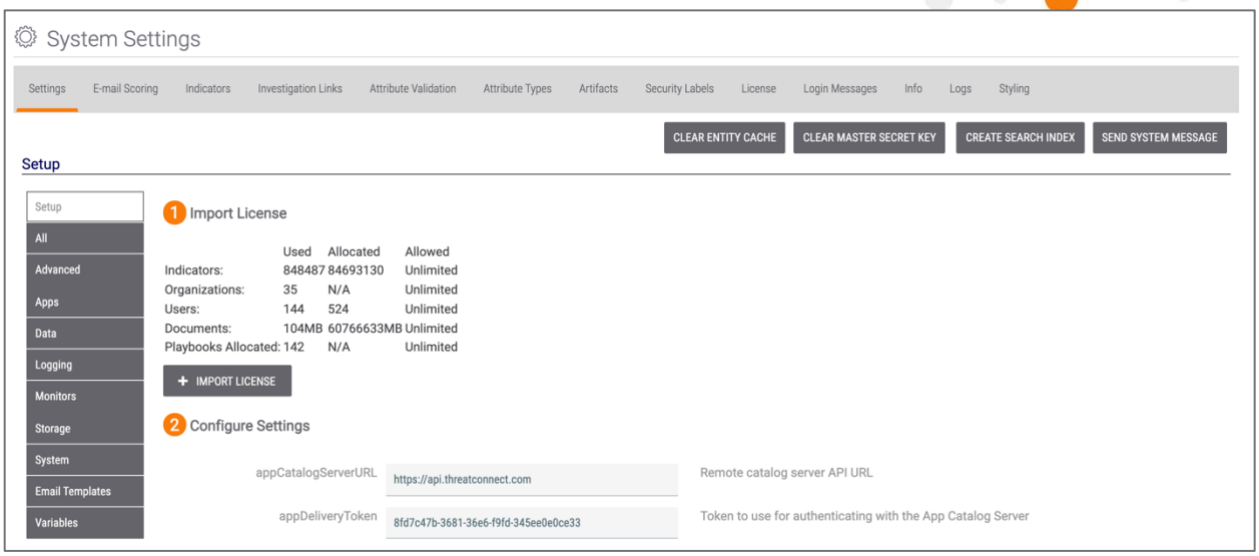

Figure 44

3. Click the **License tab**. The **License** screen will be displayed with the **License Config** subtab highlighted (Figure 45). This screen displays 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, which will open a file browser window to locate and select a license file.

Figure 45

4. Click the **Terms of Service** subtab. The **Terms of Service** screen will be displayed (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 be displayed (Figure 43). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 44).
3. Click the **Login Messages** tab. The **Login Messages** screen will be displayed (Figure 47).

Figure 47

4. Click the **+ NEW** button. The **Create Login Message** window will be displayed (Figure 48).

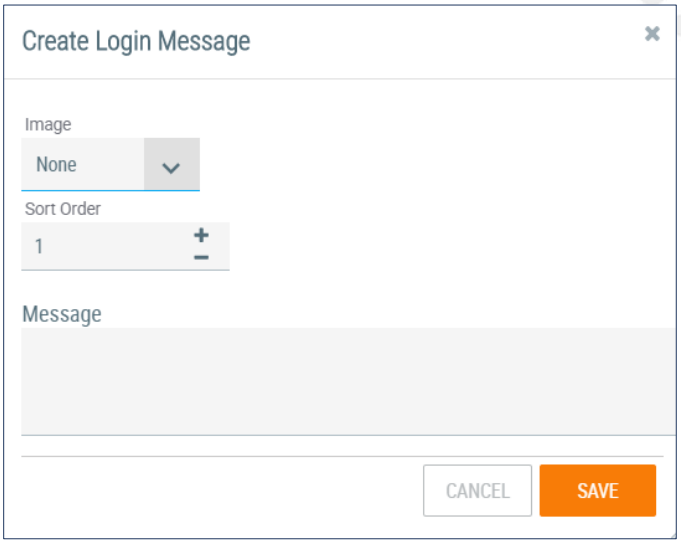

Figure 48

5. Configure the following settings for the new login message:
   - **Image:** Use the dropdown menu to select an icon to add next to the message.
     - **None:** No icon
     - **Vote:** Checkmark icon
     - **Feature:** Notebook icon
   - **Sort Order**: Click the plus and minus buttons to change the position in which the icon will be displayed on the screen next to the text.
   - **Message:** Enter the login message.
6. Click the **SAVE** button. The icon and text will be displayed on the **Login Messages** 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 be displayed (Figure 43). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 44).
3. Click on the **Info** tab. The **Info** screen will be displayed with the **Information** subtab highlighted (Figure 49). This screen displays current system hardware, software, and application database status information.

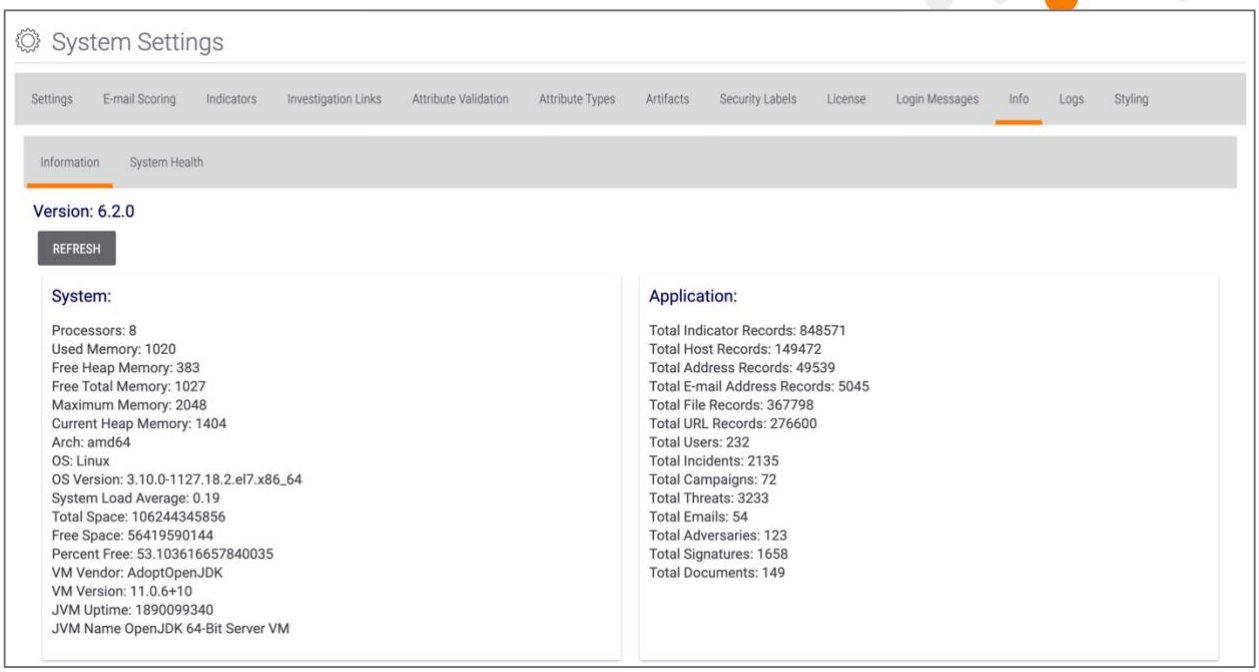

Figure 49

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

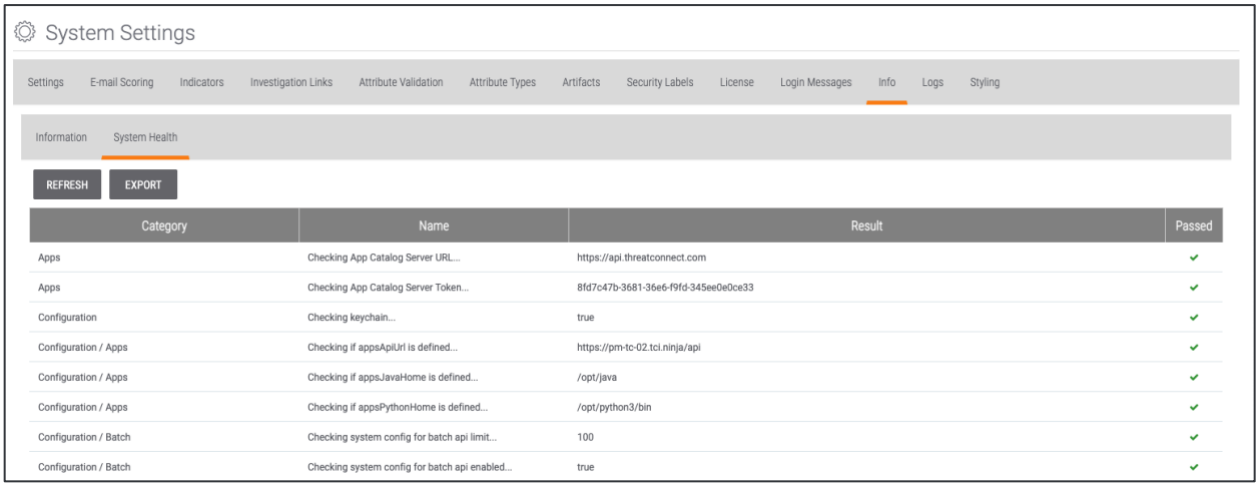

Figure 50

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 be displayed (Figure 43). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 44).
3. Click the **Logs** tab. The **Logs** screen will be displayed with the **View** subtab highlighted (Figure 51).
4. To narrow the display of table entries, enter text on which to filter in the **Source Class**, **Level**, or **Message** boxes.

