Flying Cloud CrowsNest System Integration Guide

Executive Overview

Aruba and Flying Cloud Technology have formed a partnership to create the ***only patented*** cyber security solution that prevents data exfiltration in real time**.** Flying Cloud CrowsNest integrates with ClearPass to provide immediate visibility into who, when, where and how data content was accessed, modified, or distributed. Protected by 12 patents, CrowsNest is the only data surveillance solution on the market, providing a competitive advantage and incremental revenue opportunity. This integration guide covers setup and configuration for integrating Flying Cloud CrowsNest with Aruba Networks ClearPass Policy Manager.

Introduction

CrowsNest data surveillance solutions enable enterprises to protect IP, PII, and other essential or sensitive data. It provides deep understanding and better control of data security posture with 100% visibility into every data packet. Big data storage capacity and analytics performance deliver sophisticated insight to protect data at petabyte scale, enabling security teams to identify anomalies and unprivileged data usage as they occur. Go back in time to see when threats were inserted and identify lost data assets. A patented rolling baseline of the current normal state eliminates most false positive alerts. CrowsNest enables teams to deploy effective Zero Trust security for data assets with a real-time data chain of custody. Whether delivered from the cloud or on premises, Flying Cloud enhances security efforts to protect against current and future threats.

Features:

1. CrowsNest delivers real-time visibility into an organization's data movement, usage, and changes.
2. CrowsNest analyzes incoming data, data in motion across the network, and data leaving the environment to identify and prevent data tampering, loss, and exfiltration.
3. It creates a rolling baseline of normal data patterns, so that anomalous usage, unprivileged access, and threat actors become immediately visible.
4. When anomalies appear, CrowsNest delivers real-time data forensics and analytics. Security defenders receive a data "chain of custody" that identifies exactly who, where, when, and how content was accessed, modified, or distributed.
5. CrowsNest data defense capabilities complement existing security measures.
6. Protect data security posture without adding security experts, relying on users to decide what is sensitive and what is not, or adding complexity to the existing security environment.

CrowsNest leverages fully containerized virtual images that can be deployed throughout Aruba's cloud or customer site-based infrastructure via remote access to appropriately sized systems. This installation is a high availability solution using dual Dell PowerEdge M830s in a chassis configuration. The architecture is fully integrated with Aruba's current NAC ClearPass Policy Manager and will utilize Aruba/customer network.

Aruba's ClearPass Policy Manager, part of the Aruba 360 Secure Fabric, provides role- and device-based secure network access control for IoT, BYOD, and corporate devices as well as employees, contractors, and guests across any multivendor wired, wireless and VPN infrastructure. With a built-in context-based policy engine, RADIUS, TACACS+, non-RADIUS enforcement using OnConnect, device profiling, posture assessment, onboarding, and guest access options, ClearPass is unrivaled as a foundation for network security for organizations of any size.

For comprehensive integrated security coverage and response using firewalls, UEM and other existing solutions, ClearPass supports the Aruba 360 Security Exchange Program. This allows for automated threat detection and response workflows that integrate with third-party security vendors and IT systems previously requiring manual IT intervention.

KEY FEATURES

1. Role-based, unified network access enforcement across multi-vendor wireless, wired and VPN networks
2. Intuitive policy configuration templates and visibility troubleshooting tools
3. Supports multiple authentication/authorization sources (AD, LDAP, SQL)
4. Self-service device onboarding with built-in certificate authority (CA) for BYOD
5. Guest access with extensive customization, branding and sponsor-based approvals
6. Integration with key UEM solutions for in-depth device assessments
7. Comprehensive integration with the Aruba 360 Security Exchange Program
8. Single sign-on (SSO) support works with Ping, Okta and other identity management tools to improve user experience to SAML 2.0-based applications

CPPM and Endpoint Software Requirements

The minimum software version required for ClearPass is 6.9.x. At the time of writing, ClearPass 6.9.10 / 6.10.4 is the latest available and recommended release. Any subsequent ClearPass software release will support this integration.

ClearPass Installation and Deployment Guide

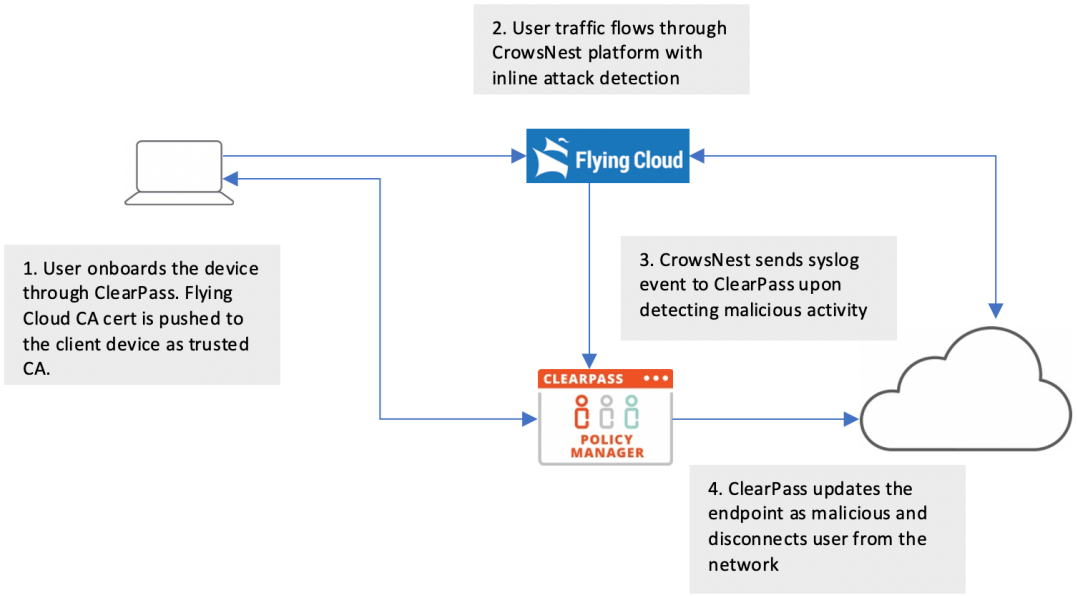
This document assumes the ClearPass environment is already configured and operational. If you require assistance with basic deployment, refer to the following deployment guide:

