Anomali STAXX

Installation and Administration Guide

Version: 3.4

March 14, 2018

ANOMALI®

Copyright Notice

Support

Support Email	support@anomali.com
Phone	+1 844-4-THREATS
Twitter	@anomali

Documentation Updates

Date	Product Version	Description
8/26/2022	3.4	Additional update for v3.4
3/14/2018	3.4	Updated for v3.4
1/24/2018	3.3	Updated for v3.3
11/17/2017	3.2	Updated for v3.2
10/12/2017	3.1	Updated for v3.1
9/14/2017	3.0	Updated for v3.0
8/10/2017	2.6	Updated for v2.6.
7/19/207	2.5	Updated for v2.5.
6/13/2017	2.4	Updated for v2.4.
5/17/2017	2.3	Updated for v2.3.

CONTENTS

About This Release

What's New in 3.4

Update Now: Update Now feature is added to the Settings interface, enabling users to bypass automatic scheduled updates and instantly check for/install applicable software updates.

See "Updating (Upgrading) Anomali STAXX" on page 16 for more information.

Note: The Anomali Limo service has reached end of life and is no longer supported. Change effective on August 14, 2022.

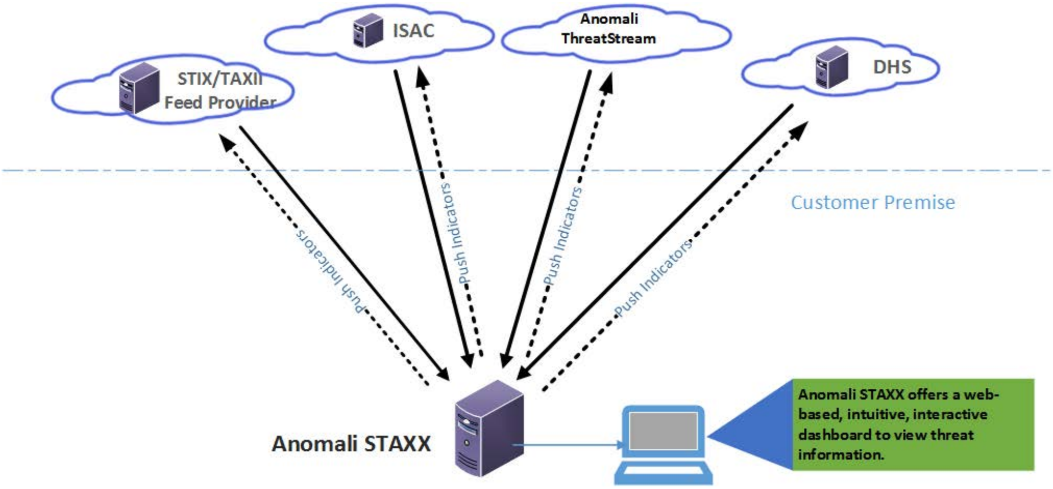
Known Issues

Issue	Description
IN-187	When an observable is pushed from Anomali STAXX to another STIX/TAXII server, the original namespace associated with the observable is not retained and changed to http://threatstream.com.
IN-108	Duplicate observables may be present in the exported file.
IN-103	On systems upgraded from Anomali STAXX 1.3 or earlier, the Severity graph on the Activity dashboard may not display any observables polled from Soltra servers.

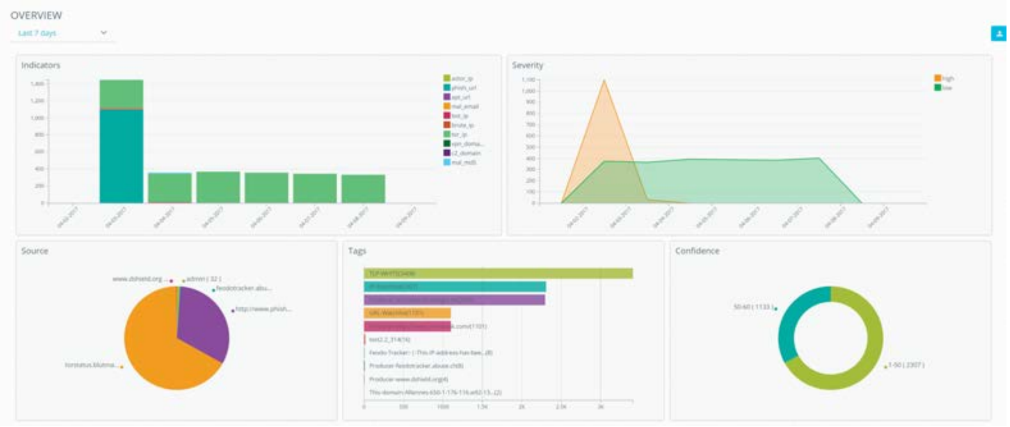
Chapter 1: Introduction

Anomali STAXX provides bi-directional sharing of threat intelligence from STIX/TAXII sources that are in the cloud (such as http://hailataxii.com, an ISAC, or Anomali ThreatStream) or on-premise. With Anomali STAXX, you can connect to STIX/TAXII servers, discover and configure their threat feeds, and poll (download) threat intelligence from those feeds. You can also import threat intelligence into Anomali STAXX and push (upload) selected observables to other STIX/TAXII servers.

The following illustration shows how Anomali STAXX integrates a STIX/TAXII server, in the cloud or on-premise. An Anomali STAXX instance can receive threat information from multiple sources.



Anomali STAXX includes an easy-to-use interface to view threat information received through STIX/TAXII feeds in interactive dashboards, as shown in the following figure. You can run a keyword search to look for a specific observable, search for an observable type over a time range of your choice, and drill-down to any of the Anomali platforms—Anomali STAXX, Anomali Reports, Anomali ThreatStream—to investigate the observable further. You can also import observables, export search results, and push observables to other STIX/TAXII servers from these dashboards.



Chapter 2: Installing and Upgrading Anomali STAXX

This chapter describes how to install Anomali STAXX. The following topics are discussed here:

About Installing Anomali STAXX

Anomali STAXX is packaged as an OVA file and can be installed on a system that meets the minimum specifications listed in "System Requirements" below.

Installation of Anomali STAXX is quick and easy. You download the Anomali STAXX OVA file, deploy it, and configure a few settings from a web interface. You are then ready to use Anomali STAXX!

Optionally, Anomali STAXX can be configured to access the Internet through a proxy.

Anomali STAXX supports multiple authentication methods for communicating with the remote STIX/TAXII sites, including two-way SSL authentication.

System Requirements

You can install Anomali STAXX onto one of the following:

- VMware ESXi serve v6.0 or greater
- Oracle Virtual Box server v5.1 or greater

The following are the **minimum** specifications for the Anomali STAXX virtual machine:

- CPUs: 2
- Memory: 4 GB

- Minimum disk space: 40 GB

Supported Browsers

The following browsers are supported for accessing the Anomali STAXX user interface:

- Chrome 56.0 and later
- Internet Explorer 11
- Firefox ESR 45 and later
- Safari 10.x

Prerequisites

- You must have internet connectivity.

  > **Note:** If you do not have internet connectivity, make sure the time on the VM reflects the time on the host system and run the following commands to stop and disable the NTPD service: `sudo systemctl stop ntpd` **and** `sudo systemctl disable ntpd`

- If your STIX/TAXII server requires two-way authentication, make sure you obtain the SSL certificate from your server. You will need to upload it when configuring the product.
- If you are deploying Anomali STAXX on Oracle Virtual Box on a Windows-based system, make sure that
  - The **Hyper-V platform is disabled** in your Windows Feature list. If Hyper-V is not disabled, you will not see the setting to enable 64-bit Guest OS version, which is required for successfully installing Anomali STAXX.
  - Intel Virtualization Technology and VT-d are both enabled in the BIOS of the host system.

    > *Reason for disabling Hyper-V:* By default, Oracle Virtual Box on Windows-based systems does not display the option to choose 64-bit Guest OS version until Hyper-V is disabled on it. Anomali STAXX is based on a 64-bit OS and must be installed on a system that is 64-bit.

Installing Anomali STAXX

The installation process involves deploying the Anomali STAXX OVA file (.ova file) and configuring a few settings.

Follow these steps:

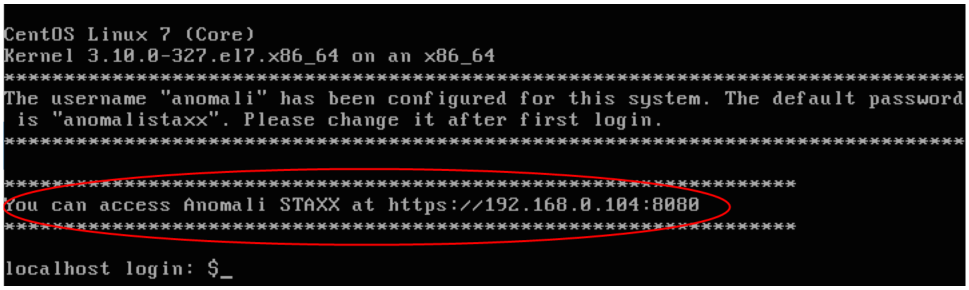
1. Make sure all prerequisities have been met before you begin. See "Prerequisites" on the previous page.

2. Import the .ova file to the system on which you want to install Anomali STAXX.

   This step creates a new VM and installs Anomali STAXX.

3. Power on your VM.

   You will see the following message on your screen, indicating that all services are up. The message also displays the URL you will need to access the web interface of Anomali STAXX. **Make a note of this URL.**

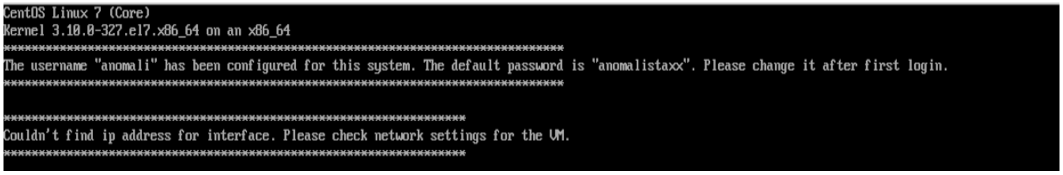
   

   ```
   CentOS Linux 7 (Core)
   Kernel 3.10.0-327.el7.x86_64 on an x86_64
   *********************************************************************************
   The username "anomali" has been configured for this system. The default password
    is "anomalistaxx". Please change it after first login.
   *********************************************************************************

   *******************************************************************
   You can access Anomali STAXX at https://192.168.0.104:8080
   *******************************************************************

   localhost login: $_
   ```

   If you see the following message, indicating that a valid IP was not detected for your VM, check your VM network settings and select an appropriate network.

   ```
   CentOS Linux 7 (Core)
   Kernel 3.10.0-327.el7.x86_64 on an x86_64
   *********************************************************************************
   The username "anomali" has been configured for this system. The default password is "anomalistaxx". Please change it after first login.
   *********************************************************************************

   ******************************************************************
   Couldn't find ip address for interface. Please check network settings for the VM.
   ******************************************************************
   ```

4. Log in to the console using the following default credentials:

   User name: anomali

   Password: anomalistaxx

   Upon logging in, the default password can no longer be used and you must set your own. Before setting a new password, take a snapshot of your VM that can be used to restore Anomali STAXX if your password is lost.

   After taking a snapshot of your VM, reset your password by doing the following:

a. When prompted to enter the **(current) UNIX password**, enter the default password.

b. Enter your new password.

c. Re-enter your new password.

If you forget this password and are locked out of the "anomali" user account, see "Recovering the "anomali" User CLI Password" on page 63.

Note:

- STAXX services are installed as startup services so all services are up and running when the system is installed. If you need to stop or start services later, refer to the " Anomali STAXX Commands" on page 62.
- By default, the deployed VM uses Bridge-type network adapter. Anomali recommends using this adapter to ensure reliable access to the Anomali STAXX interface.
- SSH daemon (`sshd`) is disabled by default. However, if you would like to remotely access Anomali STAXX through SSH, do the following:

  i. Log in to the console using the following default credentials:

  User name: anomali

  Password: *[password set in the previous step]*

  ii. Run the following commands:

  ```
  sudo systemctl enable sshd
  ```

  ```
  sudo systemctl start sshd
  ```

5. By default, Anomali STAXX is configured for Pacific timezone. If you are installing Anomali STAXX in a different timezone, follow these steps to change the default value:

   a. SSH to the Anomali STAXX console and log in using the following default credentials:

   User name: anomali

   Password: *[password set in the previous step]*

   b. Enter the following command:

   ```
   sudo timedatectl set-timezone <timezone>
   ```

   where <timezone> is your local timezone. For example, Europe/Paris or America/New_York.

> **TIP:** To obtain a list of timezones, run this command: `timedatectl list-timezones`

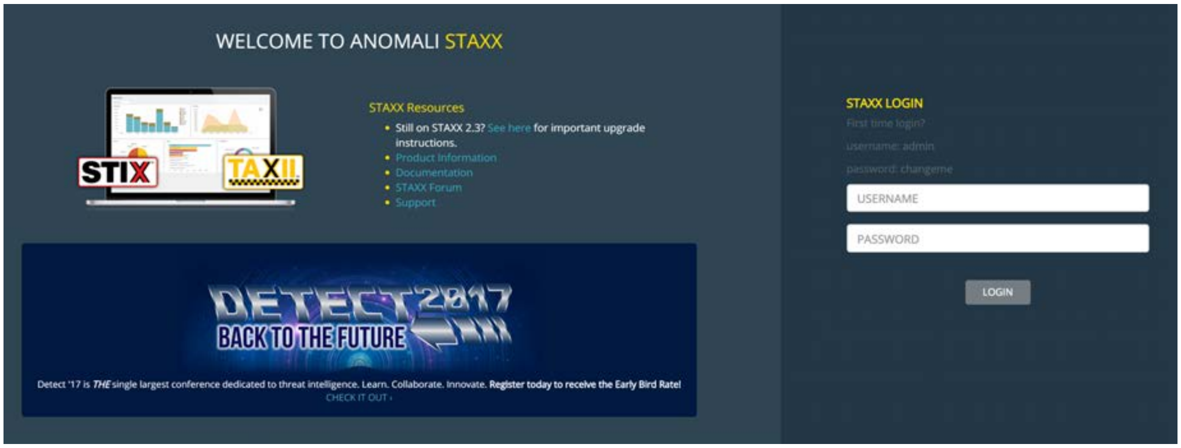
c. To confirm that Anomali STAXX has been set to your local timezone, enter this command:

```
date
```

The screen output should show the local date and time. For example:

```
Thu Feb 9 22:45:56 CET 2017
```

6. Connect to the URL you noted in the previous step and configure Anomali STAXX, as described in "Installing Anomali STAXX" on page 9.



WELCOME TO ANOMALI STAXX

STAXX Resources

- Still on STAXX 2.3? See here for important upgrade instructions.
- Product Information
- Documentation
- STAXX Forum
- Support

Detect '17 is *THE* single largest conference dedicated to threat intelligence. Learn. Collaborate. Innovate. **Register today to receive the Early Bird Rate!**
CHECK IT OUT ›

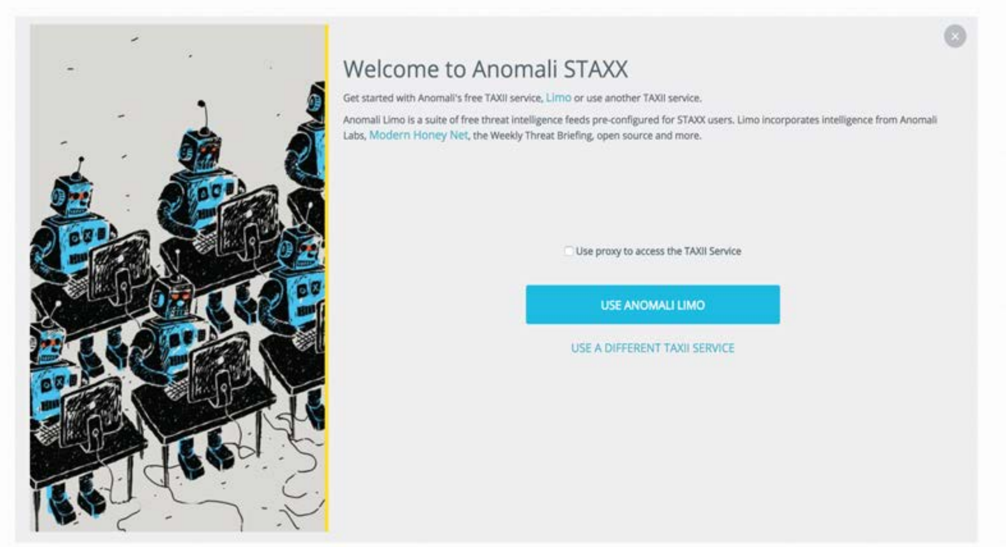
STAXX LOGIN
First time login?
username: admin
password: changeme

> **Note:** To login to Anomali STAXX the first time, use the following default admin credentials:
>
> **User name:** admin
>
> **Password:** changeme
>
> You are then prompted to change your password.

First-Time Setup of Anomali STAXX

The first time you connect to a newly installed Anomali STAXX, a simple and intuitive configuration wizard steps you through the initial setup.

The setup wizard enables you to add an initial TAXII service so you can start receiving STIX/TAXII data on Anomali STAXX.



Welcome to Anomali STAXX

Get started with Anomali's free TAXII service, Limo or use another TAXII service.

Anomali Limo is a suite of free threat intelligence feeds pre-configured for STAXX users. Limo incorporates intelligence from Anomali Labs, Modern Honey Net, the Weekly Threat Briefing, open source and more.

☐ Use proxy to access the TAXII Service

Notes:

- The Anomali Limo service reached end of life August 14, 2022. The **Use Anomali Limo** button cannot be used anymore.
- TAXII services can be added after setup. See Configuring Anomali STAXX After First-Time Setup for more information.
- If terminated upon initial setup, the configuration wizard will be displayed the next two times you log in to Anomali STAXX.

Getting Started on Anomali STAXX with a TAXII Service of Your Choice

When you select an initial TAXII service, the wizard steps you through the manual feed configuration process.

To add a TAXII service of your choice:

1. (Optional) If you want to use a proxy server to connect to a TAXII service, select **Use proxy to access the TAXII Service**.
2. Click **Use A Different TAXII Service**.
3. If you selected **Use proxy to access the TAXII Service**, enter your proxy configuration settings. See "Setting up a Proxy Server During First-Time Setup of Anomali STAXX" on page 14 for a list of fields and definitions.

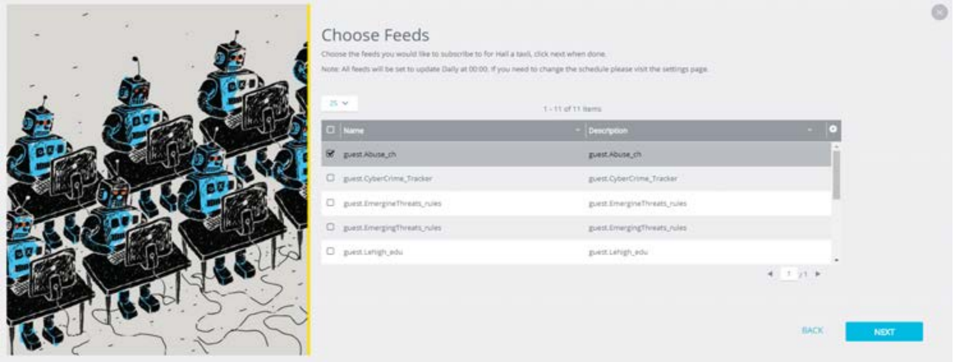
   Note: If a connection to the TAXII service cannot be established, you will be directed to setup a proxy.

