JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

11100 Johns Hopkins Road • Laurel, Maryland 20723-6099

AOS-16-0458

April 11, 2016
v0.8

(U) Cyber & Threat Intelligence Sharing

(U) MARTI Configuration Guide

T. Christian Anthony
Project Manager
Asymmetric Operations Sector
MARTI@jhuapl.edu

1 Introduction

Mission Analysis and Research of Threat Information (MARTI) is a modular, analytic platform that allows cyber threat intelligence analysts to organize and manage data, share selected information with trusted analysts, analyze malware and threat relationships, and document findings. MARTI is a customized version of the open-source Collaborative Research into Threats (CRITs) software developed by The MITRE Corporation[1]. MARTI uses STIX™ and TAXII™, developed by The MITRE Corporation for the Department of Homeland Security, to enable users to share information as desired between instances of MARTI.

This Configuration Guide provides step-by-step instructions for configuring user and administrative settings. Each organization has its own MARTI instance on an Ubuntu[2] virtual machine that includes a local database, users, sources, services, and data. Users access their local MARTI server via a secure web portal where they can add data, release data to selected feeds, and receive data from feeds to which they are subscribed. Each community of interest that wishes to share data with others has one TAXII™ server that distributes the data feeds according to the configurations in this document.

2 Adding a New User or Editing a Current User in MARTI

Each organization has its own MARTI instance that includes a local database, users, sources, services, and data. This section describes how to add a new user and how to edit an existing user (including changing the password) in MARTI.

1. Log into MARTI as an administrator at https://<MARTI server IP address or hostname>. The default credentials are provided in Appendix A – Default Credentials.
2. From the top menu, select Admin, then CRITs Control Panel, and then Users. [Figure 1]

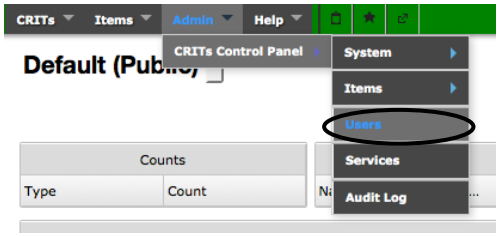

Figure 1. Select Users from the Top Menu

3. Select Add User. [Figure 2]

[1] CRITs license agreement provided at https://github.com/crits/crits/blob/master/LICENSE.
[2] Ubuntu license agreement provided at http://www.ubuntu.com/about/about-ubuntu/licensing.

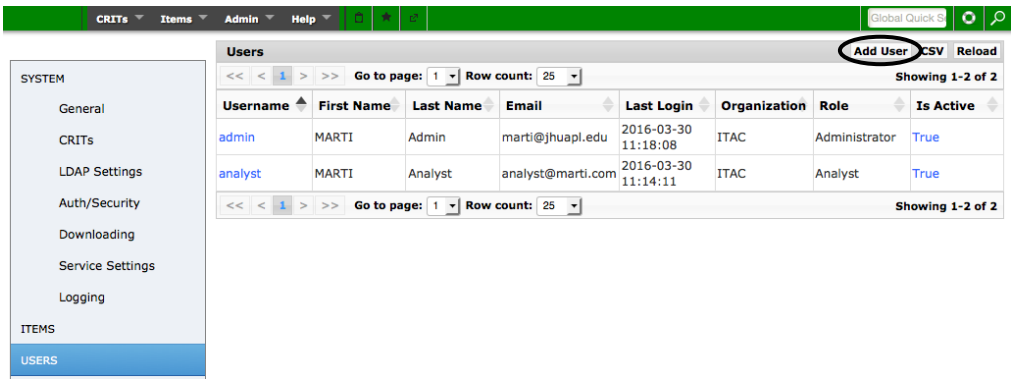

Figure 2. Select Add User

4. To edit a current user (including changing a password), select the username from the top drop-down menu. Enter the desired information and select the desired Sources that will be visible to the user. When complete, select Add/Edit User. Blue fields indicate required information. [Figure 3]

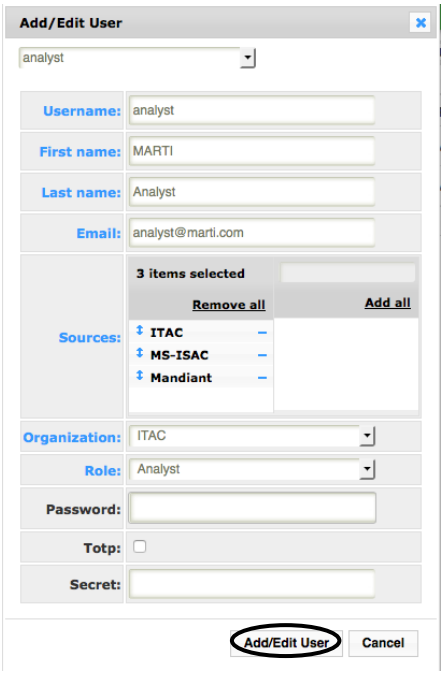

Figure 3. Edit Current User and Select Add/Edit User

5. To add a new user, enter the desired information and select Add/Edit User. Blue fields indicate required information. [Figure 3]

3 Enabling/Disabling a User in MARTI

Users in MARTI can be enabled and disabled as described in this section.

