Using Trusted IPs

This application note describes how to use Trusted IPs. You can enable this feature using ACEmanager and AirLink Management Service (ALMS).

For more information about getting started with ALMS, see source.sierrawireless.com/airvantage/alms/

For general information about configuring your system using ALMS, see doc.airvantage.net/av/reference/monitor/howtos/changeASystemConfiguration/

Trusted IPs—Inbound restricts access to the AirLink gateway and all LAN connected devices. When enabled, IP packets with a source address not matching those in the list or range of trusted hosts will be ignored/dropped by the gateway.

Warning: *Please note, once Trusted IP functionality is enabled, you will be unable to connect to any services on the gateway, including ACEmanager, unless your IP is in the trusted IP range or list.*

Configuring Inbound Trusted IPs using ACEmanager

You can configure Trusted IPs for inbound traffic on the ACEmanager Security page.

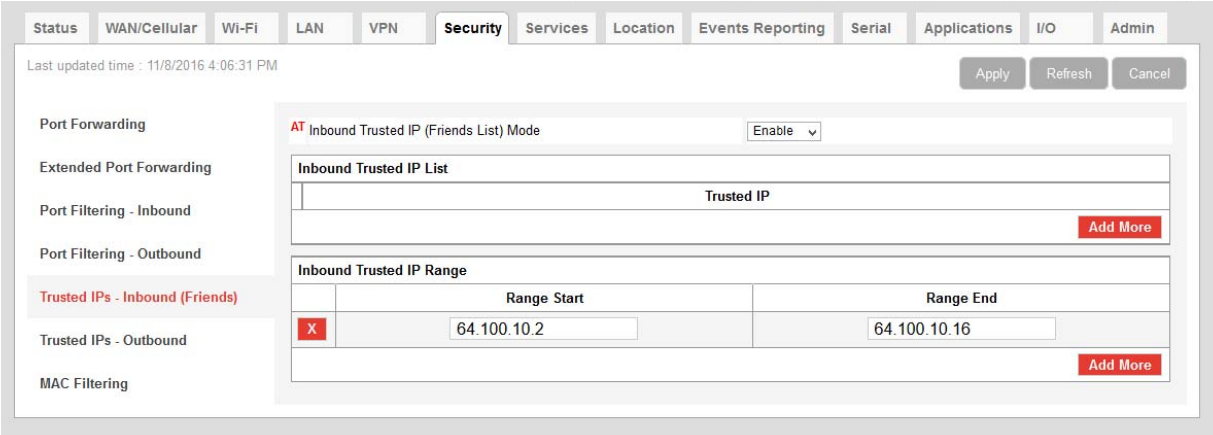


Figure 1: ACEmanager: Security >Trusted IPs - Inbound (Friends)

Field	Description
Inbound Trusted IP (Friends List) Mode	Disables or Enables port forwarding rules. Options are Disable (default) or Enable.
Inbound Trusted IP List	Enter a single trusted IP address for example 64.100.100.2. Click Add More to add additional IP addresses to the list.
Inbound Trusted IP Range	Use this section of the page to enter a range of trusted IP addresses.

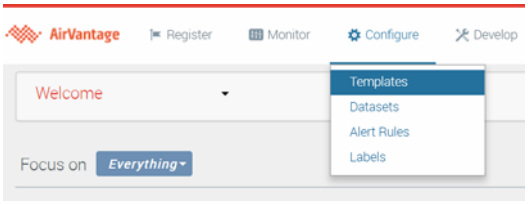
Field	Description
Range Start	Specify the start and end IP addresses for the trusted IP address range, for example, entering 64.100.10.2 as the Range Start and 64.100.10.15 as the Ranges End would allow 64.100.10.5 but would not allow 64.100.10.16.
Range End	

Configuring Trusted IPs using ALMS

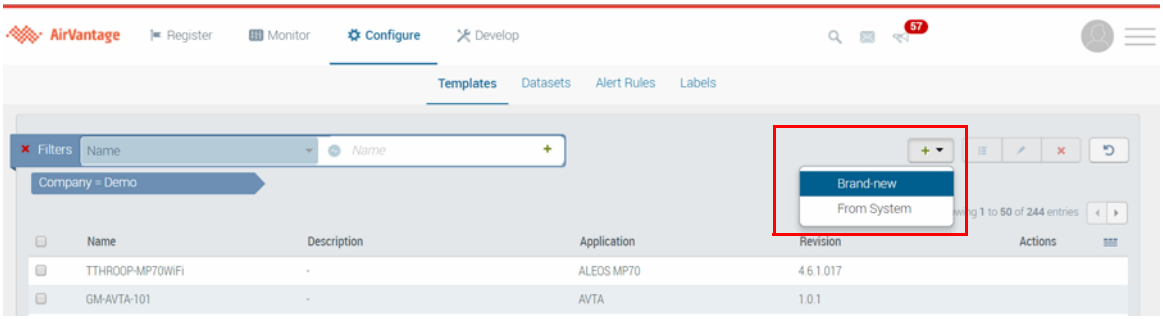
The most efficient way to configure Trusted IPs is to create a template and then apply the template to several devices at once.