4. Enter the following information:

Setting	Description
Name	A meaningful name for the site.
Discovery URL	URL for the STIX/TAXII server.
Use Basic Authentication	Select this option if you want to provide username and password information for the STIX/TAXII server. Then, enter the following information: ▪ Username ▪ Password **Note:** You can configure both authentication methods—Basic and SSL—at the same time.
Use SSL Two-Way Certificate	Select this option to upload an SSL certificate, **in .p12 format**, that Anomali STAXX should use to authenticate with the STIX/TAXII server or FS-ISAC feed. If you checked this option, click **Choose File** to upload the SSL certification file. Then enter the (optional) Key Passphrase to use for the file. **Notes:** ▪ You can configure both authentication methods—Basic and SSL—at the same time. ▪ If the SSL certificate expires, you must delete the site and then re-configure it with the new certificate.

5. Click **Discover** to proceed to feed discovery.

6. Select the feeds that you want to subscribe to on the TAXII service and click **Next**.



Choose Feeds

Choose the feeds you would like to subscribe to for Hail a taxii, click next when done.

Note: All feeds will be set to update Daily at 00:00. If you need to change the schedule please visit the settings page.

25

1 - 11 of 11 items

☐	Name	Description
☑	guest.Abuse_ch	guest.Abuse_ch
☐	guest.CyberCrime_Tracker	guest.CyberCrime_Tracker
☐	guest.EmergineThreats_rules	guest.EmergineThreats_rules
☐	guest.EmergingThreats_rules	guest.EmergingThreats_rules
☐	guest.Lehigh_edu	guest.Lehigh_edu

Anomali STAXX will begin receiving data from the previous 7 days for the feeds to which you subscribed shortly. You can edit this default Poll Time Range within Anomali STAXX settings. See "Configuring Feeds" on page 49 for more information.

7. Click **Let's Try STAXX** to exit the wizard.

Completing Initial Setup of Anomali STAXX

After you exit the wizard, a What's New pop up lists new features in the latest release.

It includes the End User License Agreement (EULA), which you must accept before you can proceed further. You can also (optionally) click the "I agree to send statistics back to Anomali..." check box. By sending statistics about your Anomali STAXX back to Anomali, you are contributing to the performance and feature improvements of Anomali STAXX. If you enable this option, summary information such as the Anomali STAXX version and build number, number of sites configured, number of imports and pushes performed, is sent back to Anomali once per day. No personally identifiable information is transmitted. Click **Agree** to proceed.

You have finished your first time setup of Anomali STAXX!

Automatic updates are enabled by default. See "Updating (Upgrading) Anomali STAXX" on page 16 for more information on automatic updates. You can review and adjust all default settings by visiting **Settings** > **Setup**. See "Setup Settings" on page 55 for more information.

Once you have performed the initial configuration, you are ready to view threat information received from a STIX/TAXII server on the Anomali STAXX UI. See "Viewing STIX/TAXII Observables" on page 17 for more information.

Setting up a Proxy Server During First-Time Setup of Anomali STAXX

Setting up a proxy server is optional. If you selected **Use proxy to access the TAXII Service**, you will be prompted to configure the following settings.

Setting	Description
Proxy Hostname	IP address or hostname of the proxy server. Do not specify the proxy host in the URL format. See Known Issues for more information.

Setting	Description
Proxy Port	Port on which proxy server listens for connections.
Username	User name that Anomali STAXX should use to connect to the proxy server.
Password	Password for the user name you entered.

Updating (Upgrading) Anomali STAXX

Upgrade paths:

Anomali STAXX version	**Actions Required for Upgrade**
v1.1 onwards (except v2.3)	If you have the **Automatic Updates** setting enabled, Anomali STAXX is updated to version 3.4.
v2.3	Contact Anomali Customer Support for assistance performing this upgrade.
v1.0	You must download and install version 3.4 as a fresh installation.

You can update Anomali STAXX in one of two ways:

1. By enabling **Automatic Updates**:

   When Automatic Updates are enabled, Anomali STAXX is automatically updated when new versions become available. To read more about configuring automatic updates, see "Setup Settings" on page 55 for further information.

2. By using the **Upgrade Now** button:

   Anomali STAXX can also be upgraded on an ad-hoc basis using the **Upgrade Now** button. Anomali STAXX updates to the next available version on demand.

   To update Anomali STAXX in this way, navigate to **Settings** and then under the **Automatic Updates** section, select the **Upgrade Now** button. See "Setup Settings" on page 55 for further information. The button is blue when updates are available, but it becomes grayed out when no updates are available.

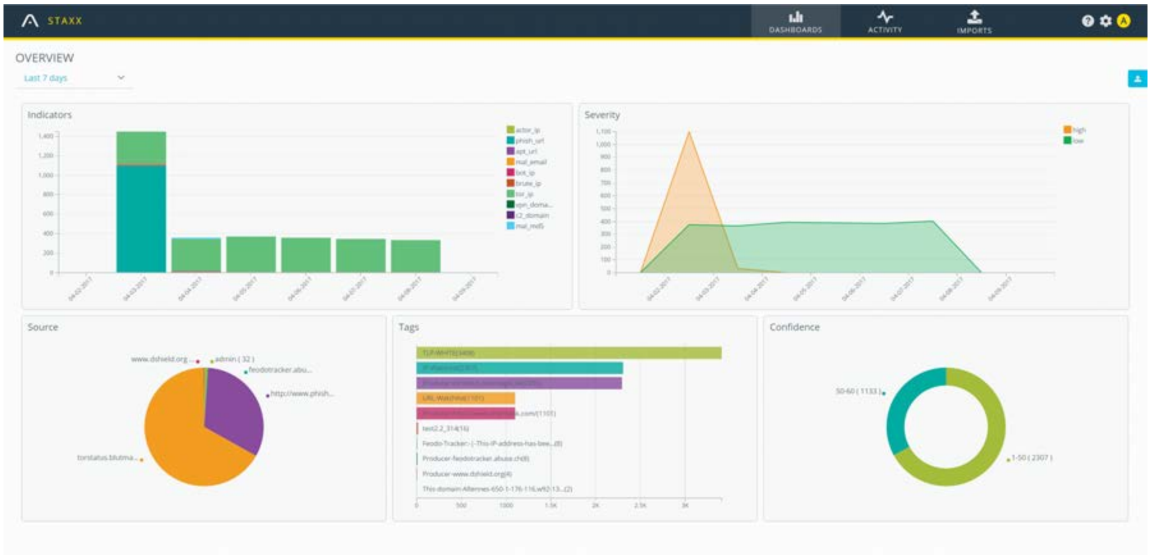
Chapter 3: Viewing STIX/TAXII Observables

This chapter gives an overview of the dashboards available through the web interface of Anomali STAXX. The dashboards allow you to view and interactively search for threat observables received through the threat feeds and investigate an observable on Anomali's platforms for deeper insights.

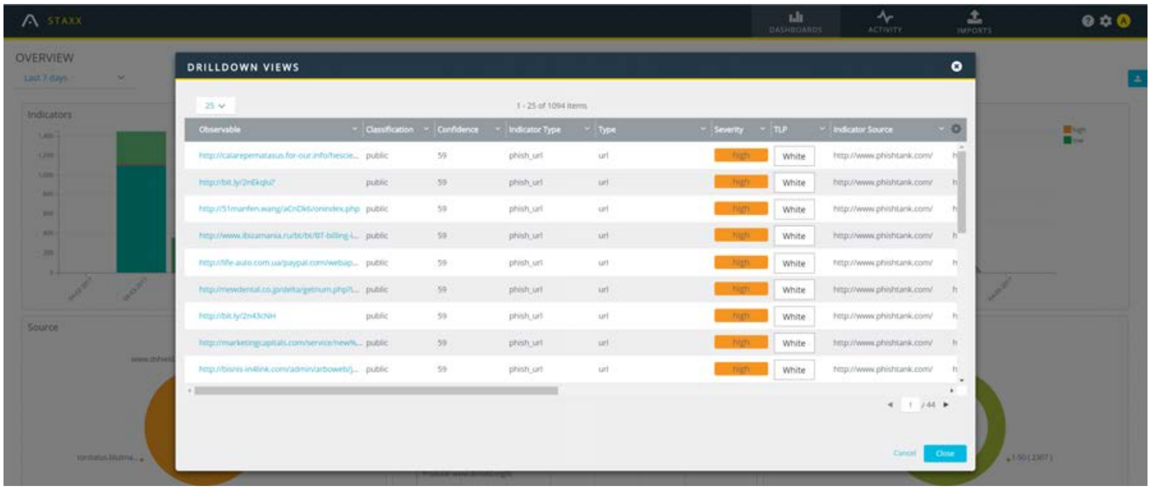
Dashboard

Dashboard provides a summary of all observables stored on Anomali STAXX in the specified time period. Several graphical views within Dashboard show observables by observable type, severity, source (of the observable), confidence, and so on.

You can click on any chart element such as a bar chart or a pie chart section to drill down for more details. The Confidence, Severity, and Tags are values assigned to the observables by the site from which the observable was polled or when the observable was imported into Anomali STAXX. For information about observable type, see "Available Indicator Types" on page 68.



For example, if you want to see all of the observables associated with the IP-Watchlist tag, click on the bar labeled “IP-Watchlist” in the Tags bar chart to open its drilldown view.



DRILLDOWN VIEWS

25

1 - 25 of 1094 items

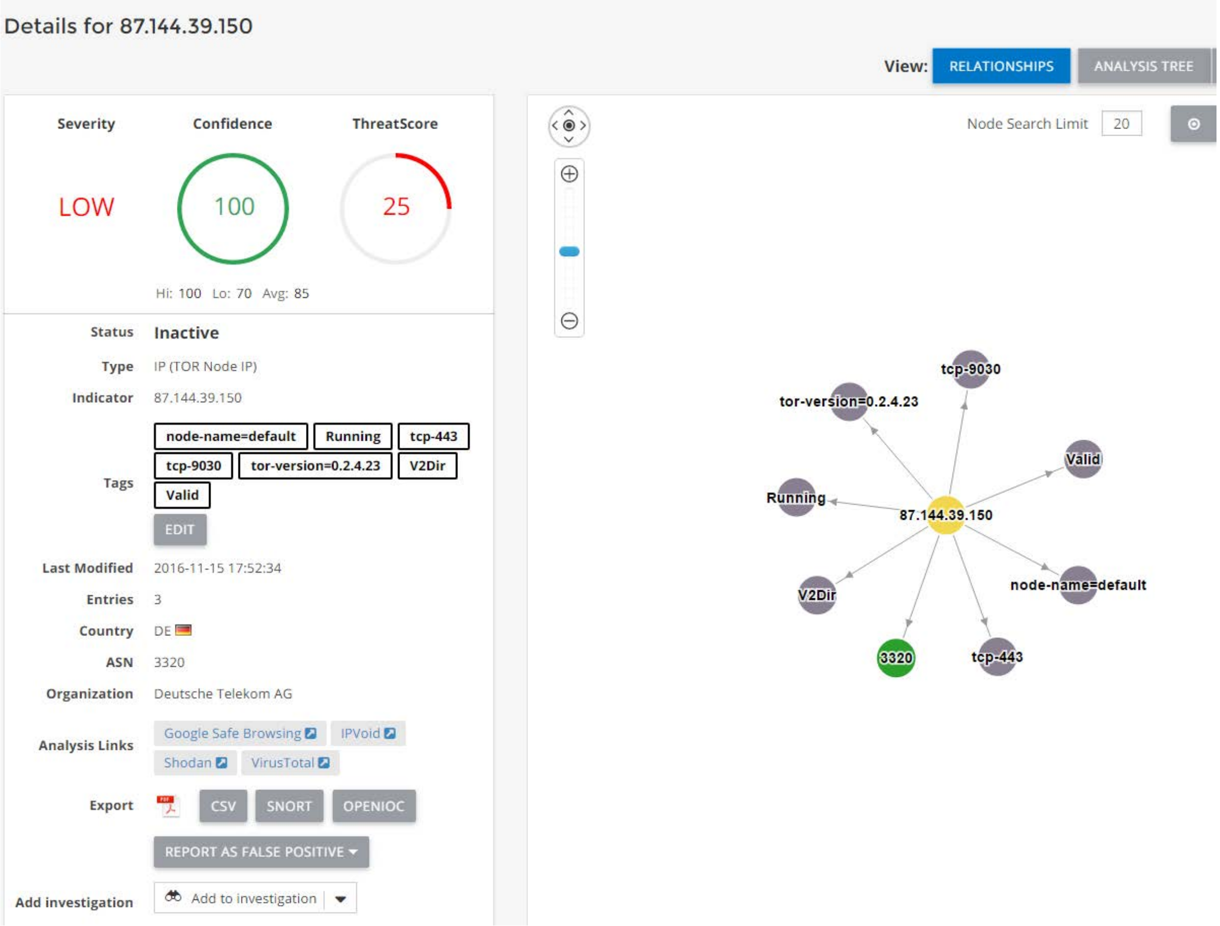
Observable	Classification	Confidence	Indicator Type	Type	Severity	TLP	Indicator Source
http://calarepematasus.for-our.info/hescie...	public	59	phish_url	url	high	White	http://www.phishtank.com/
http://bit.ly/2nEkqlu?	public	59	phish_url	url	high	White	http://www.phishtank.com/
http://51manfen.wang/aCnDk6/onindex.php	public	59	phish_url	url	high	White	http://www.phishtank.com/
http://www.ibizamania.ru/bt/bt/BT-billing-l...	public	59	phish_url	url	high	White	http://www.phishtank.com/
http://life-auto.com.ua/paypal.com/webap...	public	59	phish_url	url	high	White	http://www.phishtank.com/
http://newdental.co.jp/delta/getnum.php?i...	public	59	phish_url	url	high	White	http://www.phishtank.com/
http://bit.ly/2n43cNH	public	59	phish_url	url	high	White	http://www.phishtank.com/
http://marketingcapitals.com/service/new%...	public	59	phish_url	url	high	White	http://www.phishtank.com/
http://bisnis-in4link.com/admin/arboweb/j...	public	59	phish_url	url	high	White	http://www.phishtank.com/

1 / 44

Cancel Close

You can investigate an observable further on any of the Anomali's platforms, which offers an in-depth view of the observable. Click on the link in the Observable column to investigate.

You will need to authenticate with the Anomali platforms to see this information. See "Setup Settings" on page 55 for more information on Anomali platforms you can use.



Details for 87.144.39.150

Severity: LOW

Confidence: 100

ThreatScore: 25

Hi: 100 Lo: 70 Avg: 85

Status: Inactive

Type: IP (TOR Node IP)

Indicator: 87.144.39.150

Tags: node-name=default, Running, tcp-443, tcp-9030, tor-version=0.2.4.23, V2Dir, Valid

EDIT

Last Modified: 2016-11-15 17:52:34

Entries: 3

Country: DE

ASN: 3320

Organization: Deutsche Telekom AG

Analysis Links: Google Safe Browsing, IPVoid, Shodan, VirusTotal

Export: CSV SNORT OPENIOC

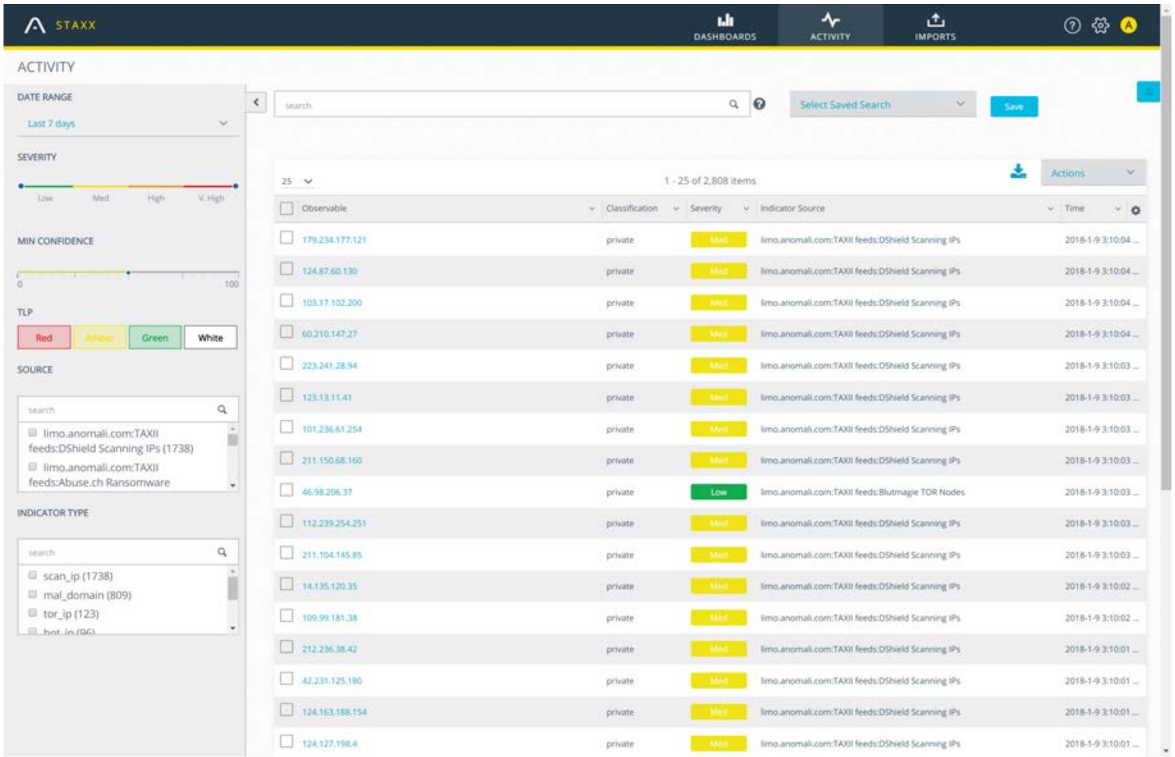
REPORT AS FALSE POSITIVE

Add investigation: Add to investigation

Activity

The Activity menu provides an interactive dashboard to search for observable activity that matches a specified criteria, in a specified time period. You can run a simple keyword search to look for observables. You can also specify multiple keywords. The boolean AND operation is assumed when multiple keywords are specified. Additionally, you can select from several criteria, such as Date Range, Severity, Minimum Confidence, TLP, Source, and observable Type, which are conveniently located on the left side of the dashboard.

The default Activity dashboard displays matches for all observables received in the last 7 days.