1. Log into MARTI as an administrator. The default credentials are provided in Appendix A – Default Credentials.
2. From the top menu, select Admin, then CRITs Control Panel, and then Users. [Figure 4]

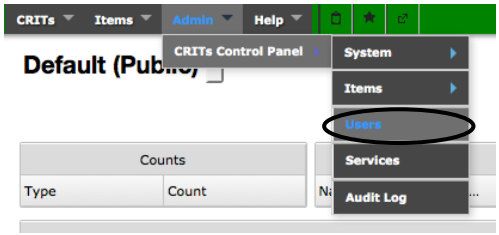

Figure 4. Select Users from the Top Menu

3. Under the Is Active column, click on True or False for the desired username to toggle its status. [Figure 5]

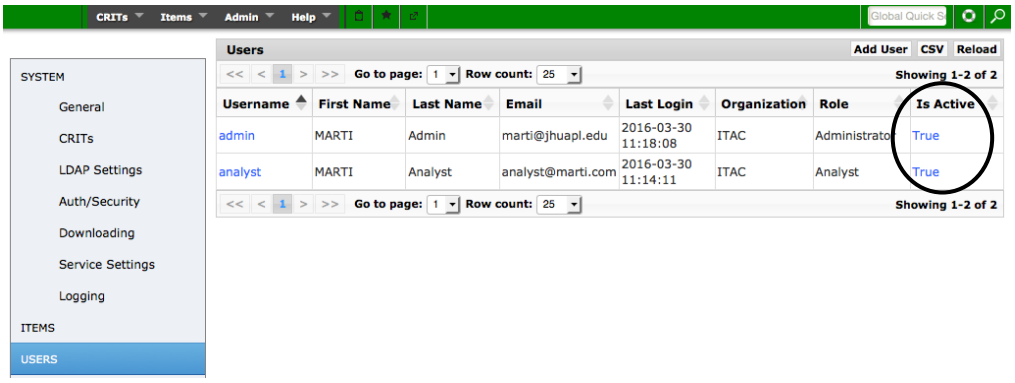

Figure 5. Select True or False to Toggle a User's Status

4 Customizing the Dashboard in MARTI

The dashboard in MARTI is the main screen to keep situational awareness of your data and view recently added items. This section describes how to customize the layout, tables, and columns in a dashboard to suit your organization or individual users.

Dashboards can be public or private. A dashboard that is not Public or Modified is Private to the user. An administrator creates Public dashboards and makes them available for all users. When you edit a Public dashboard that you did not create, MARTI makes a local copy of it and labels it as "Modified." If you delete your Modified version, the system reverts back to the Public dashboard. If the creator of a Public dashboard changes its configuration, you will be notified and given the choice to update to the new version.

1. While on the Dashboard page, the top left drop-down menu shows all of the dashboards that you have available. Select one to switch to that dashboard. [Figure 6]

Figure 6. Select the Drop-down List to Select a Dashboard

2. While on the Dashboard page, select the arrow (<) to view the Dashboard menu. [Figure 7]

Figure 7. Select the Arrow (<) to View the Dashboard Menu

3. The Dashboard menu will now be visible. [Figure 8]

Figure 8. Dashboard Menu

3.1.  Toggle Edit Mode – Allows you to turn editing mode on and off. When selected, the dashboard background is shaded gray and you can rearrange tables by dragging them. Click the check mark to save the new arrangement.

3.2.  Save – Saves changes made to the dashboard.

3.3.  Add Searches – Allows you to add saved searches to the dashboard.

3.4.  Reset – Resets table widths and locations to the default settings.

3.5.  Configurations – Takes you to the Dashboard Configurations page to edit tables, remove tables, or turn on/off tables.

4. To make a dashboard the default dashboard, change its name, or delete it, select the top left arrow in the Configurations list and select the desired action. [Figure 9]

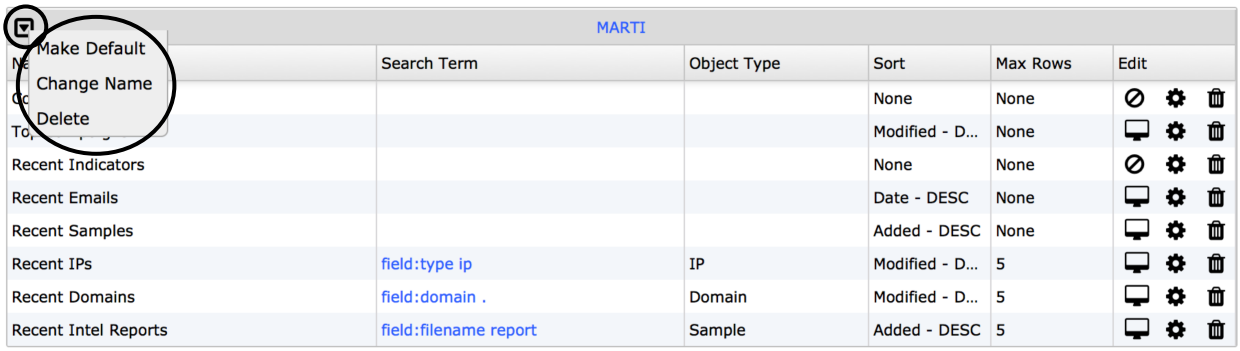

Figure 9. Modify a Dashboard in the Configurations List

5. In the Dashboard Configuration list, the icons in the Edit column allow you to modify the tables in the dashboard.

5.1. Toggle between displaying and hiding the selected table on the dashboard.

5.2. Open a configuration page to edit the selected table.

5.2.1. Drag column headings into/out of the table, rearrange columns, resize columns, and select columns to sort. [Figure 10]

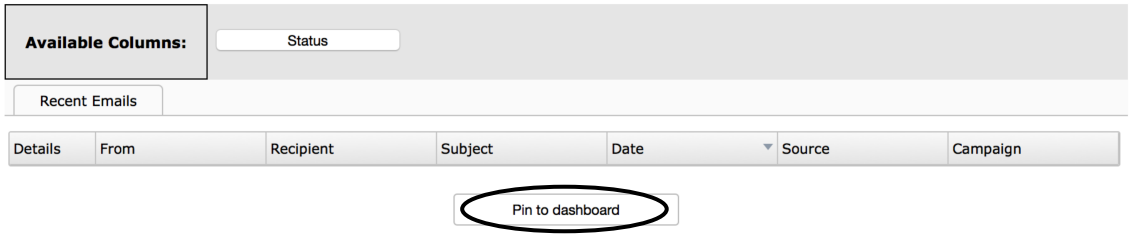

Figure 10. Edit the Table and Then Select Pin to Dashboard

5.2.2. Select the destination dashboard, name the table, and select the maximum number of rows desired. Select Pin when complete. [Figure 11]