To create and save a template:

1. On the AirVantage menu, click Configure and select Templates.

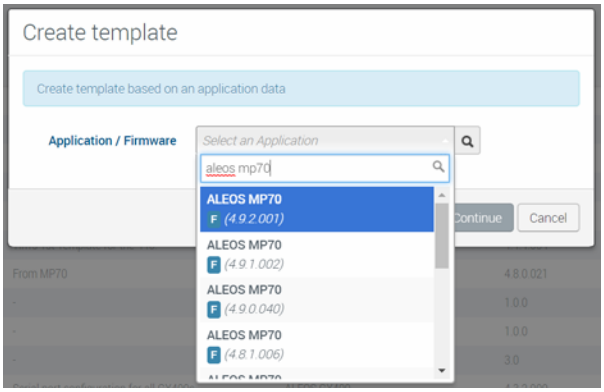


2. Click the Create button, and select Brand-new.



The Create template window appears.

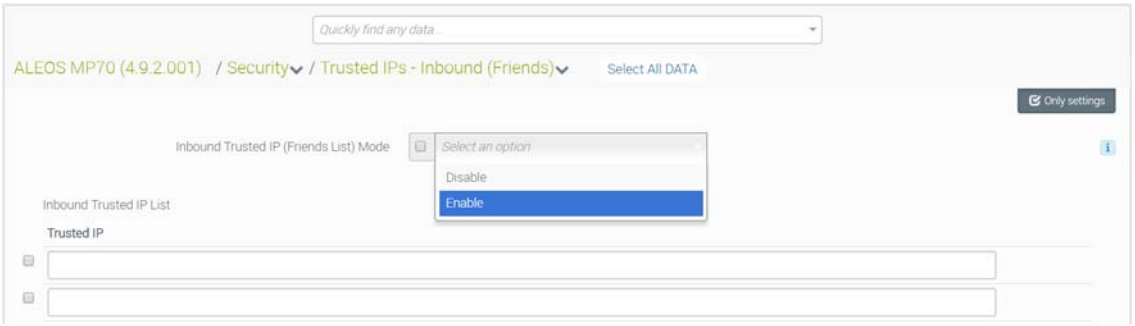
3. Select the application and firmware to which you want to apply the template.



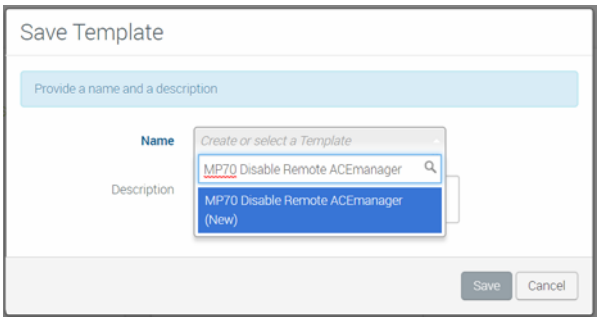
4. Click Continue.

A page of ALEOS setting appears.

5. Click Security > Trusted IPs.
6. On the Inbound Trusted IP (Friends List) Mode field, select Enable.



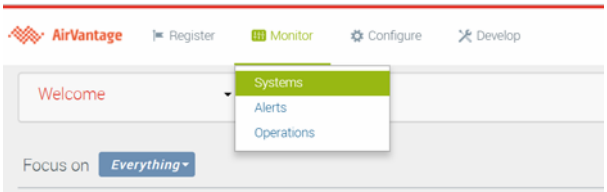
7. In the fields below Inbound Trusted IP List, enter trusted IP addresses; for example, 64.100.100.2.
8. In the fields below Inbound Trusted IP Range, specify the start and end IP addresses for the trusted IP address range; for example, entering 64.100.10.2 as the Range Start and 64.100.10.15 as the Range End would allow 64.100.10.5 but would not allow 64.100.10.16.
9. In the Modified settings window at the bottom of the page, click Save.
10. In the Save Template window, enter a name and description for your template.



11. Click Save.

To apply the template to your devices:

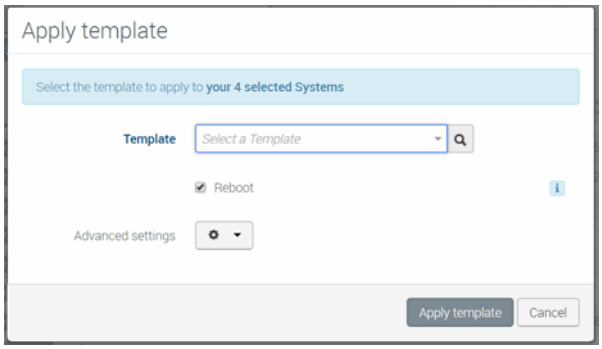
1. Click Monitor and select Systems.



The list of systems appears.

2. Using the checkboxes along the left side, select the systems you want to configure.
3. Click the Apply template button.

4. In the Apply template window, select your template.



5. Click Apply template.