DATE RANGE: Last 7 days

SOURCE:
- □ limo.anomali.com:TAXII feeds:DShield Scanning IPs (1738)
- □ limo.anomali.com:TAXII feeds:Abuse.ch Ransomware

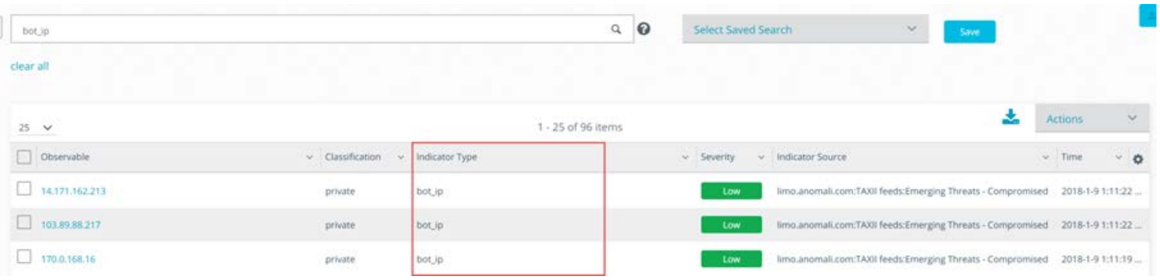
INDICATOR TYPE:
- □ scan_ip (1738)
- □ mal_domain (809)
- □ tor_ip (123)
- □ bot_ip (96)

25 1 - 25 of 2,808 items

□	Observable	Classification	Severity	Indicator Source	Time
□	179.234.177.121	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:04 ...
□	124.87.60.130	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:04 ...
□	103.17.102.200	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:04 ...
□	60.210.147.27	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:04 ...
□	223.241.28.94	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:03 ...
□	123.13.11.41	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:03 ...
□	101.236.61.254	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:03 ...
□	211.150.68.160	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:03 ...
□	46.98.206.37	private	Low	limo.anomali.com:TAXII feeds:Blutmagie TOR Nodes	2018-1-9 3:10:03 ...
□	112.239.254.251	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:03 ...
□	211.104.145.85	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:03 ...
□	14.135.120.35	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:02 ...
□	109.99.181.38	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:02 ...
□	212.236.38.42	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:01 ...
□	42.231.125.180	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:01 ...
□	124.163.188.154	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:01 ...
□	124.127.198.4	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:01 ...

Keyword Search

You can narrow the search results by specifying one or more keywords. Keywords are matched against the values of the following fields: "List of Fields" on page 66. For example, if you want to search for observables of itype=bot_ip, specify *bot_ip* in the Search String box. **There is no need to enter the field name**. This value is matched against the values of all fields in the "List of Fields" on page 66. If a match is found, the observable is returned in the search results, as shown in the following example.



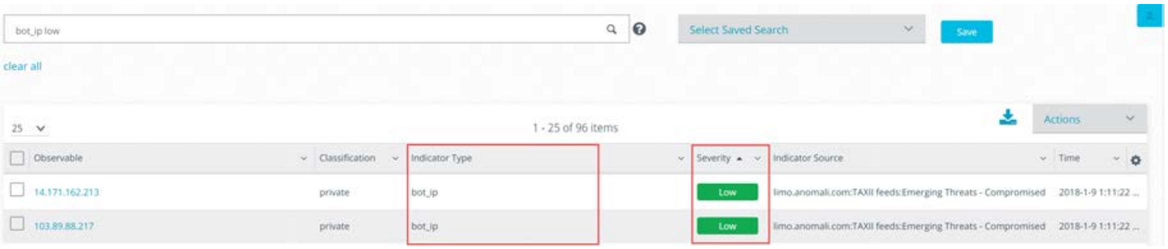
bot_ip

25 1 - 25 of 96 items

□	Observable	Classification	Indicator Type	Severity	Indicator Source	Time
□	14.171.162.213	private	bot_ip	Low	limo.anomali.com:TAXII feeds:Emerging Threats - Compromised	2018-1-9 1:11:22 ...
□	103.89.88.217	private	bot_ip	Low	limo.anomali.com:TAXII feeds:Emerging Threats - Compromised	2018-1-9 1:11:22 ...
□	170.0.168.16	private	bot_ip	Low	limo.anomali.com:TAXII feeds:Emerging Threats - Compromised	2018-1-9 1:11:19 ...

> **Note:** The keyword search looks for matches that begin with the specified keyword. For example, `phishtank` returns matches that **start with phishtank**. Matches such as http://www.phishtank.com are not returned.

If you want to search for all observables of itype=bot_ip and severity=medium, specify *bot_ip medium* in the Search String box. The two values are automatically ANDed and the observables matching *bot_ip* and *medium* are returned in the search results, as shown in the following example. **Note that you do not need to specify the field name.**



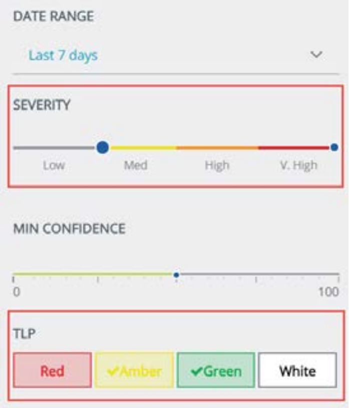
bot_ip low

1 - 25 of 96 items

Observable	Classification	Indicator Type	Severity	Indicator Source	Time
14.171.162.213	private	bot_ip	Low	limo.anomali.com:TAXII feeds:Emerging Threats - Compromised	2018-1-9 1:11:22 ...
103.89.88.217	private	bot_ip	Low	limo.anomali.com:TAXII feeds:Emerging Threats - Compromised	2018-1-9 1:11:22 ...

Interactive Search Filters

Some of the selector fields are multi-select, thus allowing you to search for more than one value for those fields. For example, you can select multiple values for Severity and TLP.



DATE RANGE: Last 7 days

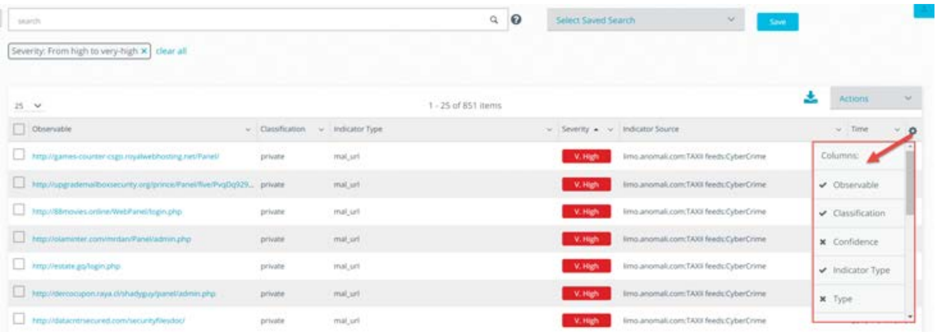
SEVERITY: Low – Med – High – V. High

MIN CONFIDENCE: 0 – 100

TLP: Red ✓Amber ✓Green White

Editing the Search Results View

You can select the fields that are displayed in the search results by clicking the field selector icon as shown in the following figure. Your selections will be maintained the next time you login to Anomali STAXX.



Severity: From high to very-high ✕

1 - 25 of 851 items

Observable	Classification	Indicator Type	Severity	Indicator Source	Time
http://games-counter-csgo.royalwebhosting.net/Panel/	private	mal_url	V. High	limo.anomali.com:TAXII feeds:CyberCrime	
http://upgrademailboxsecurity.org/prince/Panel/five/PvqDq929...	private	mal_url	V. High	limo.anomali.com:TAXII feeds:CyberCrime	
http://88movies.online/WebPanel/login.php	private	mal_url	V. High	limo.anomali.com:TAXII feeds:CyberCrime	
http://olaminter.com/mrdan/Panel/admin.php	private	mal_url	V. High	limo.anomali.com:TAXII feeds:CyberCrime	
http://estate.go/login.php	private	mal_url	V. High	limo.anomali.com:TAXII feeds:CyberCrime	
http://dercocupon.raya.cl/shadyguy/panel/admin.php	private	mal_url	V. High	limo.anomali.com:TAXII feeds:CyberCrime	
http://datacntrsecured.com/securityfilesdoc/	private	mal_url	V. High	limo.anomali.com:TAXII feeds:CyberCrime	

Columns:
- ✓ Observable
- ✓ Classification
- ✕ Confidence
- ✓ Indicator Type
- ✕ Type

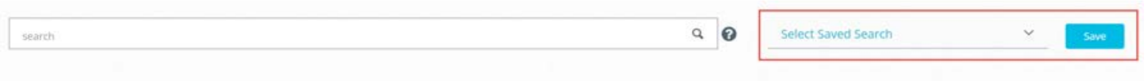
Exporting Search Results

Once you have searched for observables, you can export them or push them to other STIX sites. Select the observables that you want to include in the action and click the icon or Push Observable button to the top right of the Activity dashboard.

For more details about the export and push operations, see "Exporting Observables" on page 40 and "Pushing Observables from the Activity Dashboard" on page 25.

Saving Frequently Used Searches

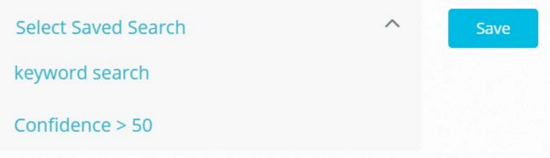
Anomali STAXX enables you to save frequently used search filters. This allows you to quickly run search queries without manually recalling parameters.



To save frequently used searches:

1. Run the search query that you want to save, including any keywords or selectors.
2. Click **Save**.
3. Enter a **Name** for the saved search.
4. (Optional) Enter a **Description** for the saved search.
5. Click **Save**.

Saved searches are enabled by default and accessible from the saved search dropdown menu.



Admin users can disable, re-enable, and delete saved searches within Anomali STAXX Settings. See "Managing Saved Searches" on page 61 for more information.

Deleting Observables

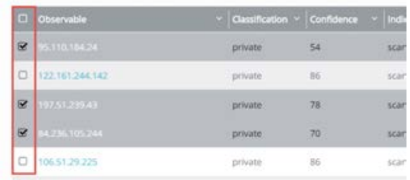
Anomali STAXX enables you to delete observables from the Activity screen. Deleting observables can come in handy when erroneous observables are accidentally imported or you think observables from a TAXII source are false positives.

Note: Observables deleted from the Anomali STAXX user interface cannot be restored. However, observables with identical values to those you have deleted may still be imported. See "Importing Observables" on page 36 for more information.

To delete observables:

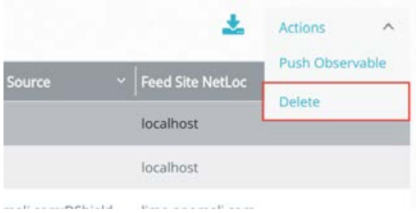
1. Click **Activity** from the top navigation menu.

2. Select the observables you want to delete.



□	Observable	Classification	Confidence	Indi
☑	95.110.184.24	private	54	scar
□	122.161.244.142	private	86	scar
☑	197.51.239.43	private	78	scar
☑	84.236.105.244	private	70	scar
□	106.51.29.225	private	86	scar

3. In the **Actions** menu, click **Delete**.



Source	Feed Site NetLoc
	localhost
	localhost

4. Click **Permanently delete x Observable(s)** to confirm.

Investigating an Observable on Anomali Platforms

Anomali STAXX provides a way to investigate an observable on Anomali's platforms—Anomali STAXX, Anomali Reports, Anomali ThreatStream. You can view details such as the threat scores, tags, and other associated intelligence. You can drill down further on the observable to discover associated observables and perform deeper analysis.

Before you can use Anomali STAXX for investigations, you will need to

- Have an account on the Anomali platform that you want to use. See "Setup Settings" on page 55 for more information.

- Configure the platform in the Anomali STAXX Setup settings, as described in "Setup Settings" on page 55.

To investigate an observable, click on the observable in the Observables column.

Chapter 4: Receiving Observables From a STIX/TAXII Server

Even though you configured a site during the first-time setup of Anomali STAXX to receive observables (see "Installing Anomali STAXX" on page 9), you may need to configure additional sites . Follow the process described in this section to configure additional sites and threat feeds for receiving observables.

The process of receiving observables on Anomali STAXX from a STIX/TAXII server involves the following steps:

1. Adding the site from which the observables will be received
2. Discovering and configuring available feeds on that site

Note: You must be logged in as the Anomali STAXX admin user to configure sites to receive observables.

Adding the Site

See "Adding a Site" on page 46.

Discovering Available Feeds

See "Adding Feeds to Receive Observables" on page 49.

Chapter 5: Pushing (Sharing) Observables to a STIX/TAXII Server

You can push (share) local observables to a STIX/TAXII server through Anomali STAXX. Local observables are the observables you imported to Anomali STAXX using the import feature, as described in "How to Import Observables" on page 36, or observables Anomali STAXX downloaded from another STIX/TAXII server.

Currently, Anomali STAXX can push observables to STIX/TAXII servers running TAXII v1.1 and v2.0, and STIX v1.1.1 and v2.0. Anomali has tested this feature with the following STIX/TAXII servers:

- Soltra Edge versions: 2.4, 2.6, 2.7, 2.8, 2.9, 2.10
- Anomali ThreatStream

The Process of Pushing Observables

Follow this process to push observables to a STIX/TAXII server:

1. Make sure that the STIX/TAXII server you want to push observable to is configured on Anomali STAXX. See "Adding a Site" on page 46 for information on adding STIX/TAXII on Anomali STAXX.
2. Collections are not discoverable on Soltra Edge servers, therefore, Anomali STAXX cannot automatically discover them. Manually add collections on Soltra Edge servers, as described in "Adding Collections Manually" on page 52.
3. If subscription IDs are required for the Collections on a site, make sure they are configured before you push observables to them. See "Specifying or Editing Subscription ID for a Collection" on page 32 for information.
4. Follow one of the following methods to push observables:
   - On ad hoc basis (see "Pushing Observables on an Ad hoc Basis" on the next page)
   - By configuring the push operation to occur on a schedule (see "Configuring a Scheduled Push on Anomali STAXX" on page 29)

Pushing Observables on an Ad hoc Basis

You can push observables to a STIX/TAXII server on an ad hoc basis from these locations in the Anomali STAXX UI:

- Activity dashboard
- Import Details page, while importing observables or thereafter

When you push observables from these UI screens, the properties (such as confidence, severity, type, indicator type, TLP) associated with the observables are included along with the observable value.

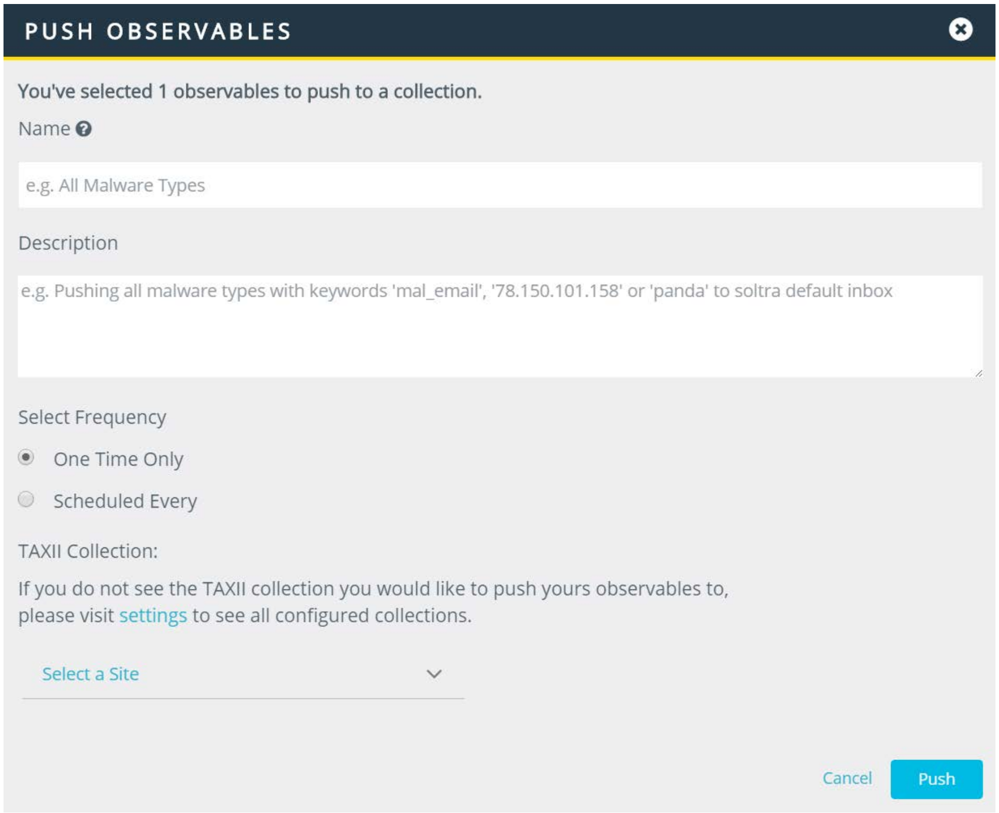
Pushing Observables from the Activity Dashboard

If you come across any observables on the Anomali STAXX Activity dashboard that you want to share with other STIX/TAXII servers you use, you can do so from the Activity dashboard.

To push observables:

1. Click **Activity** from the top menu bar.
2. Run a search.
3. Identify and select the observables you want to push.

4. In the **Actions** menu, click **Push Observable**.



PUSH OBSERVABLES

You've selected 1 observables to push to a collection.

Name

e.g. All Malware Types

Description

e.g. Pushing all malware types with keywords 'mal_email', '78.150.101.158' or 'panda' to soltra default inbox

Select Frequency

● One Time Only

○ Scheduled Every

TAXII Collection:

If you do not see the TAXII collection you would like to push yours observables to, please visit settings to see all configured collections.

5. Enter the following information:

   - Name—A meaningful name for this push operation. This name is associated with the push operation, similar to a job ID.

   - Description—Add a note explaining the context of the push. This field is optional.

   - Select Frequency—To run a single ad hoc push, select **One Time Only**. To configure the push to run on a schedule, select **Scheduled Every** and specify the frequency on which you want the push to run.

   - Select a Site—Select the site to which you want to push the observable. Only sites configured under Settings > Sites are listed in this dropdown. See "Adding a Site" on page 46.

     If you are pushing observables to ThreatStream, make sure the ThreatStream user configured for the site has the permission to push to ThreatStream. This permission is configured on Anomali ThreatStream.

   - Select a Collection—If the Site supports Collections, select the Collection to which you want to push the observable.

If the Site requires a subscription ID for its Collections, you must configure the subscription ID before pushing the observables, otherwise the push operation will not succeed. To configure the subscription ID for a Collection, see "Specifying or Editing Subscription ID for a Collection" on page 32.

Note: Soltra, ThreatStream, and DHS servers support Collections; however, Collections are not discoverable on Soltra Edge servers. Therefore, Anomali STAXX is not able to discover them. In such cases, you must manually create a Collection on Anomali STAXX as described in "Adding Collections Manually" on page 52.

6. Click **Push**.

Pushing Observables While Importing Into Anomali STAXX

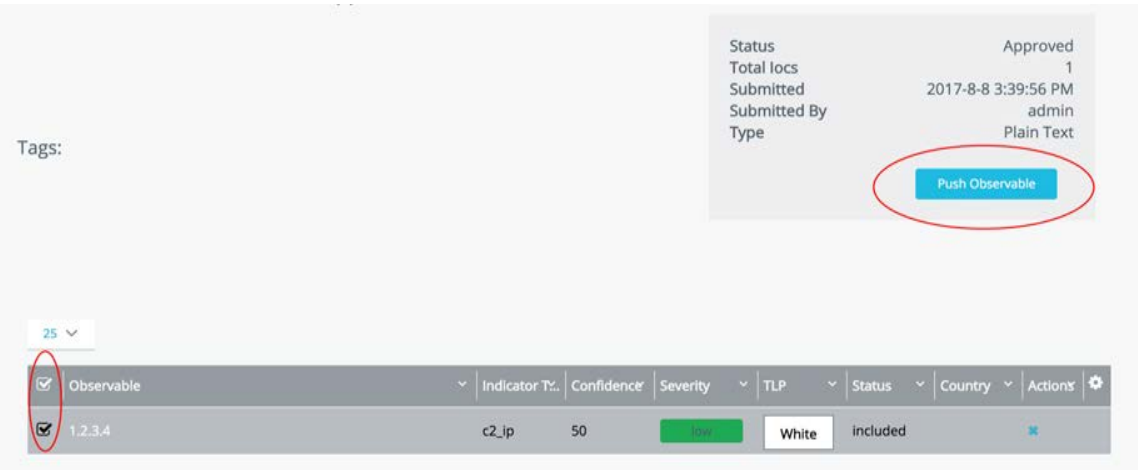
You can push observables to other STIX/TAXII servers either at the time of approving observables for import or later from the Import Details page of an approved job.