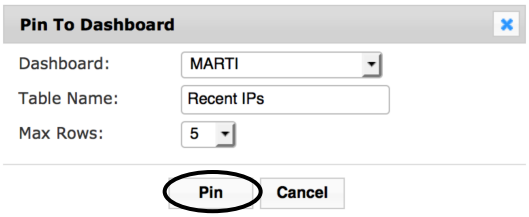

Figure 11. Enter Data to Configure the Table and Select Pin

5.3. Delete the selected table from the dashboard.

6. Create new tables for the dashboard by searching for desired terms and fields.

6.1. From the top menu, search for desired terms (e.g., search for “report” to find all entries with that string). [Figure 12]

Figure 12. Search for Strings or Fields

6.2. To make this search a table in your dashboard, select Configure for Dashboard at the bottom left. [Figure 13]

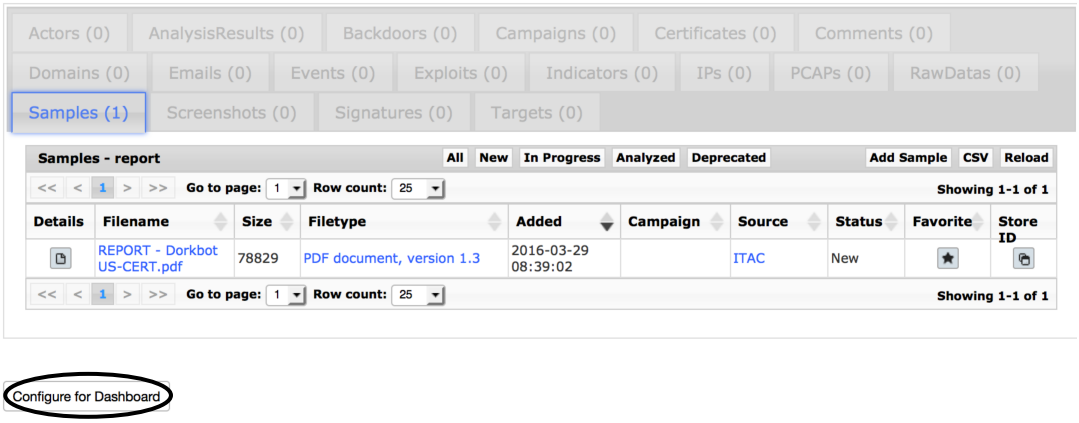

Figure 13. Select Configure for Dashboard

6.3. Drag column headings into/out of the table, rearrange columns, resize columns, and select columns to sort. [Figure 14]

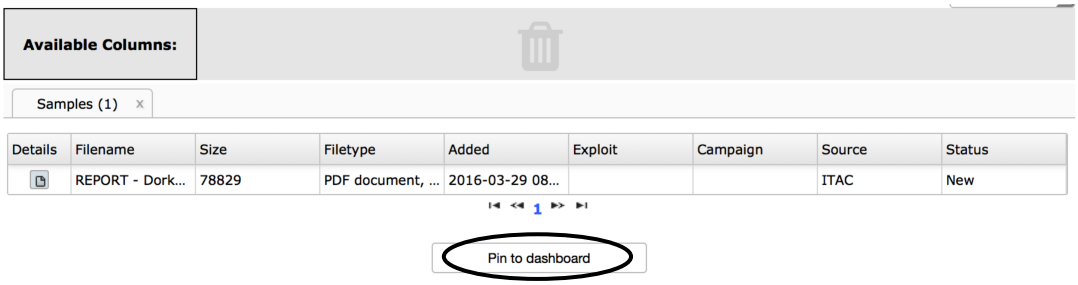

Figure 14. Configure the Table and Then Select Pin to Dashboard

6.4. Select the destination dashboard, name the table, and select the maximum number of rows desired. Select Pin when complete.

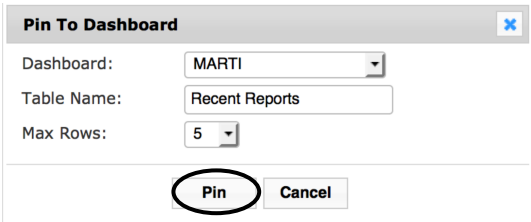

Figure 15. Enter Data to Configure the Table and Select Pin

5 Customizing the MARTI Bottom Banner

The bottom banner in MARTI shows your local organizational information. This information is also used to identify your organization when you send data via STIX™ and TAXII™ to others.

1. Log into MARTI as an administrator. The default credentials are provided in Appendix A – Default Credentials.
2. From the top menu, select Admin, then CRITs Control Panel, then System, and then CRITs Configuration. [Figure 16]

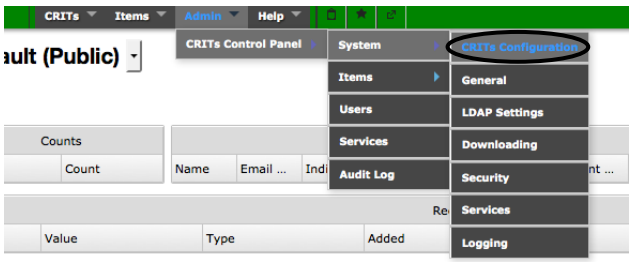

Figure 16. Select CRITs Configuration from the Top Menu

3. Edit the desired information. The Company name field is used to identify your organization when sending information to others via STIX™ and TAXII™. Blue fields are required. Select Submit; a small red "Success!" will appear at the top of the page when complete.

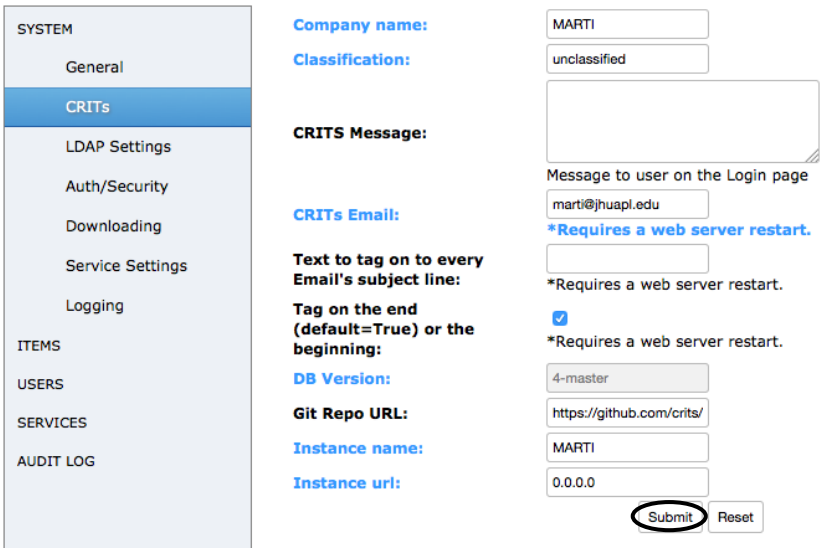

Figure 17. Edit Desired Information and Select Submit

6 Adding a New Feed to Yeti

Adding a new data feed for the community of interest requires configurations in each participating organization's MARTI server as well as the TAXII™ server. MARTI uses Yeti as the TAXII™ server; this section describes the steps to establish a new feed in the Yeti server.