https://www.arubanetworks.com/techdocs/ClearPass/6.9/Aruba_DeployGd_HTML/Default.htm

Pictorial View of the Integration

Aruba Networks and Flying Cloud Technology have formed a partnership to create a fully integrated Zero Trust solution in order for preventing damage from cyber attack. The integration of ClearPass and CrowsNest provides a network and software business application that coordinates security connections between the network and application data layer. It includes integrated data and network device access level management performing packet level surveillance of all data traversing customer networks. Identified attack data triggers CrowsNest to immediately notify ClearPass, isolating suspicious activity and removing rogue devices from network.

Figure 1: *Pictorial view of the integration*



High-Level Benefits

1. Automated/integrated device governance (admissions, segmentations, and immediate unwarranted device eliminations)
2. Centralized, scalable solution that will be able to grow globally and will meet all international standards for data security and user information privacy, such as SAMR (China), CMMC (USA), and GDRP (EU)
3. Centralized device authentication
4. Dynamic rules baseline; non static rule tables
5. No change in data structure
6. Real time detection and notification of anomalies
7. Smart devices in zero trust network lake

Example Support Matrix (only list products that are required):

Components	Tested Version	Notes
CrowsNest	2.0.2	
Aruba Switch	xxxxxx	
Aruba AP	xxxxxxxxx	
ClearPass Policy Mgr (CPPM)	6.10.x	
Hardware see below*		

*System sizing requirements - examples

Small

Remote locations/sites warrant reduced compute and storage footprint for Crows Nest deployment.

• 1 x Chassis based system
o 2 x Intel® Xeon® processor E5-4600 v4 o 4 x 32GB DDR4 DIMM
o 1 x 1Gbe
o 1 x 10Gbe
o IPMI or iDrac License

• Storage capacity based on daily ingest, and retention period
▪ 20TB @ 2TB daily (searchable data & 2 weeks data retention) ▪ 250-500GB raid'd disk for OS and Apps

Medium

- 1 x Chassis based system
- 2 x Compute Servers (applicable to chassis mfg)

o 2 x Intel® Xeon® processor E5-4600 v4 o 4 x 32GB DDR4 DIMM
o 4 x 16GB DDR4 DIMM
o 2x1Gbe

o 2 x 10Gbe

o IPMI or iDrac License
• Storage capacity based on daily ingest, and retention period

Large

- Blade Enclosure
- 4 x Blade Servers

o 2 x Intel® Xeon® Scalable processors o 4 x 32GB DDR4 DIMM per M640
o 4 x 1Gbe
o 8 x 10Gbe

o IPMI or iDrac
• Storage capacity based on daily ingest, and retention period

Installing CrowsNest

*CrowsNest installation (using Linux Ubuntu 20.04 machine):

1. Install PF_RING kernel driver from 8.0.0-stable branch
2. Install and run sslsplit for decrypting traffic and mirroring. (Could be changed to Palo Alto)
3. Set gateway mode for CrowsNest machine and add PF_RING dummy mirroring ethernet device
4. Install docker and docker-compose
5. Add registry.flyingcloudtech.com account
6. Run specified docker-compose.yml script to start CrowsNest

VMWare OVF template for virtual machine… autoloading integration to ClearPass

https://flyingcloudtechnology-my.sharepoint.com/:u:/g/personal/mikhail_martyushov_flyingcloudtech_com/ESIUZAVrs3FEm7UgI3X4ZVsBRXarN6rPQkMkpLvK1vKAWA?e=NRrOFr

Troubleshooting

Notes: A Docker image has two components: the base image and the application image. To patch a containerized system, you must update the base image and then rebuild the application image. So in the case of a vulnerability like Heartbleed, if you want the ensure that the new version of SSL is on every container, you would update the base image and recreate the container in line with your typical deployment procedures. A sophisticated deployment automation process (which is likely already in place if you are containerized) would make this simple.

One of the most promising features of Docker is the degree to which application dependencies are coupled with the application itself, offering the potential to patch the system when the application is updated, i.e., frequently and potentially less painfully. But somewhat counterintuitively, Docker also offers a bright line between systems and development teams:

systems teams support the infrastructure, the compute clusters, and patch the virtual instances; development teams support the containers. If you are trying to get to a place where your development and systems teams work closely together and responsibilities are clear, this is an attractive feature.