To push imported observables from an approved imported job:

1. Click **Imports** from the top menu bar.

2. Click on the import job that contains the observables you want to push.

3. On the import job details page, select the observables you want to push.

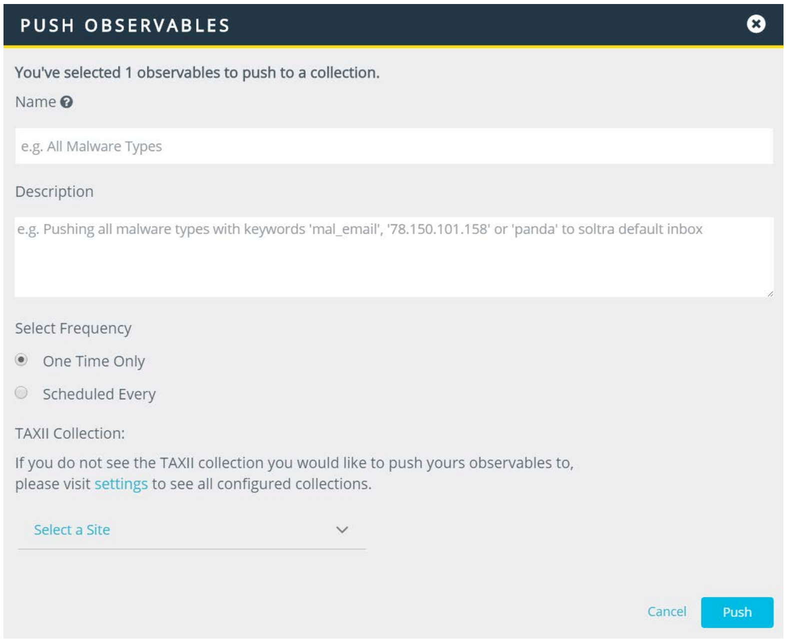


Tags:

Status	Approved
Total locs	1
Submitted	2017-8-8 3:39:56 PM
Submitted By	admin
Type	Plain Text

☑	Observable	Indicator T...	Confidence	Severity	TLP	Status	Country	Actions
☑	1.2.3.4	c2_ip	50	low	White	included		✖

4. Click **Push Observable**.



PUSH OBSERVABLES

You've selected 1 observables to push to a collection.

Name

e.g. All Malware Types

Description

e.g. Pushing all malware types with keywords 'mal_email', '78.150.101.158' or 'panda' to soltra default inbox

Select Frequency

● One Time Only

○ Scheduled Every

TAXII Collection:

If you do not see the TAXII collection you would like to push yours observables to, please visit settings to see all configured collections.

Select a Site

5. Enter the following information:

- Name—A meaningful name for this push operation. This name is associated with the push operation, similar to a job ID.

- Description—Add a note explaining the context of the push. This field is optional.

- Select Frequency—To run a single ad hoc push, select **One Time Only**. To configure the push to run on a schedule, select **Scheduled Every** and specify the frequency on which you want the push to run.

- Select a Site—Select the site to which you want to push the observable. Only sites configured under Settings > Sites are listed in this dropdown. See "Adding a Site" on page 46.

  If you are pushing observables to ThreatStream, make sure the ThreatStream user configured for the site has the permission to push to ThreatStream. This permission is configured on Anomali ThreatStream.

- Select a Collection—If the Site supports Collections, select the Collection to which you want to push the observable.

  > If the Site requires a subscription ID for its Collections, you must configure the subscription ID before pushing the observables, otherwise the push operation will not

succeed. To configure the subscription ID for a Collection, see "Specifying or Editing Subscription ID for a Collection" on page 32.

Note: Soltra, ThreatStream, and DHS servers support Collections; however, Collections are not discoverable on Soltra Edge servers. Therefore, Anomali STAXX is not able to discover them. In such cases, you must manually create a Collection on Anomali STAXX as described in "Adding Collections Manually" on page 52.

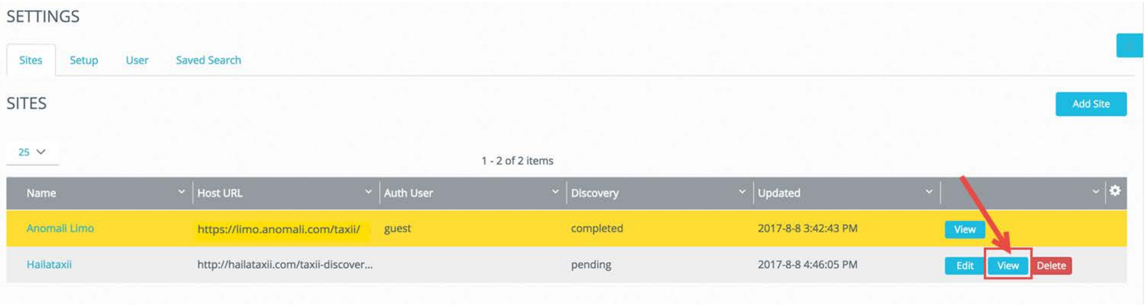
6. Click **Push**.

Configuring a Scheduled Push on Anomali STAXX

Note: You must be logged in as the Anomali STAXX admin user to configure a scheduled push on Anomali STAXX.

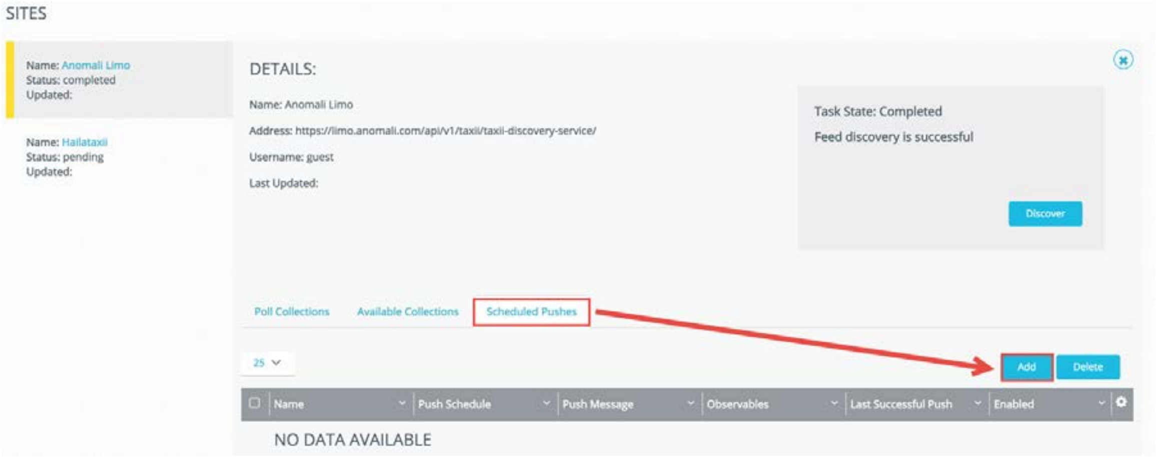
To configure a scheduled push:

1. Click ⚙ to the top right of your screen.
2. Click the **Sites** tab.
3. Click **View** for the site for which you want to configure a scheduled push.



Name	Host URL	Auth User	Discovery	Updated	
Anomali Limo	https://limo.anomali.com/taxii/	guest	completed	2017-8-8 3:42:43 PM	View
Hailataxii	http://hailataxii.com/taxii-discover...		pending	2017-8-8 4:46:05 PM	Edit View Delete

4. On the Sites details page, click the **Scheduled Pushes** tab, as shown in the following figure.



SITES

Name: Anomali Limo
Status: completed
Updated:

Name: Hailataxii
Status: pending
Updated:

DETAILS:

Name: Anomali Limo
Address: https://limo.anomali.com/api/v1/taxii/taxii-discovery-service/
Username: guest
Last Updated:

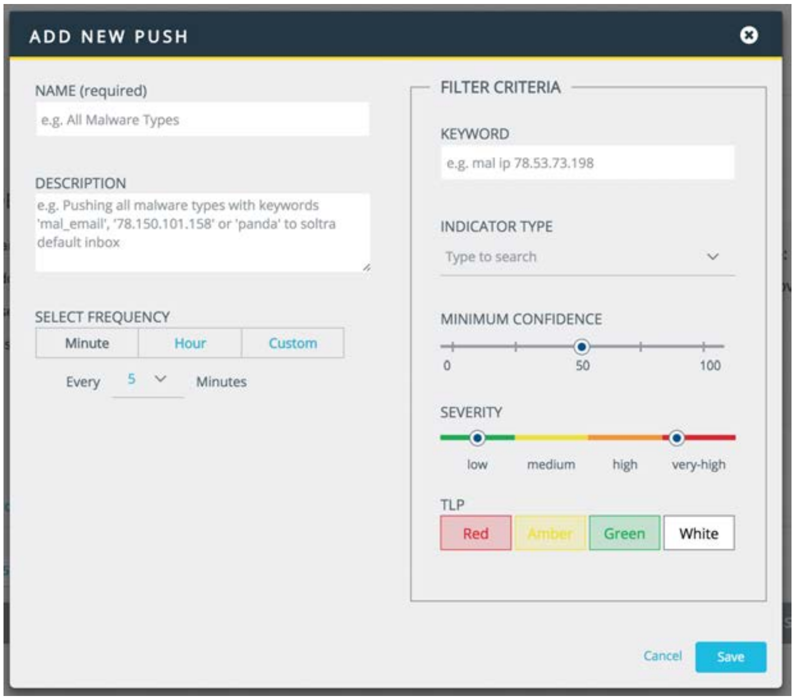
Task State: Completed
Feed discovery is successful

☐	Name	Push Schedule	Push Message	Observables	Last Successful Push	Enabled

NO DATA AVAILABLE

5. Click **Add**.

6. Enter the information in the form:



ADD NEW PUSH

NAME (required)
e.g. All Malware Types

DESCRIPTION
e.g. Pushing all malware types with keywords 'mal_email', '78.150.101.158' or 'panda' to soltra default inbox

SELECT FREQUENCY
Minute | Hour | Custom
Every 5 Minutes

FILTER CRITERIA

KEYWORD
e.g. mal ip 78.53.73.198

INDICATOR TYPE
Type to search

MINIMUM CONFIDENCE
0 50 100

SEVERITY
low medium high very-high

TLP
Red Amber Green White

- Name—A meaningful name for the push operation.
- Description—A meaningful description for the push operation.
- Collection—Only shown if the Site supports Collections. Select the Collection to which you want to push the observable.
- Frequency—How frequently will the observables be pushed.

- Filter Criteria—Specify a criteria by which the observables will be filtered before they are pushed.

Keyword	Specify one or multiple keywords. Keywords are matched against the values of the following fields: "List of Fields" on page 66. For example, if you want to include observables of itype=phish_url, specify *phish_url* in the Keyword box. **There is no need to enter the field name**. This value is matched against the values of all fields in the "List of Fields" on page 66. If you want to include all observables of itype=phish_url and severity=high, specify *phish_url high* in the Keyword box. The two values are automatically ANDed and the observables matching *phish_url* and *high* are returned in the search results. **Note that you do not need to specify the field name or the boolean operator.**
Indicator Type	Specify the observable types; for example, apt_ip, mal_url, phish_domain, tor_ip. See "Available Indicator Types" on page 68 for more information.
Minimum Confidence	Specify the minimum confidence value on a slider scale (from 0 - 100)
Severity	Specify the severity (low, mid, high, very high). By default, a severity range (low to very high) is selected in the UI. To change the severity range, move the end points of the slider scale accordingly. To specify one value for severity, make sure the two end points of the slider scale overlap.
TLP	Traffic Light Protocol level for the observables. You can select multiple TLP levels.

7. Click **Save**.

Viewing Available Collections for Pushing Observables

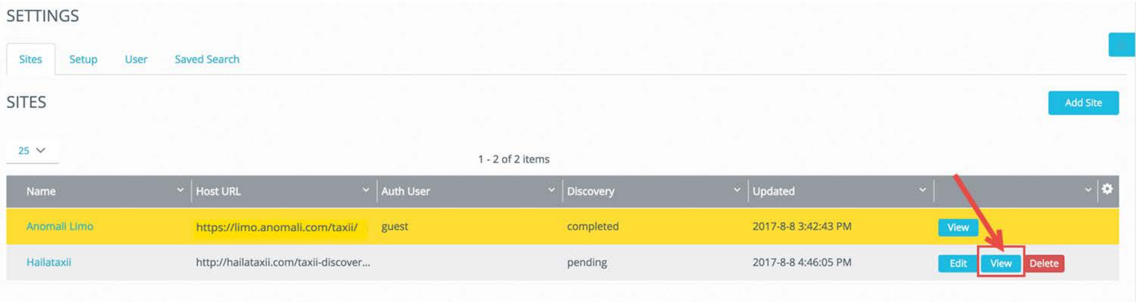
Note: Soltra, ThreatStream, and DHS servers support Collections; however, Collections are not discoverable on Soltra Edge servers. Therefore, Anomali STAXX is not able to discover them. In such cases, you must manually create a Collection on Anomali STAXX as described in "Adding Collections Manually" on page 52.

To view all available Collections for a site:

1. Click ⚙ to the top right of your screen.

2. Click the **Sites** tab.

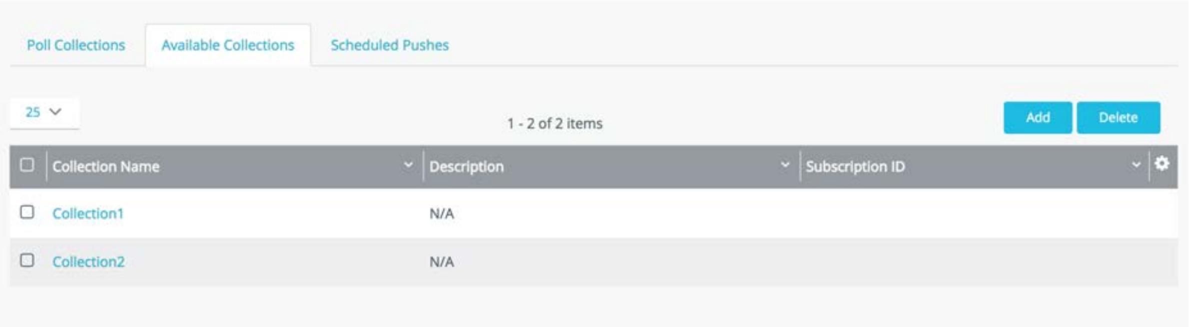
3. Click **View** for the site.



Name	Host URL	Auth User	Discovery	Updated	
Anomali Limo	https://limo.anomali.com/taxii/	guest	completed	2017-8-8 3:42:43 PM	View
Hailataxii	http://hailataxii.com/taxii-discover...		pending	2017-8-8 4:46:05 PM	Edit View Delete

4. On the Sites details page, click the **Available Collections** tab.

   The currently available Collections are displayed.



□	Collection Name	Description	Subscription ID
□	Collection1	N/A	
□	Collection2	N/A	

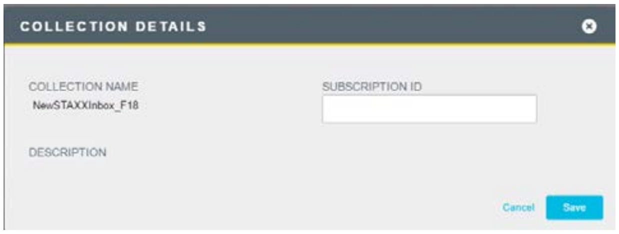
Specifying or Editing Subscription ID for a Collection

To specify or edit the subscription ID for a collection:

1. Follow the procedure to view all available collections, as described in "Viewing Available Collections for Pushing Observables" on the previous page.

2. Click the link for collection whose subscription ID you want to specify or edit.

3. Enter the subscription ID.



COLLECTION NAME
NewSTAXXInbox_F18

SUBSCRIPTION ID

DESCRIPTION

4. Click **Save**.

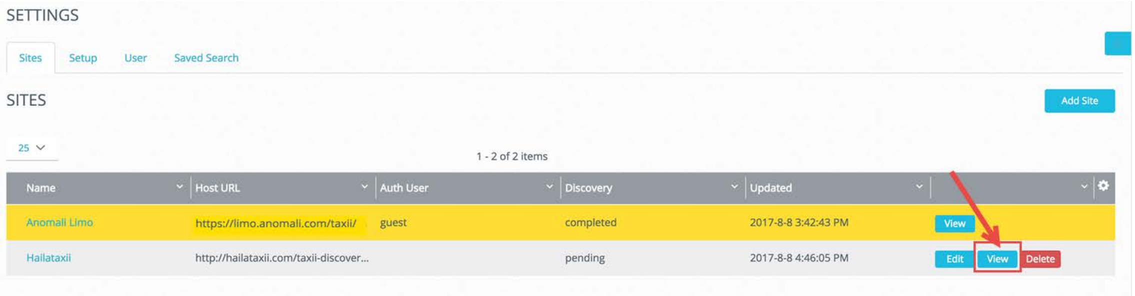
Deleting Available Collections

To delete available collections on Anomali STAXX:

1. Click ⚙ to the top right of your screen.

2. Click the **Sites** tab.

3. Click **View** for the site for which you want to delete an outgoing collection.



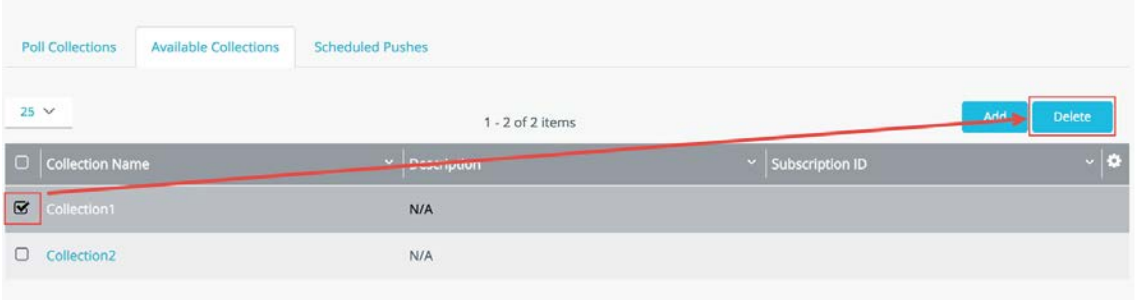
1 - 2 of 2 items

Name	Host URL	Auth User	Discovery	Updated	
Anomali Limo	https://limo.anomali.com/taxii/	guest	completed	2017-8-8 3:42:43 PM	View
Hailataxii	http://hailataxii.com/taxii-discover...		pending	2017-8-8 4:46:05 PM	Edit View Delete

4. On the Sites details page, click the **Available Collections** tab.

   The currently available collections are displayed.