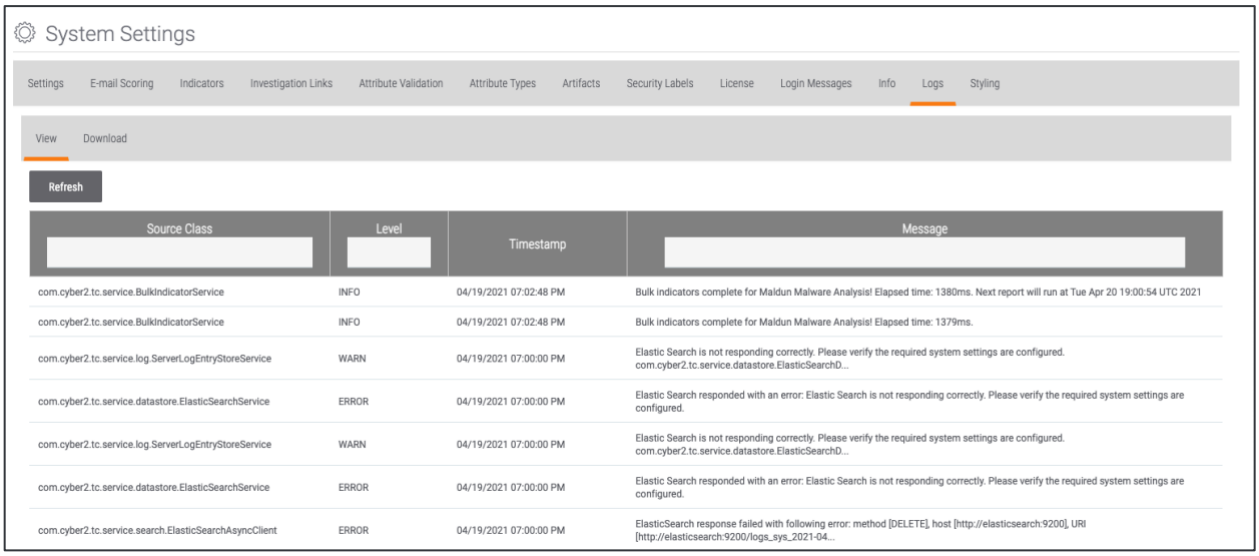

Figure 51

5. Click on an entry to view its **Log Details** (Figure 52).

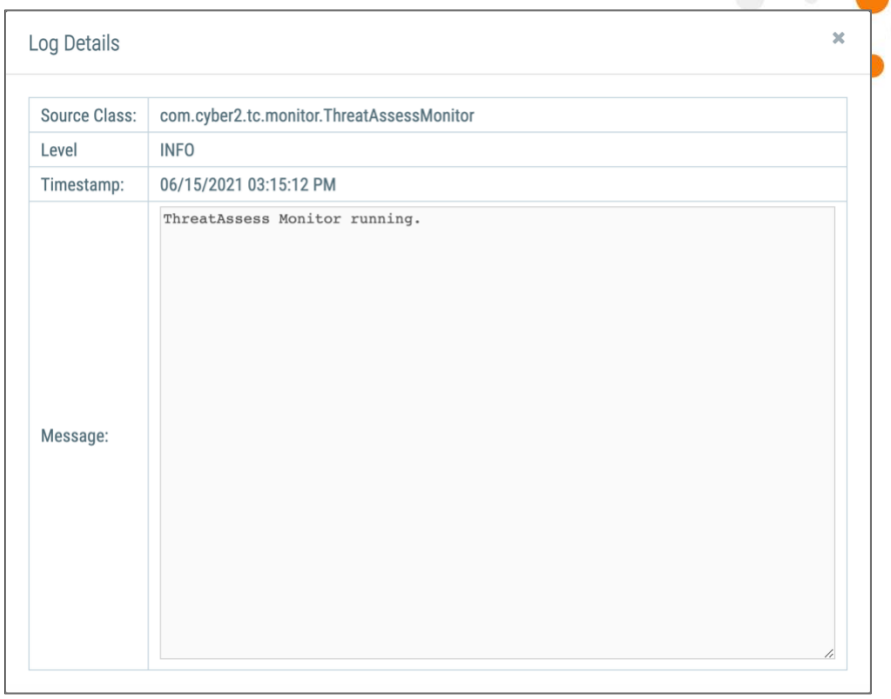

Figure 52

6. Click the **Download** subtab. The **Download** screen will be displayed (Figure 53).

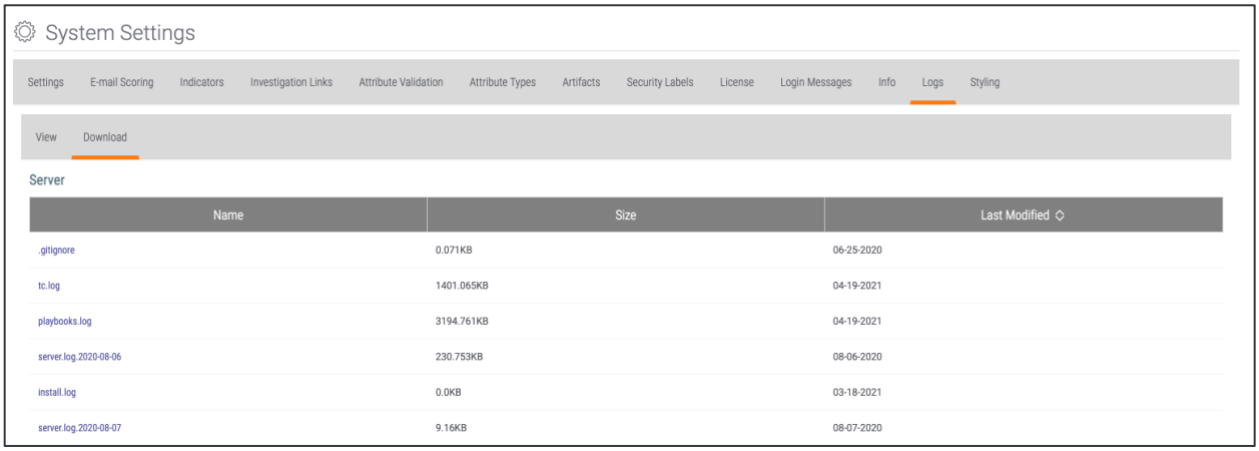

Figure 53

7. Click on an entry to download its 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 be displayed (Figure 43). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 44).

3. Click the **Styling** tab. The **Styling** screen will be displayed (Figure 54). This screen shows the default ThreatConnect headers and footer that will be used if no other images are uploaded.

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

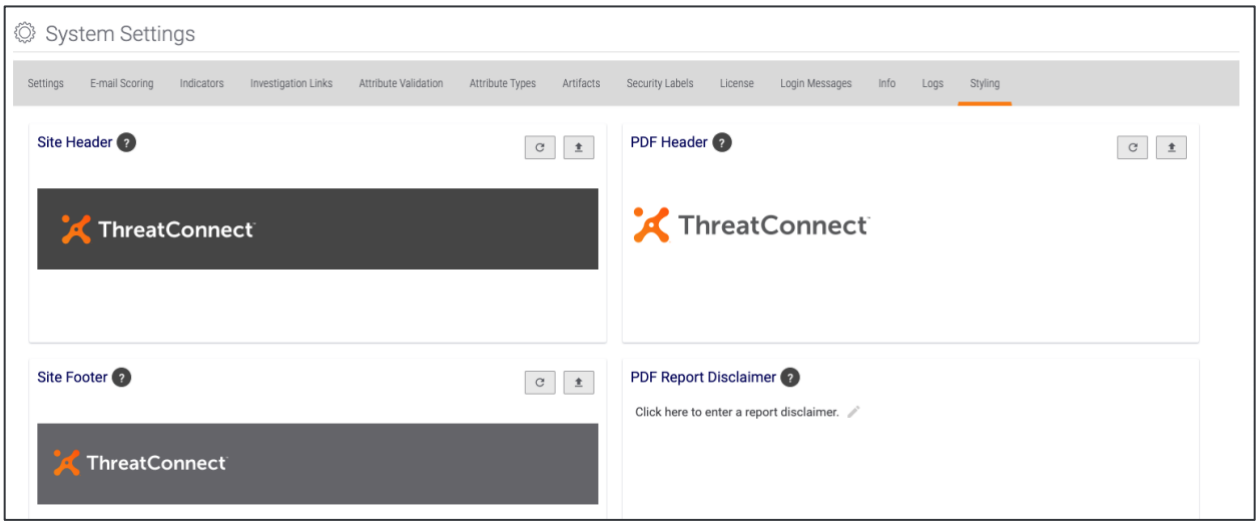

Figure 54

4. Click the **Upload** button next to the standard header or footer, and select a JPEG or PNG image file. The selected image will now appear in the appropriate header or footer box. It will also appear as a header for downloaded PDFs or as a header or footer for the user's ThreatConnect site.

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

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 the*** *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 allow 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 be displayed (Figure 43). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will be displayed (Figure 56). The **Installed** tab will be highlighted, displaying all installed applications.

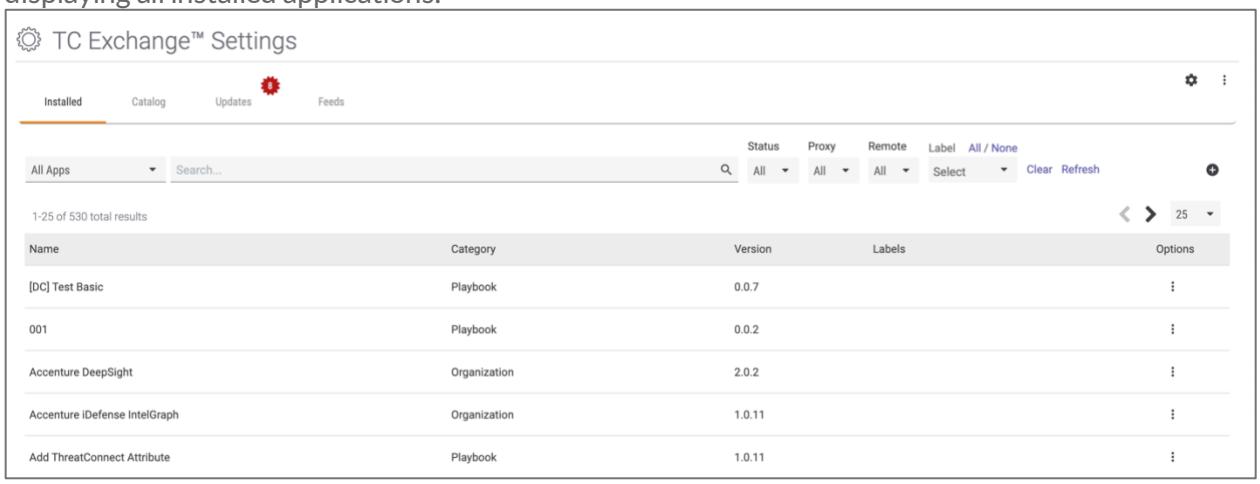

Figure 56

3. To view apps by category, use the dropdown menu located below the **Installed** tab. Application categories include Custom Apps, Custom Trigger, Feed Apps, Playbook, Playbook Template, REST API, Spaces, STIX, Third Party, Web Hook Trigger, and Workflow Templates. To search for an app, enter a term in the search box to return all applications matching the search term.

4. Apps on the **Installed** tab can be sorted and filtered using the menus to the right of the search bar:

   - **Status**: Use the **Status** dropdown menu to filter installed apps based on whether the app is **Active** or **Deprecated**.
   - **Proxy**: Use the **Proxy** dropdown menu to filter installed apps based on whether the **Use External Proxy** option is turned on or turned off.
   - **Remote**: Use the **Remote** dropdown menu to filter installed apps based on whether the **Allow Remote Execution** option is turned on or turned off.
   - **Label**: Use the **Label** dropdown menu to display a scrollable multi-select list of available labels. Selecting one or more labels will display only installed apps with those labels applied.

To select all labels, click **All** above the **Label** dropdown menu. To deselect all selected labels, click **None** above the **Label** dropdown menu.

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

5. Select an app, and click the vertical ellipsis icon in the **Options** column to display the app's **Options** menu (Figure 57).

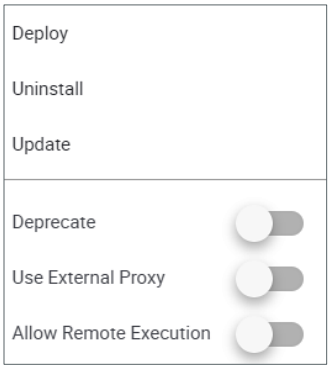

Figure 57

NOTE: Figure 57 is an example of an** Options **menu for a specific app. The number of options available may vary for different applications.

6. From the **Options** 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.**

7. Click the **Install App** button at the upper right of the screen. The **Install App** window will be displayed (Figure 58).

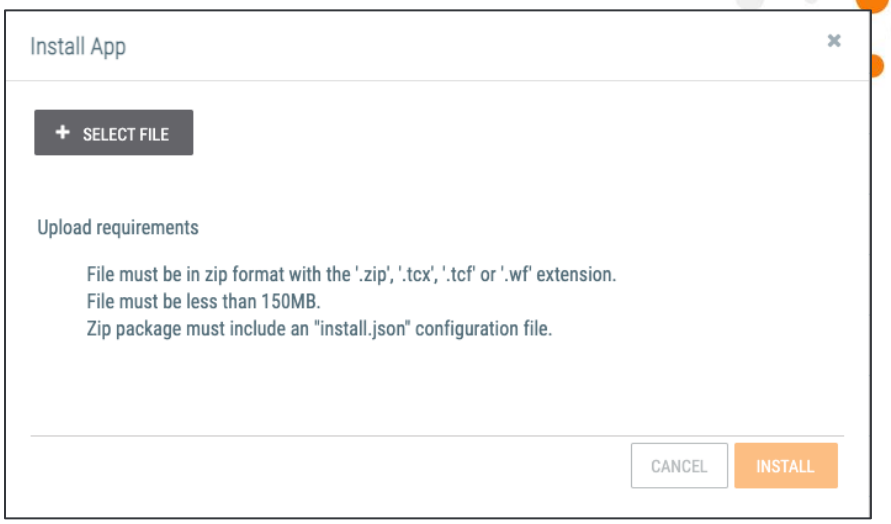

Figure 58

8. 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.

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

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

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 be displayed (Figure 43). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will be displayed (Figure 56).

3. Select an app and click the vertical ellipsis  icon in the **Options** column to view the app's **Options** menu (Figure 57).

4. Click **Deploy**. The **Feed Deployer** screen will be displayed with the **Source** tab highlighted

(Figure 59).

