



RSA Ready Implementation Guide for RSA Security Analytics

Last Modified: October 1st, 2014

Partner Information

Product Information	
Partner Name	APCON, Inc.
Web Site	http://www.apcon.com
Product Name	IntellaFlex Series 3000
Version & Platform	ACI-3036 v2.20 build 002
Product Description	In today's competitive business environment, network uptime offers a critical advantage. In generating revenue. APCON understands this focus on performance and designed the Series 3000 switching family to achieve maximum uptime.



Solution Summary

The APCON INTELLAFLEX Series 3000 intelligent network monitoring switch is a scalable solution to address enterprise-grade datacenter requirements for scaling usage of network analysis tools. With up to 288 non-blocking ports of INTELLAFLEX 10G Ethernet in a single 8RU chassis, APCON provides both data throughput capacity and chassis port density. APCON has introduced an XR series of products to facilitate aggregation requirements and advanced features such as deduplication, time stamping, packet slicing, and protocol tag removal.

By combining APCON IntellaFlex with RSA Security Analytics, you empower network forensic and packet capture devices by providing customized data streams aggregated from multiple points on the production network. Advantages of such a solution include preventing data loss, collecting more relevant data per packet capture device, de-duplication for tool optimization and masking to address compliance concerns.

RSA Security Analytics Tested Features	
IntellaFlex Series 3000 ACI-3036 v2.20 build 002	
Flow / Traffic Mapping	Yes
De-duplication	N/A***



***The ACI-3036 chassis as tested does not support deduplication. To support deduplication, an advanced services blade is required. Deduplication-capable blades are available for both the 3000 Series and XR Series platforms from APCON.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the APCON IntellaFlex device with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All APCON components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! > Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure the APCON IntellaFlex is properly configured and secured before deploying to a production environment. For more information, please refer to the APCON IntellaFlex documentation or website.

APCON IntellaFlex Configuration

Launching the WebX Management Interface

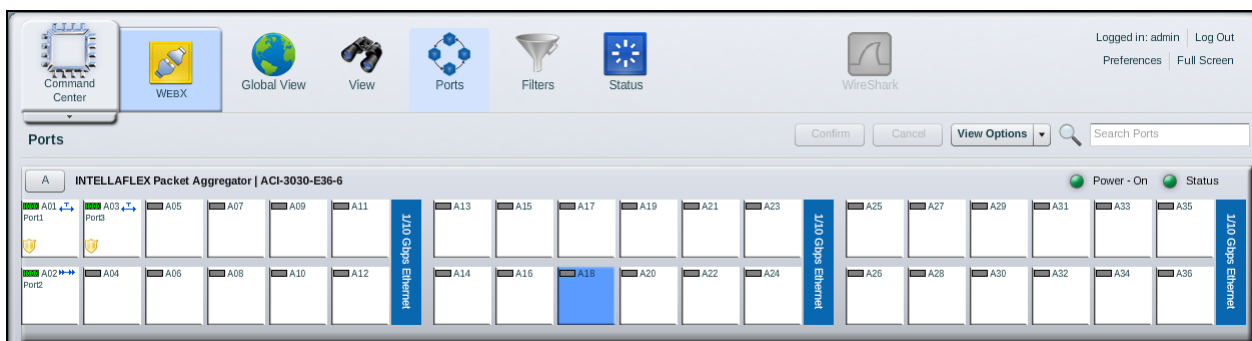
WebX provides a state-of-the-art interface for managing the IntellaFlex Series 3000 switches. The software is embedded in the switch; no initial installation is required. WebX includes tools to manage switch settings and easy-to-use ways to create and monitor connections through the switch.

