

Content Exchange User Guide



Content Exchange User Guide

Updated  14 Nov 2017

NOTICE OF RESTRICTIONS

This document includes information that shall not be disclosed outside of Raytheon. It shall not be further duplicated, used, or disclosed for any purpose unless explicitly authorized by Raytheon. The information subject to this restriction is contained in all sheets marked with the following legend: "Use or disclosure of any information contained herein is subject to the restrictions set forth on the title page of this document."

- 1 Content Exchange User Guide
 - 1.1 Updated 14 Nov 2017
- 2 Product Overview
- 3 Architecture
- 4 Login
- 5 Navigation
 - 5.1 Primary Navigation
 - 5.2 User Menu
 - 5.3 Administration
 - 5.4 Client Subscriptions
 - 5.5 My Account
 - 5.6 User Guide
 - 5.7 Version
- 6 General Interface
 - 6.1 My Dashboard
 - 6.2 Content
 - 6.2.1 Add Content
 - 6.2.2 Modify Content
 - 6.2.3 View Content
 - 6.2.4 Workflow States
 - 6.3 Deployment
 - 6.3.1 Workflow States
 - 6.3.2 Deploy
 - 6.3.3 Recall
 - 6.3.4 Expired
 - 6.4 Declining Content or Deployment
- 7 Administration Interface
 - 7.1 Accounts
 - 7.1.1 User Permissions
 - 7.2 Attack Phases
 - 7.2.1 Add Attack Phase
 - 7.2.2 Modify Attack Phase
 - 7.3 Dependencies
 - 7.3.1 Custom
 - 7.3.1.1 Add Custom Input
 - 7.3.1.2 Modify Custom Input
 - 7.3.2 Logs
 - 7.3.2.1 Add Log
 - 7.3.2.2 Modify Log
 - 7.3.3 Packets
 - 7.3.3.1 Add Packet
 - 7.3.3.2 Modify Packet
 - 7.4 Platforms
 - 7.4.1 Add Platform

- 7.4.2 [Modify Platform](#)
 - 7.5 [Protocols](#)
 - 7.5.1 [Add Protocol](#)
 - 7.5.2 [Modify Protocol](#)
 - 7.6 [Settings](#)
 - 7.6.1 [Modify Setting](#)
 - 7.7 [Threat Actors](#)
 - 7.7.1 [Add Threat Actor](#)
 - 7.7.2 [Modify Threat Actor](#)
 - 7.8 [Threat Categories](#)
 - 7.8.1 [Add Threat Category](#)
 - 7.8.2 [Modify Threat Category](#)
- 8 [Client Interface](#)
 - 8.1 [Clients](#)
 - 8.1.1 [Show My Clients](#)
 - 8.1.2 [Show All Clients](#)
 - 8.1.3 [Add Client](#)
 - 8.1.4 [Modify Client](#)
- 9 [Appliance Interface](#)
 - 9.1 [Add Appliance](#)
 - 9.2 [Edit Appliance](#)
- 10 [Search and Filter](#)
- 11 [Signing Out](#)
- 12 [Glossary](#)

Product Overview

Content Exchange is an application which stores rules, queries and other content used to support and provide Raytheon Cyber Services.

Architecture

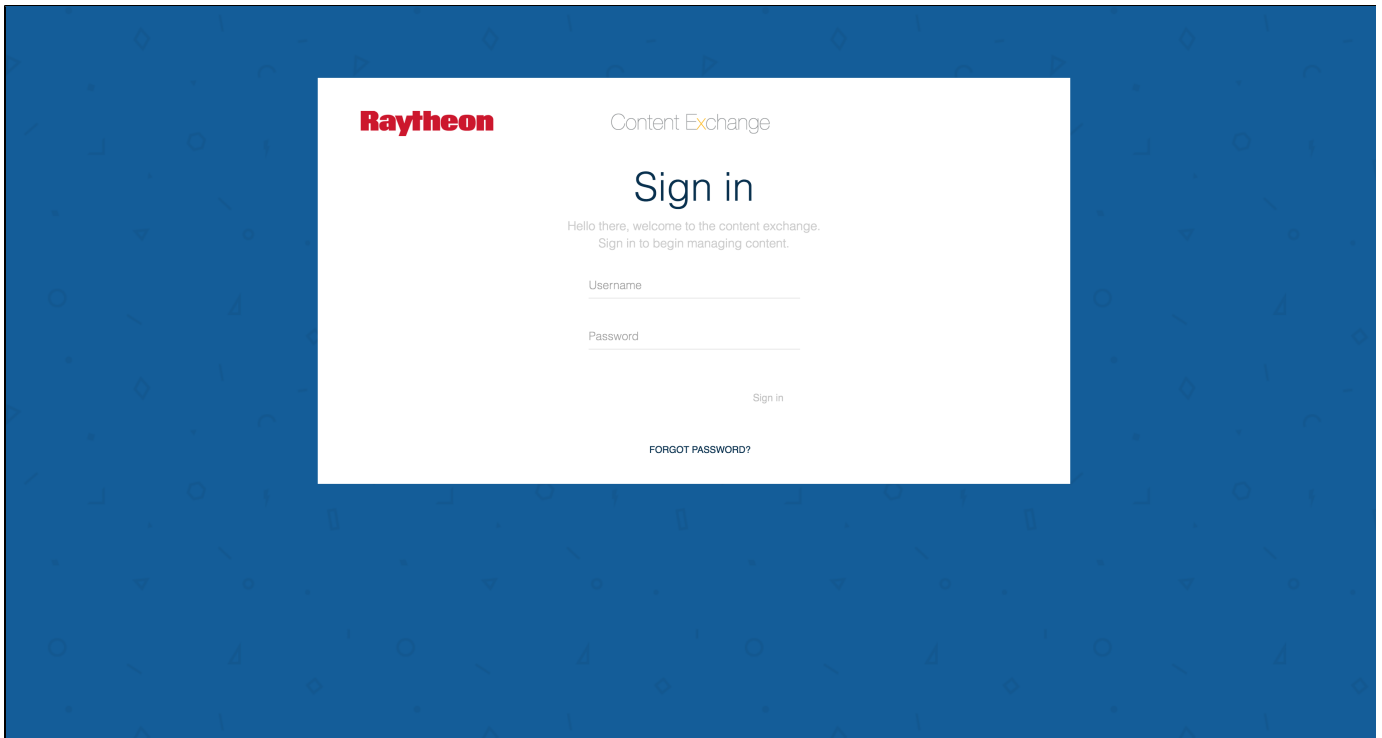
This application uses a Django API server and Angular user interface.

Login

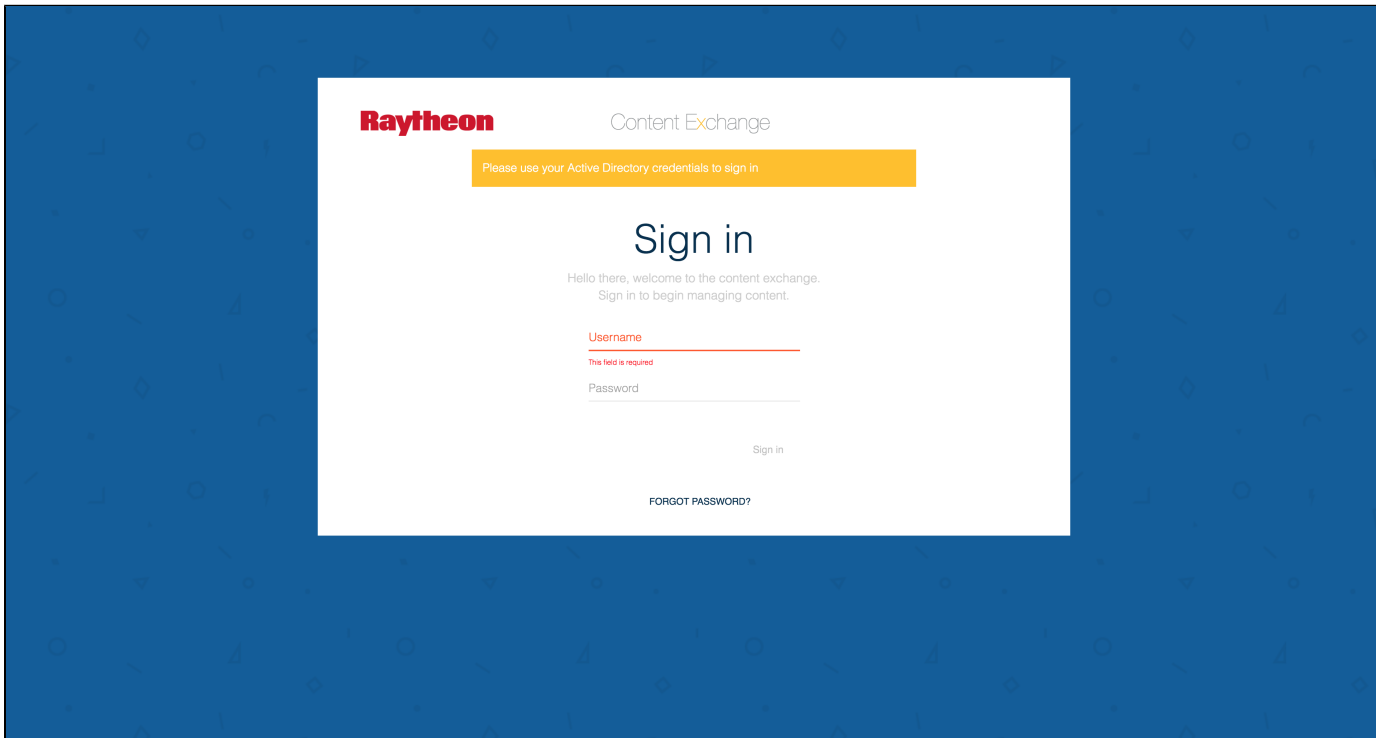
Enter your Username and Password, then click the