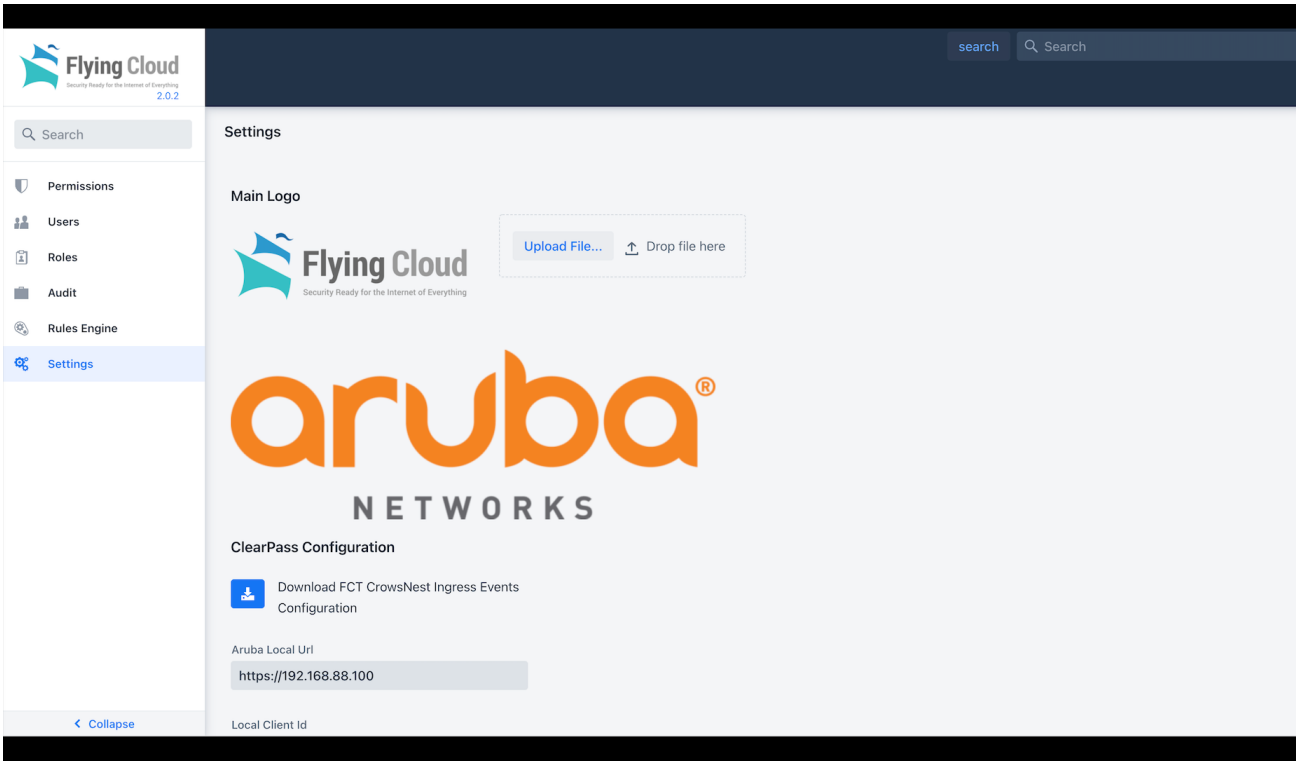
Company will provide Technical Support to Customer via both telephone and electronic mail on weekdays during the hours of 9:00 am through 5:00 pm Pacific time, with the exclusion of Federal Holidays ("Support Hours"). Customer may initiate a helpdesk ticket during Support Hours by emailing support@flyingcloudtech.com.

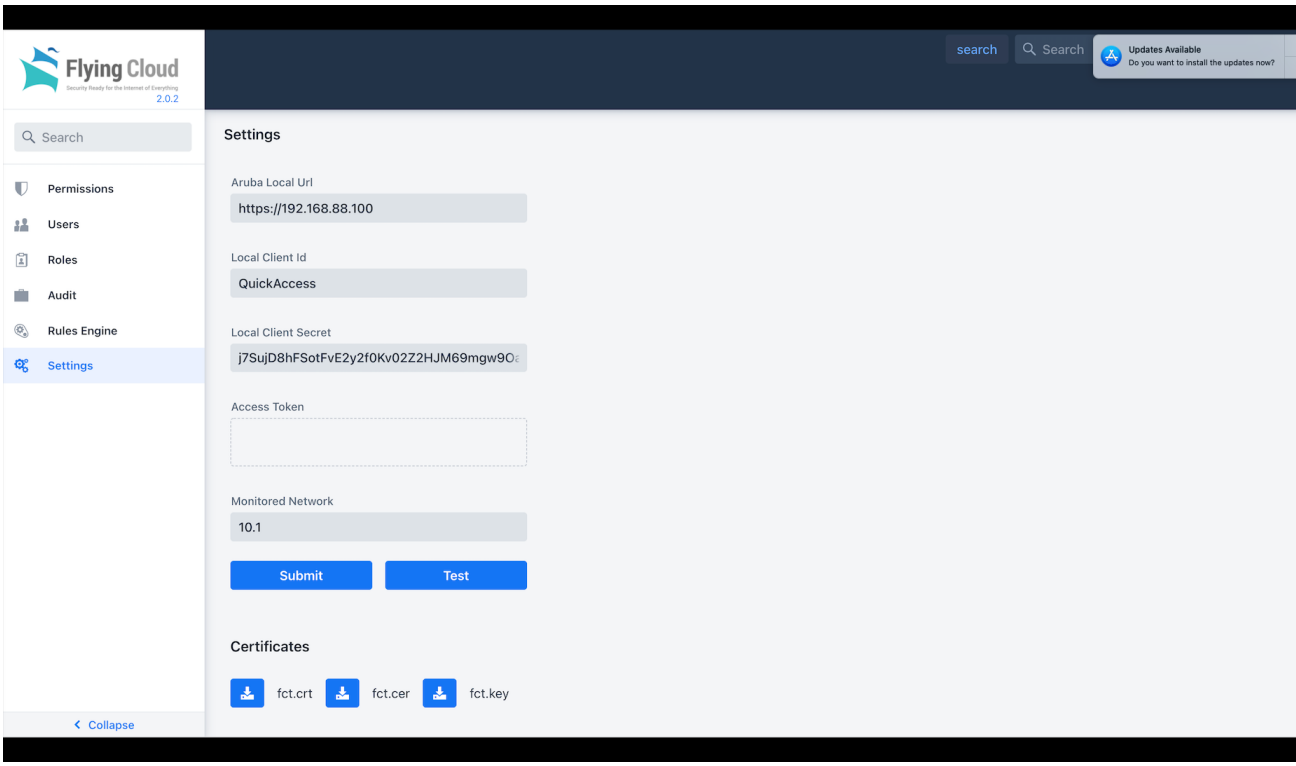
Company will use commercially reasonable efforts to respond to all Helpdesk tickets within one (1) business day.