1. Open a web browser and navigate to the Yeti server at https://<yeti IP or domain name>/admin, where <yeti IP or domain name> is the IP address or domain name of the Yeti server.
2. Log into the Yeti server. Default credentials are listed in Appendix A – Default Credentials.

3. Add a new Data Collection.
   3.1. Click on TAXII_SERVICES. [Figure 18]

Figure 18. Select TAXII_SERVICES

   3.2. Click on the +Add next to Data Collections. [Figure 19]

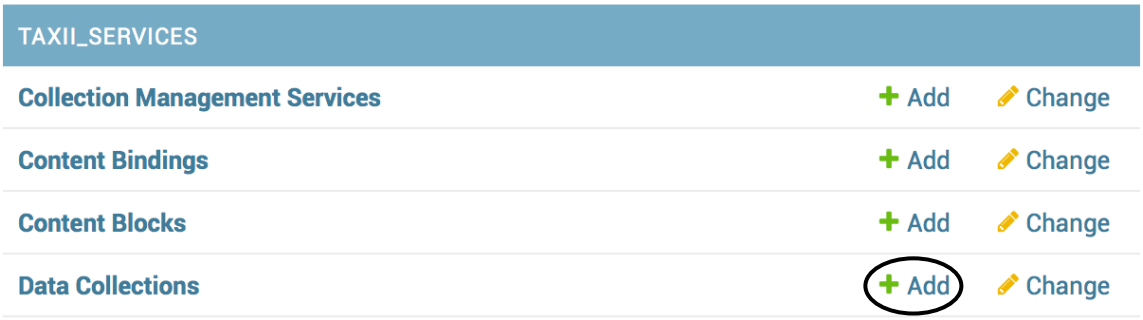

Figure 19. Select +Add Next to Data Collections

   3.3. Add the new feed name in Data Collections.
      3.3.1. Enter the name of the new feed.
      3.3.2. Type: Data Feed
      3.3.3. Enabled = True
      3.3.4. Accept all content = True
      3.3.5. Select Save.

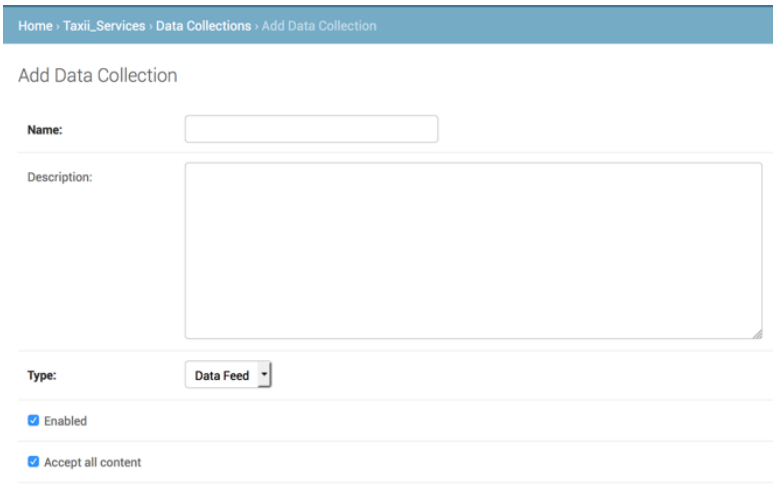

Figure 20. Add Data Collection for New Feed Name

4. Add feed to Inbox Services so users can send to the new feed.
   4.1. Click on TAXII_SERVICES.
   4.2. Click on Inbox Services. [Figure 21]
   4.3. Click on Default Inbox Services.
   4.4. Scroll to the bottom and select all desired entries in Data collections. [Figure 22]
   4.5. Select Save.
5. Add feed to Poll Services so users can receive from the new feed.
   5.1. Click on TAXII_SERVICES.
   5.2. Click on Poll Services. [Figure 21]
   5.3. Click on Default Poll Services.
   5.4. Scroll to the bottom and select all desired entries in Data collections. [Figure 22]
   5.5. Select Save.

