New and Changed Information

This chapter contains the following sections:

New and Changed Information

The following tables provide an overview of the significant changes to this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Information for Cisco APIC Release 6.1(4)

Feature	Description	Where Documented
SPAN session scale mode	SPAN session support in scale mode for FX2 and newer switches. In scale mode, there is no limit to the number of source interfaces per switch; however, the "no filter" option is not supported. The filter mode supports a maximum of 63 source interfaces per switch. Prior to the 6.1(4) release, the filter mode was implicitly used as the only mode for all SPAN sessions.	SPAN session in the scale mode

Table 2: New Features and Changed Information for Cisco APIC Release 6.1(3)

Feature	Description	Where Documented
Korea SES custom password requirements	When a local user is configured using the GUI, the password must meet additional requirements. Password strength parameters can be configured by either creating **Custom Conditions** or by selecting the **Default Three Conditions**, which include lowercase letters, digits, and special characters.	Configuring a Local User

Table 3: New Features and Changed Information for Cisco APIC Release 6.1(2)

Feature	Description	Where Documented
ERSPAN Destination on ACI Access Span L3Uut	Use the SPAN destination group feature to direct ERSPAN traffic to a remote endpoint behind an L3Out.	Configuring a Destination Group for a Tenant SPAN Policy Using the Cisco APIC GUI

Table 4: New Features and Changed Information for Cisco APIC Release 6.1(1)

Feature	Description	Where Documented
Restrict Cisco APIC OOB management subnet IP addresses from accessing the OOB IP address	You can restrict access to the Cisco APIC by enabling Strict Security on the Cisco APIC out-of-band (OOB) subnet. In previous releases, a user could access the Cisco APIC using its OOB IP address from the same subnet using ICMP, SSH, HTTP, HTTPS, or TCP 4200, regardless of the user's configuration.	Adding Management Access in the GUI
Support for AES128-CMAC for the Network Time Protocol	You can use the AES128-CMAC authentication scheme for the Network Time Protocol (NTP).	Time Synchronization and NTP