Sign in

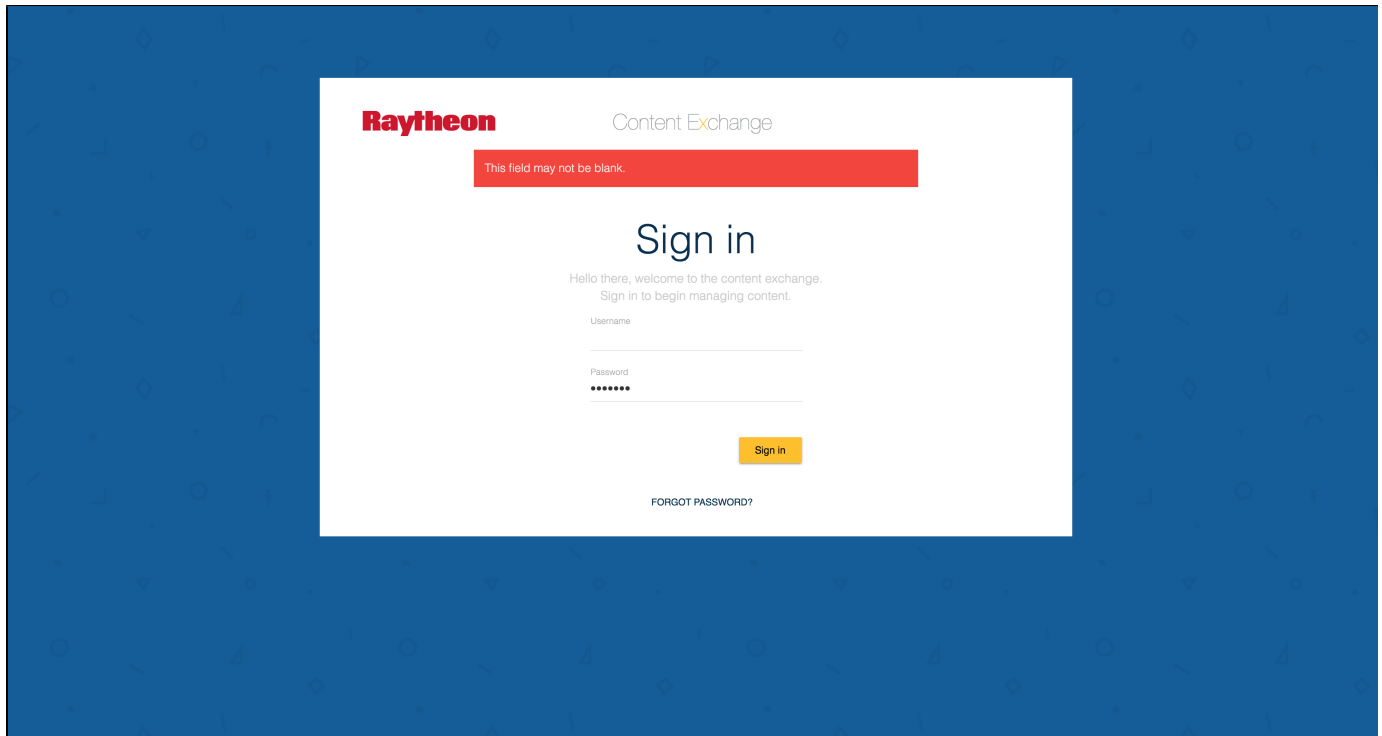
button.



If you forgot your password, you can click "Forgot Password". You will then be prompted with a message to use your Active Directory credentials.



If the Active Directory does not recognize your account, you will be unable to log in. You will be prompted for required fields if any are missing.



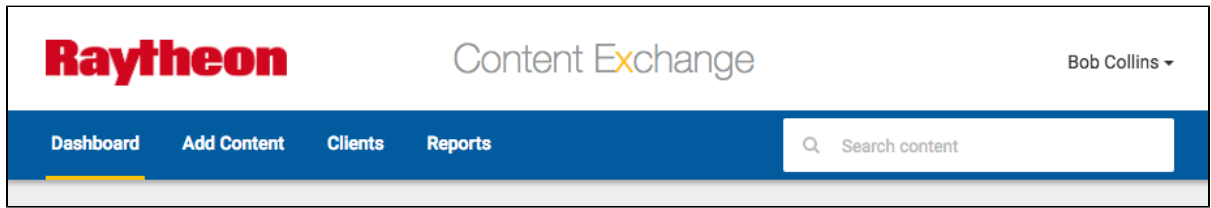
After successfully signing in, your personal Dashboard screen will display.

Navigation

Primary Navigation

The primary navigation options are displayed after a successful sign in. The options displayed depend on the user's access rights. All users have access to the Dashboard, Clients and Reports.

If the user has the access rights to add new content into the application, the 'Add Content' option will also be available in the navigation menu.



User Menu

Clicking on the user's name will display the user menu. Users in the Administrator group will see the 'Administration' menu option. The other menu options are available for all users.

Raytheon

Content Exchange

My Dashboard

Add Content

Clients

Reports

Search content

My Dashboard

Content

Develop 6

Deploy 0

Recall 0

Development 1

ELSA sampletitle

08/22/2017 7:12 PM

QA Review 2

Splunk - Queries

TrickyBot

08/23/2017 5:37 PM

ELSA

Bobs wicked title

08/22/2017 7:12 PM

ENG Review 2

ArcSight - Active Channel

Rules

test 2

08/22/2017 7:12 PM

ArcSight - Rules

My first title

08/23/2017 5:38 PM

SME Review 1

NetWitness - App Rules

rigEK

08/22/2017 7:12 PM

Bretny Khamphavong

Administration

Client Subscriptions

My Account

User Guide

Sign Out

Content Exchange 1.3.1

Administration

Users in the Administrator group has access to the Administration screens to manage user accounts and list data. Click the 'Administration' option in the User Menu to display the administration screen. See "[Administration Interface](#)" for instructions for Accounts.

Raytheon

Content Exchange

Bob Collins

Dashboard

Add Content

Clients

Reports

Search content

Accounts

Clients

Dependencies

Phases

Platforms

Protocols

Settings

Threat Actors

Threat Categories

Accounts

Name	Groups	Email
Bob Collins	Administrator, Author, QA	bcollins@beyondmanagedsecurity.com
Brandon Denker	Administrator	bdenker@beyondmanagedsecurity.com
Bretny Khamphavong	Administrator	bkhamphavong@beyondmanagedsecurity.com
David Amacker	Administrator	damacker@beyondmanagedsecurity.com
Jeremiah Bess	Administrator	jbess@beyondmanagedsecurity.com
Joseph Chlanda	Administrator	jchlanda@beyondmanagedsecurity.com
Kevin Li		kli@beyondmanagedsecurity.com
Mark Bartlett	Administrator, Author, Engineer	mbartlett@beyondmanagedsecurity.com
Ross Mathews	Administrator	rmathews@beyondmanagedsecurity.com
William Miskimen	Administrator	bmiskimen@beyondmanagedsecurity.com

Client Subscriptions

As a user, you have the option to subscribe to clients by clicking 'Client Subscriptions' in the dropdown.

The screenshot shows the 'Client Subscription' modal window. It has a title bar with a close button. Inside, there are two columns: 'Clients Available' on the left and 'Clients Subscribed' on the right. The 'Clients Available' column contains a list of client names: Client 0, Client 1, Client 2, Test Client 0, Test Client 1, Test Client 10, Test Client 11, Test Client 12, Test Client 13, Test Client 14, Test Client 15, Test Client 2, Test Client 3, Test Client 4, Test Client 5, Test Client 6, Test Client 7, Test Client 8, and Test Client 9. The 'Clients Subscribed' column contains a list of client names: Test Client 13, Test Client 15, Test Client 5, Test Client 8, and Test Client 9. At the bottom right of the modal, there are two buttons: 'Cancel' and 'Update'.

Choose the clients you would like to subscribe to by clicking on the client name in the 'Clients Available' list on the left and dragging it over to the right.

Click



after selecting your subscribed clients, or



if you wish to exit.