5. Select the collections that you want to delete and click the **Delete** button, as shown in the following figure.



1 - 2 of 2 items

□	Collection Name	Description	Subscription ID
☑	Collection1	N/A	
□	Collection2	N/A	

6. Select **Delete Collection** at the confirmation prompt.

   The Collections are deleted from the list.

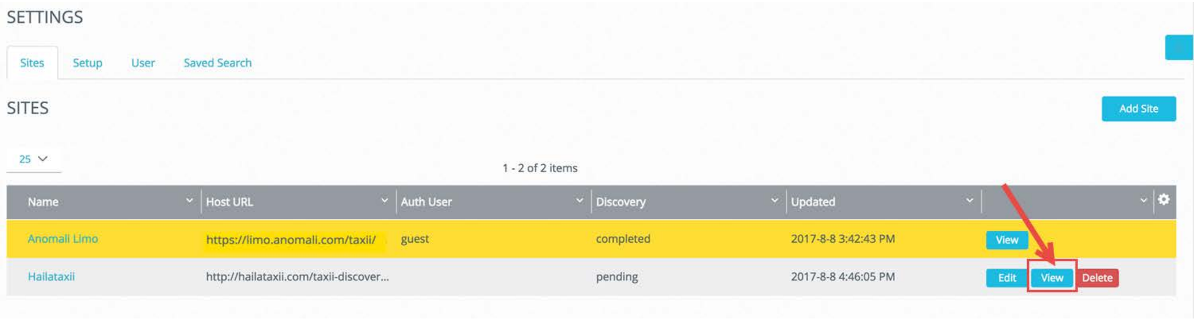
> **TIP:** To add a Collection back for Anomali ThreatStreamand DHS sites, click **Discover**. The discovery process rediscovers a site's Collections and adds back the Collections that were deleted earlier. You must add Soltra Collections manually by following the instructions in "Adding Collections Manually" on page 52.

Disabling a Scheduled Push Job

You can disable a scheduled push job if you want to temporarily stop pushing observables to it.

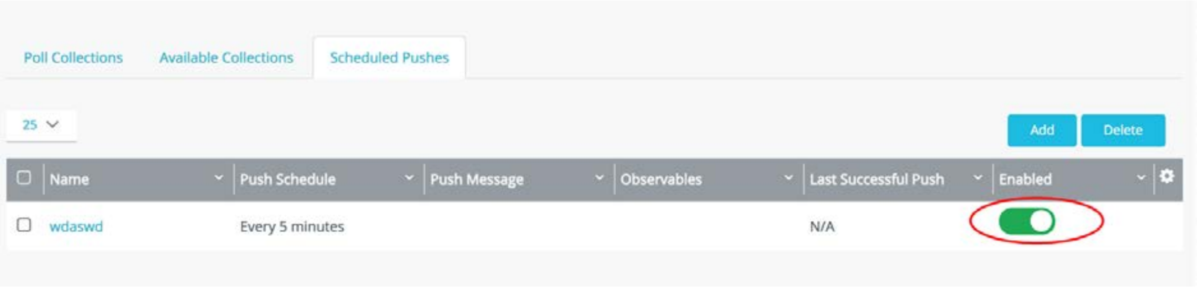
To disable a scheduled push job:

1. Click ⚙ to the top right of your screen.
2. Click the **Sites** tab.
3. Click **View** for the site whose scheduled push you want to disable.



Name	Host URL	Auth User	Discovery	Updated
Anomali Limo	https://limo.anomali.com/taxii/	guest	completed	2017-8-8 3:42:43 PM
Hailataxii	http://hailataxii.com/taxii-discover...		pending	2017-8-8 4:46:05 PM

4. Click the **Scheduled Pushes** tab.
5. Locate the outgoing push job that you want to disable.
6. Under Enable, click the green slider to disable the push job.



□	Name	Push Schedule	Push Message	Observables	Last Successful Push	Enabled
□	wdaswd	Every 5 minutes			N/A	

The color changes to gray when the push job is disabled.

Pushing Data to DHS AIS Feeds

Anomali STAXX enables non-federal customers in the DHS AIS data pool to push intelligence to DHS AIS feeds. To comply with DHS protocol and ensure data sent from Anomali STAXX is accepted, the fields listed below are sent with values set by Anomali. Be advised that existing values in these fields are overwritten with the listed default values when pushed to DHS AIS feeds.

Field	Default Value
TLP	White
Source	Anomali
AIS	Not_Proprietary
CISA_Proprietary	False

Chapter 6: Importing and Exporting Observables

This chapter describes how to import and export observables from Anomali STAXX. It contains the following topics:

Importing Observables

You can import observables (observables) into Anomali STAXX from other sources such as a text file or manually enter raw data, such as article from the Internet, on the Anomali STAXX UI. Anomali STAXX parses the data and extracts the following types of observables from it:

- IP Address (v4 only)
- Domain
- URL
- Email
- MD5 Hash

All imported observables are associated with the same threat type, severity, confidence, TLP, and tags. For example, if a file has two IP addresses, each IP will be assigned the same threat type—malware or apt.

The imported data in an import job must be reviewed and approved before it becomes part of threat intelligence on Anomali STAXX. Approved observables can also be pushed to STIX/TAXII servers through Anomali STAXX.

How to Import Observables

observables can be imported using the Anomali STAXX user interface or by making a REST API call to Anomali STAXX.

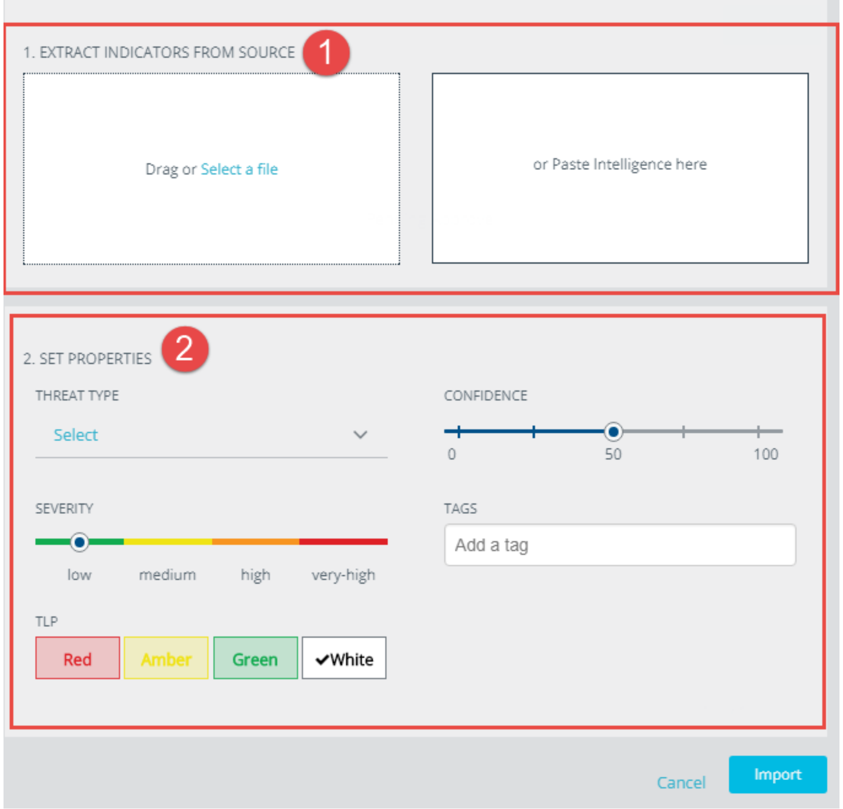
To import observables into Anomali STAXX using the user interface::

1. Click **Imports** from the top menu bar then click the **Import** button on the resulting page.

   OR

   Click the ⬆ icon on any UI screen.

2. Enter the following information:



1. EXTRACT INDICATORS FROM SOURCE

Drag or Select a file

or Paste Intelligence here

2. SET PROPERTIES

THREAT TYPE: Select

CONFIDENCE: 0 – 50 – 100

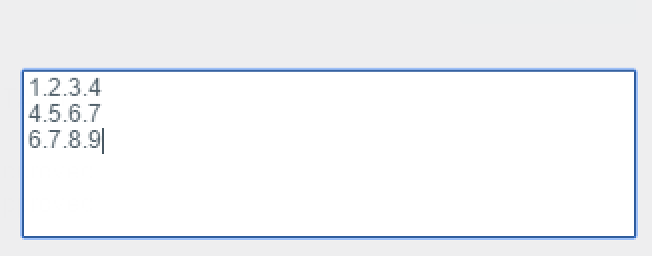
SEVERITY: low, medium, high, very-high

TAGS: Add a tag

TLP: Red, Amber, Green, ✓White

1 Select or drag-and-drop a text file from which observables will be extracted, OR, type in observable information in the "Paste Intelligence here".

If you are typing in intelligence, make sure that each observable is on a separate line, as shown in this example:



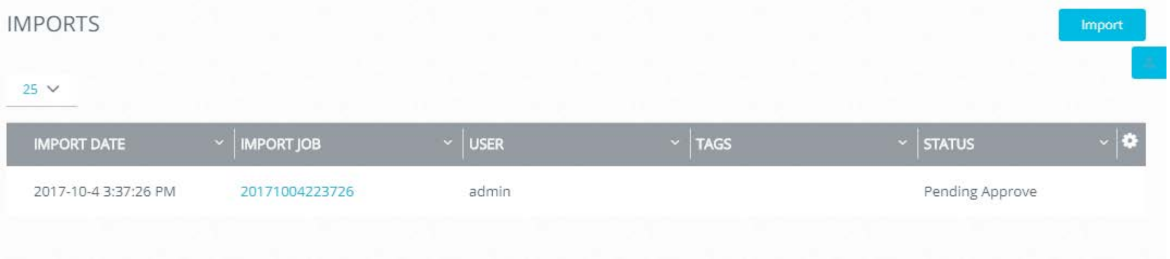
```
1.2.3.4
4.5.6.7
6.7.8.9
```

2 Properties to be assigned to imported observables:

- Threat type—Assign the threat type; for example, malware, phish, tor. See "Available Indicator Types" on page 68 to determine the threat type to use for a specific observable types.
- Confidence—Specify the confidence value on a slider scale (from 0 - 100) that you want to assign to the imported observables.
- Severity—Specify the severity (low, medium, high, very-high).
- Tags—Specify tags you want to assign to observables, as a comma-separated list; for example, suspicious-domain, victim-finance.
- TLP—Traffic Light Protocol level for the observables. The TLP color provides a mechanism to communicate to consumers of the observable whether further dissemination of this observable is allowed; if yes, how freely can this information be distributed. By default, the color White is assigned to pushed observables. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

3. Click **Import**.

   An import job is created, which must be approved by an Anomali STAXX user before the observables are imported into Anomali STAXX.



IMPORT DATE	IMPORT JOB	USER	TAGS	STATUS
2017-10-4 3:37:26 PM	20171004223726	admin		Pending Approve

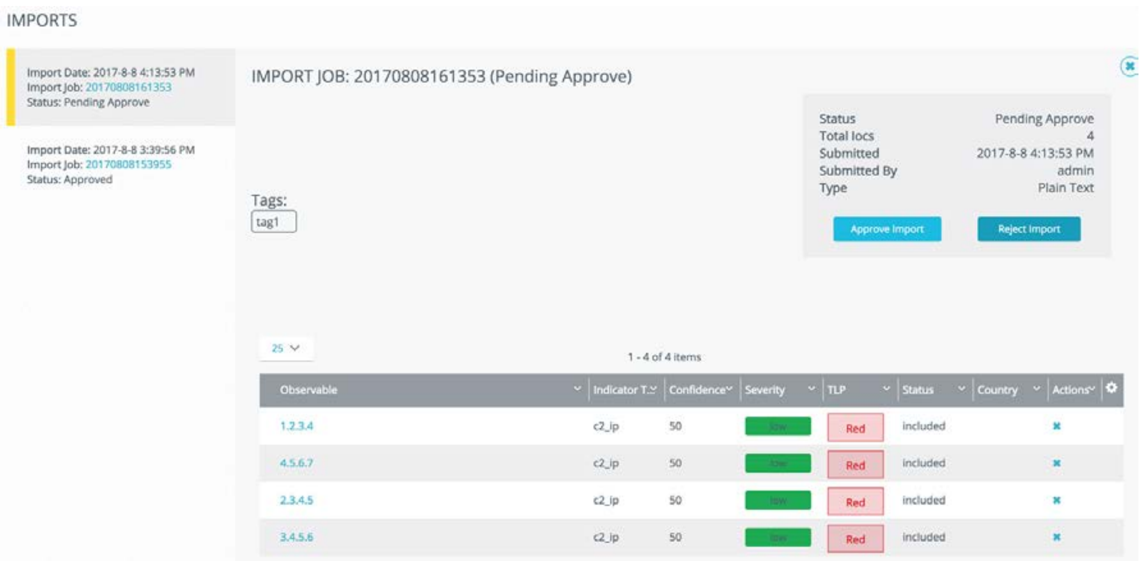
To import observables into Anomali STAXX by making a REST API call:

See "Using REST APIs to Import and Export Observables" on page 41.

Approving or Rejecting an Import Job

To approve or reject an import job:

1. Click **Imports** from the top menu bar.
2. Click on the import job that you want to approve or reject.
3. On the import job details page, you can:



IMPORTS

Import Date: 2017-8-8 4:13:53 PM
Import Job: 20170808161353
Status: Pending Approve

Import Date: 2017-8-8 3:39:56 PM
Import Job: 20170808153955
Status: Approved

IMPORT JOB: 20170808161353 (Pending Approve)

Status	Pending Approve
Total Iocs	4
Submitted	2017-8-8 4:13:53 PM
Submitted By	admin
Type	Plain Text

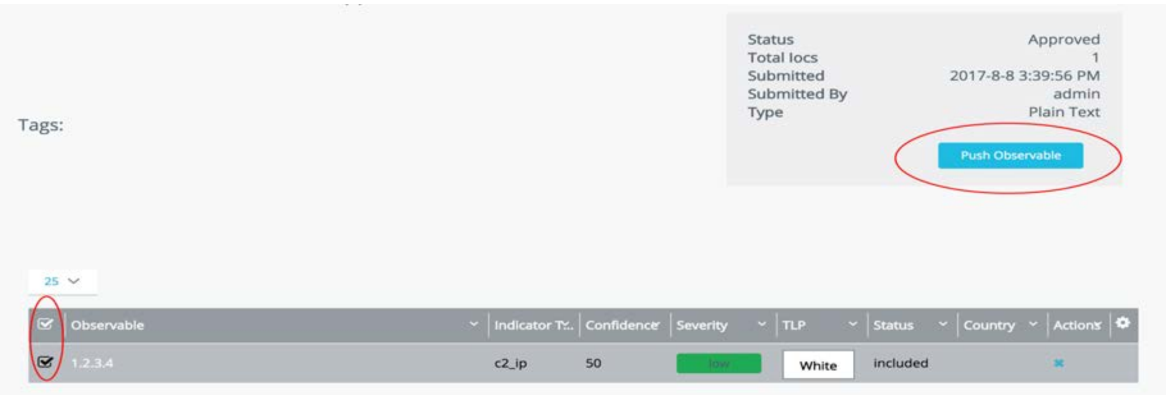
Tags:
tag1

1 - 4 of 4 items

Observable	Indicator T...	Confidence	Severity	TLP	Status	Country	Actions
1.2.3.4	c2_ip	50	low	Red	included		✖
4.5.6.7	c2_ip	50	low	Red	included		✖
2.3.4.5	c2_ip	50	low	Red	included		✖
3.4.5.6	c2_ip	50	low	Red	included		✖

- Review the observables included in the import job.
- Click **X** in the Actions column to delete any observables you do not want to import.
- Click **Approve Import** to approve the job.

  You can push (share) observables to other STIX/TAXII servers right after approving them. Once you approve observables, you can select the ones you want to push, as shown in the following example. To learn more about pushing observables, see "Pushing Observables While Importing Into Anomali STAXX" on page 27.



Tags:

Status	Approved
Total Iocs	1
Submitted	2017-8-8 3:39:56 PM
Submitted By	admin
Type	Plain Text

☑	Observable	Indicator T...	Confidence	Severity	TLP	Status	Country	Actions
☑	1.2.3.4	c2_ip	50	low	White	included		✖

- Click **Reject Import** to reject the job.

Viewing Import Jobs

To view all import jobs (pending and approved), click **Imports** from the top menu bar.

Pushing Imported Observables to Another STIX/TAXII Server

See "Pushing Observables While Importing Into Anomali STAXX" on page 27.

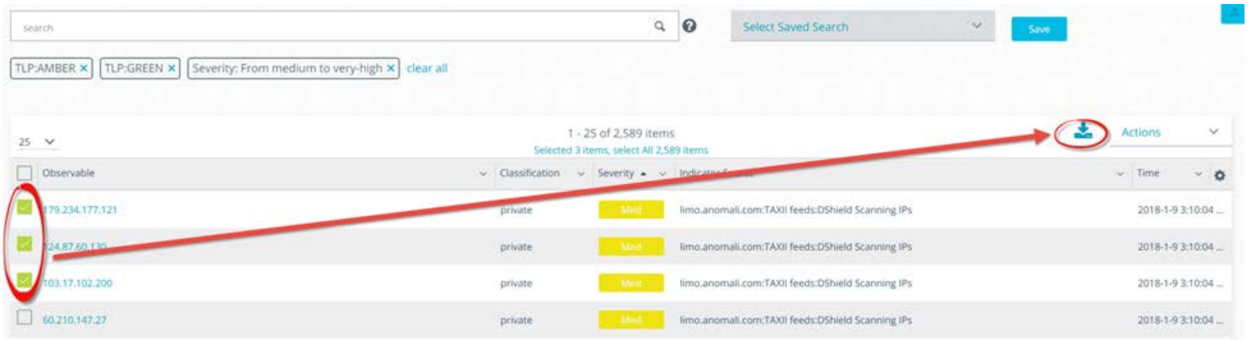
Exporting Observables

You can export observables from Anomali STAXX to a file in CSV or JSON format. Observables can be exported using the Anomali STAXX user interface or by making a REST API call to Anomali STAXX.

The Anomali STAXX user interface allows you to search for observables using keywords. However, the REST API call allows you to search by keywords and by field values. You can use Boolean logic to create and specify complex field-based queries. Supported fields are listed in "Appendix: Filter Fields and Indicator Types" on page 66.

To export observables from Anomali STAXX using the user interface:

1. Click **Activity** from the top menu bar.
2. Search for the observables that you want to export.
3. Once the search results are ready, either select the observables you want to export or click the box at the top of the selector column to select all observables.

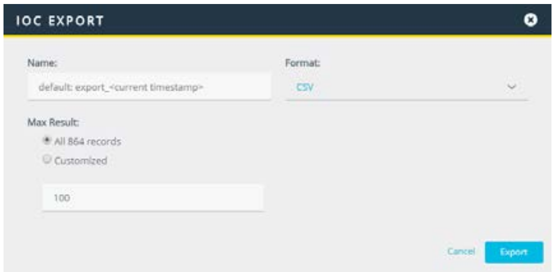


1 - 25 of 2,589 items
Selected 3 items, select All 2,589 items

	Observable	Classification	Severity	Indicator Source	Time
☑	179.234.177.121	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:04 ...
☑	124.87.60.130	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:04 ...
☑	103.17.102.200	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:04 ...
□	60.210.147.27	private	Med	limo.anomali.com:TAXII feeds:DShield Scanning IPs	2018-1-9 3:10:04 ...