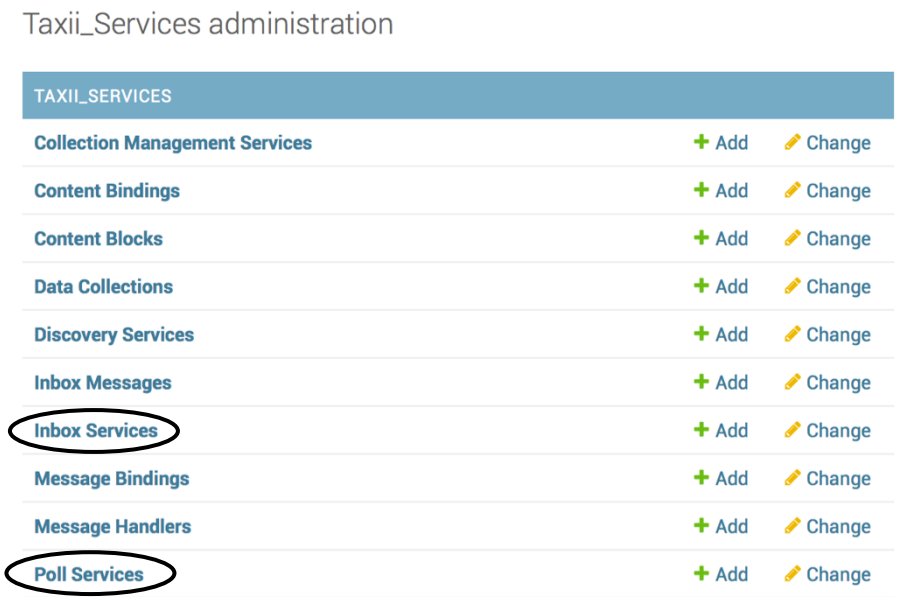

Figure 21. Select Inbox Services and Then Poll Services

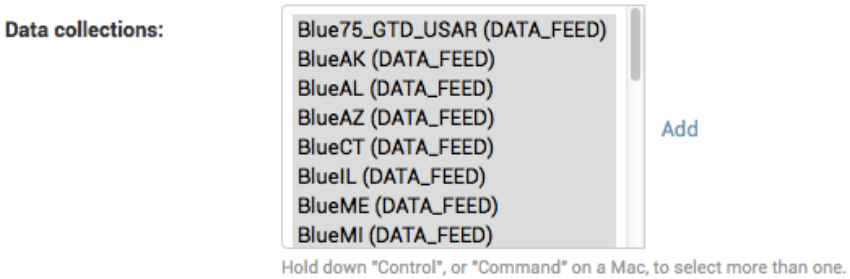

Figure 22. Select All Desired Data Collections (i.e., Feeds) for Inbox and Poll Services

7 Adding a New Source to MARTI

A Source denotes a category of information that you can allow selected users to view. This could be information from a certain report or partner, such as the Verizon Data Breach Report or US-CERT Alerts. Sources serve two purposes in MARTI: the first is as a local tag on the data to control per-user visibility, while the second is to send and receive information from data feeds in a community of interest. These Source names are assigned to selected users for their ability to view that data feed, and they also allow the user to send information to that data feed.

This section describes how to create a new Source in MARTI for both purposes. Once a Source has been created, Section 8 describes how to configure a Source to be a data feed for information sharing across a community of interest.

1. Log into MARTI as an administrator. The default credentials are provided in Appendix A – Default Credentials.
2. Add the new Source to MARTI.
   2.1. From the top menu, select Admin, then CRITs Control Panel, then Items, and then Sources. [Figure 23]

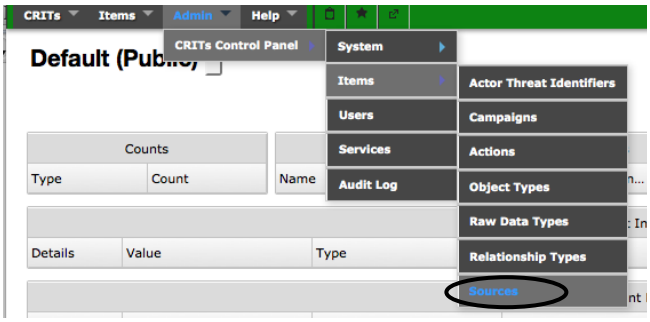

Figure 23. Select Sources from the Top Menu

   2.2. Select Add SourceAccess in the top right. [Figure 24]

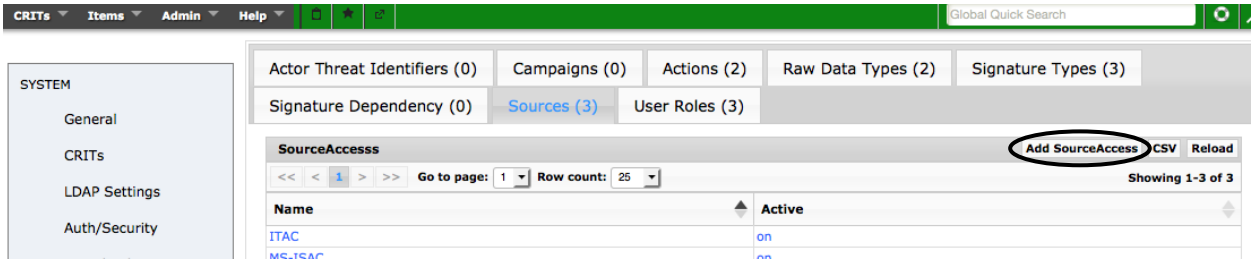

Figure 24. Select Add SourceAccess

   2.3. Enter the new Source name and select New Source. [Figure 25]

Figure 25. Enter the New Source Name and Select New Source

2.4. After the Source is successfully added, close the window with the X. [Figure 26]

Figure 26. Close the Window with the X

3. Add the new Source to the desired users so they can view entries from this Source and assign new entries to this Source.