To log into WebX:

Open a web browser and enter the IP address of the IntellaFlex switch. The WebX log-in window is displayed:




1. The WebX Ports window is displayed. The number and type of ports displayed reflects the current configuration of blades installed in the chassis:



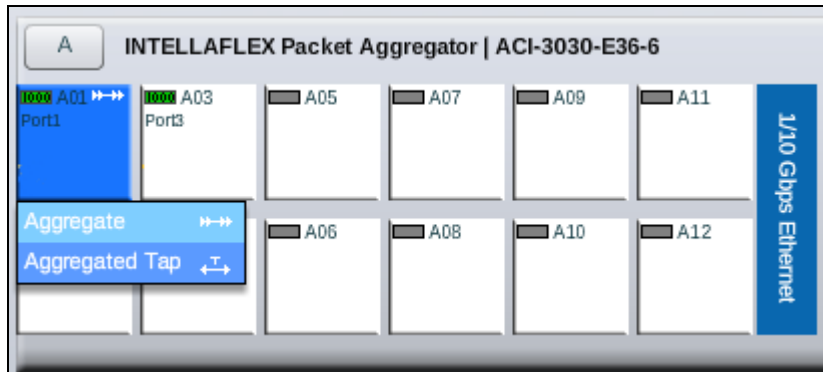
Configuring Port Connections

With WebX, you can quickly make several types of connections, depending on the blades installed in the chassis. In this instance, an aggregated TAP connection was created for the purposes of testing the integration.

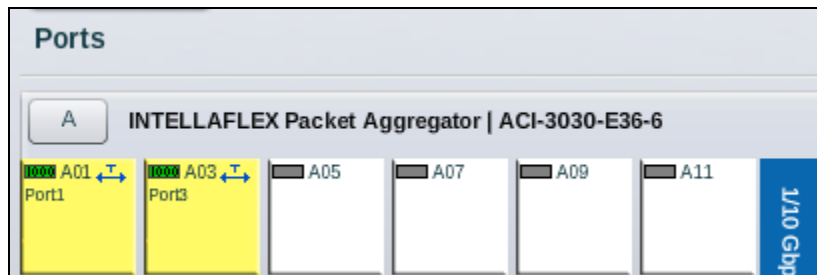
 **Note:** For more information on the many connection types supported and their associated configuration steps, consult the document entitled **WebX User Manual with NetVis**.

The basic steps to create an aggregated TAP connection are as follows:

1. On the WebX Ports page, select a port. The port is highlighted in blue until you select a connection.
2. From the connection menu, choose **Aggregated TAP**. The port is now highlighted and displays the aggregated TAP connection indicator:

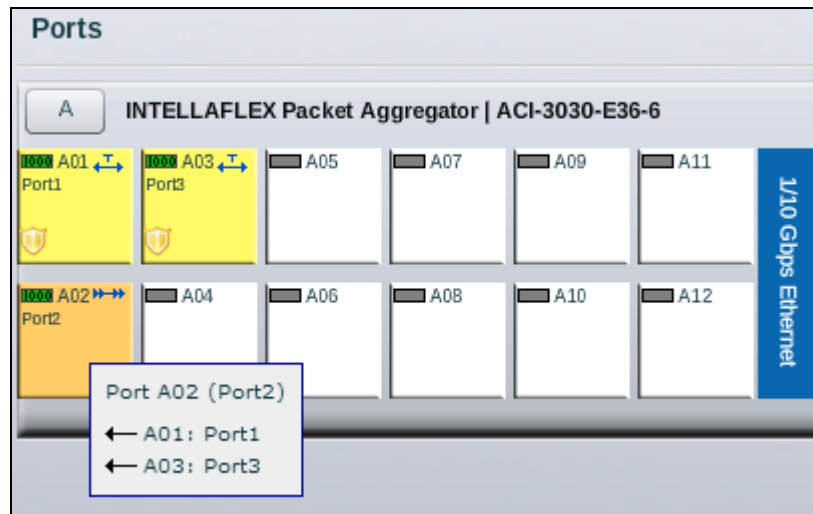


3. Select another port. The selected port highlights yellow and displays the aggregated TAP connection indicator.

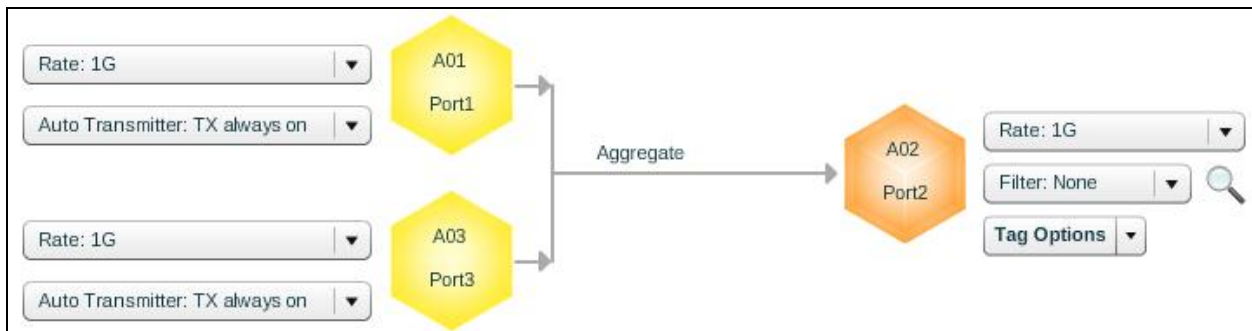


4. Continue to select pairs of source ports if needed. Any additional source ports also highlight in yellow and display the aggregated TAP connection indicator.
5. After selecting pairs, click **Set**.

6. Select a destination port. The port is highlighted in orange and displays the aggregated connection indicator:




7. Click **Confirm**. Once the connection has been created you can view its properties by selecting **Edit Connection**:



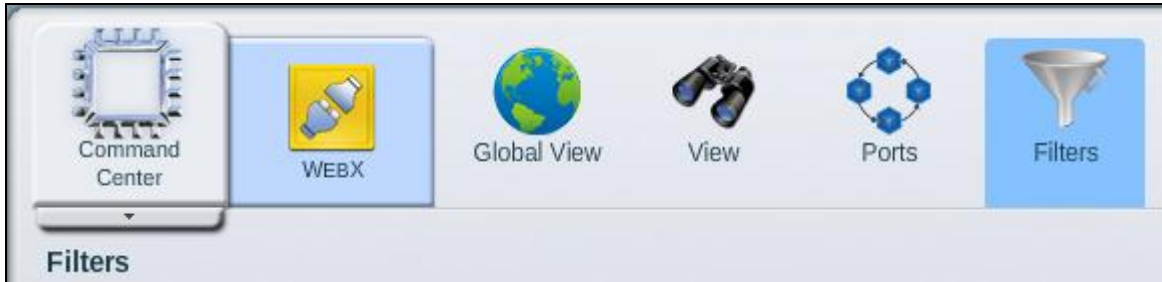
Configuring Traffic Filtering

APCON's intelligent network monitoring switches provide the ability to filter data streams as they enter the switch (at the ingress port) or exit the switch (at the egress port). APCON also has a Multi-Stage Filtering option available enabling filter channels mapping filter matches to specific egress ports. Filtering options allow you to aggregate and filter multiple streams to pass along only the packets that you want to monitor. With this reduction of packet volume, an analyzer such as the RSA Security Analytics Packet Decoder, is not overwhelmed with irrelevant data and network monitoring tools are better utilized.

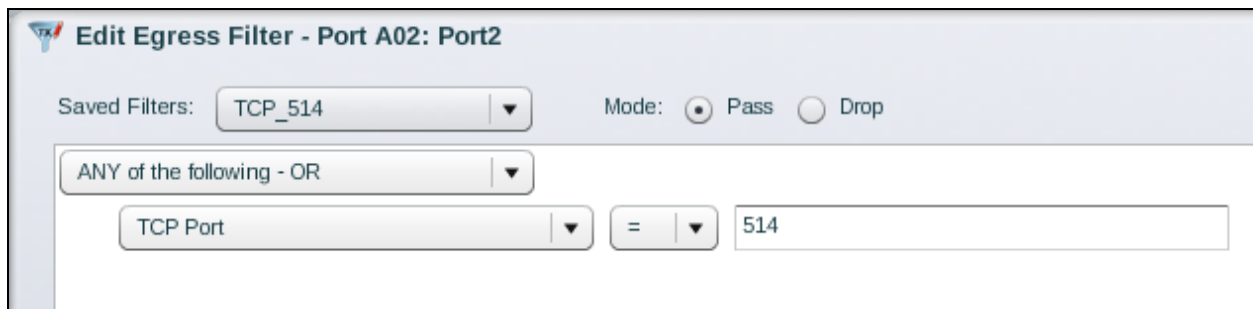
 **Note:** For more information on defining filters and how to configure them, consult the *APCON Filters Guide – Ingress, Egress, and Multi-Stage Filters for firmware release v4.3x.xx*.