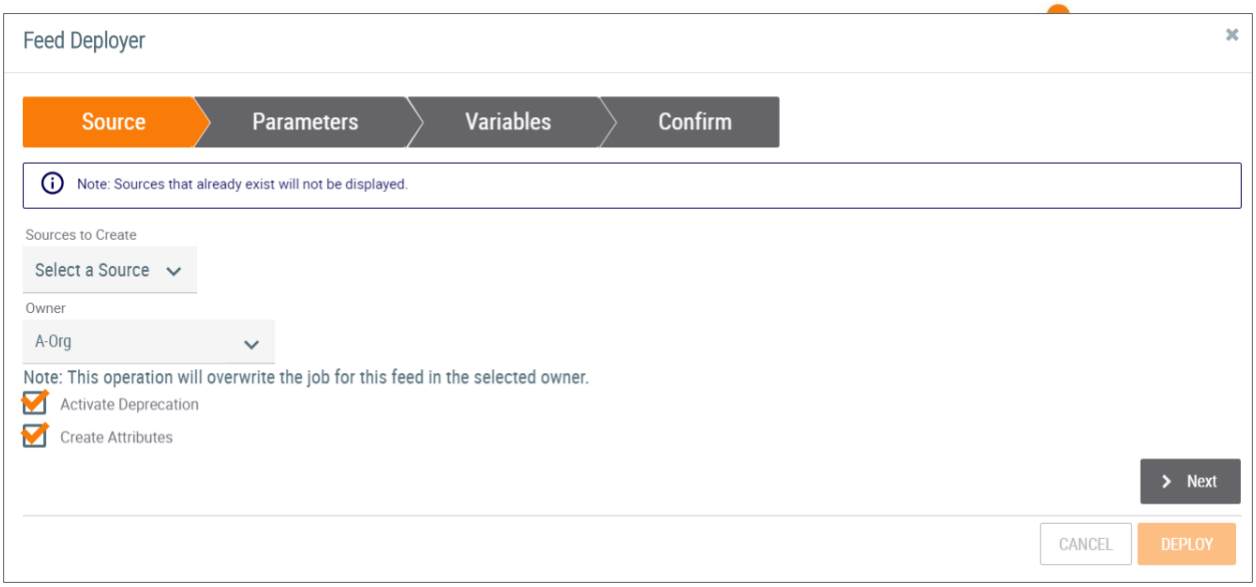

Figure 59

5. Select a **Source** (or Sources) and an **Owner** by using the respective dropdown menus, and select the **Activate Deprecation** and the **Create Attributes** checkboxes if desired.
6. Click the **Next** button. The **Parameters** screen will be displayed (Figure 60).

   NOTE: Parameters are customized and unique for each individual app.

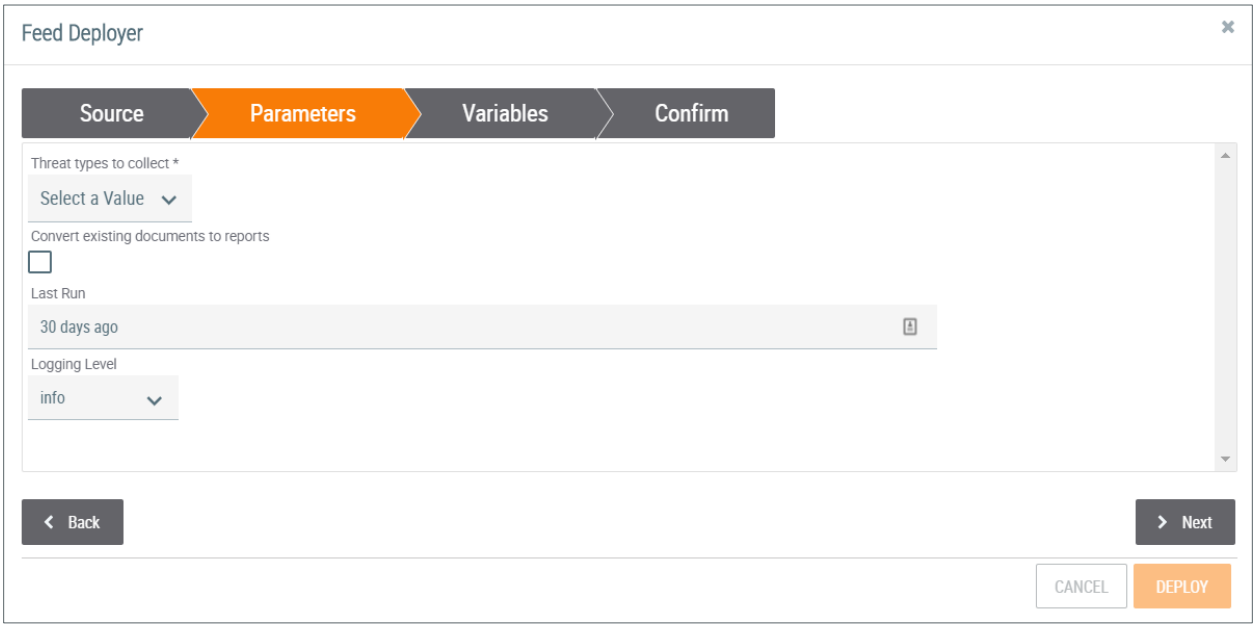

Figure 60

7. In this example, use the **Threat types to collect** dropdown menu to select a **Threat Type Value**

and **Logging Level**, select the **Convert existing documents to reports** checkbox, and use the **Last Run** dropdown menu to select the Last Run Date for the app.

8. Click the **Next** button. The **Variables** screen will be displayed (Figure 61), which will create a specified variable as part of the deployment, if required for the specified Source.

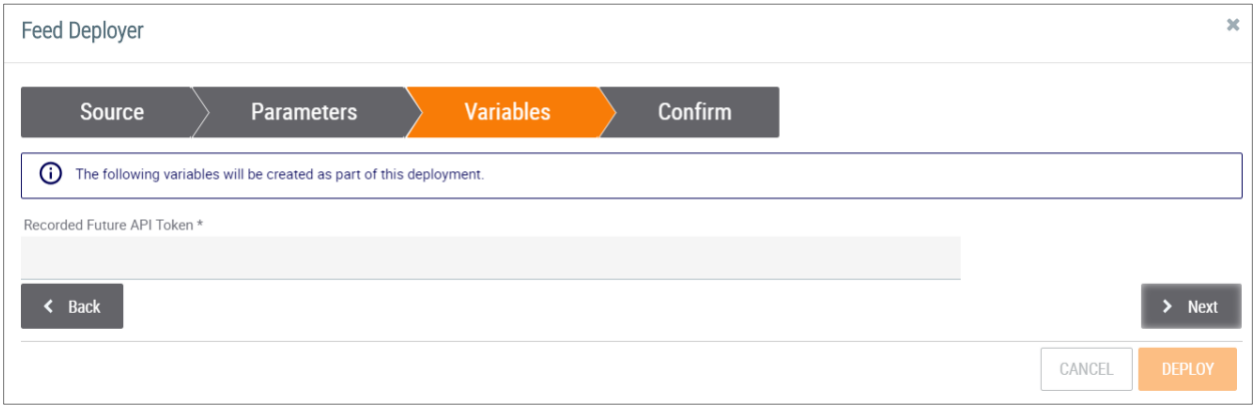

Figure 61

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

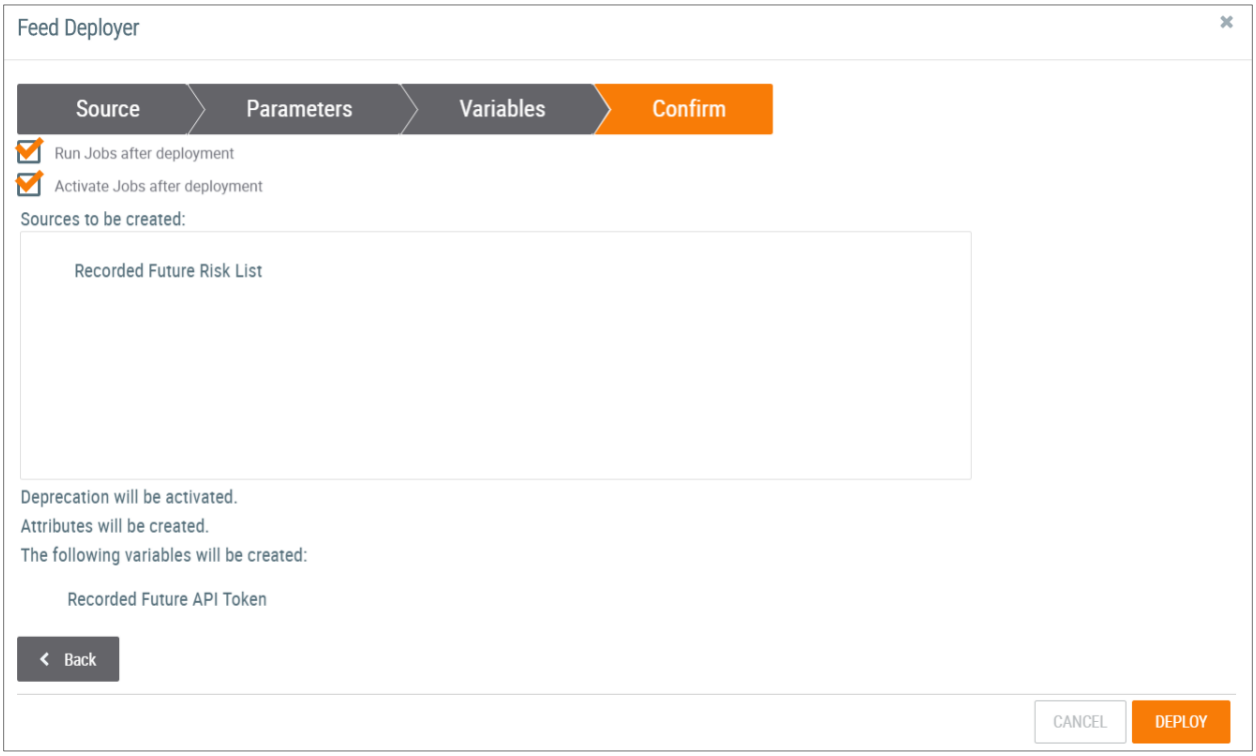

Figure 62

10. Select the **Run Jobs after deployment** and the **Activate Jobs after deployment** checkboxes if desired, 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://api.threatconnect.com**.

Follow these steps 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 be displayed (Figure 64).

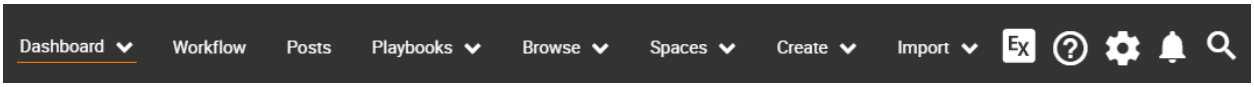

Figure 63

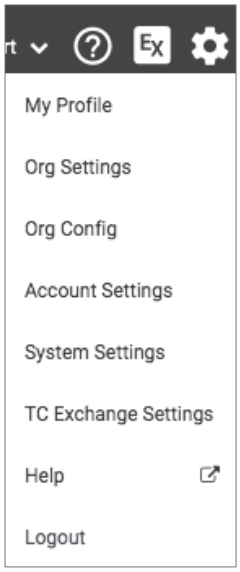

Figure 64

3. Select **System Settings**, and the **System Settings** screen will be displayed (Figure 65).

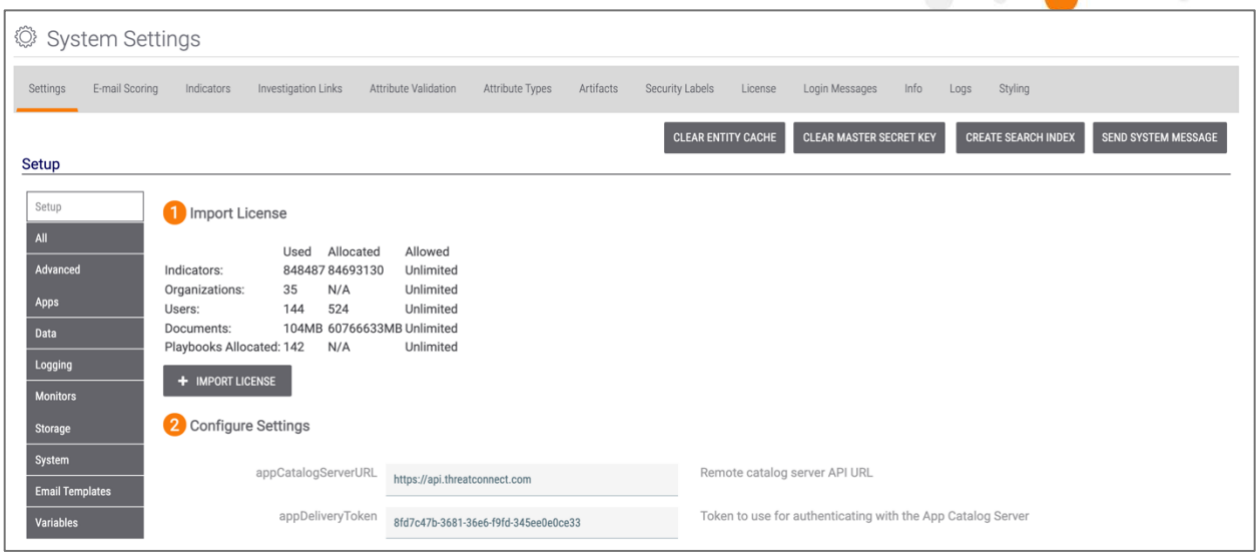

Figure 65

4. On the left-hand menu, click the **Apps** button. Configure the following settings:
   - **appCatalogServer**: Select the **Enabled** checkbox.
   - **appCatalogServerURL**: Leave this field blank to have the machine act as a server.
   - **appDeliveryToken**: Leave this field blank to have the machine act as a server.
5. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon, and the **Settings** menu will be displayed (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will be displayed (Figure 56).
6. The **Installed** tab will be highlighted, displaying all installed applications. Refer to the "Installing an App" section for more information on how to search for and filter installed apps.
7. The **Catalog** tab displays available apps on the remote catalog server that may be installed for the client. This tab is disabled when the machine is acting as a server.
8. The **Updates** tab displays available app updates that can be accessed by the client. This tab is disabled when the machine is acting as a server.
9. The **Feeds** tab allows access to apps data from created feeds.