4. Click the export icon at the top right as shown in the previous figure.

5. Enter the following information and click **Export** in the dialog box.



IOC EXPORT

Name: default: export_<current timestamp>

Format: CSV

Max Result:
● All 864 records
○ Customized

100

- Name—A meaningful name for the exported file.
- Format—Format of the exported file. You can select from CSV or JSON.
- Max Results—Maximum number of observables that will be exported. You can select from All or specify a number in the Customized field.

An export file, in the format you selected, is generated in your browser's default downloads location. By default, the file name is `export_<current_timestamp>.<format_extension>`. However, if you specified a different name in the dialog box above, that name is used to create the export file.

To export observables from Anomali STAXX by making a REST API call:

See "Using REST APIs to Import and Export Observables" below.

Using REST APIs to Import and Export Observables

This section describes how to import and export observables from Anomali STAXX using the REST APIs.

Importing Observables using REST API

To import observables into Anomali STAXX by making a REST API call:

1. Use the `login` endpoint to authenticate with Anomali STAXX and obtain a token ID:

   ```
   curl -kv -H 'Content-Type: application/json' 'https://<STAXX_IP_
   address>:8080/api/v1/login' -d '{"username":"user_a",
   "password":"<password>"}'
   ```

   where *STAXX_IP_address* is the IP address of the Anomali STAXX system.

   password is the password of the user "user_a" on Anomali STAXX.

   If the user is authenticated successfully, this call returns a token ID. For example, `{"token_id": "ef31868f094ef4932f00e0f0f279ffca"}`

2. Follow the command that applies to your use case.

   Observables to be imported are **specified in a file**:

   ```
   curl -kv -F 'file_name=@<filename_including_path>' -F import_params='
   {"tlp":"TLP:<TLP_color>", "severity":"<severity>", "threat_type": "<threat_
   type>", "auto_approve":"[yes|no]","confidence":"<confidence_value>",
   "tags":"<comma_separated_tags>", "token":"<token_id>"}' https://<STAXX_IP_
   address>:8080/api/v1/import_intel
   ```

   Observables to be imported are **specified in the API call**:

   ```
   curl -kv -F import_params='{"tlp":"TLP:<TLP_color>",
   "severity":"<severity>", "threat_type": "<threat_type>", "auto_approve":"
   [yes|no]","confidence":"<confidence_value>", "tags":"<comma_separated_
   tags>", "intel_str":"<indicator_1>, <indicator_2>","token":"<token_id>"}'
   https://<STAXX_IP_address>:8080/api/v1/import_intel
   ```

   Observables to be imported are **specified in a file and in the API call**:

   ```
   curl -kv -F 'file_name=@<filename_including_path>' -F import_params='
   {"tlp":"TLP:<TLP_color>", "severity":"<severity>", "threat_type": "<threat_
   type>", "auto_approve":"[yes|no]","confidence":"<confidence_value>",
   "tags":"<comma_separated_tags>", "intel_str":"<indicator_1>, <indicator_2>",
   "token":"<token_id>"}' https://<STAXX_IP_address>:8080/api/v1/import_intel
   ```

   Note: If the API call contains duplicate keys, the results may be undesirable.

Attribute	Description
file_name	If the observables to be imported are contained in a file, specify the filename, including path. The file should be a text file with .txt extension. For example, `/opt/files/myintel.txt` **Note:** Observables must be specified through at least one of the attributes: `file_name` or `intel_str`. Both attributes can also be used in the same command, as shown in the example above.
import_ params	Specifies a list of parameters that will be associated with the imported observables. The parameters you can specify are listed in the following rows in this table.
tlp	Specify the TLP value for the observables. Possible values RED, AMBER, GREEN, WHITE
severity	Specify the severity. Possible value: low, medium, high, very-high
threat_type	Assign the threat type; for example, malware, phish, tor. See "Available Indicator Types" on page 68 to determine the threat type to use for a specific observable types.
auto_ approve	Whether to automatically approve the observables for import or require a manual approval through the user interface. Possible values: yes, no. If manual approval is set, an import job is created in the Imports section of the user interface. You must connect to the user interface and approve the job before the observables become part of the intelligence on Anomali STAXX. See "Approving or Rejecting an Import Job" on page 39 for more information.
confidence	Specify the confidence value that you want to assign to the imported observables. Possible values: 0 - 100
tags	Specify tags you want to assign to observables, as a comma-separated list; for example, suspicious-domain, victim-finance.
intel_str	If you want to specify observables in the API call, use this parameter. Specify the observables as a comma-separated list. For example,www.mystream.com, b4867a4ad05aadbadd0511e3f8b08b29
token	Is the token that was returned in the previous step.

Examples

The following examples show how to use the import_intel endpoint to import observables into Anomali STAXX.

Example 1: In this example, the observables are contained in a file called myintel.txt and will be automatically approved upon import.

```
curl -kv -F 'file_name=@/opt/files/myintel.txt' -F import_params='
{"tlp":"TLP:RED", "severity":"medium", "threat_type": "p2p", "auto_
approve":"yes","confidence":"60", "tags":"tag1,tag2",
"token":"6cc3f200b35705e3c4536c5f510a6a5e"}' https://staxx_
host.mycompany.com:8080/api/v1/import_intel
```

Example 2: In this example, the observables are contained in a file called myintel.txt and are also specified in the API call. In this case, the observables will require manual approval through the user interface before they are imported into Anomali STAXX.

```
curl -kv -F 'file_name=@/opt/files/myintel.txt' -F import_params='
{"tlp":"TLP:GREEN", "severity":"high", "threat_type": "malware", "auto_
approve":"no","confidence":"60", "tags":"tag1,tag2", "intel_
str":"www.mystream.com, b4867a4ad05aadbadd0511e3f8b08b29",
"token":"497eb2fe83e7a838e945b3d087f410f2"}' https://staxx_
host.mycompany.com:8080/api/v1/import_intel
```

Exporting Observables Using REST API

To export observables from Anomali STAXX by making a REST API call:

1. Use the `login` endpoint to authenticate with Anomali STAXX and obtain a token ID:

   ```
   curl -kv -H 'Content-Type: application/json' 'https://<STAXX_IP_
   address>:8080/api/v1/login' -d '{"username":"user_a",
   "password":"<password>"}'
   ```

   where *STAXX_IP_address* is the IP address of the Anomali STAXX system.

   password is the password of the user "user_a" on Anomali STAXX.

   If the user is authenticated successfully, this call returns a token ID. For example, `{"token_id": "ef31868f094ef4932f00e0f0f279ffca"}`

2. Use the `intelligence` endpoint to export search results based on the query specified in the API call:

   ```
   curl -kv -H 'Content-Type: application/json' 'https://<STAXX_IP_
   address>:8080/api/v1/intelligence' -d '{"token":"<token_id>",
   "query":"<user_defined_query>", "type":["csv" |"json"], "size":10}'
   ```

   where *token_id* is the token that was returned in the previous step.

   user_defined_query is the query (or filter) that you can define to specify the search criteria. You can specify a keyword or a field-based query. See "Appendix: Filter Fields and Indicator Types" on page 66 for a list of supported fields.

Examples of field-based queries: Unless a value contains a space, enclosing the value in single quotes is optional.

```
confidence>50

confidence>50 AND severity=high

confidence>80 AND itype=c2_domain AND date_last>-14d

confidence>80 AND itype=c2_domain AND date_last>=2016-12-14T01:57:51 AND
date_last<=2016-12-21T01:57:51

confidence>=50 and date_last >= '2016-11-22T00:21:01' and date_last
<='2016-12-22T00:21:01' and (itype = 'apt_url' OR itype = 'phish_url' OR
itype = 'c2_ip')

confidence>60 AND (itype contains apt OR itype contains domain) AND
severity=very-high
```

`type` is the file format in which search results will be exported. Specify either CSV or JSON.

`size` is the number of search results to export. This parameter is optional.

Chapter 7: Anomali STAXX Administration

This chapter provides information about various administrative functions you can perform on Anomali STAXX. You must belong to the admin group to perform these functions. The following topics are discussed here:

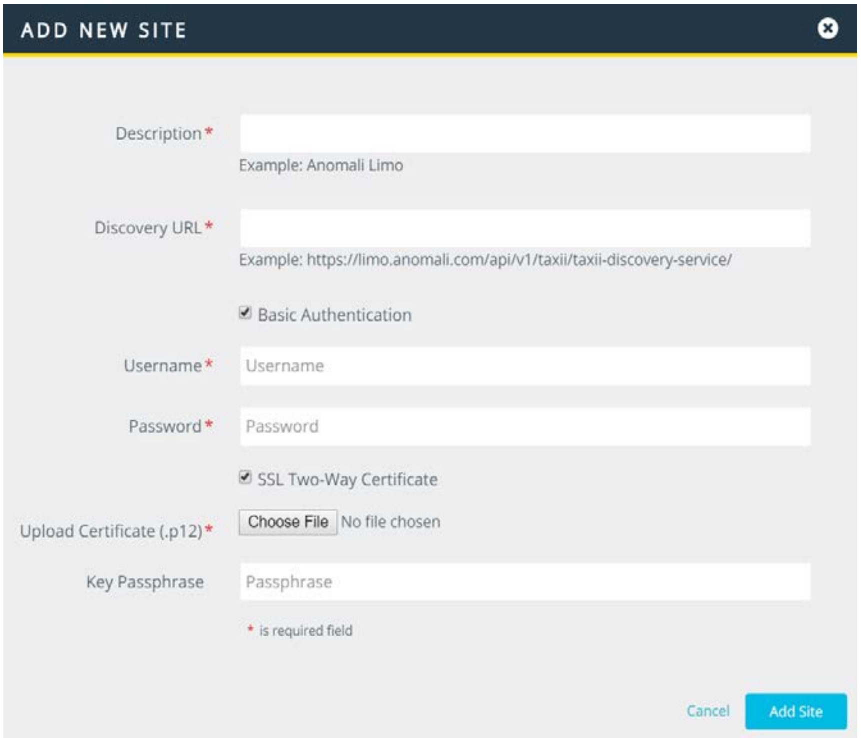
Sites

Before Anomali STAXX starts receiving observables, you need to add and configure sites from which you want to receive threat feeds or to push observables. Follow the procedure in this section to add and configure sites. If the necessary sites already exist, you need to discover and configure feeds. See "Adding Feeds to Receive Observables" on page 49 for more details.

Adding a Site

Use this procedure to configure STIX/TAXII sites. The sites may be in cloud or a local STIX/TAXII server.

1. Click ⚙ to the top right of your screen.
2. Click the **Sites** tab.
3. Click **Add Site** to the top right of your screen.



ADD NEW SITE

Description*

Example: Anomali Limo

Discovery URL*

Example: https://limo.anomali.com/api/v1/taxii/taxii-discovery-service/

☑ Basic Authentication

Username* Username

Password* Password

☑ SSL Two-Way Certificate

Upload Certificate (.p12)* Choose File No file chosen

Key Passphrase Passphrase

* is required field

4. Enter the following information.

Setting	Description
Description	A meaningful name for the site.
Discovery URL	URL for the STIX/TAXII server or FS-ISAC feed.
Basic Authentication	Select this option if you want to provide username and password information for the STIX/TAXII server or FS-ISAC feed.Then, enter the following information: ▪ User name ▪ Password **Note:** You can configure both authentication methods—Basic and SSL—at the same time.

Setting	Description
SSL Two-Way Certificate	Select this option to upload an SSL certificate, **in .p12 format**, that Anomali STAXX should use to authenticate with the STIX/TAXII server or FS-ISAC feed. If you checked this option, click **Choose File** to upload the SSL certification file. Then enter the (optional) Key Passphrase to use for the file. **Notes:** ■ You can configure both authentication methods—Basic and SSL—at the same time. ■ If the SSL certificate expires, you must delete the site and then re-configure it with the new certificate.

5. Click **Add Site**.

   The site is added to the list of Sites.

6. Click **View** to view the details of the site you just added.

7. Click **Discover** to discover available feeds and collections on the site.

   All available poll feeds and collections are discovered. *Poll Collections* are feeds from which you can received threat information. *Available Collections* are the collections to which you can push observables from Anomali STAXX.

> **Note:** Soltra, ThreatStream, and DHS servers support Collections. However, Collections are not discoverable on Soltra servers; therefore, Anomali STAXX is not able to discover them. In such cases, you must manually create a Collection on Anomali STAXX as described in "Adding Collections Manually" on page 52.

Editing a Site

Previously configured sites can be edited from the Sites tab within Anomali STAXX Settings.

Use this procedure to edit sites.

1. Click ⚙ to the top right of your screen.

2. Click the **Sites** tab.

3. Click Edit for the site that you want to edit.

4. Make required changes.

5. Click **Save Site**.

Deleting a Site

To delete a site, click the **Delete** button for the site.

Adding Feeds to Receive Observables

You must first add the site from which you want to receive a feed. See "Adding a Site" on page 46 for information.

If the site already exists on Anomali STAXX, follow the "Configuring Feeds" below procedure in this section.

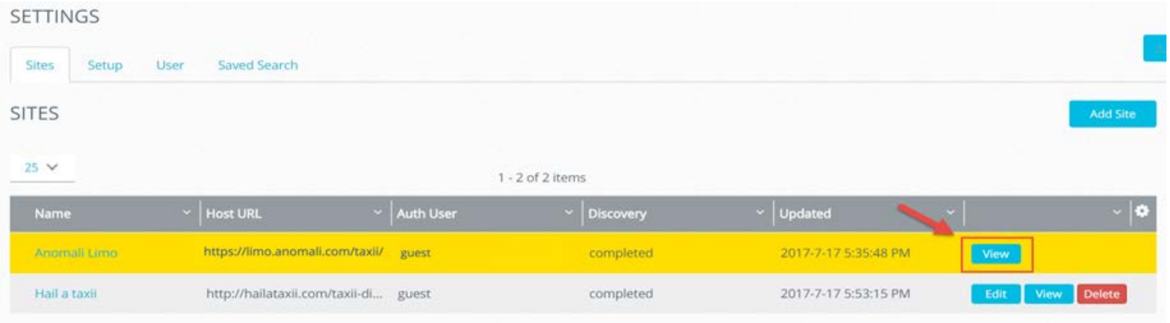
Configuring Feeds

Use this procedure to discover and configure feeds from a site that will be used to poll observables.

1. Click ⚙ to the top right of your screen.

2. Click the **Sites** tab.

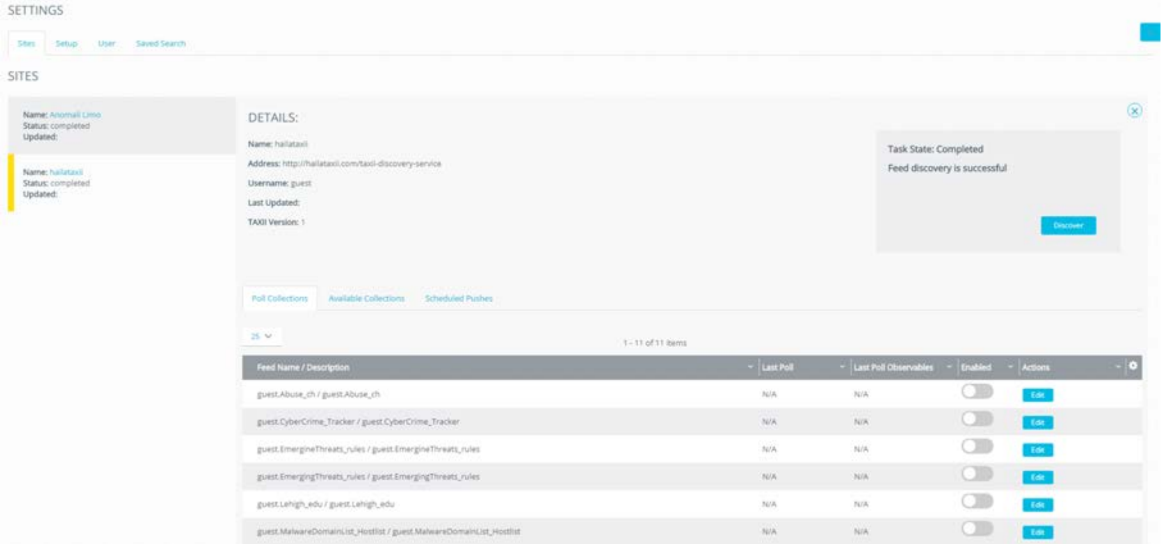
3. Click **View** for the site for which you want to discover feeds.



Name	Host URL	Auth User	Discovery	Updated	
Anomali Limo	https://limo.anomali.com/taxii/	guest	completed	2017-7-17 5:35:48 PM	View
Hail a taxii	http://hailataxii.com/taxii-di...	guest	completed	2017-7-17 5:53:15 PM	Edit View Delete

4. Click **Discover** to the top right of the page.

   Once the available feeds from the STIX/TAXII site have been discovered, they are listed in the Poll Collections tab on the page.



Name: Anomali Limo
Status: completed
Updated:

Name: hailataxii
Status: completed
Updated:

DETAILS:

Name: hailataxii
Address: http://hailataxii.com/taxii-discovery-service
Username: guest
Last Updated:
TAXII Version: 1

Task State: Completed
Feed discovery is successful

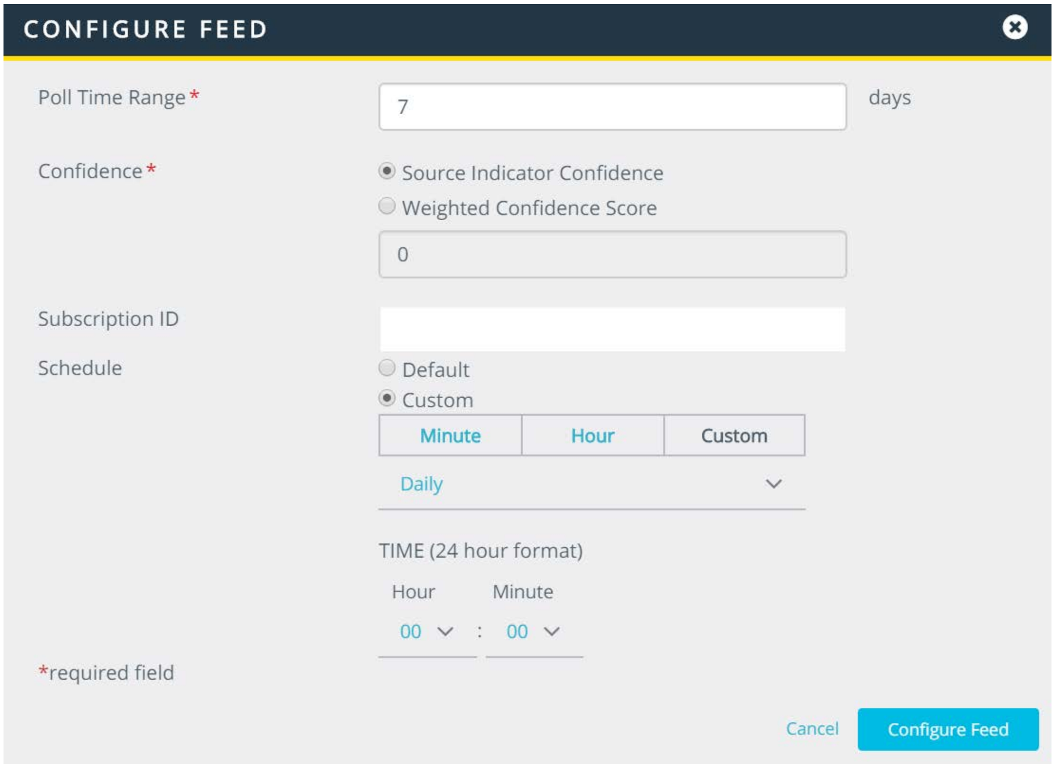
1 - 11 of 11 items

Feed Name / Description	Last Poll	Last Poll Observables	Enabled	Actions
guest.Abuse_ch / guest.Abuse_ch	N/A	N/A	○	Edit
guest.CyberCrime_Tracker / guest.CyberCrime_Tracker	N/A	N/A	○	Edit
guest.EmergineThreats_rules / guest.EmergineThreats_rules	N/A	N/A	○	Edit
guest.EmergingThreats_rules / guest.EmergingThreats_rules	N/A	N/A	○	Edit
guest.Lehigh_edu / guest.Lehigh_edu	N/A	N/A	○	Edit
guest.MalwareDomainList_Hostlist / guest.MalwareDomainList_Hostlist	N/A	N/A	○	Edit

5. Under **Enabled**, click the slider to enable each feed that you want to configure.

   Sliders are green when feeds are configured on Anomali STAXX.