My Account

User Guide

On any screen, you can download this user guide and save it to your computer in a PDF file format by choosing the User Guide dropdown menu option.

Version

On any screen, you can view the version details of the application by clicking on the user's name in the user menu. A version number for Content Exchange will be listed at the bottom of the dropdown.

General Interface

My Dashboard

All users have access to their personal Dashboard which displays Content they have created or are responsible for reviewing. Click on the "My Dashboard" option in the primary navigation menu.

Raytheon

Content Exchange

author TestUser

My Dashboard

Add Content

Clients

Search

Q

Search content

My Dashboard

Content

Develop 12

Deploy 0

Recall 0

Development3

ArcSight - Active Channel Rules

Test Title 69

10/18/2017 4:43 PM

ArcSight - Rules

Test Title 8

10/18/2017 4:42 PM

Bluecoat - Security Analytics

Test Title 135

10/19/2017 9:32 AM

QA Review3

ArcSight - Active Channel Rules

Test Title 347

10/18/2017 4:43 PM

ArcSight - Rules

Test Title 19

10/18/2017 4:42 PM

Bluecoat - Security Analytics

Test Title 999

10/18/2017 4:42 PM

ENG Review3

ArcSight - Active Channel Rules

Test Title 908

10/19/2017 9:37 AM

ArcSight - Rules

Test Title 543

10/18/2017 4:42 PM

Bluecoat - Security Analytics

Test Title 732

10/19/2017 9:41 AM

SME Review3

ArcSight - Active Channel Rules

Test Title 24

10/18/2017 4:43 PM

ArcSight - Rules

Test Title 782

10/18/2017 4:42 PM

Bluecoat - Security Analytics

Test Title 395

10/18/2017 4:43 PM

A count will display for the number of content in Develop, Deploy, or Recall status. Click on the Content card and the Content details will display. Clicking on the



button will display the Content Edit screen. The gold warning icon indicates the content requires client customization during deployment at the client site. When the mouse hovers over the warning icon, the help text "Client Customization Needed" is displayed.

Content

Add Content

Users in the Author group have the ability to add new content. Click on the "Add Content" option in the primary navigation menu.

Raytheon

Content Exchange

Bretny Khamphavong

Dashboard

Add Content

Clients

Reports

Q

Search content

The New Content screen will appear.

Enter the following information:

Item	Field Type	Description	Example
Title*	Text	The name of the newly added content.	
Description*	Text	A short explanation of the new content.	
Platform	Dropdown select	The appliance which content can be published or disseminated to.	Yara, Netwitness, Snort
Threat Category	Multi-select dropdown	The type of threat associated with the content.	Exploit, RAT, Lateral Movement

Threat Actor	Dropdown select	The type of threat group or actor set associated with the activity.	Cyber Crime, State Sponsored, Hacktivist
Threat Actor Name	Text	Name of the actor associated with the activity.	APT28, Anonymous, Lotus Blossom, Dark Seoul
Attack Phase	Dropdown select	The phase in which the activity was created on. This is the Kill Chain by Lockheed Martin.	Delivery, Exploitation, Command and Control (https://en.wikipedia.org/wiki/Kill_chain)
Protocol	Dropdown select	The standard communication channel used by the associated content.	HTTP, ICMP, FTP, TCP, IRC
Malware Family	Text	The family name of the identified malware.	Vawtrack, Cridex, Plugx, Dyre, CryptoLocker
Malware Family Variant	Text	A variant name or version number of the identified malware.	v1, v0.3
Logs*	Multi-select dropdown	Information source for a platform such as email log or syslog.	Bit9, BlueCoat, Bro
Packets*	Multi-select dropdown	Information source for a platform in packet form.	
Custom*	Multi-select dropdown	Content requires specific customization before deployment.	Specific IP Range or VIP username needs to be defined within the content logic
Content Logic*	Text	The signature, rules structure, query, or report being added to the Exchange.	Query regex 'user=([a-zA-Z0-9]{0,})&ver=([0-9]{0,})&key=([a-zA-Z0-9]{0,})' && action='post','put'
Sample	Text	Optional field used to reference links to specific malware or use case samples.	
Reference	Text	Optional field used to describe or link to a description of the use case to add additional context.	
Expiration Days	Number	The number of days which the content will expire.	
CVE	Text	Common vulnerabilities and exposures identifier that is associated with the activity.	CVE-2017-0143, CVE-2017-1274
Zero Day	Checkbox	Checked if the vulnerability is not publicly reported or announced before becoming active or widely seen.	

**Denotes a required field.*

Create New Content

Title *



This field is required
Description *

Platform

ArcSight - Active Channel Rules ▾

Threat Category *

Select ▾

Threat Actor

APT ▾

Threat Actor Name

Attack Phase

Actions on Objective ▾

Protocol

ANY ▾

Malware Family

Malware Family Variant

Dependencies *

Logs *

Select ▾

Packets *

Select ▾

Custom *

Select ▾

Content Logic *

Content Source

When ready, click the

Save

button. Congratulations, you have successfully added new content to the database.

Modify Content

After Content is created, Authors and Reviewers have the ability to modify it.

Create New Content

Title *



This field is required
Description *

Platform

ArcSight - Active Channel Rules ▾

Threat Category *

Select ▾

Threat Actor

APT ▾

Threat Actor Name

Attack Phase

Actions on Objective ▾

Protocol

ANY ▾

Malware Family

Malware Family Variant

Dependencies *

Logs *

Select ▾

Packets *

Select ▾

Custom *

Select ▾

Content Logic *

Content Source

Click the

Save

button and you will be able to View Content.

View Content

The View Content screen displays the Content details and the workflow state.

Raytheon

Content Exchange

Bretny Khamphavong

DashboardAdd ContentClientsReports

Search content

View Content

DevelopmentQA ReviewENG ReviewSME ReviewQA ReviewArchiveEdit

sampletitle

sampledescription

Platform
ELSA

Threat Category
DOS
Lateral Movement

Threat Actor
Crimeware

Attack Chain Phase
Multiple

Protocol
ANY

Dependencies

Logs
Bluecoat logs
Bro logs
DNS logs
Expiration Days
180

Packets
Packet Data for email
Packet Data with direction

Custom
Definition domain
Definition privileged accounts

Content Logic

sampleContentLogic

Comments +

On the View Content screen, you have the option to click on the



button to modify the displayed Content.

Comments can be added to Content by clicking on the



button in the 'Comments' section.

Comments

Comment

Enter comment here.

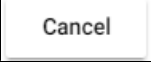
cancel

Save

Enter your comment and click



or select

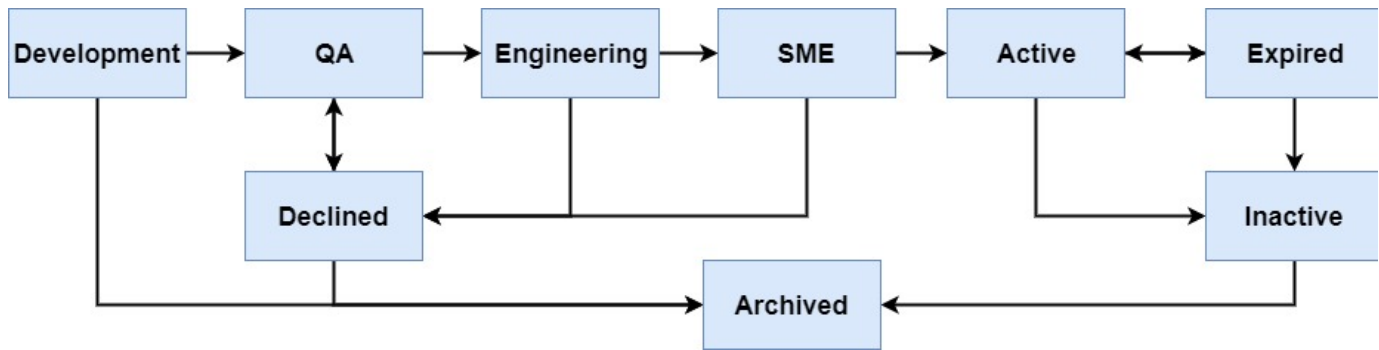


if you wish to exit.

Workflow States

Content flows through a series workflow states. User permissions assigned to a user determines who can promote pieces of Content to which state.

See the diagram below to understand how Content moves through the process.



Every Content item begins in a 'Development' state. At any time during the workflow, a piece of content can be updated to an 'Archived' state.

Once Content is promoted from 'Development' it will move into the 'QA' queue. Content in 'QA' will move into 'Engineering', and 'Engineering' into 'SME'. If Content is ready to be 'Deployed' it will become 'Active'. If Content is deemed not ready to become active, then it can be 'Declined'.

Each Content item has an expiration date. The default is set to 90 days, but can be manually configured. If Content passes the number of days specified, then it will become 'Expired'.

Deployment

Workflow States

The Deployment model is the connection between content and a client's appliance. A Deployment object has a workflow to show the status of the actual deployment.

Proposed - The application has matched the content with the appliance.