Follow these steps 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 be displayed (Figure 64). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 65).
3. On the left-hand menu, click the **Apps** button. Configure the following settings:
   - **appCatalogServer**: Deselect the **Enabled** checkbox.

- **appCatalogServerURL**: Enter the server machine API URL.
- **appDeliveryToken**: Enter the App Delivery Token, which allows access by a specific Organization on the server to all the apps to which it is entitled.

Follow these steps to obtain the App Delivery Token from a Cloud account:

1. On the top navigation bar (Figure 63), place the cursor on the **Settings** icon, and the **Settings** menu will be displayed (Figure 64). Select **Account Settings**, and the **Account Settings** screen will be displayed (Figure 66).

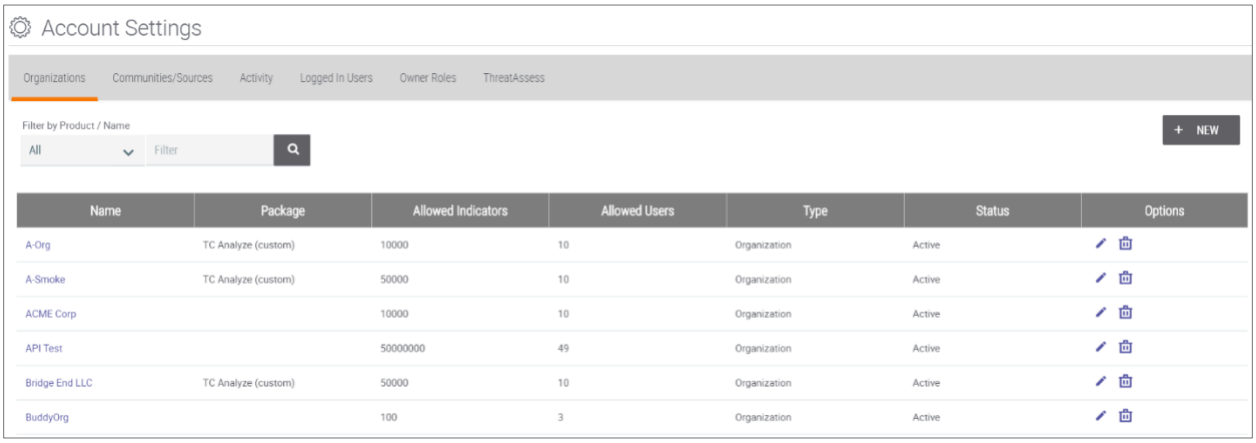

Figure 66

2. Click on an organization to view its **Organization Settings** (Figure 67).**Error! Reference source not found.**

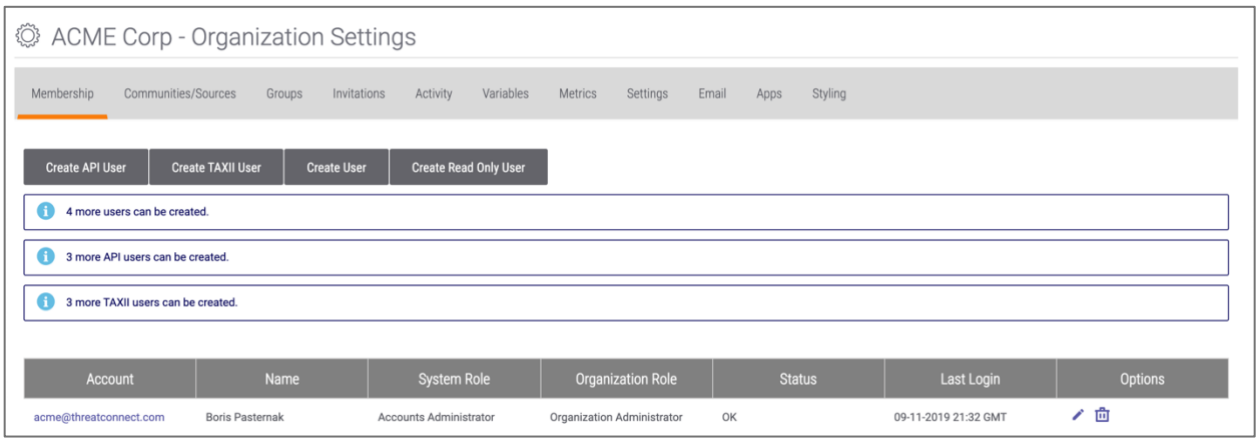

Figure 67

3. Click the **Apps** tab. The Apps screen will be displayed (Figure 68).**Error! Reference source not found.**

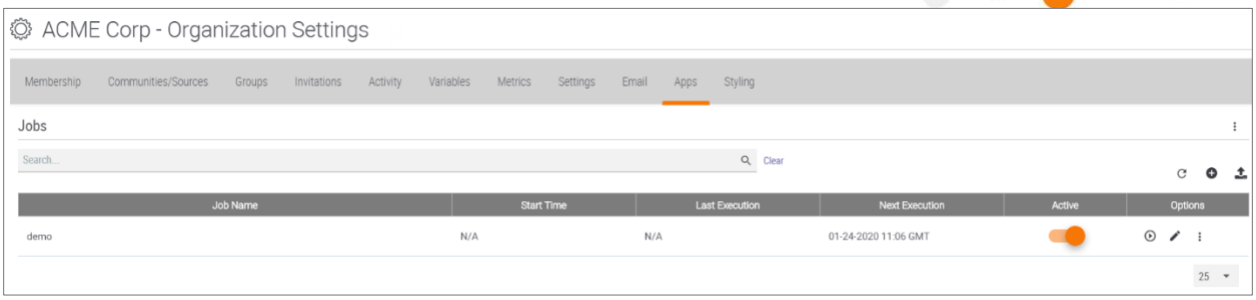

Figure 68

4. Click the vertical ellipsis  icon above the **Import Job**  icon, and select **App Delivery**. The **App Delivery Token** window will be displayed (Figure 69).**Error! Reference source not found.**

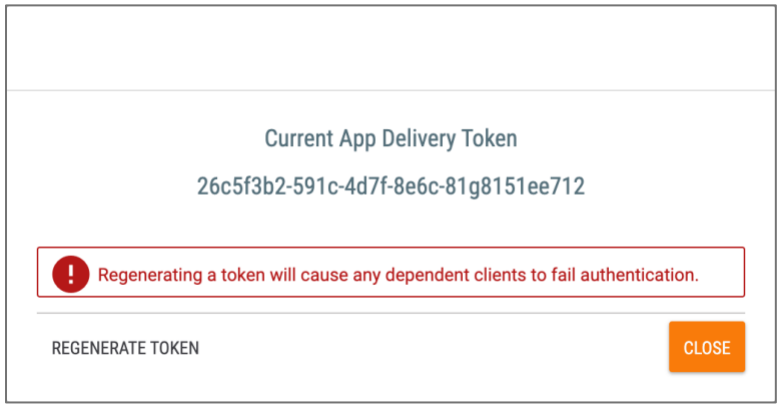

Figure 69

5. Copy the token, and then click the **CLOSE** button.
6. Return to the **System Settings** screen, and enter the token in the **appDeliveryToken** text box.
7. Return to the **TC Exchange Settings** screen. The **Catalog** and **Updates** tabs will now be enabled.
8. Click the **Catalog** tab. The **Catalog** screen will be displayed (Figure 70). This screen displays all apps available in the system.

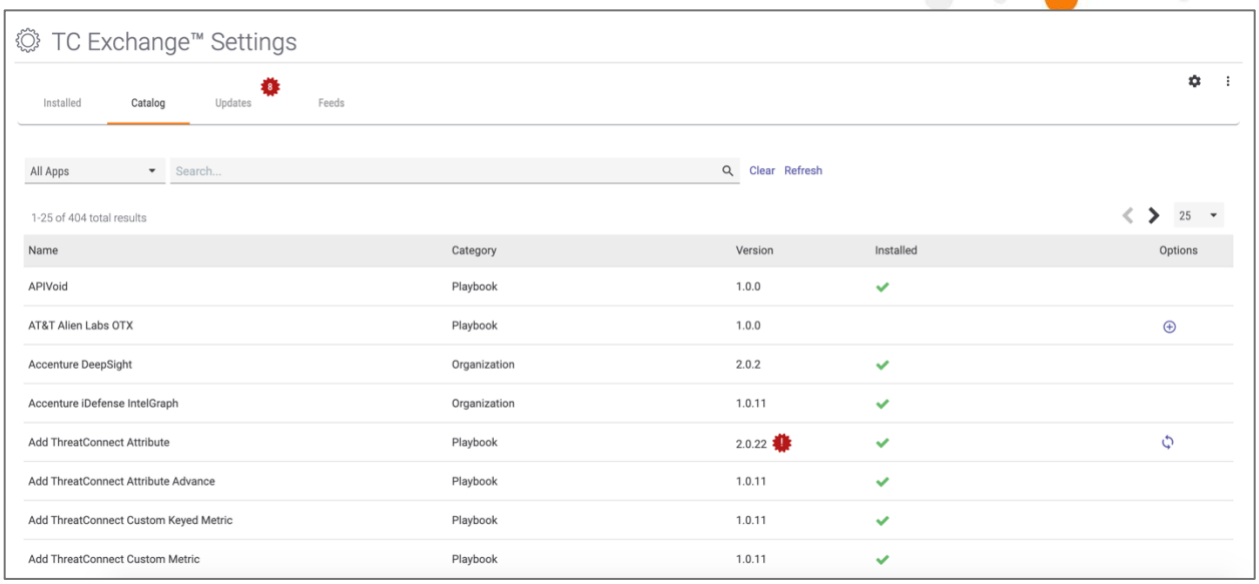

Figure 70

9. If an app is available, but has not been installed, the **Install**  icon will be displayed in the **Options** column. Click this icon to install an app. The **Release Notes** window will be displayed (Figure 71).

