New and Changed Information

This chapter contains the following sections:

New and Changed Information

The following table provides an overview of the significant changes to the organization and features in 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 Behavior for Cisco APIC Release 4.2(4)

Feature or Change	Description	Where Documented
User Lockout After Continuous Failed Attempts to Log in	Starting in release 4.2(4), you can block a user from being able to log in after the user fails a configured number of login attempts. You can specify how many failed login attempts the user can have within a specific time period. If the user fails to log in too many times, then that user becomes unable to log in for a specified period of time.	User Lockout After Continuous Failed Attempts to Log in Configuring User Lockout After Continuous Failed Attempts to Log in using the GUI

New and Changed Information