Exported - Engineer/liaison has exported the content logic from the application.

Deployed - Engineer/liaison has successfully added the content logic to the client's appliance.

Recall Needed - When the Deployment state is Deployed and the Content state is Inactive, the application will change Deployment state to Recall Needed.

Recalled - The content was deployed to the appliance then removed, probably because the content expired and became inactive.

Declined - Either 1) the engineer/liaison has decided not to deploy the content to the appliance, or 2) the client has declined to receive the content.

Deploy

My Dashboard displays the content that needs deployment to your subscribed clients.

Click the Export button to export all content for an appliance to a text file. If the content is Netwitness content, you will be prompted to provide the Key and Index variables.

Click the Deployed button to mark the content as being deployed at the client site.

Click the content's title to display the deployment detail page.

Raytheon

Content Exchange

engineer TestUser ▾

My Dashboard

Add Content

Clients

Search

Q

Search content

My Dashboard

Content

Develop 68

Deploy 6

Recall 2

Client 0

2

Client 1

2

Client 2

2

Appliance 1

Exported

1 ➤

Test Title 986

10/16/2017 3:19 PM

Appliance 2

Proposed

1 ⬆

Test Title 323

10/16/2017 3:17 PM

Appliance 1

Proposed

1 ⬆

Test Title 986

10/16/2017 3:17 PM

Appliance 2

Proposed

1 ⬆

Test Title 323

10/16/2017 3:17 PM

Appliance 1

Proposed

1 ⬆

Test Title 986

10/16/2017 3:17 PM

Appliance 2

Proposed

1 ⬆

Test Title 323

10/16/2017 3:17 PM

Deployment detail page displays the buttons for promoting the deployment through the workflow.

Directly below the deployment detail is the content detail.

Raytheon

Content Exchange

engineer TestUser ▾

My Dashboard

Add Content

Clients

Search

Q

Search content

View Deployment

Exported

Deployed

Deployed

Updated

10/16/2017 3:19 PM

Deployment for Client 0 on appliance Appliance 1.

Active

Inactive

Archive

Inactive

Port

Revise

Test Title 986

Test Description

Platform

Threat Category

Threat Actor

ArcSight - Rules

Brute Force

Blended

Author

Created

Updated

Version

Comments

author TestUser

10/16/2017 3:17 PM

10/16/2017 3:17 PM

1

0

Recall

My Dashboard displays the content that has become inactive and needs to be recalled from the client's appliance.

Click the Recalled button to mark the content as being recalled from the client.

Click the content's title to display the deployment detail page.

Raytheon

Content Exchange

engineer TestUser

My DashboardAdd ContentClientsSearch

Q Search content

My Dashboard

Content

Develop 68Deploy 6Recall 2

Client 11

Appliance 0

Recall Needed1↻

Test Title 769
10/16/2017 3:19 PM

Client 21

Appliance 0

Recall Needed1↻

Test Title 769
10/16/2017 3:19 PM

Expired

My Dashboard displays the content that has become expired and needs to go back to the active or inactive state. Only QA users will see the expired tab.

Click the content card to view the content details screen with the workflow display.

Content

Develop 0Deploy 0Recall 0Expired 1

Bluecoat - Security Analytics1

Bluecoat - Security Analytics
Test Title 335
11/07/2017 12:47 PM

Declining Content or Deployment

A user will be prompted for a required comment before a piece of Content or Deployment is declined.

Threat Actor
Unknown

Add a comment before declining this content.

Comment

I am declining this, because it needs updates.

Cancel

Save

Administration Interface

Accounts

User names and email addresses are maintained in the Active Directory. Click on a user's name to modify the group assignments. Drag and drop the groups to the appropriate columns.

Group Assignment

Brandon Denker

Groups Available

Engineer

Liaison

QA

SME

Groups Assigned

Administrator

Author

Cancel

Update

Click the

Update

button to save the group assignments. If you wish to exit, click on the

Cancel

button or



in the top right corner.

User Permissions

The actions for which a user can perform depends on the group or groups they are assigned to. The table below displays a list of permissions for each group in the application.

Group	Permission
Administrator	<ul style="list-style-type: none">• Modify all the items listed in the Admin menu.
Author	<ul style="list-style-type: none">• Add content.• Modify content from 'Develop' to 'QA' state.• Promote content from 'Decline' to 'QA' state.
QA	<ul style="list-style-type: none">• Modify content in the 'QA' state.• Promote content from 'QA' to Engineering state.• Demote content from 'QA' to Declined state.
Engineer	<ul style="list-style-type: none">• Modify content in the 'Engineering' state.• Promote content from 'Engineering' to 'SME' state.• Demote content from 'Engineering' to 'Declined' state.
SME	<ul style="list-style-type: none">• Modify content in the 'SME' state.• Promote content from 'SME' to 'Active' state.• Demote content from 'SME' to 'Declined' state.
Liaison	<ul style="list-style-type: none">• Add clients.• Modify clients.

Attack Phases

To access the Attack Phases list, click on 'Attack Phases' in the Administration panel.

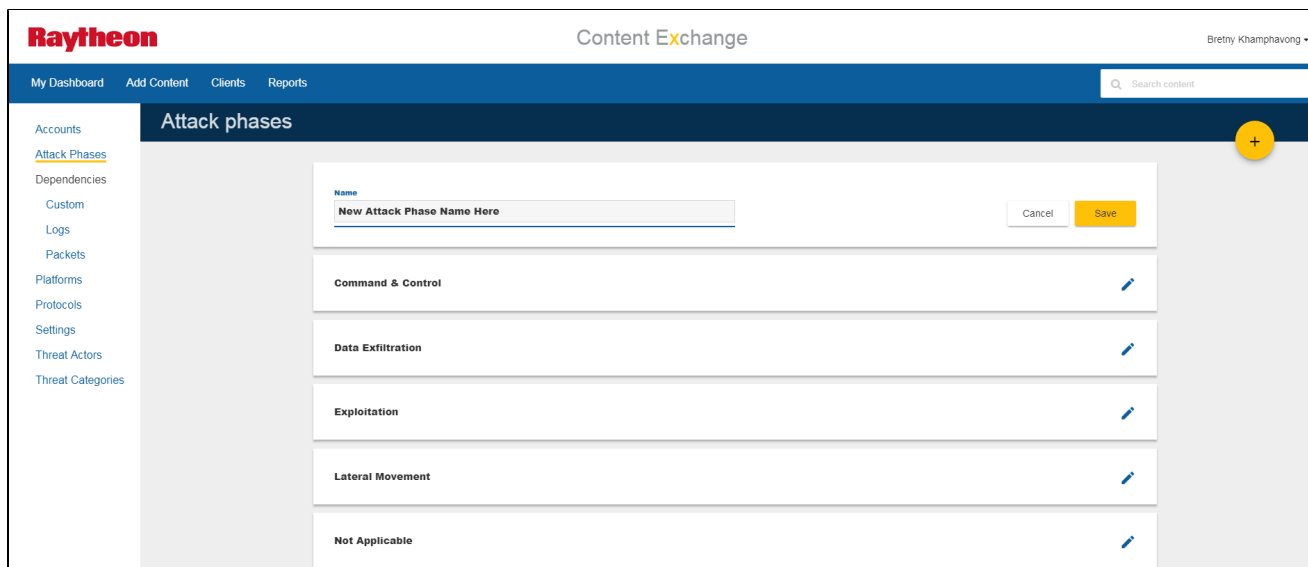
The screenshot displays the Raytheon Content Exchange web application. The top navigation bar includes the Raytheon logo, the text 'Content Exchange', and a user profile 'Bretny Khamphavong'. Below this is a secondary navigation bar with links for 'My Dashboard', 'Add Content', 'Clients', and 'Reports', along with a search bar. A left sidebar contains a list of menu items: 'Accounts', 'Attack Phases' (highlighted), 'Dependencies', 'Custom', 'Logs', 'Packets', 'Platforms', 'Protocols', 'Settings', 'Threat Actors', and 'Threat Categories'. The main content area is titled 'Attack phases' and features a list of seven attack phases, each with a blue edit icon to its right: 'Command & Control', 'Data Exfiltration', 'Exploitation', 'Lateral Movement', 'Not Applicable', 'Other', and 'Payload Delivery'. A yellow circular button with a plus sign is located in the top right corner of the main content area.

Add Attack Phase

You can add a new Attack Phase by clicking on the



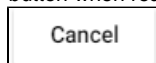
button and selecting the 'Name' field.



Enter a name for the new Attack Phase. Click the



button when ready, or click



if you wish to exit.

Modify Attack Phase

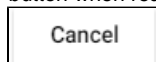
An item in the Attack Phase list can be modified by clicking on the



button. Revise the name and click the



button when ready, or click



if you wish to exit.

Dependencies

Dependencies consists of three components: Custom, Logs, and Packets. Click on any of the components to access the corresponding list.