6. Click **Edit** for each configured feed to update the following parameters or accept the default values.



Poll Time Range*	7 days
Confidence*	● Source Indicator Confidence ○ Weighted Confidence Score 0
Subscription ID	
Schedule	○ Default ● Custom Daily TIME (24 hour format) Hour 00 : Minute 00

*required field

- Poll Time Range—Specifies how many days of threat feeds to retrieve from the STIX/TAXII server **the first time** the server is polled. After the first time, updates since the last retrieval are obtained from the server. You can poll up to the previous 5 years (1825 days) of data.

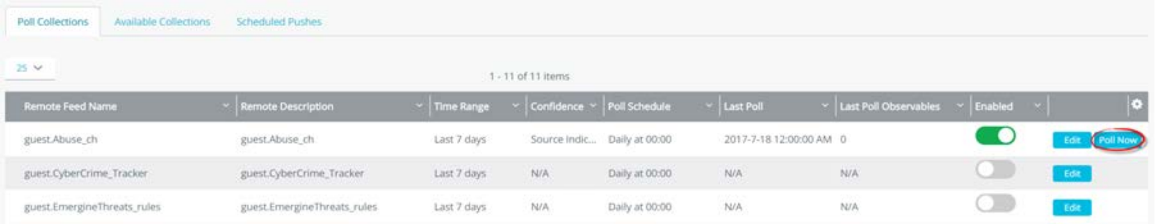
- Confidence—Choose whether to use the confidence value associated with the observable by its source feed or to assign a different confidence score when it is downloaded to Anomali STAXX. If you choose to use the associated value, select Source observable Confidence. If you choose to specify your own value, select Weighted Confidence Score and specify a value from 1-100.

- Subscription ID—If the feed requires a subscription identifier, enter it here. Otherwise, leave it blank.

- Schedule—The **Default** schedule polls feeds on a daily basis at midnight. Choose **Custom** to configure a custom polling schedule for the feed. You can select Minute (based on a fixed number of minutes), Hour (based on a fixed number of hours), or Custom (based on a specific time of the day or week).

7. Click **Configure Feed**.

Once configured, you can also poll feeds manually—in addition to scheduled polls—by clicking **Poll Now** next to the feed on the Poll Collections Table.



1 - 11 of 11 items

Remote Feed Name	Remote Description	Time Range	Confidence	Poll Schedule	Last Poll	Last Poll Observables	Enabled	
guest.Abuse_ch	guest.Abuse_ch	Last 7 days	Source Indic...	Daily at 00:00	2017-7-18 12:00:00 AM	0	●	Edit Poll Now
guest.CyberCrime_Tracker	guest.CyberCrime_Tracker	Last 7 days	N/A	Daily at 00:00	N/A	N/A	○	Edit
guest.EmergineThreats_rules	guest.EmergineThreats_rules	Last 7 days	N/A	Daily at 00:00	N/A	N/A	○	Edit

Unconfiguring Feeds

To unconfigure a feed:

1. Click ⚙ to the top right of your screen.

2. Click the **Sites** tab.

3. Click **View** for the site from which you want to unconfigure feeds.

4. In the Incoming Collections tab, click **Unconfigure** for each feed that you want to unconfigure.

Updating a Feed's Confidence Value

A feed's confidence value is one of the factors used to determine the final Confidence score shown on the Anomali STAXX Activity dashboards. If you need to update the value configured for a feed, follow these steps:

1. Unconfigure the feed, as described in "Unconfiguring Feeds" on the previous page.

2. Configure the feed again, as described in "Installing Anomali STAXX" on page 9.

   Specify the new Confidence value during the feed configuration process.

Adding Collections Manually

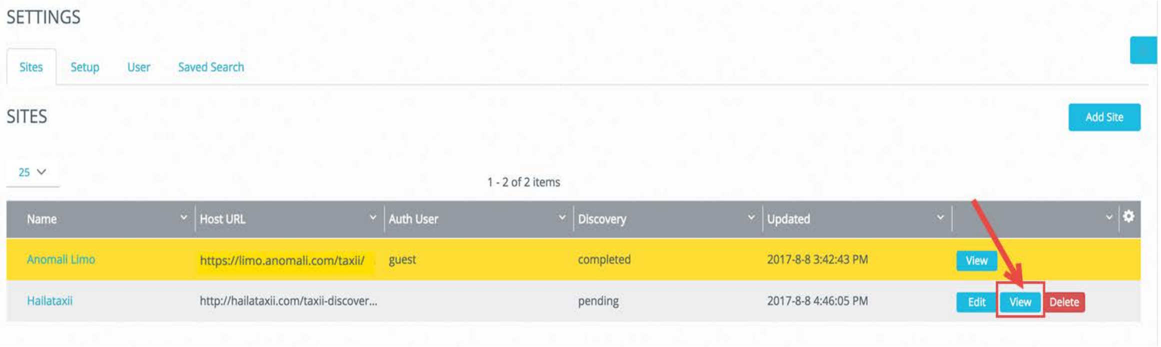
Anomali STAXX can discover Collections on a configured STIX/TAXII server automatically. However, if the server does not expose its Collections, Anomali STAXX will not be able to discover them. In such cases, you must manually create a Collection on Anomali STAXX as described in this section.

To add a Collection manually:

1. Click ⚙ to the top right of your screen.

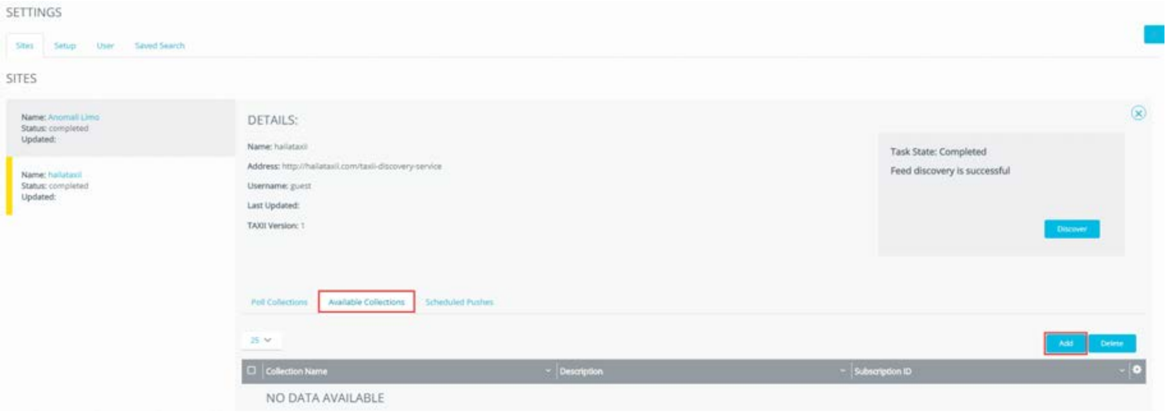
2. Click the **Sites** tab.

3. Click **View** for the site for which you want to add collections to see its details page.



Name	Host URL	Auth User	Discovery	Updated
Anomali Limo	https://limo.anomali.com/taxii/	guest	completed	2017-8-8 3:42:43 PM
Hailataxii	http://hailataxii.com/taxii-discover...		pending	2017-8-8 4:46:05 PM

4. In the site's details page, click the **Available Collections** tab.



Name: Anomali Limo
Status: completed
Updated:

Name: hailataxii
Status: completed
Updated:

DETAILS:

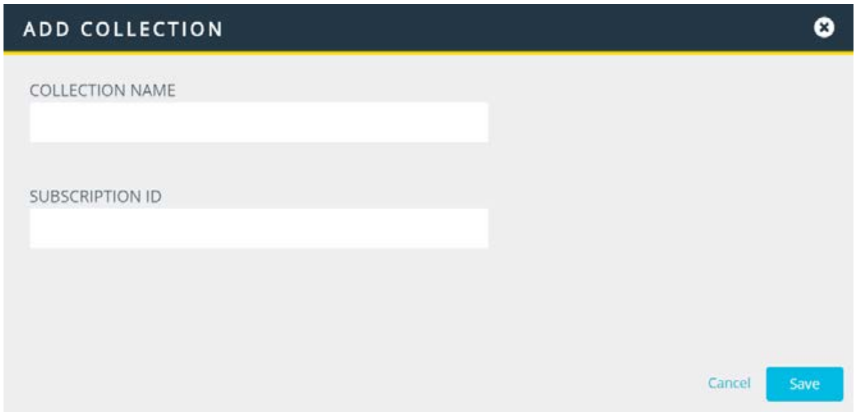
Name: hailataxii
Address: http://hailataxii.com/taxii-discovery-service
Username: guest
Last Updated:
TAXII Version: 1

Task State: Completed
Feed discovery is successful

□	Collection Name	Description	Subscription ID
	NO DATA AVAILABLE		

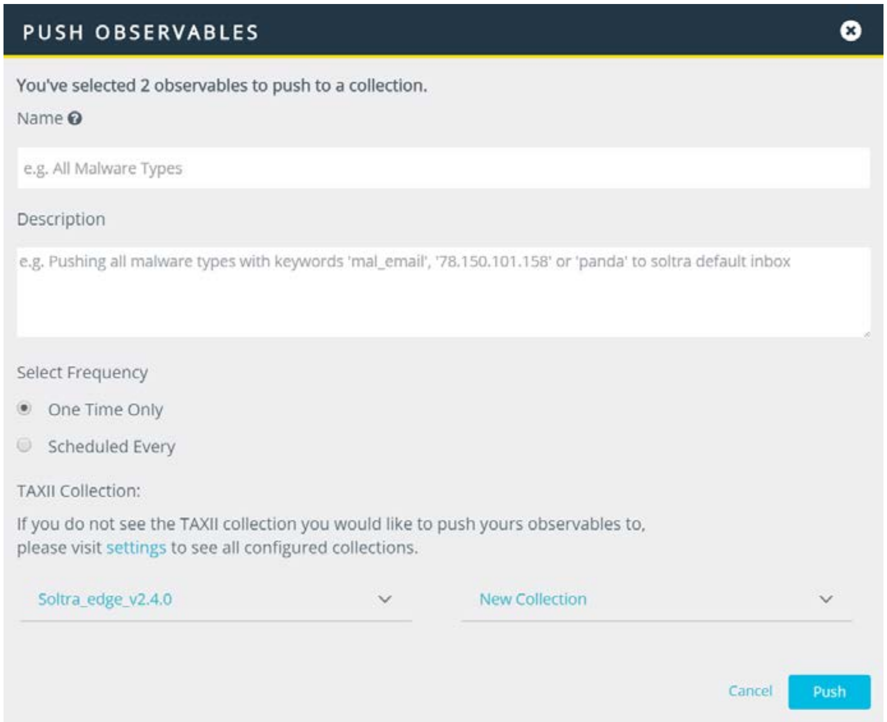
5. Click **Add**.

6. Enter the Collection Name and Subscription ID information. You must obtain this information from your STIX/TAXII server. Contact your server administrator if you do not have this information.



7. Click **Save**.

   The newly added collection is saved and is available in the drop down selection for the site, as shown in the following example.



You've selected 2 observables to push to a collection.

Name: e.g. All Malware Types

Description: e.g. Pushing all malware types with keywords 'mal_email', '78.150.101.158' or 'panda' to soltra default inbox

Select Frequency

● One Time Only

○ Scheduled Every

TAXII Collection:

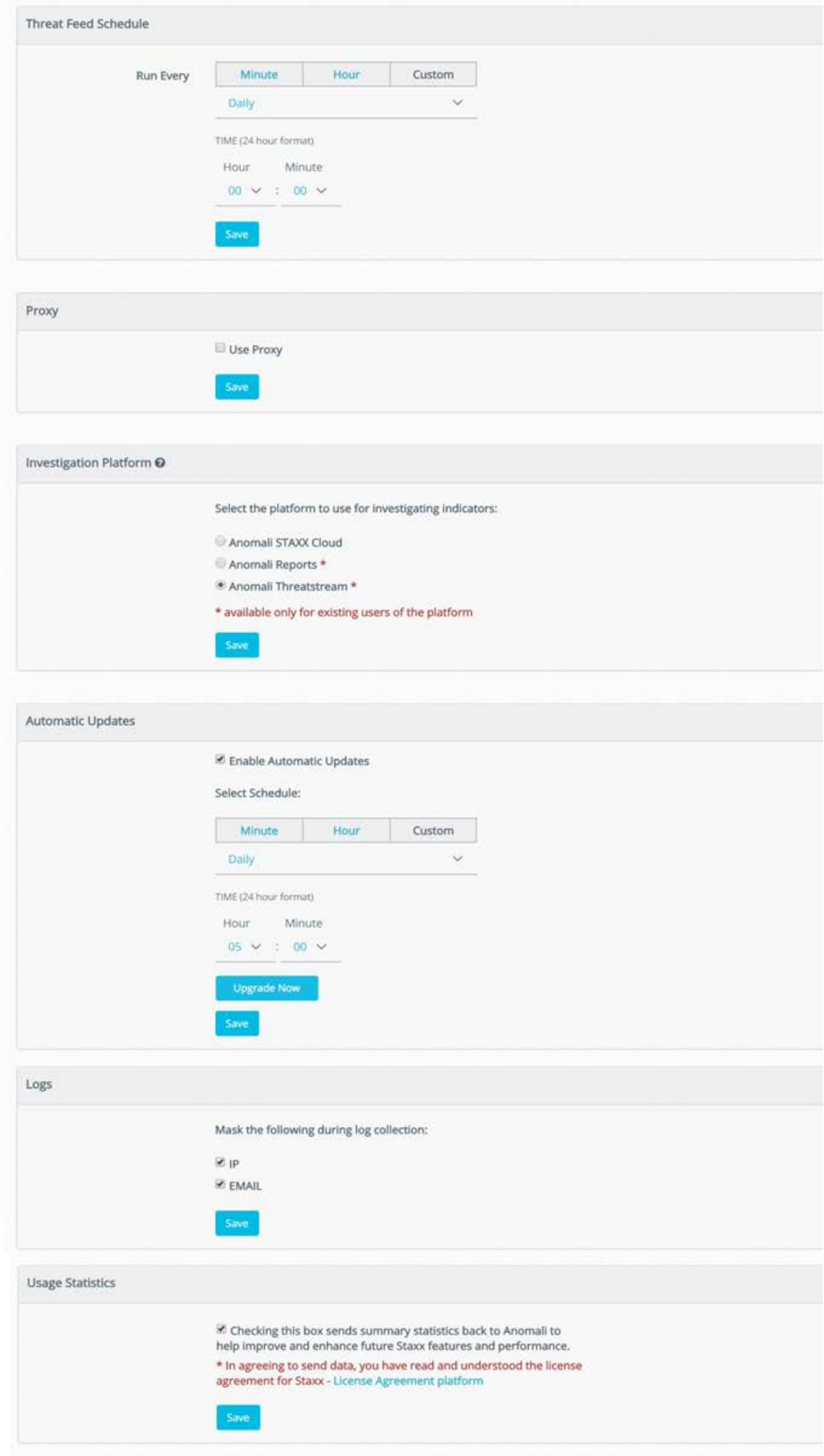
If you do not see the TAXII collection you would like to push yours observables to, please visit settings to see all configured collections.

Soltra_edge_v2.4.0 | New Collection

Deleting a Manually Added Collection

A manually added collection is deleted the same way as an automatically discovered collection. See "Deleting Available Collections" on page 33 for more information.

Setup Settings



Threat Feed Schedule

Run Every: Minute | Hour | Custom

Daily

TIME (24 hour format)

Hour 00 : Minute 00

Save

Proxy

□ Use Proxy

Save

Investigation Platform

Select the platform to use for investigating indicators:

○ Anomali STAXX Cloud
○ Anomali Reports *
● Anomali Threatstream *

* available only for existing users of the platform

Save

Automatic Updates

☑ Enable Automatic Updates

Select Schedule:

Minute | Hour | Custom

Daily

TIME (24 hour format)

Hour 05 : Minute 00

Upgrade Now

Save

Logs

Mask the following during log collection:

☑ IP
☑ EMAIL

Save

Usage Statistics

☑ Checking this box sends summary statistics back to Anomali to help improve and enhance future Staxx features and performance.

* In agreeing to send data, you have read and understood the license agreement for Staxx - License Agreement platform

Save

Setup settings allow you to configure the following:

- **Threat Feed Schedule**

  Threat Feed Schedule determines the frequency at which latest threat information is downloaded from the STIX/TAXII sites you have configured on Anomali STAXX. This setting is global and applicable to all feeds.

- **Proxy**

  The Proxy setting is for configuring a proxy server for Anomali STAXX.

- **Investigation Platform**

  You can select the Anomali platform that you want to use to investigate an observable.

- **Schedule for automatic updates of Anomali STAXX**

  You do not have to manually download updates and apply them.

  Starting with v1.1 (with the exception of v2.3), Anomali STAXX can be automatically updated when new updates and enhancements become available from Anomali. Anomali STAXX checks for updates based on the schedule configured in this setting. In the **Automatic Updates** section, check the **Enable Automatic Updates** checkbox. This activates automatic updates and expands the section to display additional schedule settings, which are set by default to check for updates once per day. To change your **Automatic Updates** schedule from default values, adjust the additional schedule settings to suit your needs. If changes are made in this section, press **Save** before exiting.

  You have the option to turn off automatic updates if you wish. In the **Automatic Updates** section, remove the check mark from the **Enable Automatic Updates** checkbox.

  Alternatively, starting with v3.4, you can also select the **Upgrade Now** button to download and install available updates immediately.

- **Logs**

  By default, IP address and email addresses are removed from the collected logs. However, if you want to change the default settings, you can do so in the Logs section.

- **Usage Statistics**

  By sending statistics about your Anomali STAXX back to Anomali, you are contributing to the performance and feature improvements of Anomali STAXX. If you enable this option, summary information such as the Anomali STAXX version and build number, number of sites configured, number of imports and pushes performed, is sent back to Anomali once per day. No personally identifiable information is transmitted.