Configurations Steps

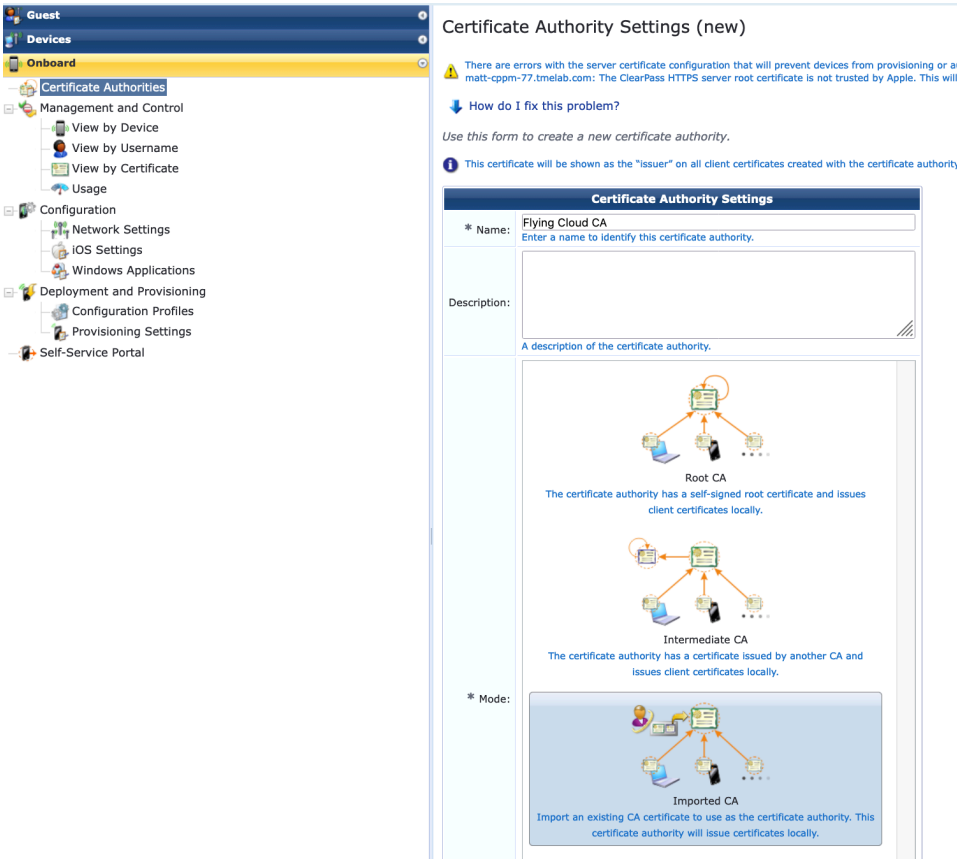
Following are the steps to set up this integration

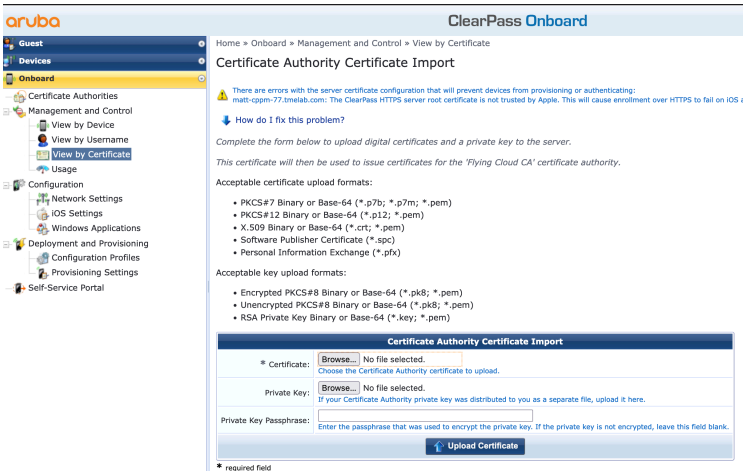
1. Login to CrowsNest and download the CA certificate and private key to be imported into ClearPass