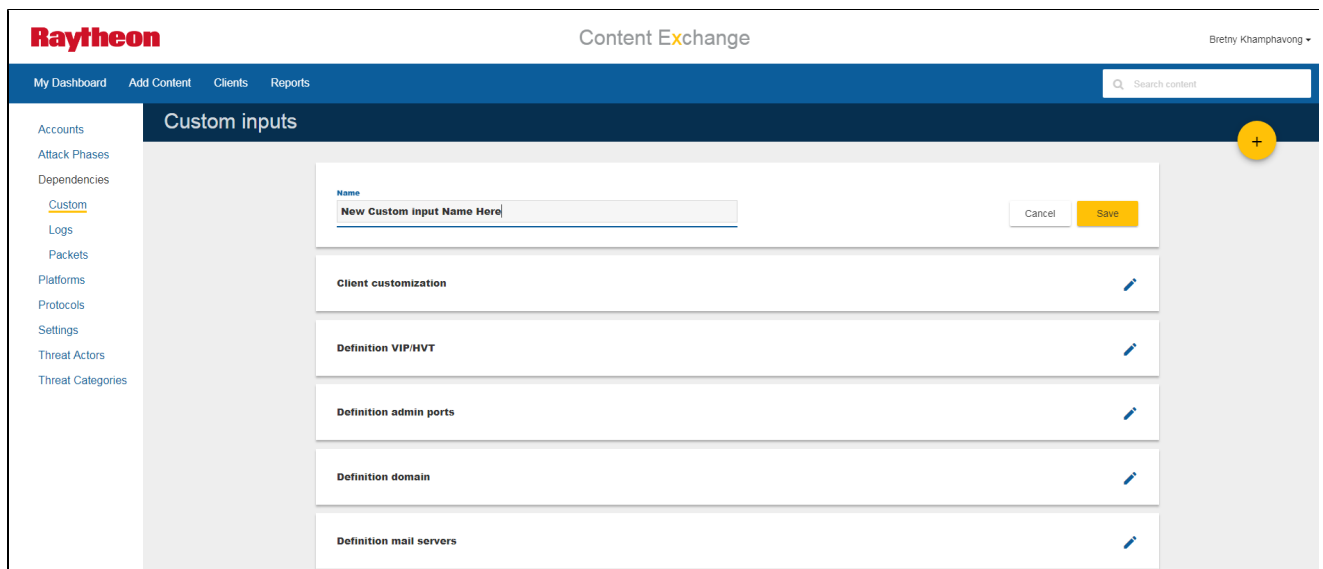
Custom

Add Custom Input

You can add a new Custom input by clicking on the



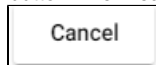
button and selecting the 'Name' field.



Enter a name for the new Custom input. Click the



button when ready, or click



if you wish to exit.

Modify Custom Input

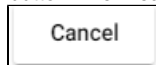
An item in the Custom inputs list can be modified by clicking on the



button. Revise the name and click the



button when ready, or click



if you wish to exit.

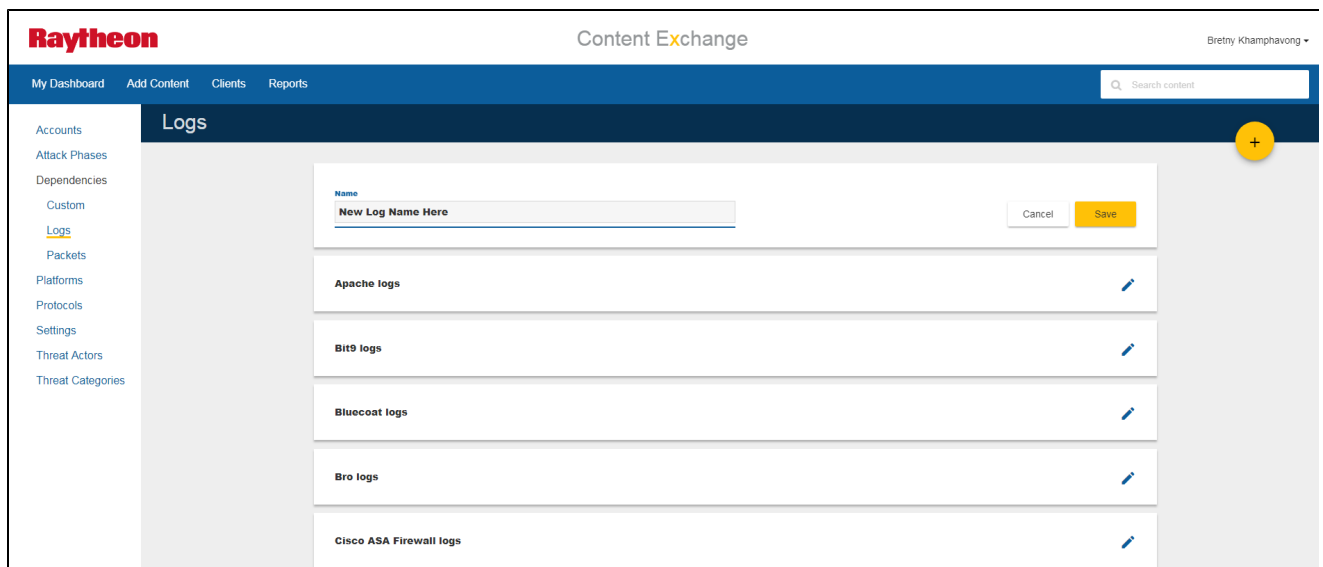
Logs

Add Log

You can add a new Log by clicking on the



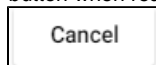
button and selecting the 'Name' field.



Enter a name for the new Log. Click the



button when ready, or click



if you wish to exit.

Modify Log

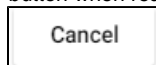
An item in the Logs list can be modified by clicking on the



button. Revise the name and click the



button when ready, or click



if you wish to exit.

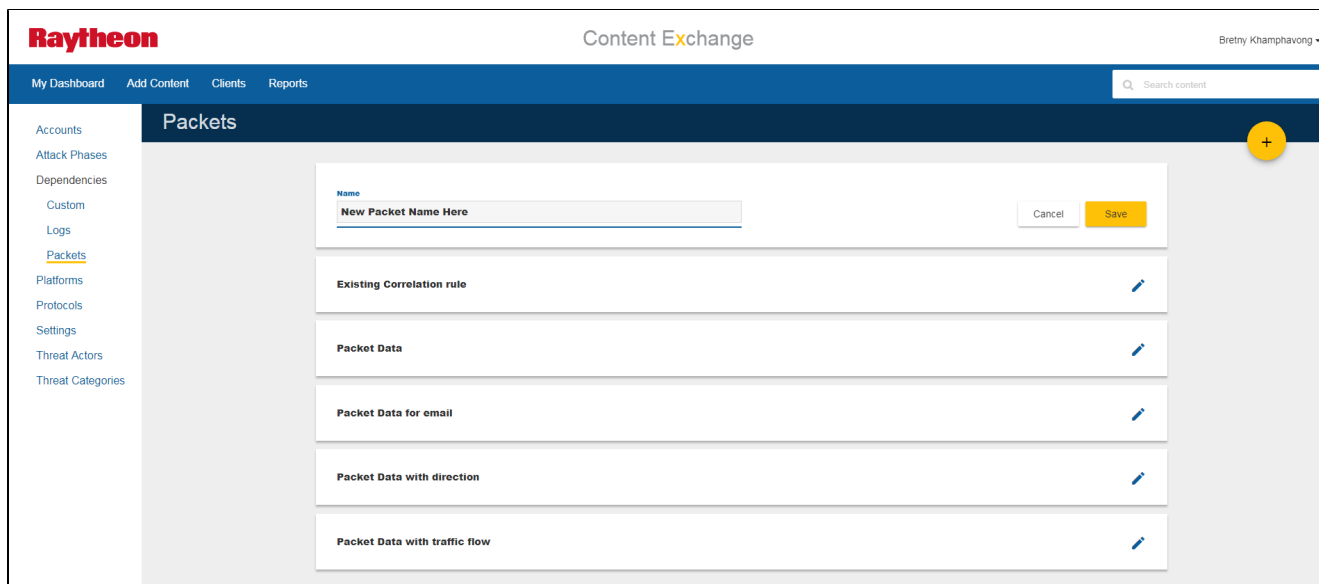
Packets

Add Packet

You can add a new Packet by clicking on the



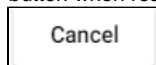
button and selecting the 'Name' field.



Enter a name for the new Packet. Click the



button when ready, or click



if you wish to exit.