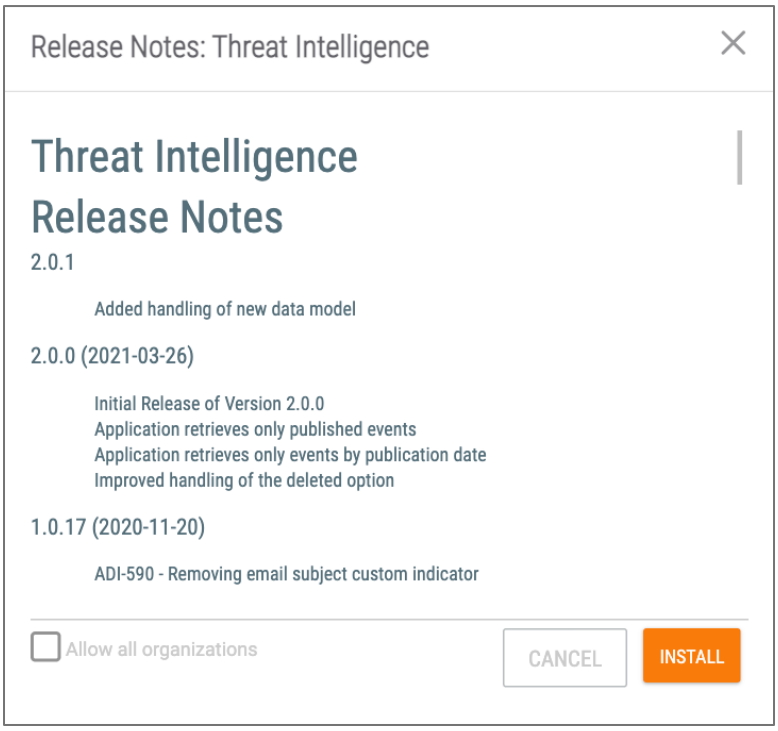

Figure 71

- **Allow all organizations:** Select this checkbox to allow all Organizations on the ThreatConnect instance to have access to the app.

10. Click the **INSTALL** button in the **Release Notes** window to install the app. A **Success** message (Figure 72) will be displayed in the lower-left corner of the screen if the app was successfully installed. The **Feed Deployer** screen (Figure 59) will also be displayed. Follow the steps in the "Feed Deployment" section to deploy the newly installed app.

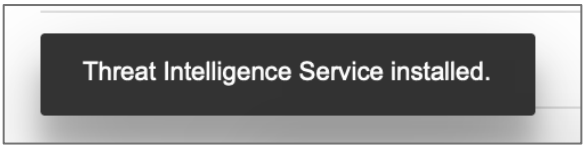

Figure 72

11. Click the **Updates** tab. The **Updates** screen will be displayed (Figure 73). This screen displays all the apps that have a pending update available.

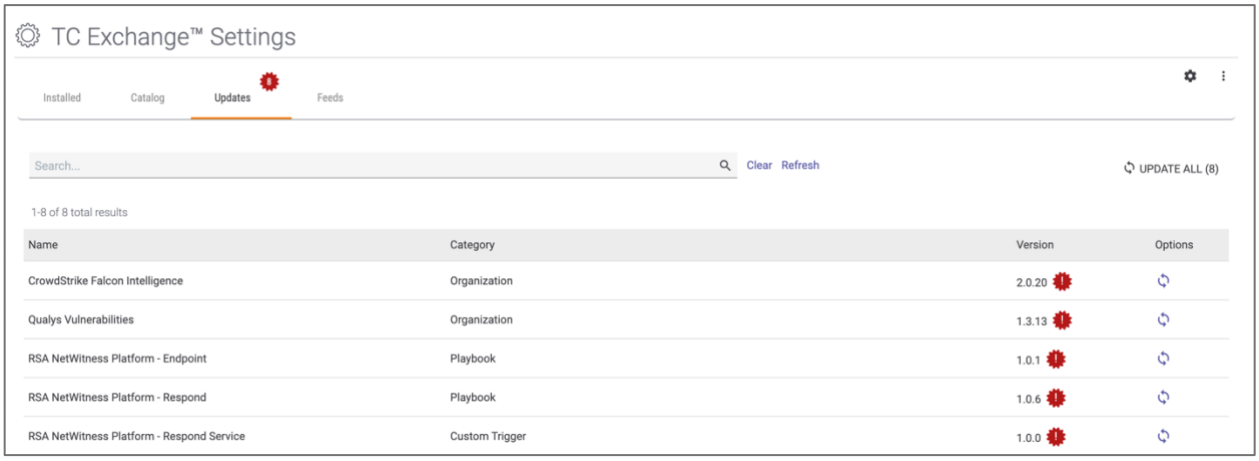

Figure 73

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

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

13. Click the **UPDATE ALL** button at the top right of the screen to install all available updates.

    Alternatively, click the **Update Now**  icon in the **Options** column to update one application at a time. The **Release Notes** window will be displayed (Figure 74).

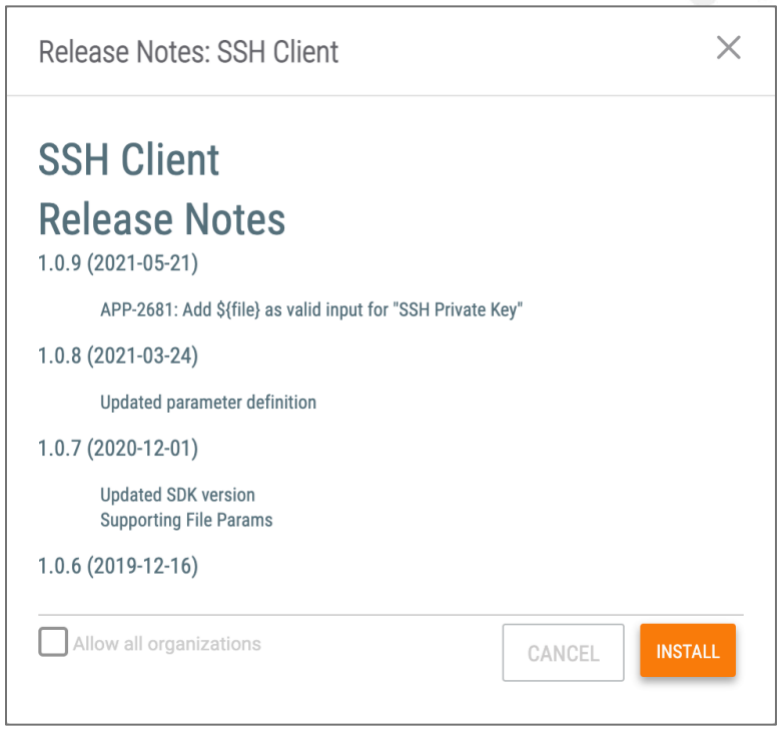

Figure 74

- **Allow all organizations:** Select this checkbox to allow all Organizations on the ThreatConnect instance to have access to the app.

14. 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 be displayed (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will be displayed (Figure 75).

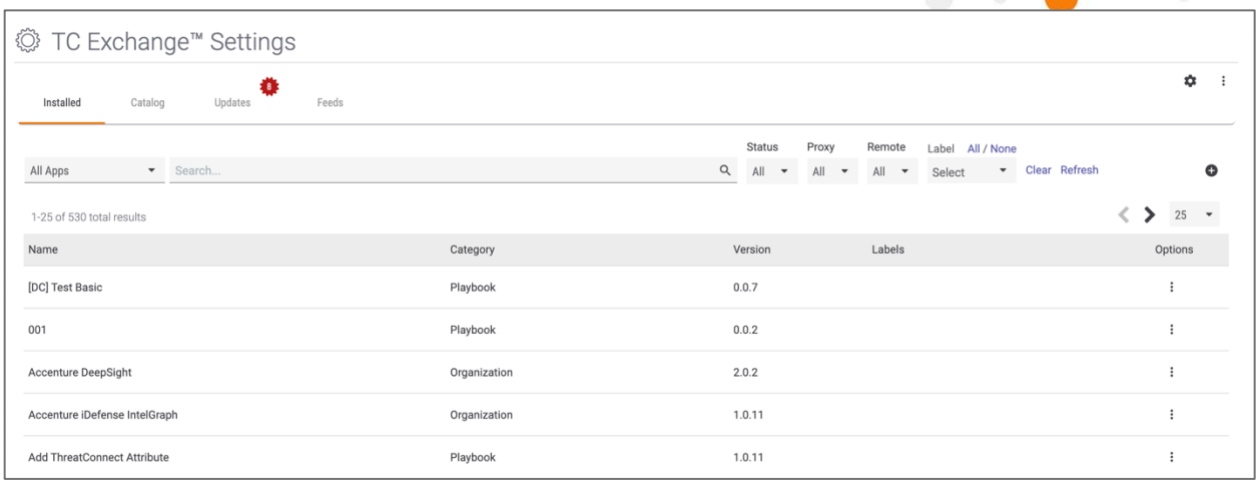

Figure 75

3. Click the **Feeds** tab. The **Feeds** screen will be displayed (Figure 76).

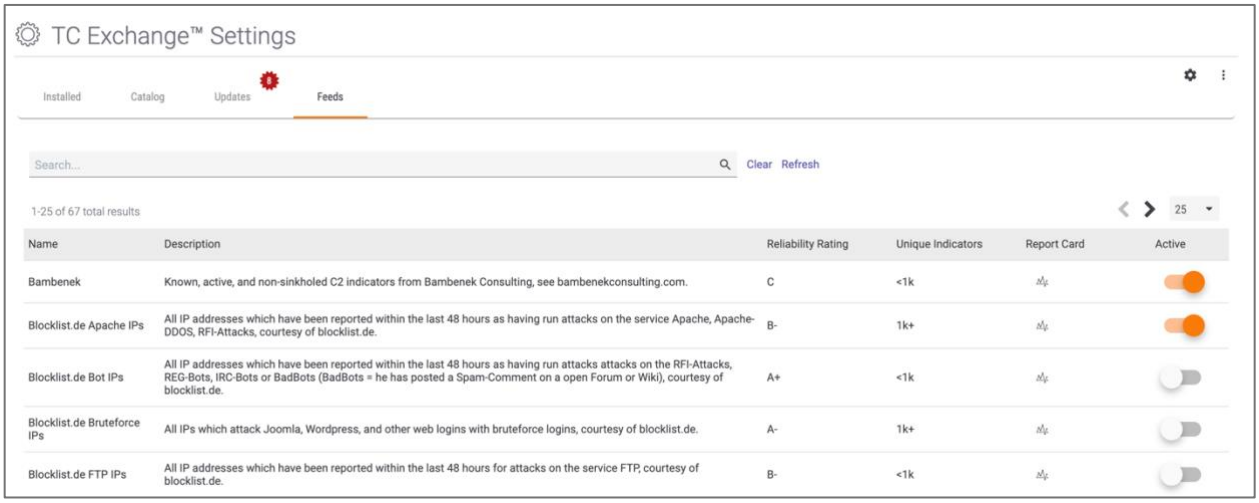

Figure 76

4. There are six columns for each feed. The **Reliability Rating** and **Unique Indicators** columns represent CAL data, which offers the user criteria for activating a feed.
5. The **Report Card** column also offers additional, CAL-generated data for users to determine whether they wish to activate a feed in their system. Click the **Graph** icon, and a graphic showing information containing metrics from other columns and how they compare with aggregated metrics from other feeds is displayed (Figure 77). See *Feed Metrics and Report Card* for more information.

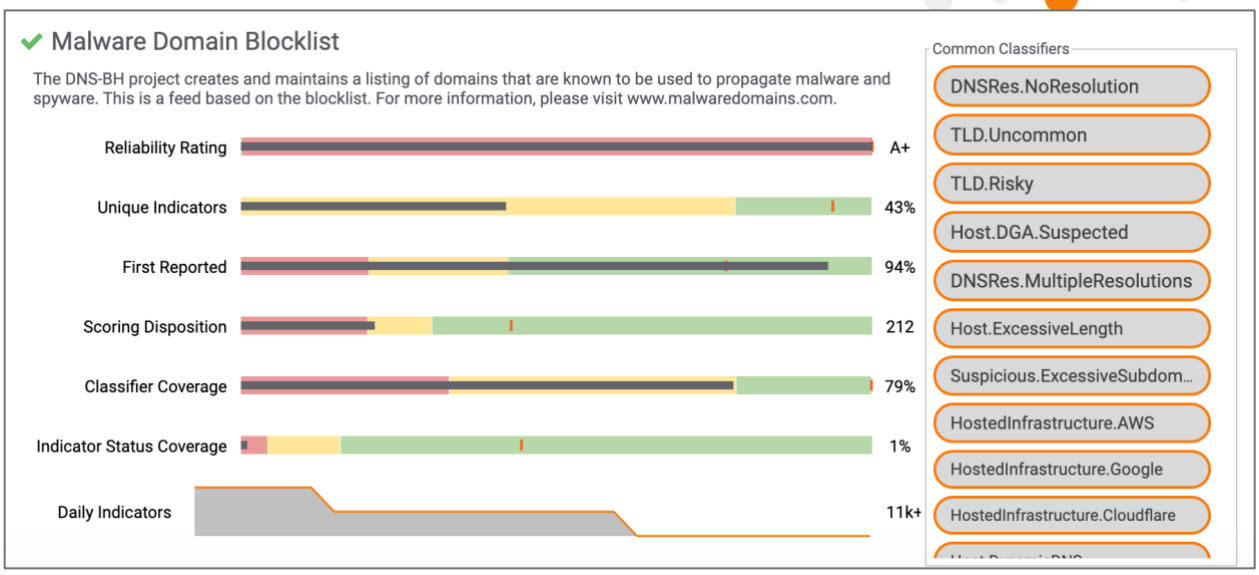

Figure 77

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

6. Click the **Gear**  icon at the top right of the screen. The **App Delivery Settings** window will be displayed (Figure 78). Use the dropdown menu at the bottom of this window to select a **Default Feed Owner**.