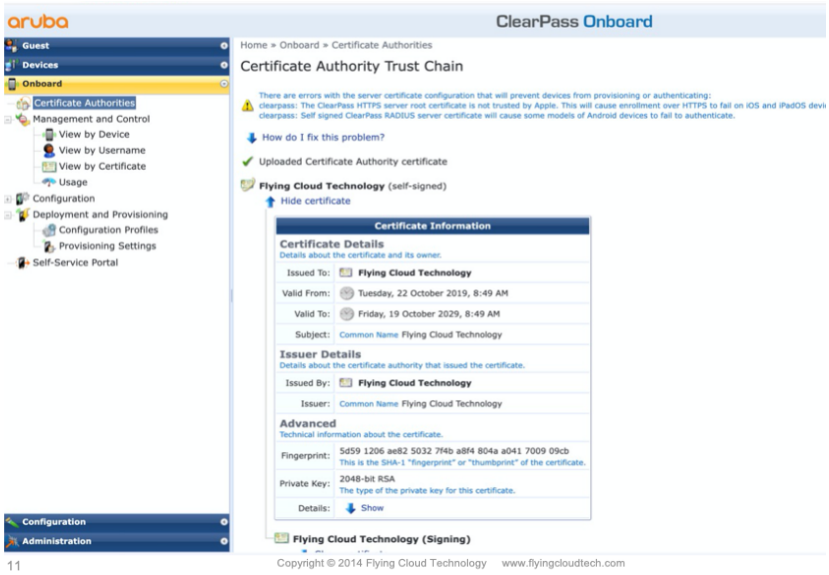




2. Create a certificate authority and Import the CA certificate and private key into ClearPass Onboard by selecting “Create new certificate authority” and then selecting CA type as “Imported CA”


Guest
Devices
Onboard
Certificate Authorities
Management and Control
View by Device
View by Username
View by Certificate
Usage
Configuration
Network Settings
iOS Settings
Windows Applications
Deployment and Provisioning
Configuration Profiles
Provisioning Settings
Self-Service Portal
Certificate Authority Settings (new)
There are errors with the server certificate configuration that will prevent devices from provisioning or a
matt-cppm-77.tmelab.com: The ClearPass HTTPS server root certificate is not trusted by Apple. This will
How do I fix this problem?
Use this form to create a new certificate authority.
This certificate will be shown as the "issuer" on all client certificates created with the certificate authority
Certificate Authority Settings
* Name:
Flying Cloud CA
Enter a name to identify this certificate authority.
Description:
A description of the certificate authority.
* Mode:
Root CA
The certificate authority has a self-signed root certificate and issues client certificates locally.
Intermediate CA
The certificate authority has a certificate issued by another CA and issues client certificates locally.
Imported CA
Import an existing CA certificate to use as the certificate authority. This certificate authority will issue certificates locally.


aruba
ClearPass Onboard
Guest
Devices
Onboard
Certificate Authorities
Management and Control
View by Device
View by Username
View by Certificate
Usage
Configuration
Network Settings
iOS Settings
Windows Applications
Deployment and Provisioning
Configuration Profiles
Provisioning Settings
Self-Service Portal
Home » Onboard » Management and Control » View by Certificate
Certificate Authority Certificate Import
There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
matt-cppm-77.tmelab.com: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS
How do I fix this problem?
Complete the form below to upload digital certificates and a private key to the server.
This certificate will then be used to issue certificates for the 'Flying Cloud CA' certificate authority.
Acceptable certificate upload formats:
PKCS#7 Binary or Base-64 (*.p7b; *.p7m; *.pem)
PKCS#12 Binary or Base-64 (*.p12; *.pem)
X.509 Binary or Base-64 (*.crt; *.pem)
Software Publisher Certificate (*.spc)
Personal Information Exchange (*.pfx)
Acceptable key upload formats:
Encrypted PKCS#8 Binary or Base-64 (*.pk8; *.pem)
Unencrypted PKCS#8 Binary or Base-64 (*.pk8; *.pem)
RSA Private Key Binary or Base-64 (*.key; *.pem)
Certificate Authority Certificate Import
* Certificate:
Browse... No file selected.
Choose the Certificate Authority certificate to upload.
Private Key:
Browse... No file selected.
If your Certificate Authority private key was distributed to you as a separate file, upload it here.
Private Key Passphrase:
Enter the passphrase that was used to encrypt the private key. If the private key is not encrypted, leave this field blank.
Upload Certificate
* required field