   3.1. From the top menu, select Admin, then CRITs Control Panel, and then Users. [Figure 27]

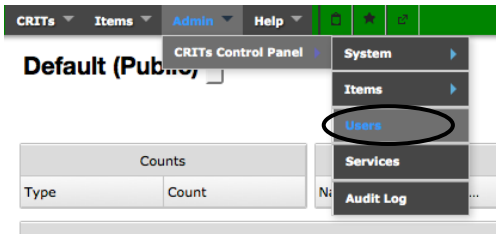

Figure 27. Select Users from the Top Menu

   3.2. Select the username you wish to edit. [Figure 28]

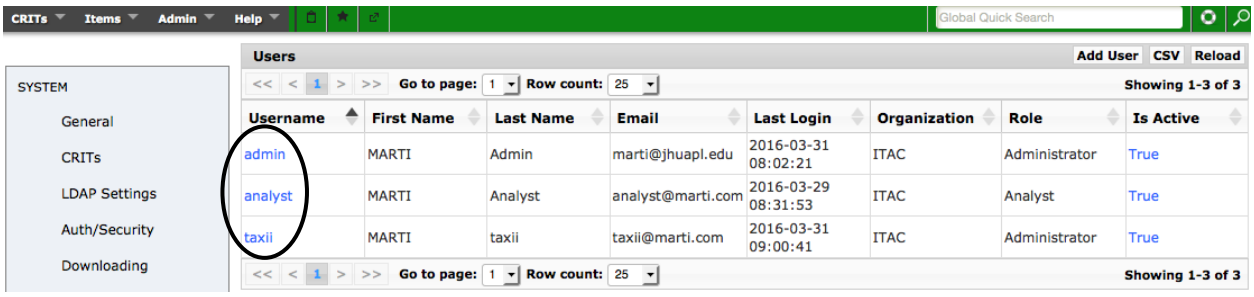

Figure 28. Select the Username to Edit

   3.3. Add the new Source using the plus sign (+) and then select Add/Edit User.

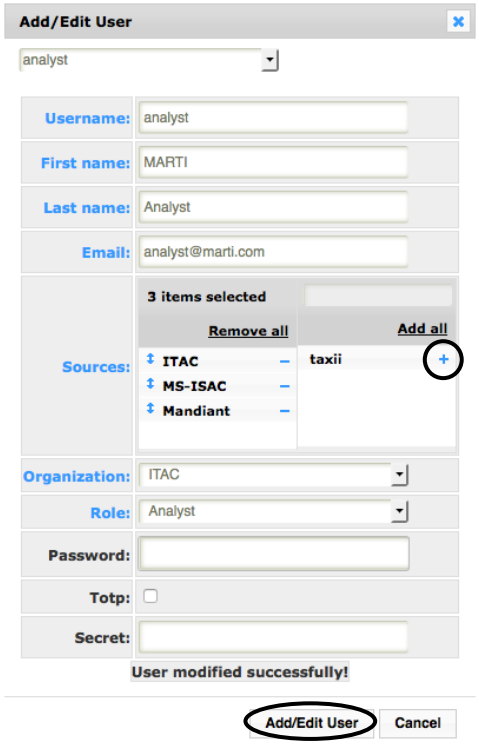

Figure 29. Select + to Add Desired Sources and Then Select Add/Edit User

8 Adding a New Feed to MARTI

Users release data to selected feeds and receive data from feeds to which they are subscribed. This section details how to add a new feed to MARTI.

1. Log into MARTI as an administrator. The default credentials are provided in Appendix A – Default Credentials.
2. Add the new feed name as a Source to MARTI as described in Section 7.
3. Configure the local TAXII service to send and receive the new feed.
   3.1. From the top menu, select Admin, then CRITs Control Panel, and then Services. [Figure 30]

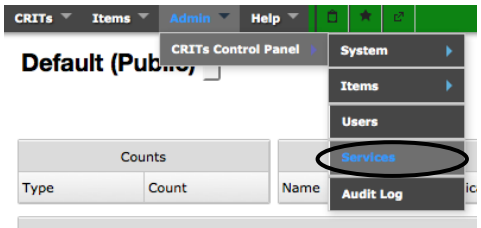

Figure 30. Select Services from the Top Menu

   3.2. Select taxii_service to edit the settings. [Figure 31]

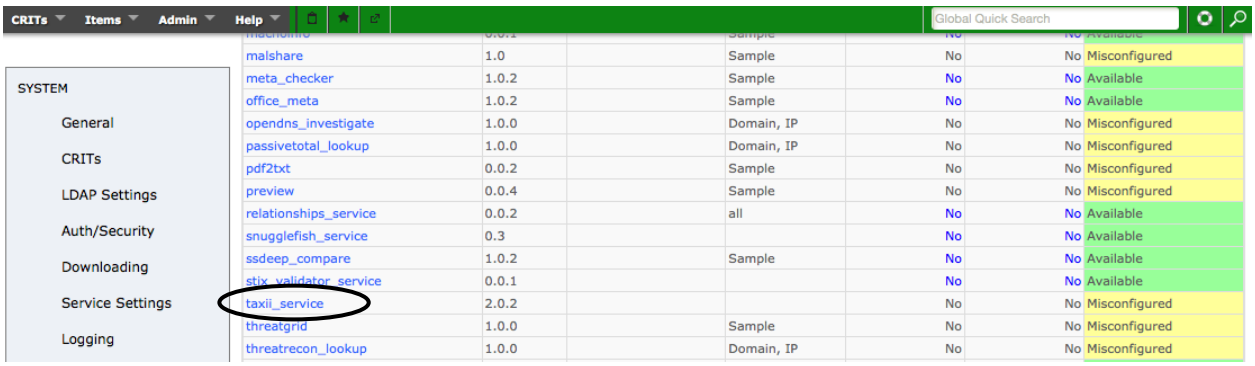

Figure 31. Select taxii_service

3.3. Select Edit to modify the feeds. [Figure 32]

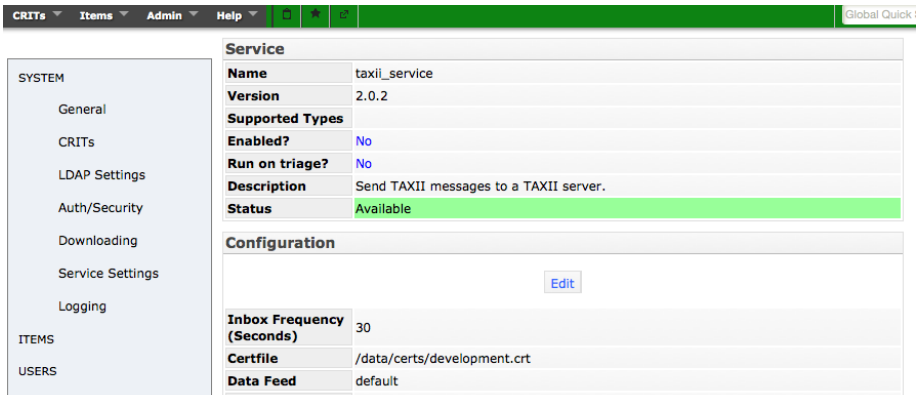

Figure 32. Select Edit to Modify the Feeds

3.4. Configure the feeds as desired for polling and inboxing. Each feed is on its own line and the format is <feed>,<feed>,<polling true/false>,<inboxing true/false>. [Figure 34]

3.4.1. To configure a feed that you can receive from but not send to, set polling to true and inboxing to false (Ex: feed1,feed1,true,false).