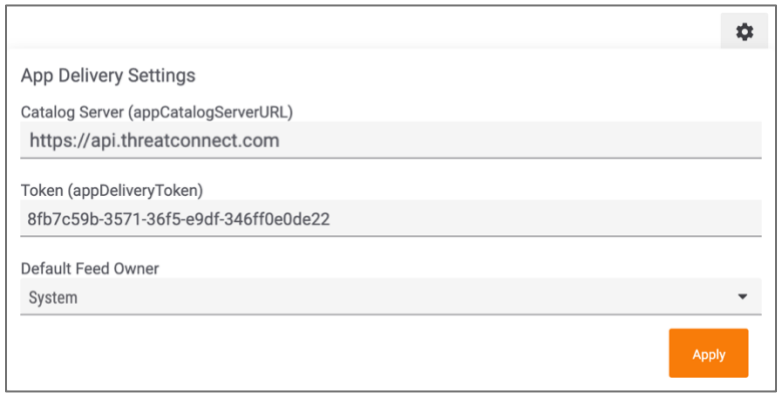

Figure 78

7. To activate a feed, select an entry from the table and toggle the slider to orange (on) in the **Active** column (Figure 79). This action will create a ThreatConnect Source that will access all data for that feed.

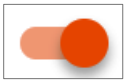

Figure 79

8. To redeploy a feed, toggle the slider to gray (off) in the **Active** column, delete the job and Source in that Organization, and then log out and log back into ThreatConnect.

App Distribution

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

Follow these steps 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 be displayed (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will be displayed (Figure 75).
3. In the **Search** bar, enter the name of an app. After the app is displayed in the search results, click the vertical ellipsis  icon in the **Options** column to view the app's **Options** menu (Figure 80).

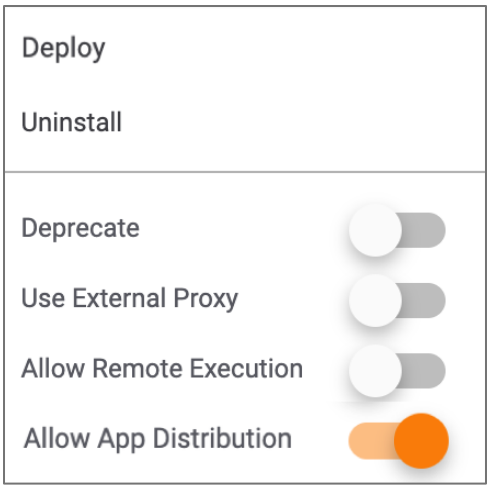

Figure 80

4. Toggle the **Allow App Distribution** slider to orange (on).

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 be displayed (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will be displayed (Figure 75).

3. Click the vertical ellipsis  icon at the top right of the screen, and select **System Jobs**. The **System Jobs** screen will be displayed (Figure 81).

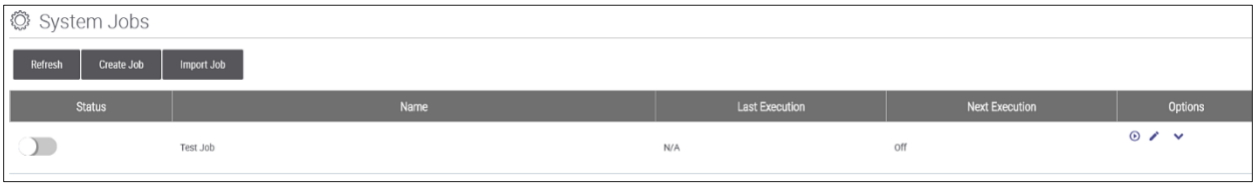

Figure 81

4. Click the **Create Job** button. The **Configure Job** window will be displayed (Figure 82).

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

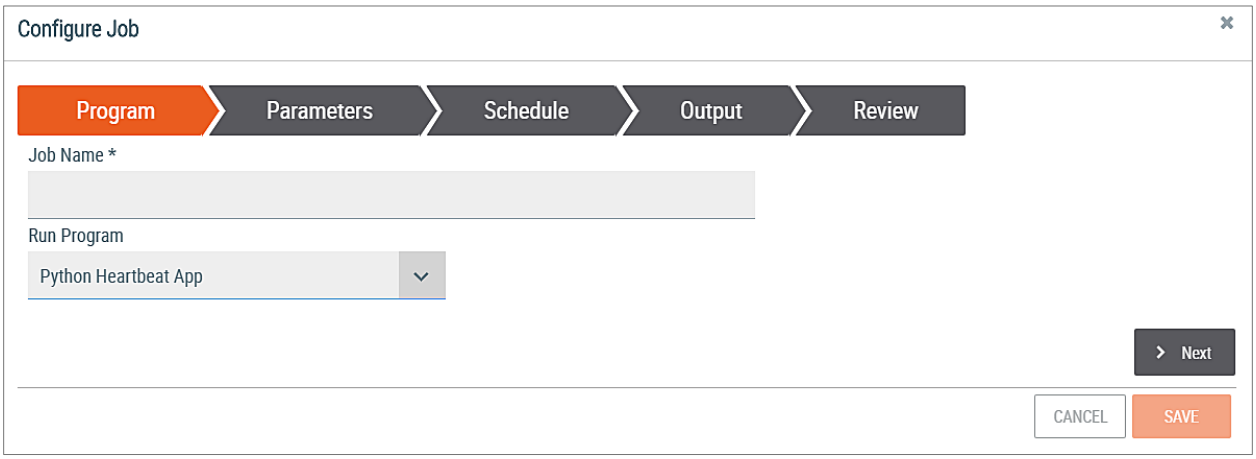

Figure 82

5. Configure the following settings for the job:
   - **Job Name**: Enter a name for the job.
   - **Run Program**: Use the dropdown menu to select a program (app).
6. Click the **Next** button. The **Parameters** screen will be displayed (Figure 83). Configure the parameters for the program.

   NOTE: Each program has different parameters.

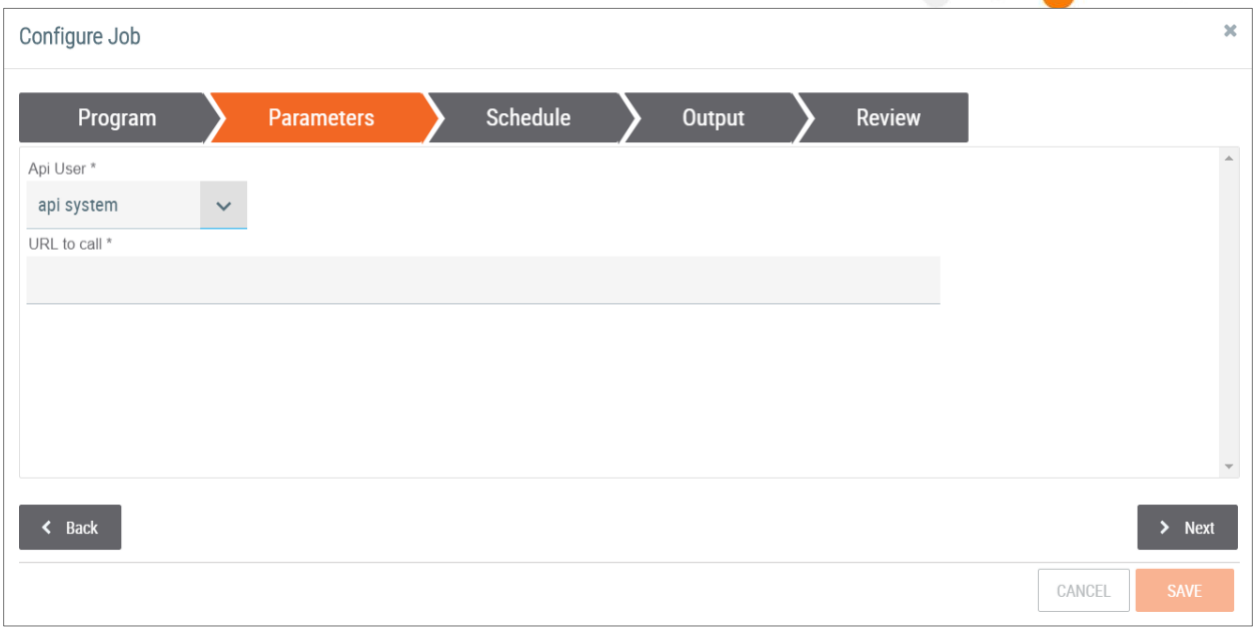

Figure 83

7. Click the **Next** button. The **Schedule** screen will be displayed (Figure 84).

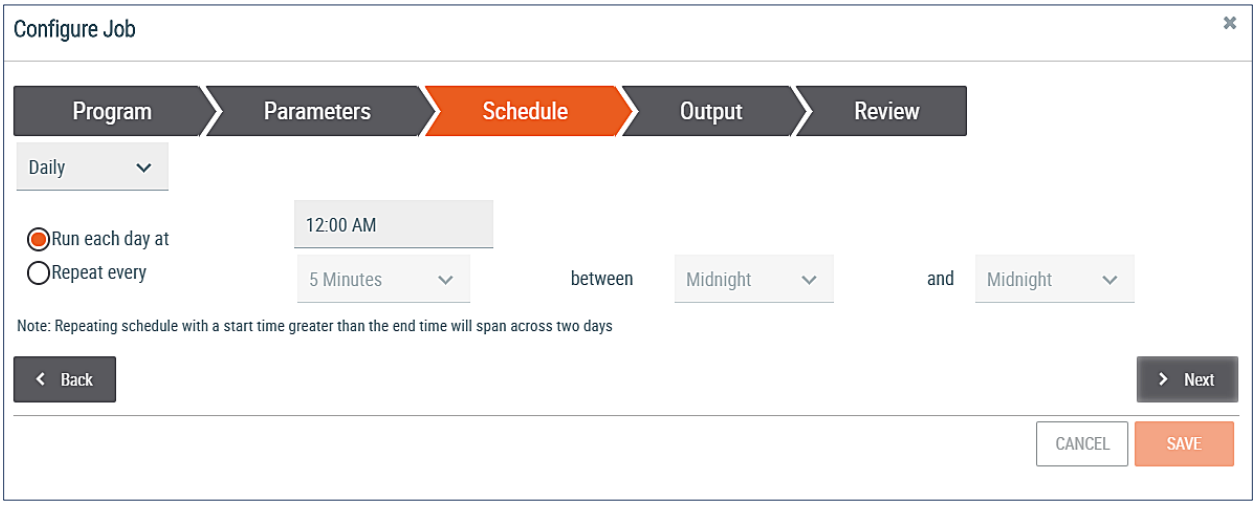

Figure 84

8. Configure the following schedule settings for the job:
   - **Daily**: Use the dropdown menu to select whether the job should run daily, weekly, or monthly.
   - **Run each day at / Repeat every**: Enter the time of day on which to run the job, or enter a time interval during which to repeat the job.
9. Click the **Next** button. The **Output** screen will be displayed (Figure 85).