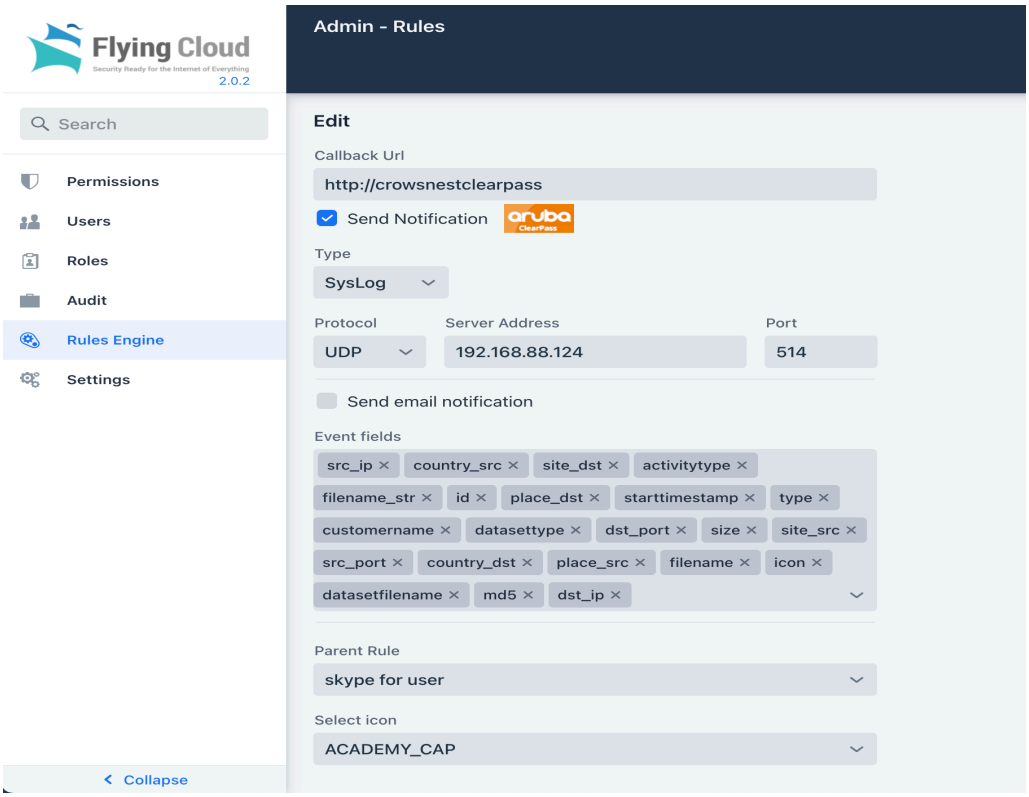
3. Set up Onboarding workflow with the issuing CA as Flying Cloud CA and gateway IP as CrowsNest platform IP.

   Detailed instructions on how to set up onboarding workflow is available in the ClearPass Onboard tech note:

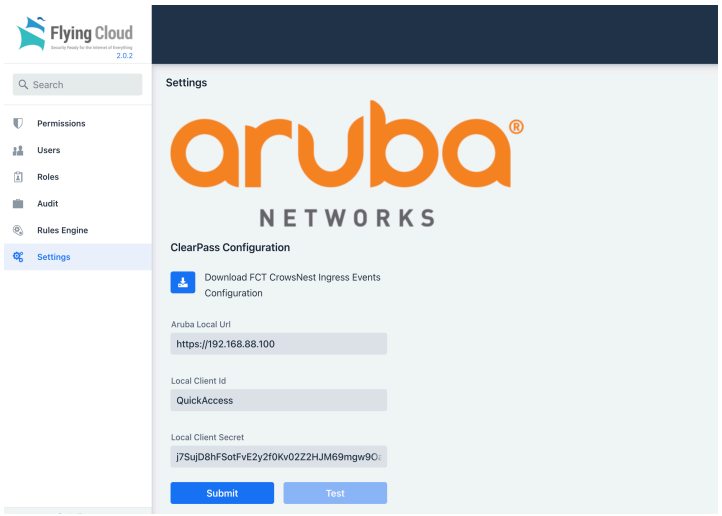
   https://asp.arubanetworks.com/downloads/documents/RmlsZTo0NDZlZmM1NC1lNmZiLTExZWEtYjE5OC04Nzc5YzY0NjgwOGY%3D

4. Onboard the client device through ClearPass. Verify that gateway and CA certificates are set up correctly. Gateway should point to CrowsNest platform IP and the Flying Cloud CA certificate added in step 1 should be pushed to the client device as a trusted CA.

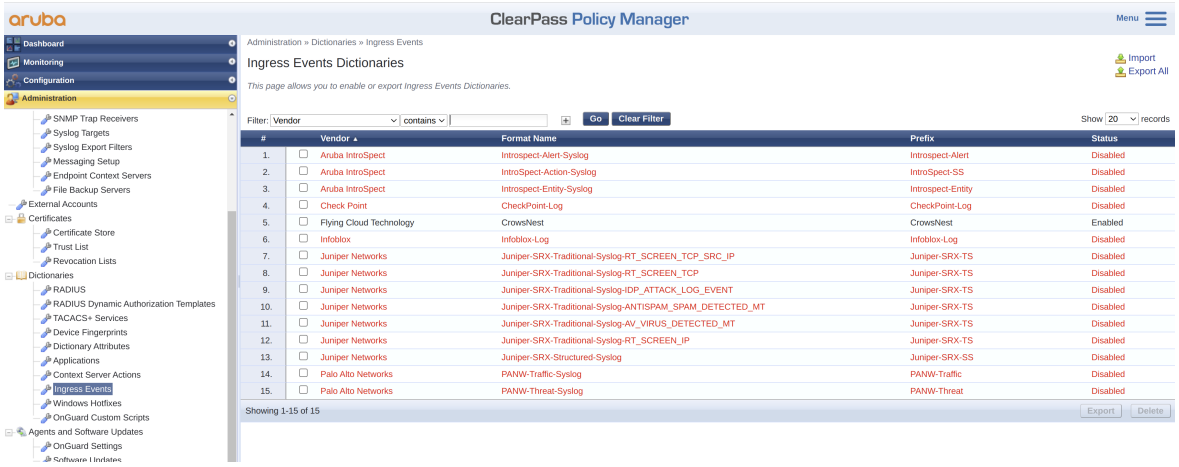
5. Set up rules on CrowsNest platform to trigger a syslog message to ClearPass when a threat is detected.