Modify Packet

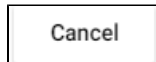
An item in the Packets list can be modified by clicking on the



button. Revise the name and click the



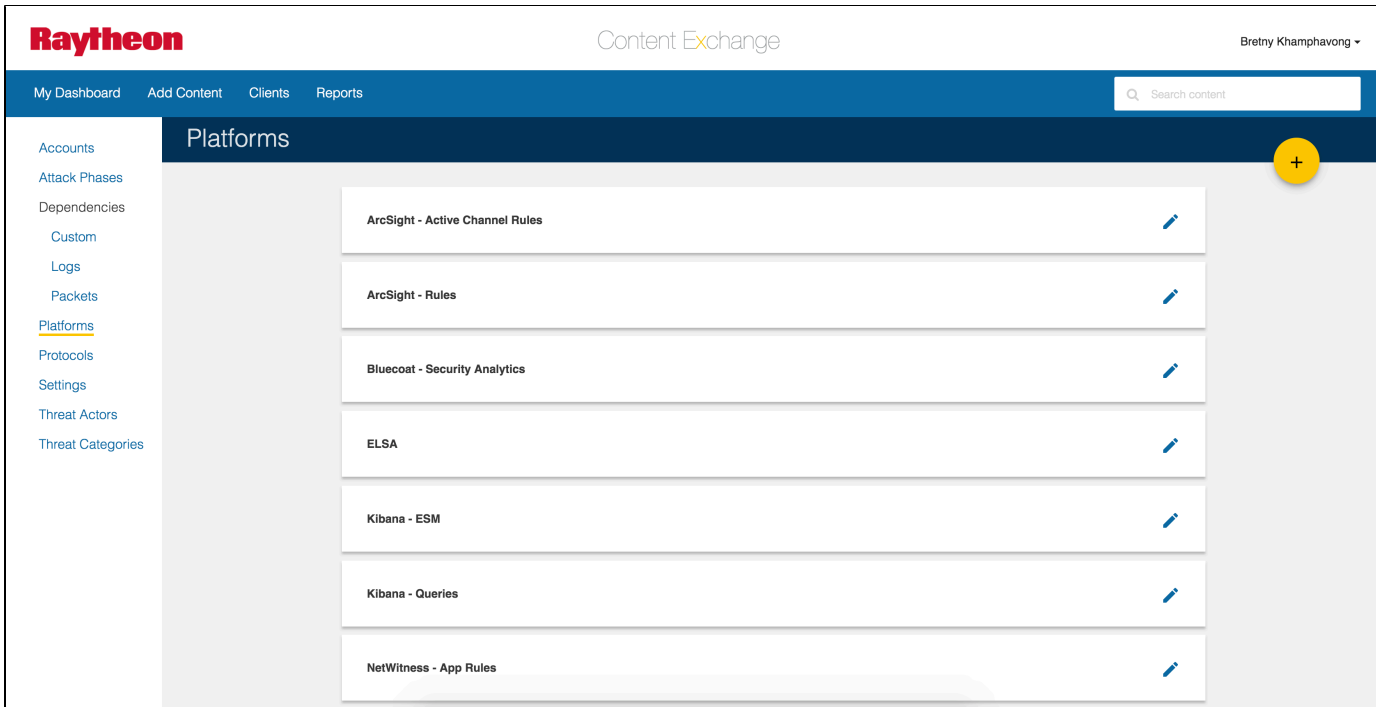
button when ready, or click



if you wish to exit.

Platforms

To access the Platforms list, click on 'Platforms' in the Administration panel.

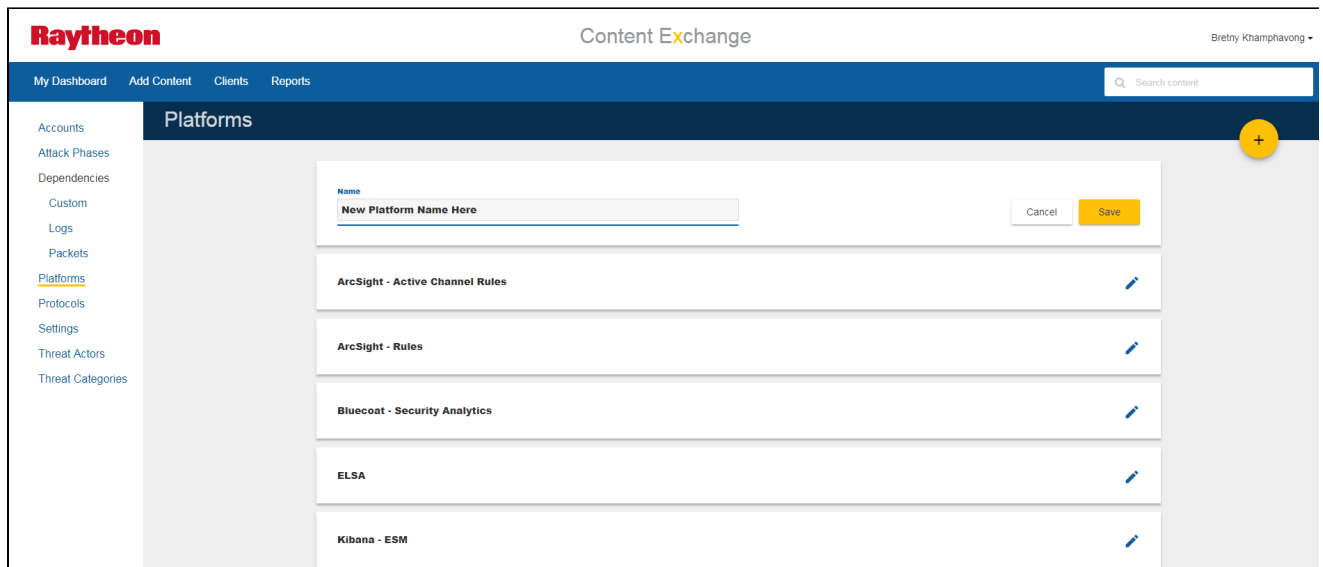


Add Platform

You can add a new Platform by clicking on the



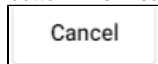
button and selecting the 'Name' field.



Enter a name for the new Platform. Click the



button when ready, or click



if you wish to exit.

Modify Platform

An item in the Platform list can be modified by clicking on the



button. Revise the name and click the

Save

button when ready, or click

Cancel

if you wish to exit.

Protocols

To access the Protocols list, click on 'Protocols' in the Administration panel.

The screenshot displays the Raytheon Content Exchange interface. The top navigation bar includes 'My Dashboard', 'Add Content', 'Clients', and 'Reports'. A search bar is located on the right. The left sidebar lists various menu items, with 'Protocols' highlighted. The main content area is titled 'Protocols' and contains a table with the following data:

Protocol Name	Action
ANY	
DNS	
FTP	
HTTP/HTTPS	
ICMP	
IRC	
LOCAL	

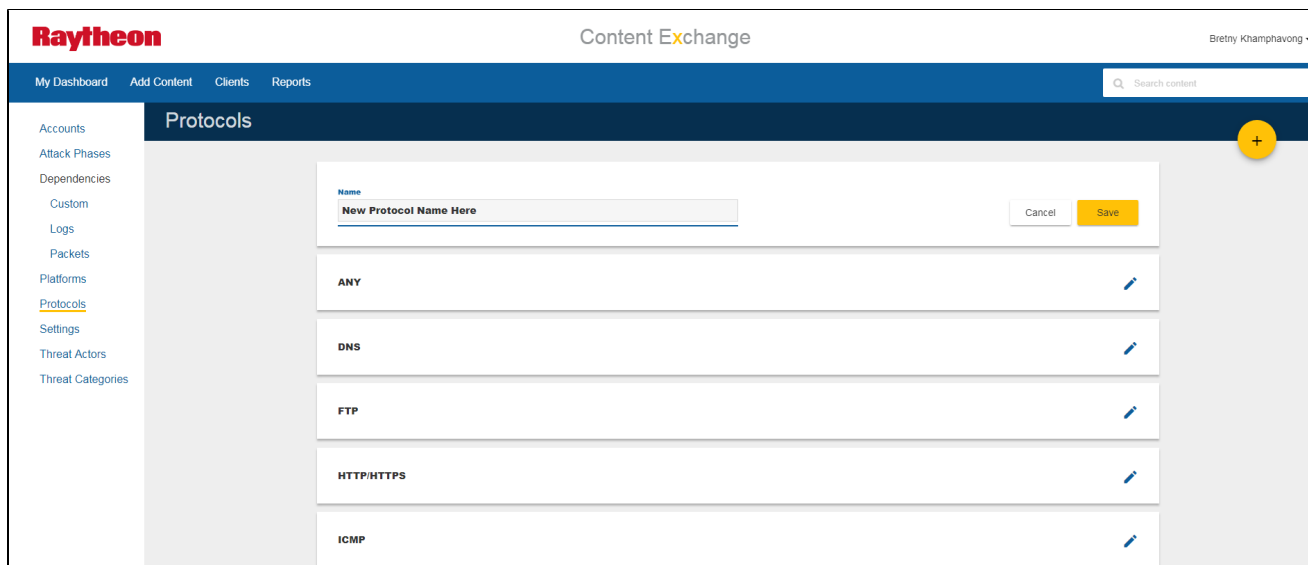
A yellow circular button with a plus sign is located in the top right corner of the Protocols section.

Add Protocol

You can add a new Protocol by clicking on the



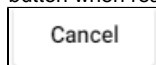
button and selecting the 'Name' field.