For the purposes of this guide we will demonstrate how to create an egress filter for sending filtered traffic to the Security Analytics Packet Decoder. To create an egress filter, perform the following steps:

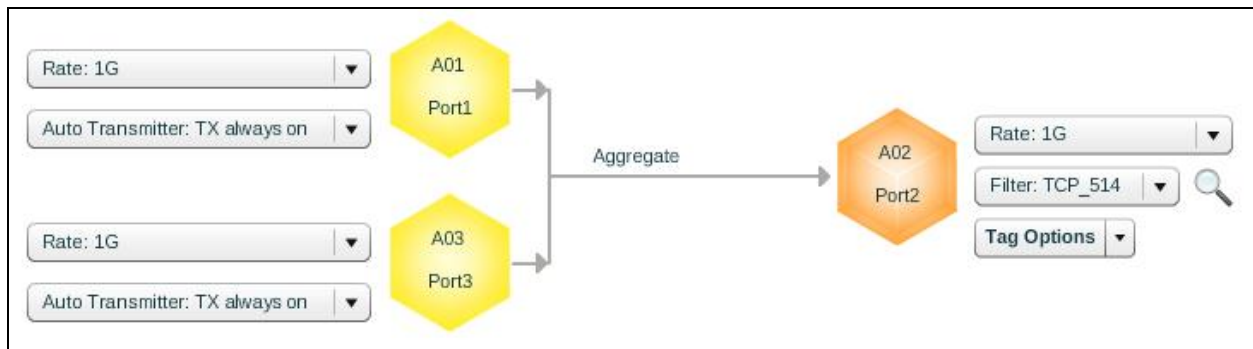
1. Click the **Filters** icon in the WebX toolbar:



2. Click **Add** to add a new filter.
3. Select the desired filter criteria from the drop down menus. In this example, the filter is configured to pass syslog traffic sent via TCP on port 514:



4. After giving the filter a name and description click **Save** to save the filter criteria.
5. Now that the filter has been created, it can be applied as an egress filter on the port that is configured to send traffic to the Packet Decoder. Right click the desired port and select **Edit Connection**:



6. Choose the filter you just created (TCP_514 in this example) to apply it as an egress filter. Click **Apply** to save your changes. Any syslog traffic passing through the aggregated tap will now be forwarded to the Security Analytics Packet Decoder for further processing.

Certification Checklist for RSA Security Analytics

Date Tested: September 29th, 2014

Certification Environment		
Product Name	Version Information	Operating System
RSA Security Analytics	10.3.4	Virtual Appliance
APCON IntellaFlex ACI-3036	v2.20 build 002	Firmware

Security Analytics Test Cases	Result
Packet Loss	
Syslog TCP data consumed by the SA Log Decoder	✓
Syslog UDP data consumed by the SA Log Decoder	✓
Various packet data consumed by the SA Packet Decoder	✓
De-duplication	
Replaying data files to the SA Packet Decoder	N/A***
Traffic Mapping	
Mapping network service ports to dedicated ports	✓
Performance	
SA Log Decoder minimal EPS performance	✓
SA Packet Decoder minimal EPS performance	✓

JEC

✓ = Pass ✗ = Fail N/A = Non-Available Function

***The ACI-3036 chassis as tested does not support deduplication. To support deduplication, an advanced services blade is required. Deduplication-capable blades are available for both the 3000 Series and XR Series platforms from APCON.