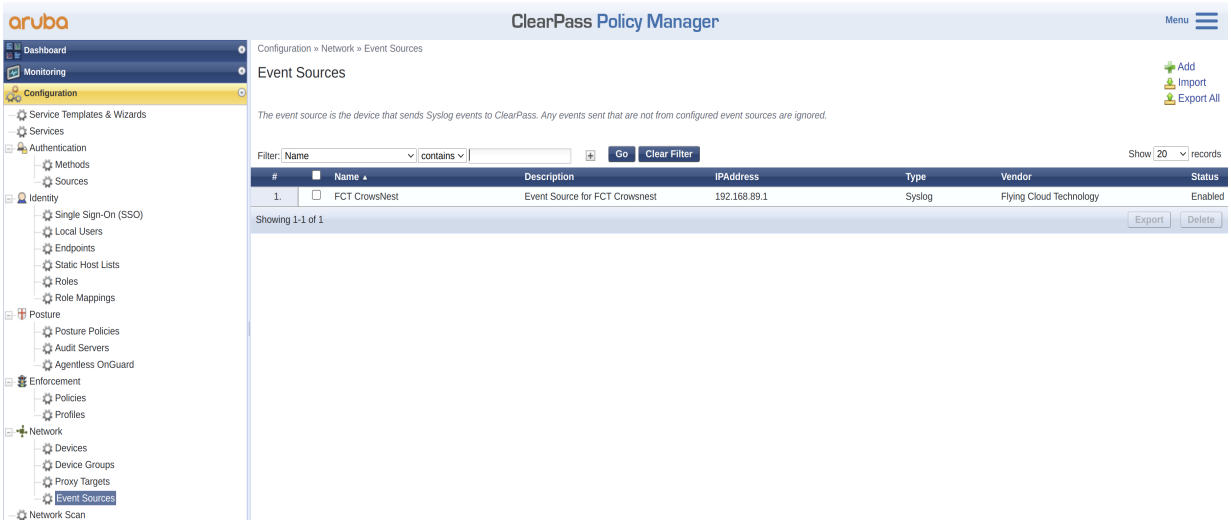
6. Download ingress event dictionary from CrowsNest platform. The dictionary contains the grok filter to parse attributes from CrowsNest syslog and a list of output attributes that can then be used for policy evaluation in ClearPass Policy Manager.



7. Import the ingress event dictionary to ClearPass



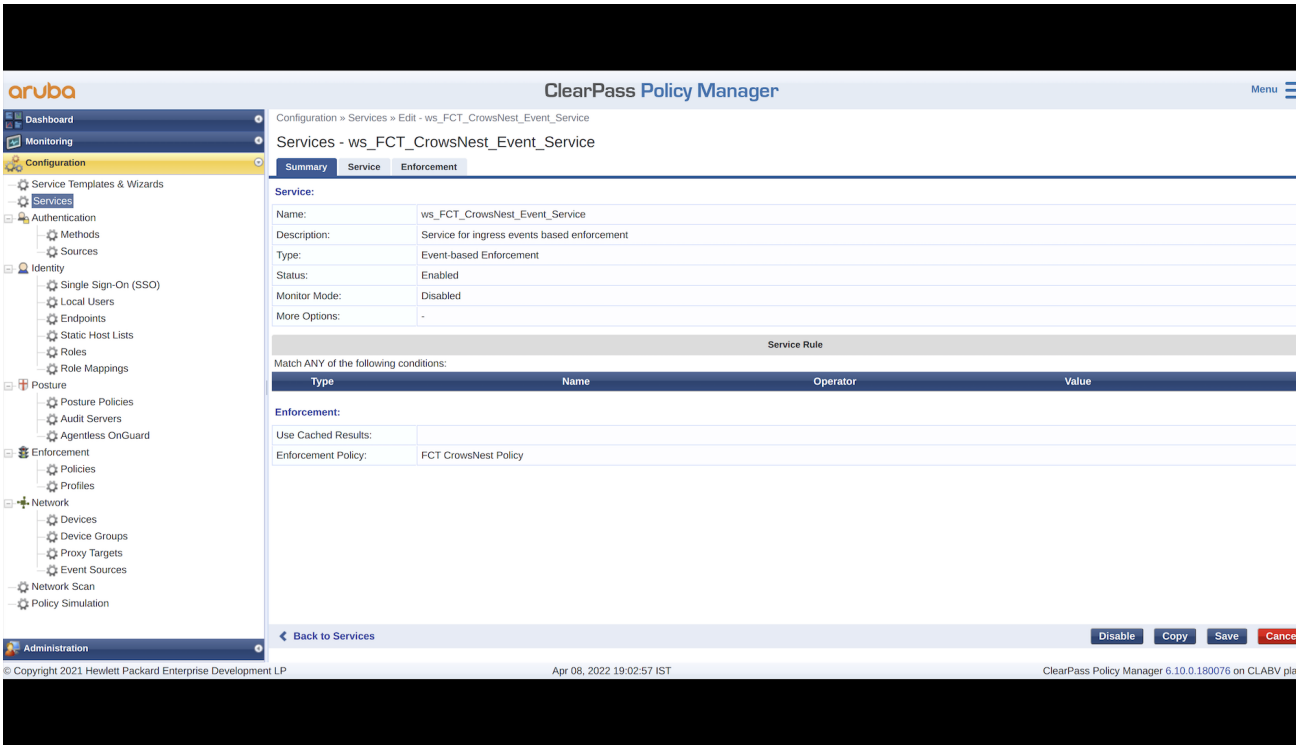
8. Create an Ingress event source with CrowsNest IP and vendor as Flying Cloud