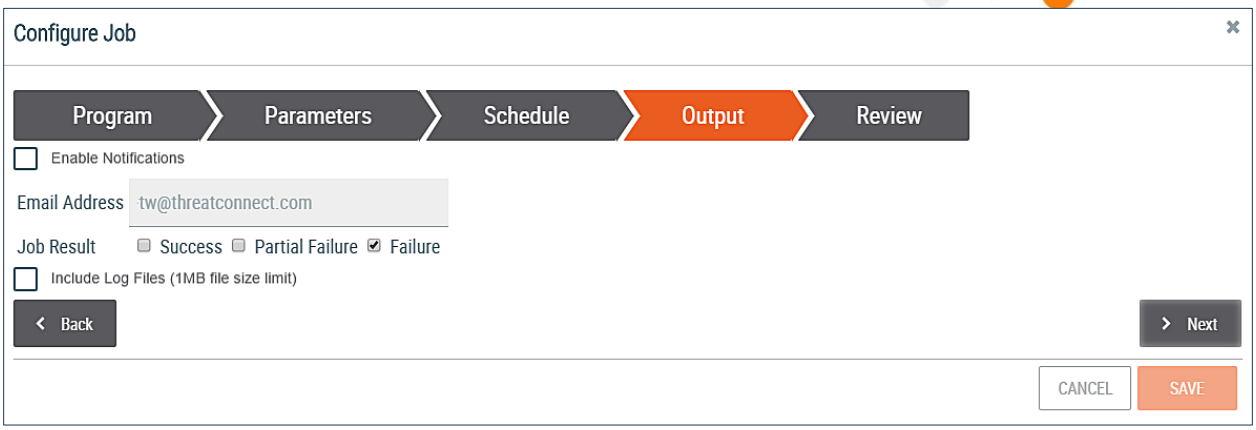

Figure 85

10. Configure the following output settings for the job:
    - **Enable Notifications**: Select the checkbox to enable notifications.
    - **Email Address**: Enter the email address where notifications should be sent.
    - **Job Result**: Select the job results checkbox(es) for which notifications should be sent.
    - **Include Log Files**: Check the box to include log files of 1MB or less in the notification email.
11. Click the **Next** button. The **Review** screen will be displayed (Figure 86).

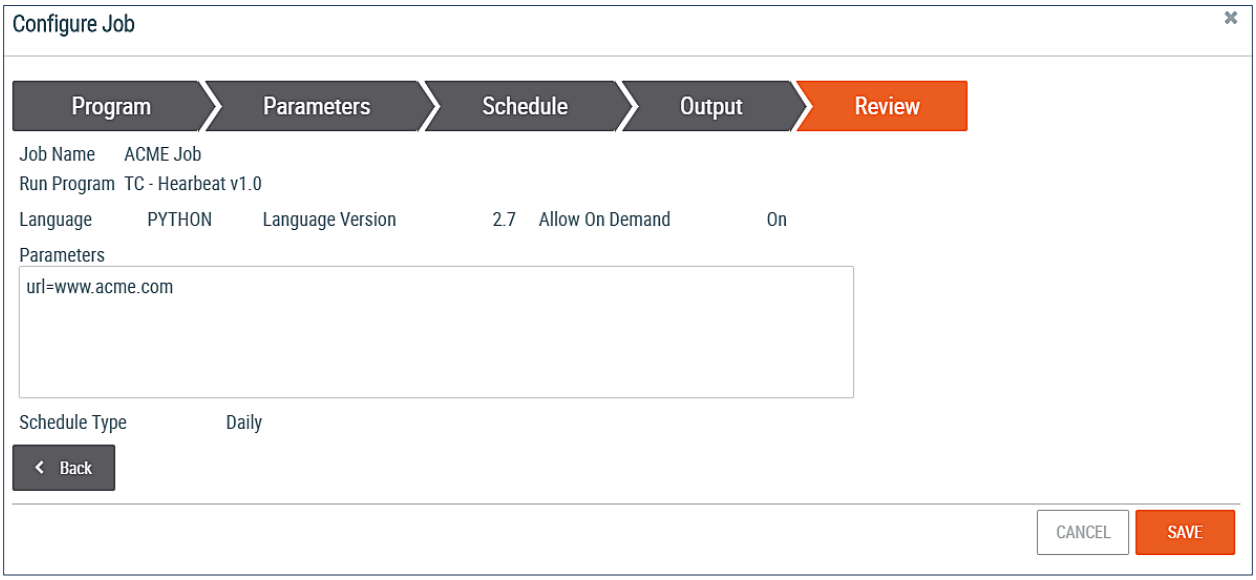

Figure 86

12. Review the **Job Name**, **Run Program**, **Language**, **Language Version**, **Allow On Demand**, **Parameters**, and **Schedule Type** values to ensure they are correct.
13. 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 be displayed (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will be displayed (Figure 75).
3. Click the vertical ellipsis  icon at the top right of the screen, and select **System Jobs**. The **System Jobs** screen will be displayed (Figure 81).
4. The following functions can be performed for an existing job in the **System Jobs** table:
   - Click 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 the **Modify**  icon to edit a job's setting.
   - Click the **Details**  icon to view the **Details** menu with the following options:
     - **Delete**: Select this option to delete the job.
     - **View Details**: Select this option to view the details for the job, including the following parameters: **Program Name**, **Peak Memory** Usage, **Peak CPU** Usage, **Exit Message**, **Session Id**, **Server** Information, **Queued** Date, **Started** Date, **Completed** Date, and **Failed** Date.
     - **View Logs**: Select this option to view logs for the job. Logs can be filtered by **Session ID**, **Level**, and **Message**.
     - **Add Attributes**: Select this option to add attributes to the job.
     - **Published Files**: Select this option to display a list of links to files published by the job.
     - **Export** Job: Select this option to export the job in a JSON file format.

DASHBOARDS

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

To create a System-level dashboard, log in as a System Administrator. Otherwise, a User can create a User-level dashboard, and an Organization Administrator can create an Organization-level dashboard. Dashboard creation and editing, as well as other functions and properties of dashboards, are not discussed in this guide. To learn more about these topics, see 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 Cloud instances to communicate with that server and run operations and applications within the firewall.

Configuring the ThreatConnect Instance

Follow these steps to configure the ThreatConnect instance for multi-environment orchestration:

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 be displayed (Figure 64). Select **System Settings**, and the **System Settings** screen will be displayed (Figure 65).
3. Click the **Apps** tab on the left side of the screen. Configure the following settings:
   - **appMessageBrokerHost**: Enter the domain name for 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.
   - **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.

Enabling Playbooks Apps to Run in a Remote Environment

Follow these steps to enable a Playbooks App to run 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 be displayed (Figure 64). Select **TC Exchange Settings**, and the **TC Exchange Settings** screen will be displayed (Figure 87**Error! Reference source not found.**). The **Installed** tab will be highlighted, displaying all installed Apps.

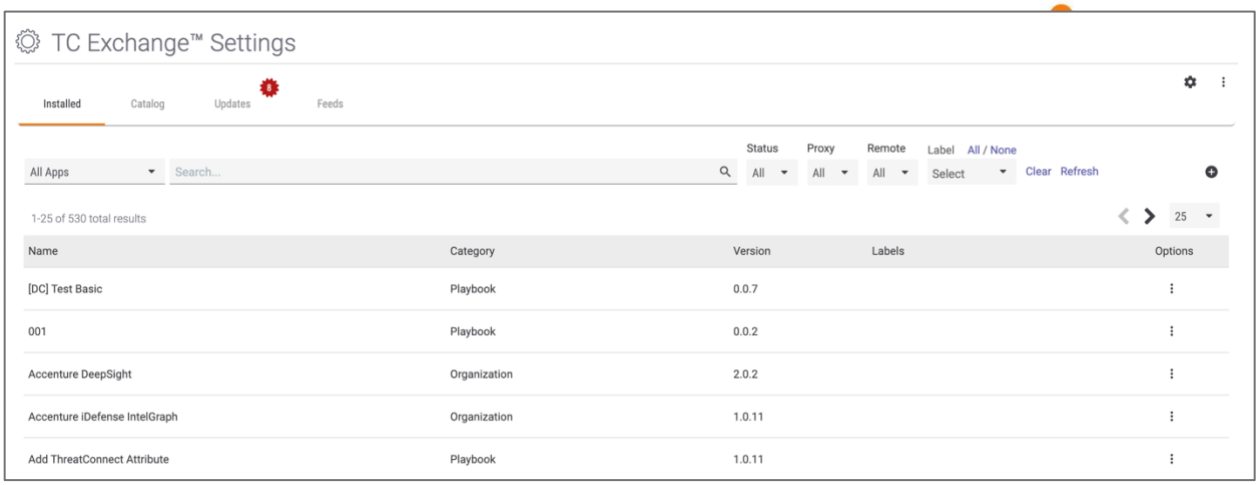

Figure 87

3. Search for and select an App, and click the vertical ellipsis icon in the **Options** column to view the **Options** menu (Figure 88).

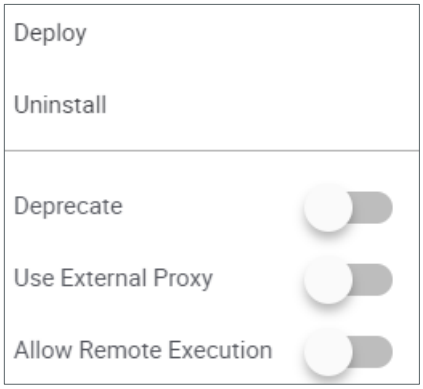

Figure 88

NOTE: This figure is an example of the Options ***menu for a specific App. The options in this menu may vary for different Apps.***

4. Toggle the **Allow Remote Execution** slider to orange (on) to enable remote execution for the App.

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

Workflow and Case Management

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

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

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;
- minimizing 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**: A Workflow Case is a single instance of an investigation, inquiry, or other procedure. It contains all required elements of a notable event in a logical structure. Cases can be used to build an Incident or capture key evidence to enable the security team to decide if the Case should be escalated.
- **Workflow Template**: Workflow typically starts with the creation of a Workflow Template, which is a codified procedure for the steps to be taken within a Case. For example, a security team might create separate Workflow Templates for phishing analysis, alert triage, and various methods of handling breaches. By codifying these processes in a Workflow Template, users can reduce the risk of missing critical steps or artifacts during an investigation, because processes and procedures that were previously stored externally are now captured and can be tied back to threat intelligence in ThreatConnect.
- **Task**: A Workflow Task is a step to perform within a Workflow Case. Tasks can be manual (i.e., performed by a user) or automated (i.e., performed by Workflow Playbook).
- **Artifact**: An Artifact in Workflow is any piece of data not captured in a Note that provides information relevant to a Case that may be useful to an analyst. If an Artifact maps to a ThreatConnect Indicator type, additional information on the Indicator will be provided, and the Indicator may be added to the user's Organization if desired. The potential Artifact types

include all ThreatConnect Indicator types, as well as a variety of other data types, which are determined by ThreatConnect and the System Administrator of the ThreatConnect instance. Examples of Artifacts include domains, email addresses, log files, emails, PCAP files, screen shots, SIEM event files, and malware documents. Not all Artifacts are significant while others can be loosely correlated to threat intelligence.

- **Note**: A Note in Workflow is freeform information entered by a user (e.g., in a Case or attached to a Task or Artifact). Notes can be used to provide commentary, directives to another user, additional details, or any information that cannot be captured elsewhere. They enable security teams to journal key data findings in an unstructured format.
- **Timeline:** The timeline in a Case is a recording of actions performed in the Case in chronological order. Timelines enable security teams 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 enable Workflow in an Organization:

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 be displayed (Figure 64).
3. Select **Account Settings**, and the **Account Settings** screen will be displayed (Figure 65).
4. Click the **Edit** icon in the **Options** column of the Organization in which Workflow is to be enabled. The **Organization Information** window will be displayed (Figure 89).