Enter a name for the new Protocol. Click the



button when ready, or click



if you wish to exit.

Modify Protocol

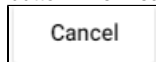
An item in the Protocol list can be modified by clicking on the



button. Revise the name and click the



button when ready, or click



if you wish to exit.

Settings

To access the Settings list, click on 'Settings' in the Administration panel.

Raytheon

Content Exchange

Bretny Khamphavong

My DashboardAdd ContentClientsReports

Search content

AccountsAttack PhasesDependenciesCustomLogsPacketsPlatformsProtocolsSettingsThreat ActorsThreat Categories

Settings

Name	Value	
RULE_ARCHIVE_DAYS	180	
Name	Value	
RULE_EXPIRATION_DAYS	180	

Modify Setting

Raytheon

Content Exchange

Bob Collins

My DashboardAdd ContentClientsReports

Search content

AccountsAttack PhasesDependenciesCustomLogsPacketsPlatformsProtocolsSettingsThreat ActorsThreat Categories

Settings

Name (Read Only)	Value		
RULE_ARCHIVE_DAYS	180	Cancel	Save
Name	Value		
RULE_EXPIRATION_DAYS	90		

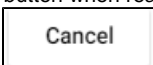
An item in the Setting list can be modified by clicking on the



button. Revise the Settings name or days value and click the



button when ready, or click



if you wish to exit.

Threat Actors

To access the Threat Actors list, click on 'Threat Actors' in the Administration panel.

The screenshot shows the Raytheon Content Exchange interface. The top navigation bar includes 'My Dashboard', 'Add Content', 'Clients', and 'Reports'. A search bar is on the right. The left sidebar lists various categories, with 'Threat Actors' highlighted. The main content area is titled 'Threat actors' and displays a list of threat actors: APT, Blended, Crimeware, Hacktivist, Insider Threat, Terrorist, and Unknown. Each entry has a blue pencil icon for editing. A yellow circular button with a plus sign is located in the top right corner of the list area.

Add Threat Actor

You can add a new Threat Actor by clicking on the



button and selecting the 'Name' field.

This screenshot is similar to the previous one, but it highlights the 'Add' button (yellow circle with a plus sign) in the top right corner of the 'Threat actors' list. The list shows the same threat actors: APT, Blended, Crimeware, Hacktivist, Insider Threat, Terrorist, and Unknown.

Enter a name for the new Threat Actor. Click the



button when ready, or click

Cancel

if you wish to exit.

Modify Threat Actor

An item in the Threat Actor list can be modified by clicking on the



button. Revise the name and click the

Save

button when ready, or click

Cancel

if you wish to exit.

Threat Categories

To access the Threat Categories list, click on 'Threat Categories' in the Administration panel.

Raytheon

Content Exchange

Bretny Khamphavong

My DashboardAdd ContentClientsReports

Search content

AccountsAttack PhasesDependenciesCustomLogsPacketsPlatformsProtocolsSettingsThreat ActorsThreat Categories

Threat categories

+

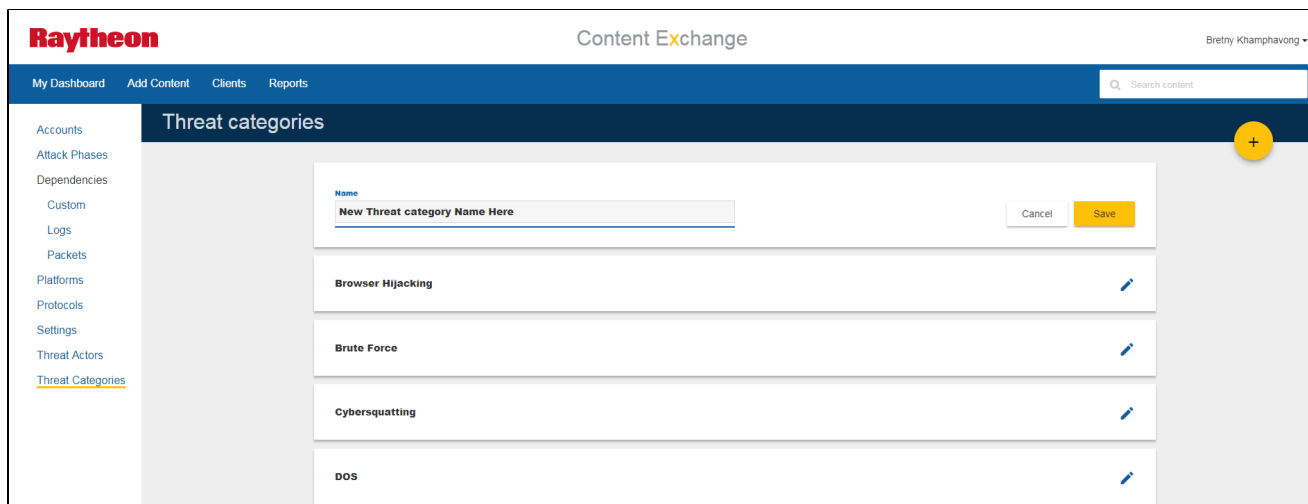
Browser Hijacking	
Brute Force	
Cybersquatting	
DOS	
Data Exfiltration	
Exploitation	
Lateral Movement	

Add Threat Category

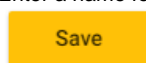
You can add a new Threat Category by clicking on the



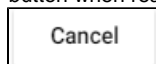
button and selecting the 'Name' field.



Enter a name for the new Threat Category. Click the



button when ready, or click



if you wish to exit.

Modify Threat Category

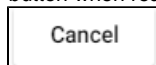
An item in the Threat Category list can be modified by clicking on the



button. Revise the name and click the



button when ready, or click

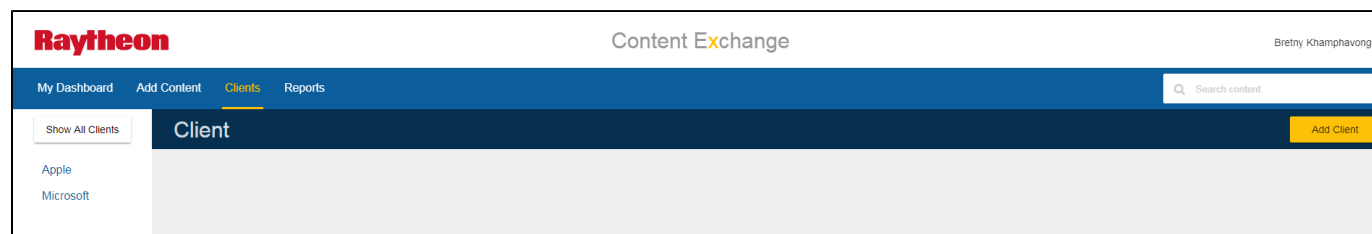


if you wish to exit.

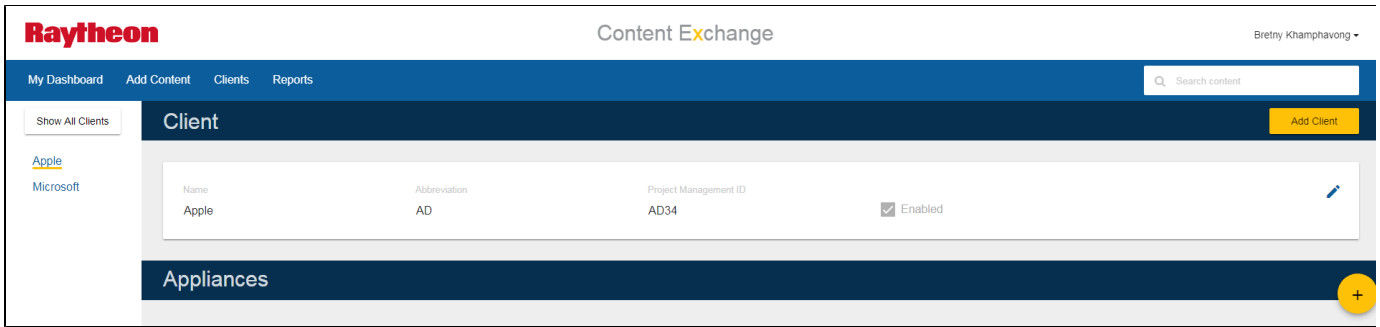
Client Interface

Clients

Clicking on 'Clients' in the primary navigation will display the Clients view. The view should be defaulted to show only the clients you have subscribed to. To subscribe to clients, see "[Client Subscriptions](#)" in the User Menu.

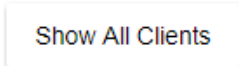


Choose any client in the left menu panel to show the client details and appliances associated.