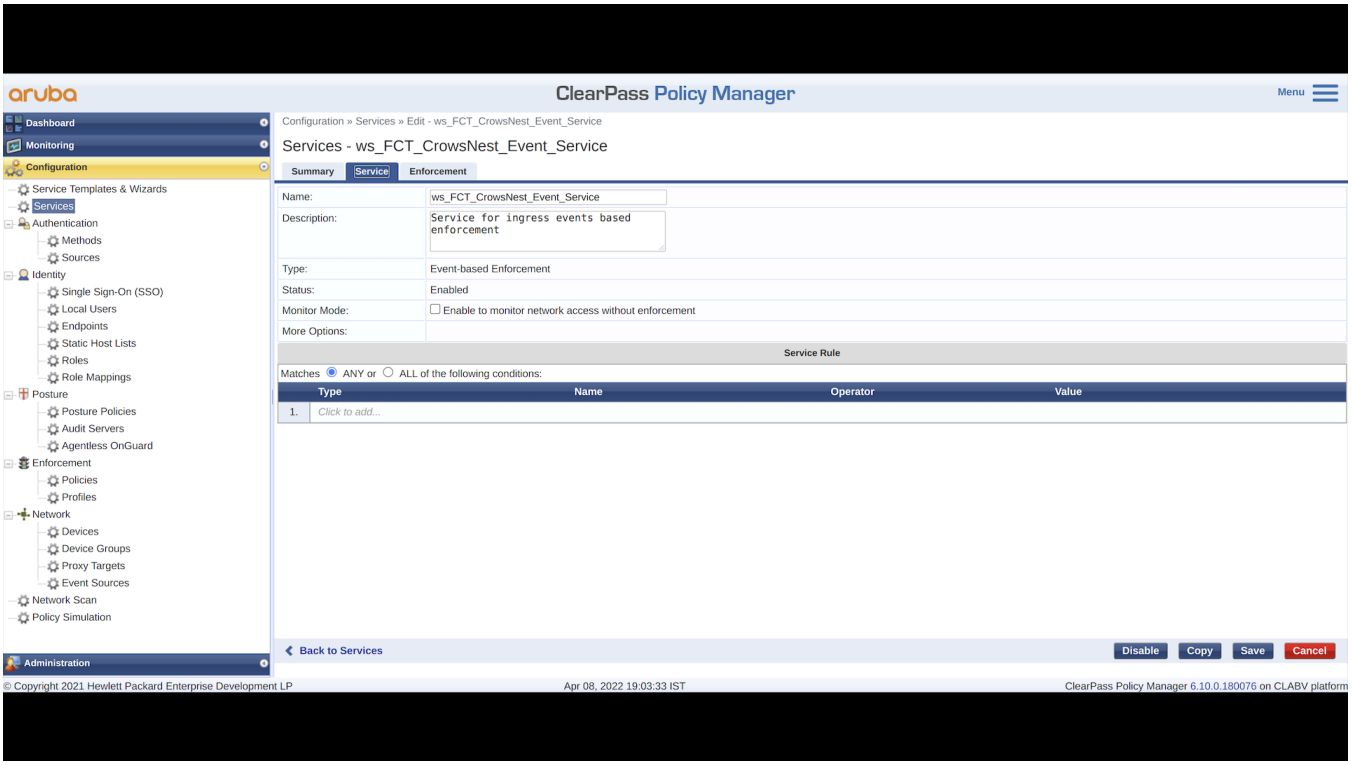


9. Configure a service in ClearPass to process ingress event (syslog) from CrowsNest. Ingress Event Engine (IEE) architecture and Event-based Enforcement service setup is described in detail in the following tech note.

   https://asp.arubanetworks.com/downloads/documents/RmlsZTowZTYxZjk5YS1kMmM0LTExZWEtOWZjOS0zZjkzYmM4MTZhMGI%3D

   The event enforcement in ClearPass can be configured to update an endpoint attribute to mark the device as compromised. We can also use RADIUS dynamic authorization type enforcement in ClearPass to disconnect the user from the network or change the role associated with the malicious user.




aruba
ClearPass Policy Manager
Menu
Dashboard
Monitoring
Configuration
Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Posture Policies
Audit Servers
Agentless OnGuard
Enforcement
Policies
Profiles
Network
Devices
Device Groups
Proxy Targets
Event Sources
Network Scan
Policy Simulation
Administration
Configuration » Services » Edit - ws_FCT_CrowsNest_Event_Service
Services - ws_FCT_CrowsNest_Event_Service
Summary
Service
Enforcement
Name:
ws_FCT_CrowsNest_Event_Service
Description:
Service for ingress events based enforcement
Type:
Event-based Enforcement
Status:
Enabled
Monitor Mode:
Enable to monitor network access without enforcement
More Options:
Service Rule
Matches ANY or ALL of the following conditions:
Type
Name
Operator
Value
1.
Click to add...
Back to Services
Disable
Copy
Save
Cancel
© Copyright 2021 Hewlett Packard Enterprise Development LP
Apr 08, 2022 19:03:33 IST
ClearPass Policy Manager 6.10.0.180076 on CLABV platform