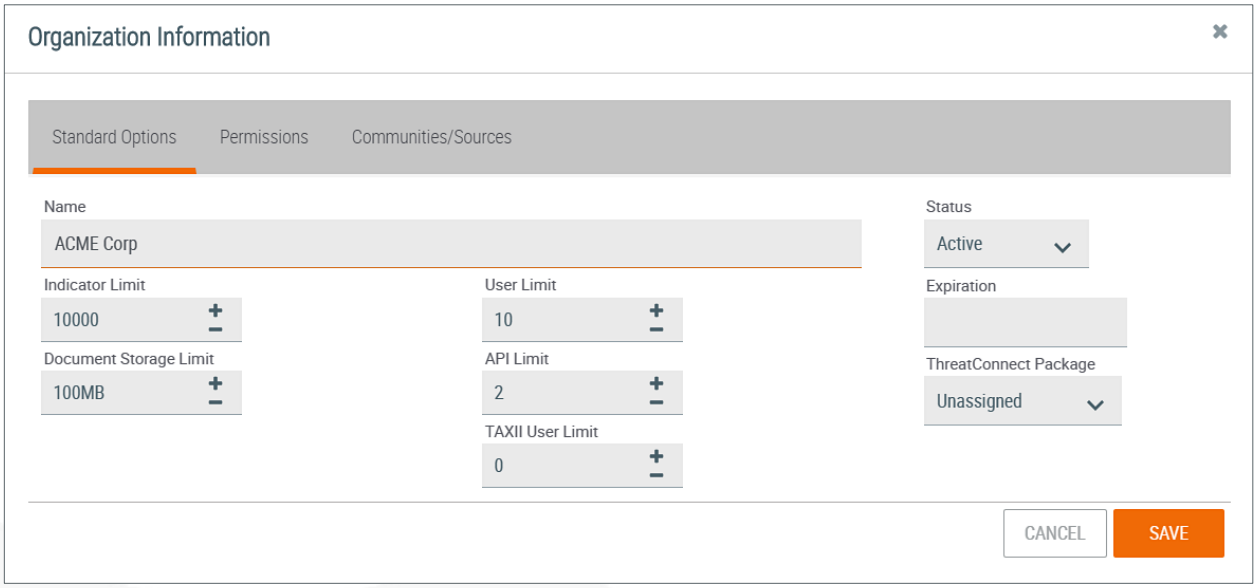

Figure 89

5. Click the **Permissions** tab. The **Permissions** screen will be displayed (Figure 90).

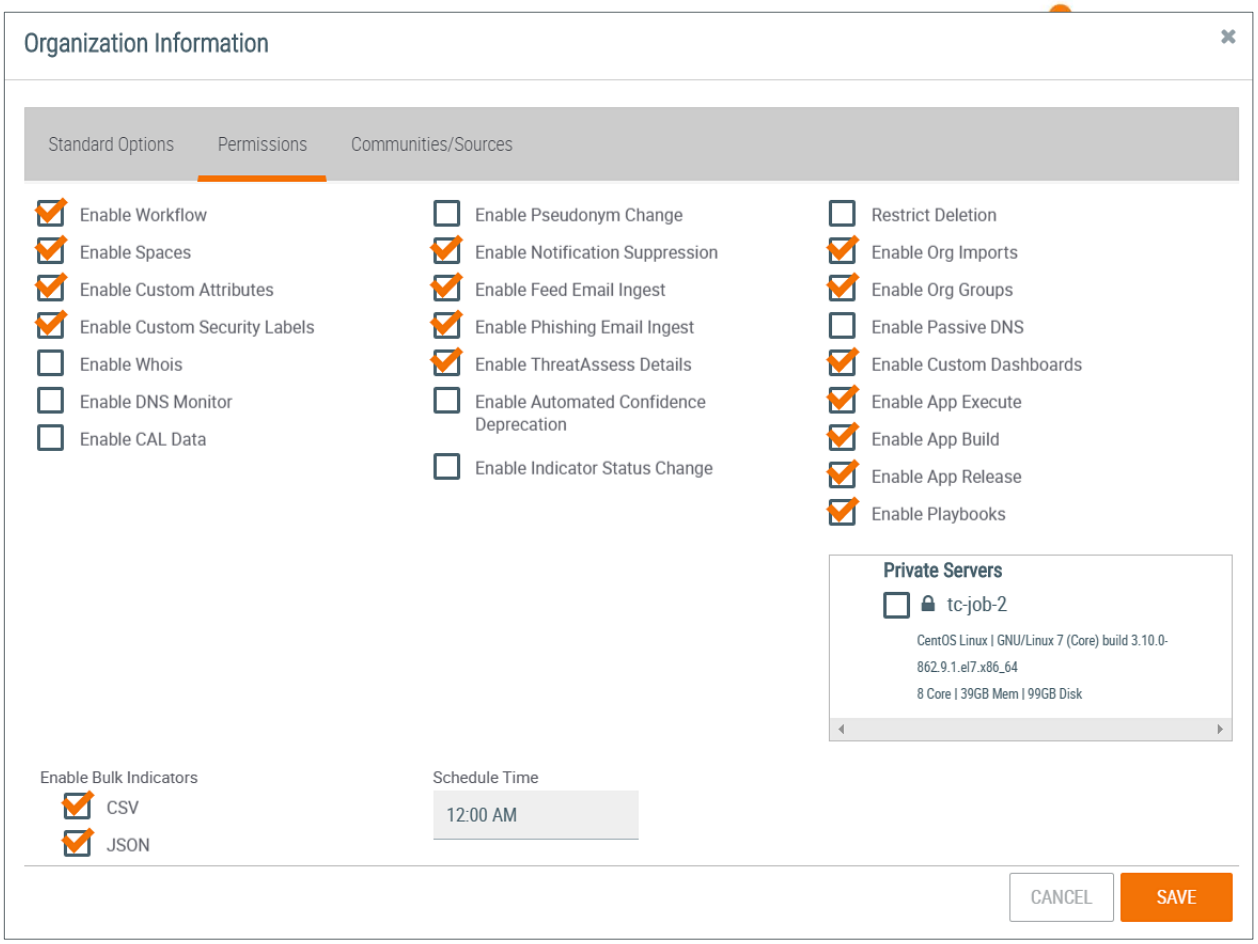

Figure 90

6. Select the **Enable Workflow** checkbox at the top right, and then click the **SAVE** button.

Playbooks System Features

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

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. See *Playbook Activity* for more information.

The Playbooks Queue

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

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

Follow these steps to view and manage the Playbooks 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 be displayed (Figure 91).

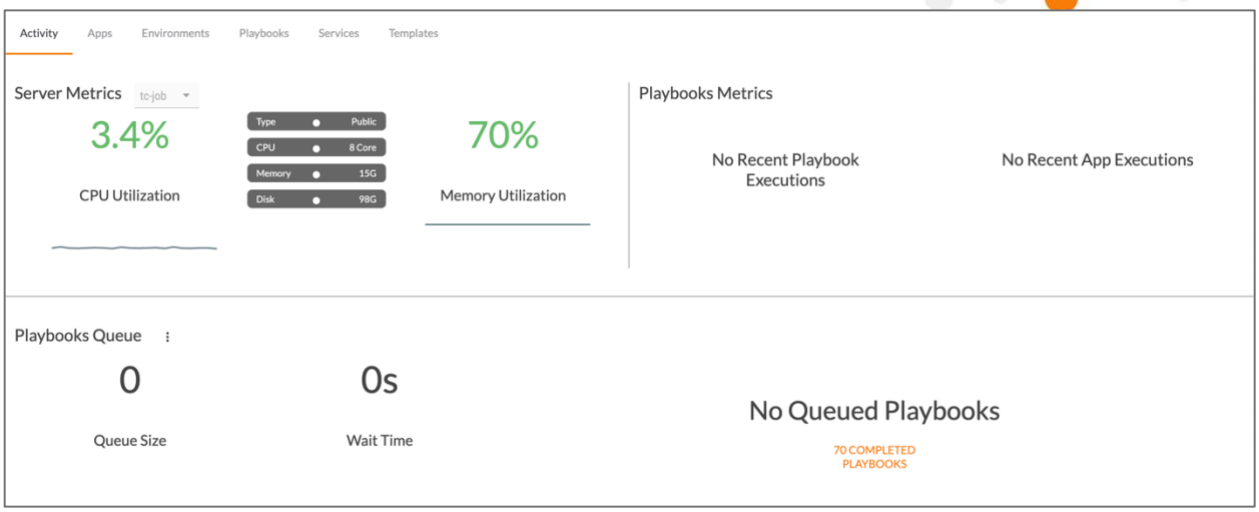

Figure 91

3. Click the vertical ellipsis icon next to **Playbooks Queue**. 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.

Follow these steps to change the count for a Worker:

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 be displayed (Figure 91).
3. Click the vertical ellipsis icon next to **Workers**, and then select **Change Worker Count**. The **Change Worker Count** window will be displayed (Figure 92).

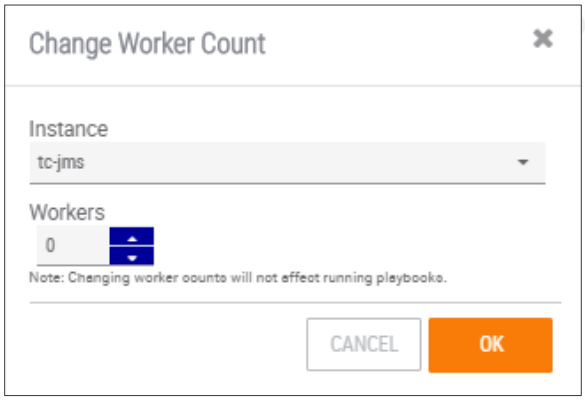

Figure 92

- **Instance**: Select the instance for which to change the Worker count.
- **Workers**: Enter the new Worker count, or use the up and down arrows to change the Worker count by increments of 1.

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

4. The new Worker count will be displayed 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. See *Playbook Environments* for more information.

Creating an Environment

Follow these steps 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 be displayed (Figure 93).

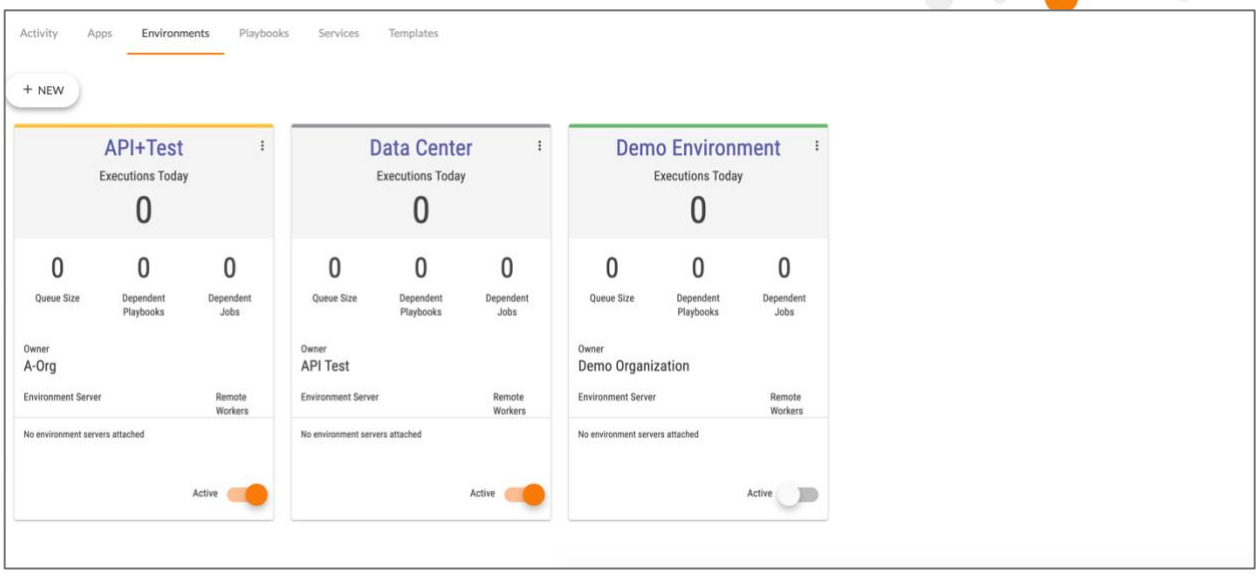

Figure 93

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

3. To create a new Environment, click the **+ NEW** button. The **New Environment** screen will be displayed (Figure 94).

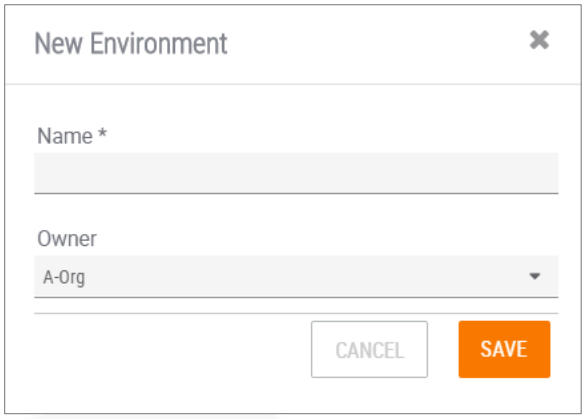

Figure 94

- **Name:** Enter a name for the Environment.
- **Owner:** Use the dropdown menu to select the Organization that will own the Environment.

4. Click the **SAVE** button.

Playbook Services

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