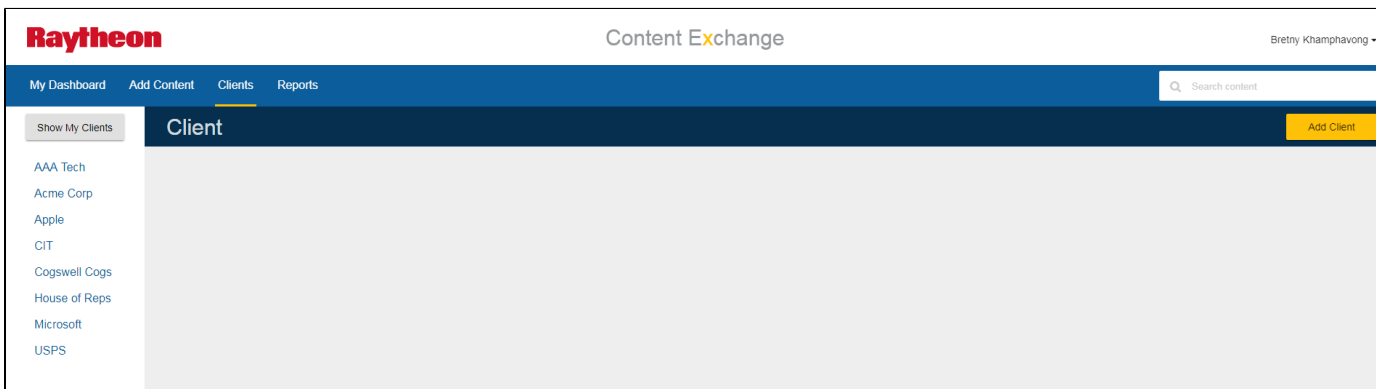


Show My Clients

Clicking on the

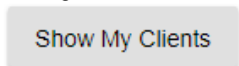


button in the left menu panel will show all the clients entered into the application.

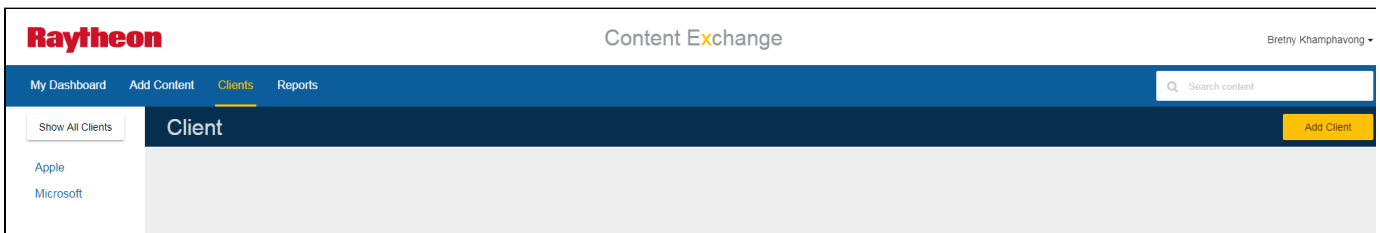


Show All Clients

Clicking on the

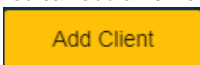


button in the left menu panel will show all the clients you have subscribed to.



Add Client

You can add a new client by clicking the



button.

Enter the Client's Name, Abbreviation, Project Management ID and Enabled/Disabled status. When a client is disabled, it will not appear on the Dashboard and the application will not identify new deployments for the client.

Raytheon

Content Exchange

liaison TestUser ▾

My Dashboard

Clients

Reports

Client 0

Client 1

Client 2

Add Client

Name *

Abbreviation *

Project Management ID *

☒ Enabled

* Required

Cancel

Save

Click the

Save

button when ready, or click

Cancel

if you wish to exit.

Modify Client

You can modify a client by clicking the



button. Revise the Client's Name, Abbreviation, Project Management ID or Enabled/Disabled status.

Raytheon

Content Exchange

Bob Collins ▾

My Dashboard

Add Content

Clients

Reports

Acme Corp

Client

Add Client

Name *

Acme Corp

Abbreviation *

ACME

Project Management ID *

AC12

☒ Enabled

* Required

Cancel

Save

Click the

Save

button when ready, or click

Cancel

if you wish to exit.

Appliance Interface

Display the list of appliances for a client by clicking on the client's name in the client list.

Client 0

Client 1

Client 2

Client

Add Client

Name	Abbreviation	Project Management ID	
Client 2	2	AC2	<input checked="" type="checkbox"/> Enabled



Appliances



Name	Platform	
Appliance 0	ArcSight - Active Channel Rules	
Logs	Custom	
Apache logs		

Name	Platform	
Appliance 1	ArcSight - Rules	
Logs	Custom	
Apache logs		

Add Appliance

You can add a new appliance to a client by clicking the



button. Enter the appliance's name, select the platform and dependencies.

Raytheon

Content Exchange

liaison TestUser

My DashboardClientsReports

Q Search content


Client 0

Client 1

Client 2

Client

Add Client

Name	Abbreviation	Project Management ID	<input checked="" type="checkbox"/> Enabled	
Client 2	2	AC2		

Appliances

Add Appliance

Name *

Platform *

Logs *

Packets *

Custom *

Select

▼ Select

▼ Select

Cancel

Save

Click the

Save


button when ready, or click

Cancel

if you wish to exit.

Edit Appliance

You can modify an existing appliance by clicking the



button.

Raytheon

Content Exchange

liaison TestUser ▾

My Dashboard

Clients

Reports

Q Search content


Client 0

Client 1

Client 2

Client

Add Client

Name	Abbreviation	Project Management ID	<input checked="" type="checkbox"/> Enabled	
Client 2	2	AC2		

Appliances

Name *

Appliance 0

Platform *

ArcSight - Active Channel Ru... ▾

Logs *

Apache logs

Packets *

▾ Select

Custom *

▾ Select

Cancel

Save

Revise the appliance's values and click the

Save

button when ready, or click

Cancel

if you wish to exit.

Search and Filter

Use the search and filter fields in the left panel to specify the content search criteria.

Click the Search button to initiate the search.

Raytheon

Content Exchange

My DashboardAdd ContentClientsSearch

Search by Text

Client
Select

Created Date
From
9/19/2017To
10/19/2017

Search

State
Select

Protocol
Select

Threat Actor
Select

Threat Category
Select

Attack Phase
Select

Platform
Select

Dependencies
Logs
Select

Packets
Select

Custom Inputs
Select

Search

Search

Search results are displayed in the right panel. The large blue text is the content's title.

Click the content's card to display the content detail page.

Raytheon

Content Exchange

author TestUser

My DashboardAdd ContentClientsSearch

Search by Text
title

Client
Select

Created Date
From
9/19/2017To
10/19/2017

Search

State
Development, Active

Protocol
Select

Threat Actor
Select

Threat Category
Select

Attack Phase
Select

Platform
Select

Dependencies

Search

Test Title 626

StatusActive

PlatformBluecoat - Security Analytics

Authorauthor TestUser

Created10/16/2017 3:13 PM

Last Updated10/16/2017 3:13 PM

Appliances3

Deployments3

Comments0

Test Title 252

StatusActive

PlatformArcSight - Rules

Authorauthor TestUser

Created10/16/2017 3:13 PM

Last Updated10/16/2017 3:13 PM

Appliances3

Deployments3

Comments0

Test Title 14

StatusActive

PlatformArcSight - Active Channel Rules

Authorauthor TestUser

Created10/16/2017 3:13 PM

Last Updated10/16/2017 3:13 PM

Appliances3

Deployments3

Comments0

Test Title 742

StatusDevelopment

PlatformBluecoat - Security Analytics

Authorauthor TestUser

Created10/16/2017 3:13 PM

Last Updated10/16/2017 3:13 PM

Appliances0

Deployments0

Comments0

Test Title 960

StatusDevelopment

PlatformArcSight - Rules

Authorauthor TestUser

Created10/16/2017 3:13 PM

Last Updated10/16/2017 3:13 PM

Appliances0

Deployments0

Comments0

Test Title 378

StatusDevelopment

PlatformArcSight - Active Channel Rules

Authorauthor TestUser

Created10/16/2017 3:13 PM

Last Updated10/16/2017 3:13 PM

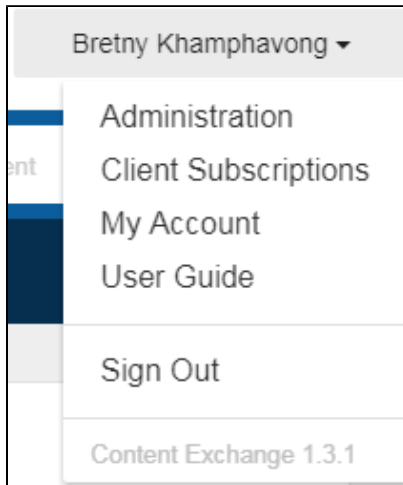
Appliances0

Deployments0

Comments0

Signing Out

On any page, you can sign out of the application by clicking on your username in the top right corner. In the dropdown User Menu, select 'Sign Out'.



You will have successfully signed out of the application.

Glossary

Client Subscriptions - Subscribe to receive email messages when content is added or changed for the selected clients.

Platform Subscriptions - Subscribe to receive email messages when content is added or changed for the selected platforms.