3.4.2. To configure a feed that you cannot receive from but can send to, set polling to false and inboxing to true (Ex: feed1,feed1,false,true).

3.4.3. To configure a feed that you can receive from and send to, set polling to true and inboxing to true (Ex: feed1,feed1,true,true).

4. Select Submit when finished. [Figure 33]

Figure 33. Set Configuration for Feeds to Poll and Inbox

9 Configure Taxii_Service in MARTI

The taxii_service controls the sending and receiving of information to and from MARTI to others in a community of interest. This section describes how to establish the basic configuration settings after the data feeds are created. Creating new data feeds in MARTI is described in Sections 7 and 8.

1. Log into MARTI as an administrator. The default credentials are provided in Appendix A – Default Credentials.
2. Verify that the MARTI Services are referring to the correct Directory.
   2.1. From the top menu, select Admin, then CRITs Control Panel, then System, and then Services. [Figure 34]

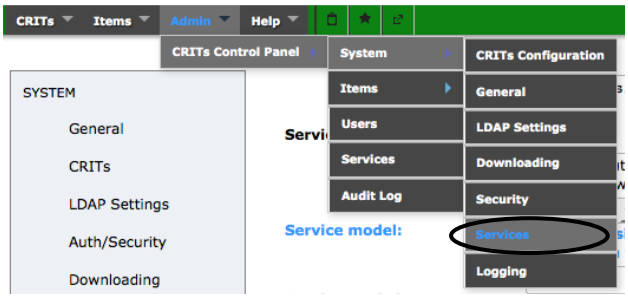

Figure 34. Select System and Then Services from the Top Menu

   2.2. Verify that the Service Directories is listed as /opt/crits/crits_services. Enter the correct directory if it is not valid and select Submit. [Figure 35]
   2.3. If this Directory is incorrect and you enter a new one, the MARTI web server requires a restart as described in Section 11 in order to load the new services.

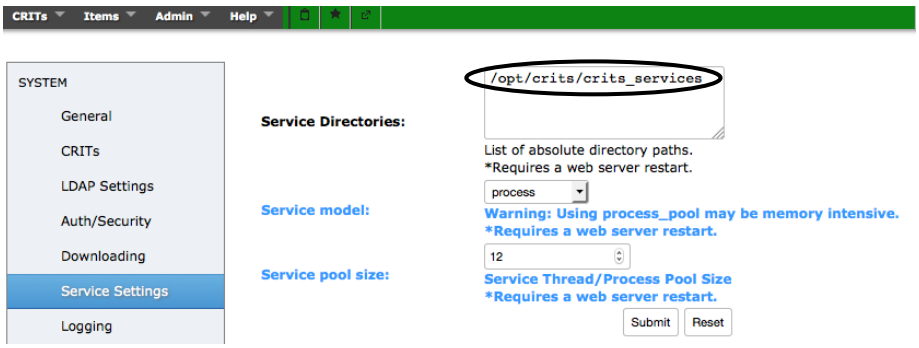

Figure 35. Verify the Entry for Service Directories

3. From the top menu, select Admin, then CRITs Control Panel, and then Services. [Figure 36]

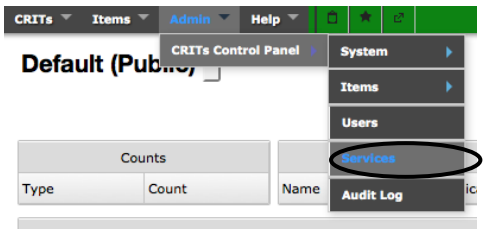

Figure 36. Select Services from the Top Menu

4. Select Edit to edit the service settings. If the service is not yet configured, an error message will appear showing the required entries. [Figure 37]

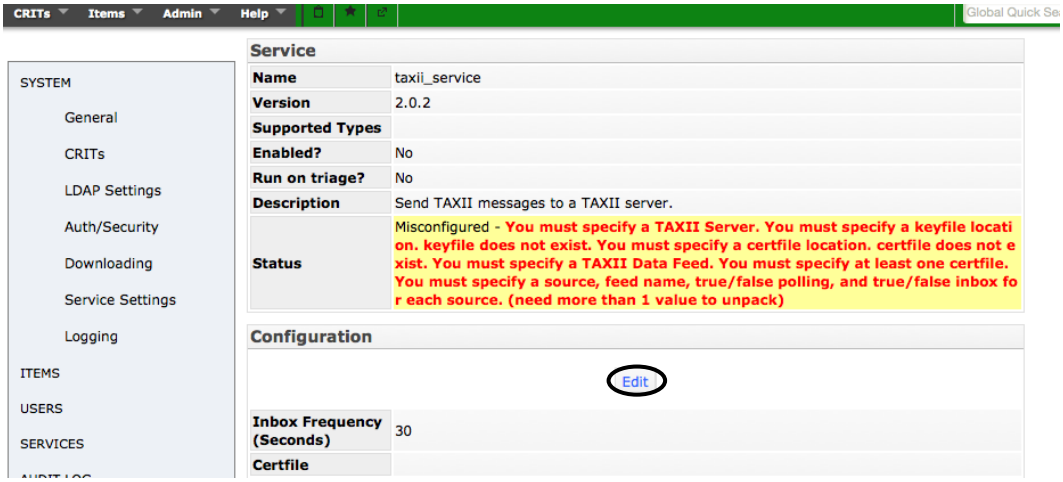

Figure 37. Select Edit

5. For the Hostname, enter the IP address of the TAXII™ server used for your community of interest.
6. Enter all other information as shown below. [Figure 38]
   6.1. Keyfile: /data/certs/development.key (or the key provided by your TAXII™ server)
   6.2. Certfile: /data/certs/development.crt (or the certificate provided by your TAXII™ server)
   6.3. Data Feed: default
   6.4. Select the check boxes for HTTPS, Events, Auto Polling, and Auto Inbox.
   6.5. Set Polling Frequency and Inbox Frequency to the desired number of seconds; 10–30 seconds is recommended.