To update these settings on Anomali STAXX:

1. Click ⚙ to the top right of your screen.
2. Click the **Setup** tab.
3. In the *Threat Feed Schedule* section, configure these settings, and click **Save**.
   - Run Every—Specifies how frequently Anomali STAXX will retrieve latest threat feeds.
   - Start After—Specifies the time to wait, starting now, before retrieving threat feeds for the first time.
4. In the *Proxy* section, configure these settings, and click **Save**.

Setting	Description
Use Proxy	Check this box if you want to use a proxy server.
Proxy Host	IP address or hostname of the proxy server. Do not specify the proxy host in the URL format. See Known Issues for more information.
Proxy Port	Port on which proxy server listens for connections.
Username	User name that Anomali STAXX should use to connect to the proxy server. If you want to use NTLM for authentication, use the DOMAIN\username format to enter user name, and check the Use NTLM Auth box.
Password	Password for the user name you entered.
Use NTLM Auth	Check this box if you want to use NTLM authentication for the proxy server.

5. In the *Investigation Platform* section, select the platform you want to use for investigating an observable further and to see its details. You can select from the following options. Click **Save** after making your selection.

Platform	Description	When to select this option...
Anomali STAXX cloud	A platform dedicated for Anomali STAXX clients.	Select this option if you do not have a user account on either Anomali Reports or Anomali ThreatStream. You will need to create an account on https://staxx.anomali.com to use this service. This account is free.
Anomali Reports	An Anomali platform that contains observable details similar to Anomali STAXX cloud.	Select this option if you already have a user account on the Anomali Reports portal.
Anomali ThreatStream	Anomali's threat intelligence portal	Select this option if you already have a user account on Anomali ThreatStream.

6. In the *Automatic Updates* section:

   - Enable Automatic Updates—Enables Anomali STAXX to automatically apply updates when they become available. To turn off automatic updates, **uncheck** this setting.

   - Schedule—Update how frequently Anomali STAXX should check for updates from Anomali, and click **Save**.

7. In the *Logs* section, you can select whether IP addresses and email addresses are excluded from the logs that are collected on Anomali STAXX. By default, this information is excluded from the logs. Click **Save**.

8. (Optional) In the Usage Statistics section, check the box to send summary statistics about your Anomali STAXX back to Anomali. Click **Save**.

User Administration

By default, a user called "admin" with default password "changeme" exists on Anomali STAXX when it is installed. You are prompted to change this user's password during the first-time setup.

You can create additional users once you have completed the first-time setup.

About User Groups

A user can belong to one of the following groups on Anomali STAXX:

- Admin - Users belonging to this group can perform administrative functions such as configuring sites, feeds, administering users, and so on.
- User - Users belonging to this group can view the Dashboard and Activity dashboards, and perform the Import operation. Users in this group cannot see the ⚙ icon; therefore, the functions available under ⚙ (Settings) cannot be performed by these users.

Adding a User

To add a new user:

1. Click ⚙ to the top right of your screen.
2. Click the **User** tab.

> **Note:** If the ⚙ icon is not displayed, you are logged in as a user who does not have the privileges to perform this function.

3. In the Add/Edit User form, configure the following settings.

Setting	Description
Group	The group to which the user will be assigned. See "About User Groups" on the previous page.
Username	User name for the user
Password	Password for the user
Confirm Password	Re-enter the password
First name	First name of the user
Last name	Last name of the user
Organization	Name of the organization to which the user belongs
E-mail	Email address of the user

4. Click **Save**.

Editing a User

To edit a user:

1. Click ⚙ to the top right of your screen.
2. Click the **User** tab.

   > **Note:** If the ⚙ icon is not displayed, you are logged in as a user who does not have the privileges to perform this function.

3. Click the **Edit** button for the user that you want to edit.
4. Update the settings in the Add/Edit User form. You can update all settings except Username.

   See "Adding a User" on the previous page for information about these settings.

5. Click **Save**.

Deleting a User

To delete a user, click **Delete** for the user that you want to delete.

Resetting a User's Password

Only users in the Admin group can reset passwords.

To reset a user password:

1. Click ⚙ to the top right of your screen.
2. Click the **User** tab.

   > **Note:** If the ⚙ icon is not displayed, you are logged in as a user who does not have the privileges to perform this function.

3. Click the **Edit** button for the user whose password you want to reset.
4. Enter the new password in the Password field.
5. Enter the same password in the Confirm Password field.
6. Click **Save**.

Changing a User's Group

To change a user's group:

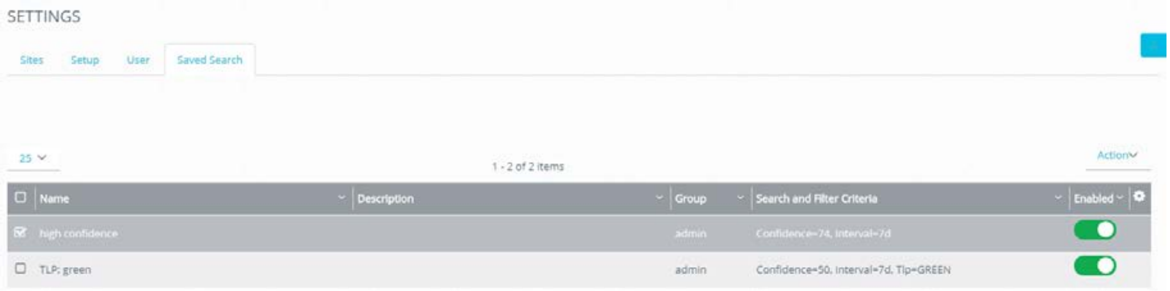
1. Click ⚙ to the top right of your screen.
2. Click the **User** tab.

> **Note:** If the ⚙ icon is not displayed, you are logged in as a user who does not have the privileges to perform this function.

3. Click the **Edit** button for the user whose group you want to change.
4. Update the Group setting.
5. Click **Save**.

Managing Saved Searches

You can enable, disable, and delete previously configured saved searches on the **Saved Search** tab within Anomali STAXX Settings.



1 - 2 of 2 items

□	Name	Description	Group	Search and Filter Criteria	Enabled
☑	high confidence		admin	Confidence=74, Interval=7d	●
□	TLP: green		admin	Confidence=50, Interval=7d, Tlp=GREEN	●

Enabling and Disabling Saved Searches

Saved searches are enabled by default. When you disable saved searches, they no longer appear in the saved search drop down on the Activity page.

To enable and disable saved searches:

1. Click ⚙ to the top right of your screen.
2. Click **Saved Search**.
3. Click the Enabled slider to toggle between enabled and disabled. Saved searches are *disabled* when sliders in the **Enabled** column are gray and *enabled* when green.

   OR

   Select the saved searches you want to enable or disable and then click **Enable** or **Disable** in the **Action** menu.

Deleting Saved Searches

When you delete saved searches, they are permanently removed from your saved search list on Anomali STAXX.

To delete saved searches:

1. Click ⚙ to the top right of your screen.
2. Click **Saved Search**.
3. Select the saved searches you want to delete.
4. Under **Action**, select **Delete**.

Replacing Anomali STAXX's Self-signed Certificate

Anomali STAXX ships with a self-signed certificate. The certificate and the private key files are located in the `/opt/staxx/etc/auth` folder:

- `web_cert.pem`—self-signed certificate
- `web_key.pem`—private key

To replace Anomali STAXX's self-signed certificate with your own self-signed or CA-signed certificate:

1. Replace the `/opt/staxx/etc/auth/web_cert.pem` and `/opt/staxx/etc/auth/web_key.pem` files with your certificate and private key files. Make sure that the replacement files are named the same as shown in the list above.
2. Restart Anomali STAXX, as described in " Anomali STAXX Commands" below.

Anomali STAXX Commands

> **Note:** The following commands must be run as a non-root user.

Start Anomali STAXX: `sudo systemctl start xlink`

Stop Anomali STAXX:`sudo systemctl stop xlink`

Restart Anomali STAXX: `sudo systemctl restart xlink`

Check status of Anomali STAXX: `sudo systemctl status xlink`

Reset admin account password to default for accessing the Anomali STAXX UI:

```
/opt/staxx/bin/xlink reset_passwd
```

Recovering the "anomali" User CLI Password

In the event that you forget the password for the anomali user account, which you set during Anomali STAXX setup from the CLI, Anomali recommends following the instructions below to recover access to your account.

To recover your anomali user CLI password:

1. Follow the instructions listed here: https://wiki.centos.org/TipsAndTricks/ResetRootPassword
2. Once the root shell is displayed, run the following command:

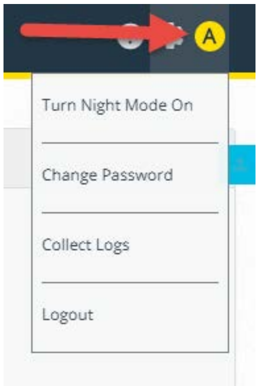
   ```
   passwd anomali
   ```

3. Enter a new password for the anomali user.
4. Log out as the root user.
5. Log in as the anomali user with the new password.

Chapter 8: Other Operations and Settings

This chapter describes settings such as changing to night mode and changing user password. The following topics are covered here:

All of the operations described in this chapter are performed through the drop down menu available by clicking the profile icon on the top right corner of your Anomali STAXX UI screen.



Turn Night Mode On

You can change the background color of the Anomali STAXX UI by switching to "night mode". When you select the night mode, the background color changes to dark gradient blue-gray and the text color is inverted to white for a better reading experience.

The Night Mode setting is a system-level setting, which means all users connected to the Anomali STAXX will experience night mode once you switch to this mode.

To turn on Night Mode, select **Turn night mode on** from the menu shown above.

Selecting the Night Mode color

By default, Night Mode is set to change to dark gradient blue-gray. You can select another color for Night Mode through the Update Profile setting.

When you select Update Profile, a color palette is displayed from which you can pick a new color.

Change Password

To change the currently logged in user's password, select **Change Password** from the menu shown on page 64 and enter the new password in the form that is displayed.

Collect Logs

You can easily collect logs for Anomali STAXX using the **Collect Logs** option. Anomali Customer Support will require logs to troubleshoot Anomali STAXX issues. When requested, select Collect Logs from the menu shown on page 64 and click Collect to start log collection. A .zip file is generated in your browser's default downloads location. Email this file to Anomali Customer Support.

By default, IP address and email addresses are removed from the collected logs. However, if you want to include this information, you can change the default settings as described in "Setup Settings" on page 55.

Appendix: Filter Fields and Indicator Types

This appendix lists the fields against which you can run a search and the indicator types available on Anomali STAXX.

List of Fields

This section lists fields against which the keywords are matched on Anomali STAXX.

Field	Available Values	Description
actor	Any valid actor value	An actor associated with the observable.
campaign	Any valid campaign value	A campaign associated with the observable.
classification	private public	Indicates whether an observable is private or from a public feed and available publicly.
confidence	Any whole number between 0 and 100 0 = false positive 1-100 = Confidence score in increasing order of confidence	Confidence is assigned by Anomali based on quality of data and whether the indicator is in fact malicious.
date_first	Any time and date value that follows the format specified in the Description column.	Time stamp of when the indicator was last seen in Anomali STAXX. Date can be specified as follows: • In this format: *YYYY-MM-DD*T*hh:mm:ss*, where T denotes the start of the value for time. For example, modified_ts > 2014-10-02T20:44:35. • As a relative time unit, in this format: -<n><unit>, where n is a whole number and unit is w, d, h, m, s (for week, days, hour, minutes, and seconds, respectively). For example, -2w denotes two weeks, starting NOW.

date_last	Any time and date value that follows the format specified in the Description column.	Time stamp of when the indicator was last seen in Anomali STAXX. Date can be specified as follows: • In this format: *YYYY-MM-DD***T***hh:mm:ss*, where T denotes the start of the value for time. For example, modified_ts > 2014-10-02T20:44:35. • As a relative time unit, in this format: -<n><unit>, where n is a whole number and unit is w, d, h, m, s (for week, days, hour, minutes, and seconds, respectively). For example, -2w denotes two weeks, starting NOW.
detail	Any valid value for the Tag field.	
feed_name	Any valid value for the STIX/TAXII feed.	Name of the feed that was the source of the observable.
feed_site_ netloc	Any valid value for the STIX/TAXII site.	Site where the feed is located that originated the observable.
id	Any valid value for the observable identifier.	Identifier associated with the observable.
indicator	Observable value	Value associated with the observable.
itype	See "Available Indicator Types" on the next page.	Indicator Type. See "Available Indicator Types" on the next page.
severity	low medium high very-high	Severity assigned to the indicator by Anomali based on the level of impact it can cause to an organization.
source	Any valid source URL or IP address associated with the observable source.	Observable source URL.
tlp	White Green Yellow Red	Traffic Light Protocol level for the observable.

type	Any valid Threat Type value. See the Threat Type column in "Available Indicator Types" below.	Threat type associated with the observable.

Available Indicator Types

The following table lists all available indicator types and their Threat Type mapping.

Indicator Type	Threat Type	Indicator Name	Indicator Description
actor_ip	p2p	Actor IP	IP address associated with a system involved in malicious activity.
adware_domain	adware	Adware Domain	A domain name associated with adware or other Potentially Unwanted Applications (PUA).
anon_proxy	anonymization	Anonymous Proxy IP	IP address of the system on which anonymous proxy software is hosted.
anon_vpn	anonymization	Anonymous VPN IP	IP address associated with commercial or free Virtual Private Networks (VPN).

Indicator Type	Threat Type	Indicator Name	Indicator Description
apt_domain	apt	APT Domain	Domain name associated with a known Advanced Persistent Threat (APT) actor used for command and control, launching exploits, or data exfiltration.
apt_email	apt	APT Email	Email address used by a known Advanced Persistent Threat (APT) actor for sending targeted, spear phishing emails.
apt_ip	apt	APT IP	IP address associated with known Advanced Persistent Threat (APT) actor for command and control, data exfiltration, or targeted exploitation.
apt_md5	apt	APT MD5 File Hash	MD5 hash of a malware sample used by a known Advanced Persistent Threat (APT) actor.
apt_subject	apt	APT Subject Line	Email subject line used by a known Advanced Persistent Threat (APT) actor.

Indicator Type	Threat Type	Indicator Name	Indicator Description
apt_ua	apt	APT User Agent	User agent string used by a known Advanced Persistent Threat (APT) actor.
apt_url	apt	APT URL	URL used by a known Advanced Persistent Threat (APT) actor for command and control, launching web based exploits, or data exfiltration.
bot_ip	bot	Infected Bot IP	IP address of an infected machine acting as an autonomous bot.
brute_ip	brute	Brute Force IP	IP address associated with password brute force activity.
c2_domain	c2	Malware C&C Domain Name	Domain name used by malware for command and control communication.
c2_ip	c2	Malware C&C IP	IP address used by malware for command and control communication.
compromised_domain	compromised	Compromised Domain	Domain name of website or server that has been compromised.

Indicator Type	Threat Type	Indicator Name	Indicator Description
compromised_email	compromised	Compromised Account Email	Email address that has been compromised and/or taken over by a threat actor.
compromised_ip	compromised	Compromised IP	IP address of website or server that has been compromised.
compromised_url	compromised	Compromised URL	URL of the website or server that has been compromised.
ddos_ip	ddos	DDOS IP	IP address associated with Distributed Denial of Service (DDoS) attacks.
dyn_dns	dyn_dns	Dynamic DNS	Domain name used for hosting Dynamic DNS services.
exfil_domain	exfil	Data Exfiltration Domain	Domain name associated with the infrastructure used for data exfiltration.
exfil_ip	exfil	Data Exfiltration IP	IP address used for data exfiltration.
exfil_url	exfil	Data Exfiltration URL	URL used for data exfiltration.
exploit_domain	exploit	Exploit Kit Domain	Domain name associated with the web server hosting an exploit kit or launching web-based exploits.

Indicator Type	Threat Type	Indicator Name	Indicator Description
exploit_ip	exploit	Exploit Kit IP	IP address associated with the web server hosting an exploit kit or launching web-based exploits.
exploit_url	exploit	Exploit Kit URL	URL used for launching web-based exploits.
geolocation_url	anomalous	IP Geolocation URL	URL that can be used to provide IP Geo location services.
hack_tool	hack_tool	Hacking Tool	MD5 hash of general hacking software tools used by threat actors.
ipcheck_url	anomalous	IP Check URL	URL that can be used to provide IP checking services, such as echoing the Internet facing IP address of the client.
mal_domain	malware	Malware Domain	Domain contacted by malware sample; could be for command and control commands, or to check if the client is online.
mal_email	malware	Malware Email	Email address used to send malware through malicious links or attachments.

Indicator Type	Threat Type	Indicator Name	Indicator Description
mal_ip	malware	Malware C&C IP	IP address contacted by malware sample; could be for command and control commands, or to check if the client is online.
mal_md5	malware	Malware MD5 File Hash	MD5 hash of malware sample.
mal_ua	malware	Malware User Agent	User agent string used by malware sample when communicating via HTTP.
mal_url	malware	Malware URL	URL contacted by malware sample when run on an infected host.
p2pcnc	p2p	Peer-to-Peer C&C IP Address	IP address associated with a peer-to-peer command and control infrastructure.
parked_ip	parked	Domain Parking IP	An IP address used for parking newly registered or inactive domain names.
pastesite_url	data_leakage	Paste Site URL	A URL that can be used for sharing pastes or text content anonymously.

Indicator Type	Threat Type	Indicator Name	Indicator Description
phish_domain	phish	Phishing Domain	A domain used to perform phishing or spear phishing attacks or contained in a phishing email.
phish_email	phish	Phishing Email Address	An email address associated with sending phishing or spear phishing emails to victims.
phish_url	phish	Phishing URL	A URL used to perform phishing or spear phishing attacks or contained in a phishing email.
proxy_ip	anonymization	Open Proxy IP	IP address hosting open or anonymous proxy software. Allows user to hide their IP address from target.
scan_ip	scan	Scanning IP	IP address observed to perform port scanning and vulnerability scanning activities.
sinkhole_domain	sinkhole	Sinkhole Domain	A domain name that researchers or security companies typically sinkhole.

Indicator Type	Threat Type	Indicator Name	Indicator Description
sinkhole_ip	sinkhole	Sinkhole IP	An IP address that is known to be used to sinkhole malicious domain names.
spam_domain	spam	Spam Domain	A malicious domain name contained in the SPAM email messages.
spam_email	spam	Spam Email	An email address associated with sending SPAM emails to victims.
spam_ip	spam	Spammer IP	An IP address that is known to send SPAM emails.
spam_url	spam	Spam URL	A malicious URL contained in the SPAM email messages.
speedtest_url	anomalous	Speed Test URL	A URL that can be used to before internet speed tests or bandwidth measurements of the client's network connection.
ssh_ip	brute	SSH Brute Force IP	IP addresses associated with SSH brute force attempts.
suppress	suppress	Suppress	Not a true iType. Used by Arcsight for suppressing false positives.

Indicator Type	Threat Type	Indicator Name	Indicator Description
suspicious_domain	suspicious	Suspicious Domain	A domain name that appears to be registered for suspect reasons, but may not be associated with known malicious activity yet.
tor_ip	tor	TOR Node IP	An IP address operating as part of The Onion Router (TOR) Network, also know as a TOR exit node.
torrent_tracker_url	p2p	Torrent Tracker URL	A URL used for tracking bittorrent file transfer activity.
vpn_domain	anonymization	Anonymous VPN Domain	A domain name associated with commercial or free Virtual Private Networks (VPN).
vps_ip	vps	Cloud Server IP	An IP address that is used for hosting Virtual Private Servers (VPS) or other server rentals.