Additional ACI Security Features

This chapter contains the following sections:

Additional Security Features

The following are a list of security features currently supported in ACI but documented in other configuration guides found at https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html:

- For **Contract** configuration see the *Cisco APIC Basic Configuration Guide, Release 3.x* and the *Operating Cisco Application Centric Infrastructure*.
- For **EPG Communication Rules** see the *Use vzAny to Automatically Apply Communication Rules to all EPGs in a VRF* Knowledge-Based article.
- For **In-Band and Out-of-Band Management Access** see the *Cisco APIC and Static Management Access* Knowledge-Based article, and the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 2.2(3)*.
- For **Intra-EPG Isolation Enforcement** see the *Cisco ACI Virtualization Guide, Release 3.0(1)*.
- For **Traffic Storm Control** see the *Cisco APIC Layer 2 Networking Configuration Guide*.

Turning Off Generated Session Log Files in APIC

This section describes how turn off the generated logs in APIC. If you have configured any sort of monitoring for your fabric, you will see the following log file:

```
Body of session record log example:
From-127.0.0.1-client-type-REST-Success
```

To turn off the generated session log files in APIC, perform the following steps:

Step 1 On the menu bar, choose **ADMIN** > **AAA**.

Step 2 In the **AAA** pane, click **Security**.

Step 3 In the **User Management – Security** pane, verify that the default **Management Settings** pane is chosen.

Step 4 In the **Include Refresh in Session Records** field, uncheck the box to disable the generated session log files.

Step 5 Click **Submit**.

Step 6 Click **Submit Changes**.