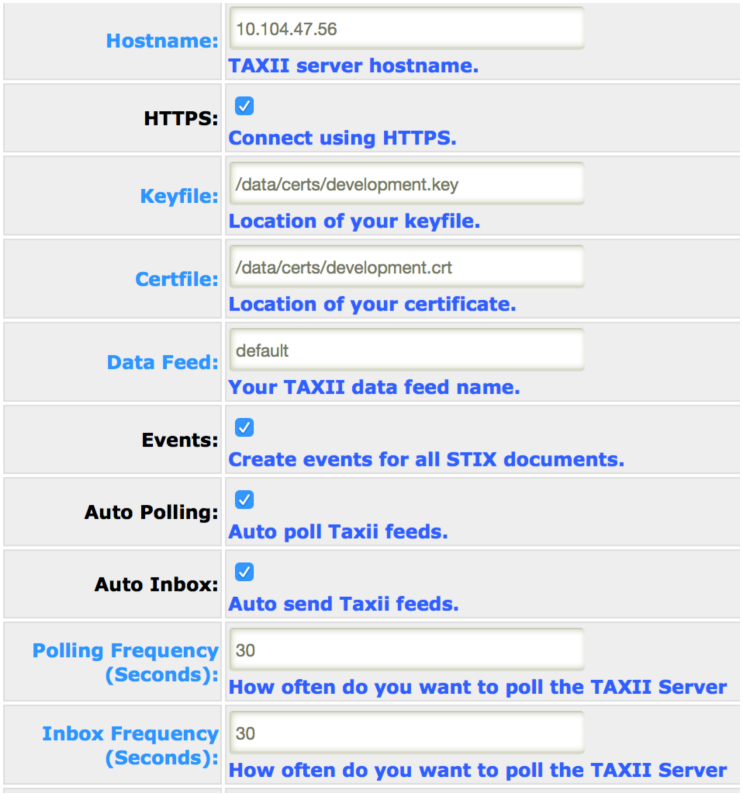

Figure 38. Set taxii_service Configuration as Shown

7. Configure the feeds as desired for polling and inboxing. Each feed is on its own line and the format is <feed>,<feed>,<polling true/false>,<inboxing true/false>. [Figure 39]
   7.1. To configure a feed that you can receive from but not send to, set polling to true and inboxing to false (Ex: feed1,feed1,true,false).
   7.2. To configure a feed that you cannot receive from but can send to, set polling to false and inboxing to true (Ex: feed1,feed1,false,true).
   7.3. To configure a feed that you can receive from and send to, set polling to true and inboxing to true (Ex: feed1,feed1,true,true).
8. Select Submit when finished. [Figure 39]

Figure 39. Set Configuration for Feeds to Poll and Inbox

9. At the top of the screen, verify that there is a Yes next to Enabled. If there is a No, then click on No to enable the taxii_service. [Figure 40]

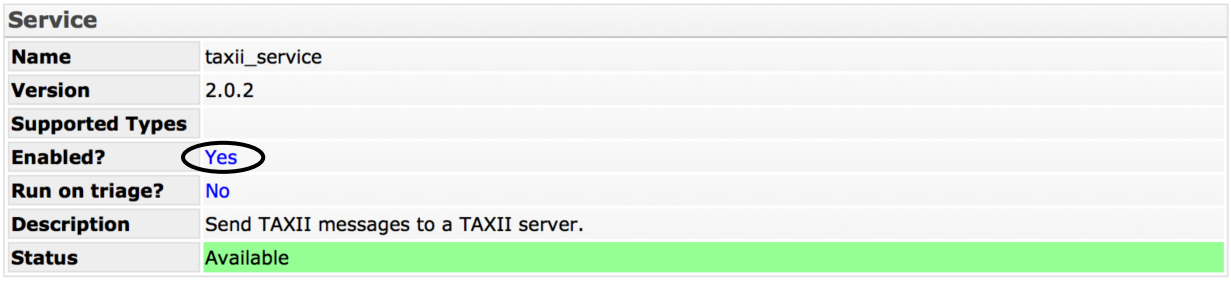

Figure 40. Toggle Yes/No to Enable/Disable the taxii_service

10. If the taxii_service is recently enabled, the MARTI web server requires a restart as described in Section 11 in order to load the new service.

10 Developing and Using Additional Services

MARTI is a customized version of the CRITs open-source library. The Application Program Interface (API) enables the development of customized services for data collection, analysis, and visualization. MARTI has significant modifications to the core of CRITs as well as the taxii_service. The remainder of the API and additional services is the same as the standard CRITs library. For information about how to use the API and services to customize your MARTI interfaces and user experience, visit https://github.com/crits/crits/wiki/.

11 Restarting the MARTI Web Server

Some configuration settings require a web server restart before they will take effect. This section describes how to restart the web server.

1. Open a terminal window and connect to the web server via Secure Shell (SSH). The default credentials are listed in Appendix A – Default Credentials.
2. Use the following format “ssh <server user>@<server domain name or IP>” (Ex: ssh crits@10.10.10.10).
3. Follow the prompts to enter the user password and complete the login.
4. Enter “sudo service apache2 restart”. Follow the prompt to enter the root administrator password for the server.

12 Appendix A – Default Credentials

The following credentials are delivered by default with MARTI. Good security practice dictates changing these default usernames and passwords.

The Yeti Virtual Machine and web page have username “yeti” and password “passw0rd”, with a zero in place of the letter “o”. Similarly, the MARTI virtual machine has username “crits” and

password “passw0rd”. Neither the Yeti nor the MARTI virtual machines have a root account, so use “sudo” for any commands that require root privilege.

The MARTI web portal has three default accounts.

1. The primary administrator account is username “admin” and password “Passw0rd”, with a capital letter “P” and the number zero in place of the letter “o”.
2. The default user is an analyst (i.e., user without administrator privileges) with username “analyst” and password “Passw0rd”, with a capital letter “P” and the number zero in place of the letter “o”.
3. The third default account is an administrator account with username “taxii” and password “Passw0rd” and is used for sending and receiving STIX™ messages via TAXII™. This account needs to remain unmodified (though the password should be changed) for the sending and receiving to function properly.

When a user downloads a sample from MARTI, these files are password protected to reduce the likelihood of accidental malware infections. The default password for these files is “infected”.