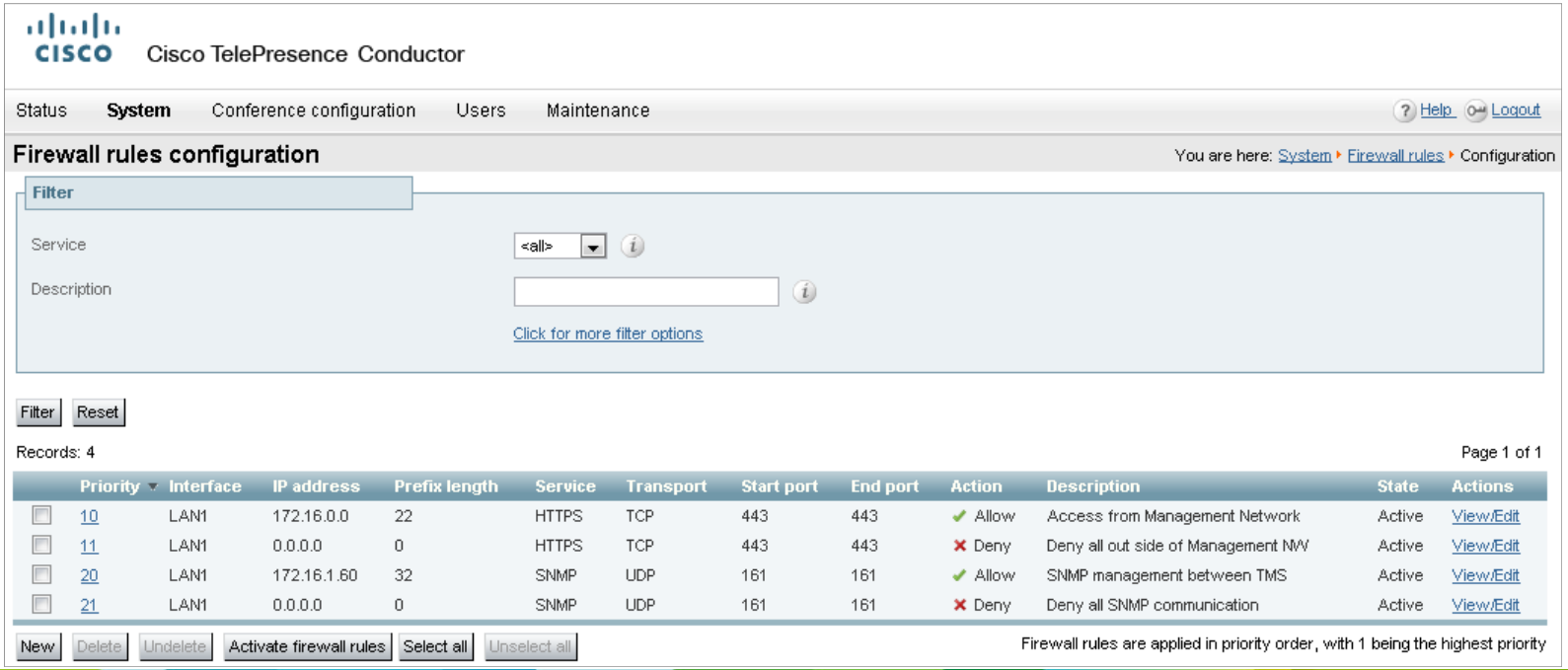
Cisco TelePresence Conductor XC2.0 Introduction

Security Enhancement

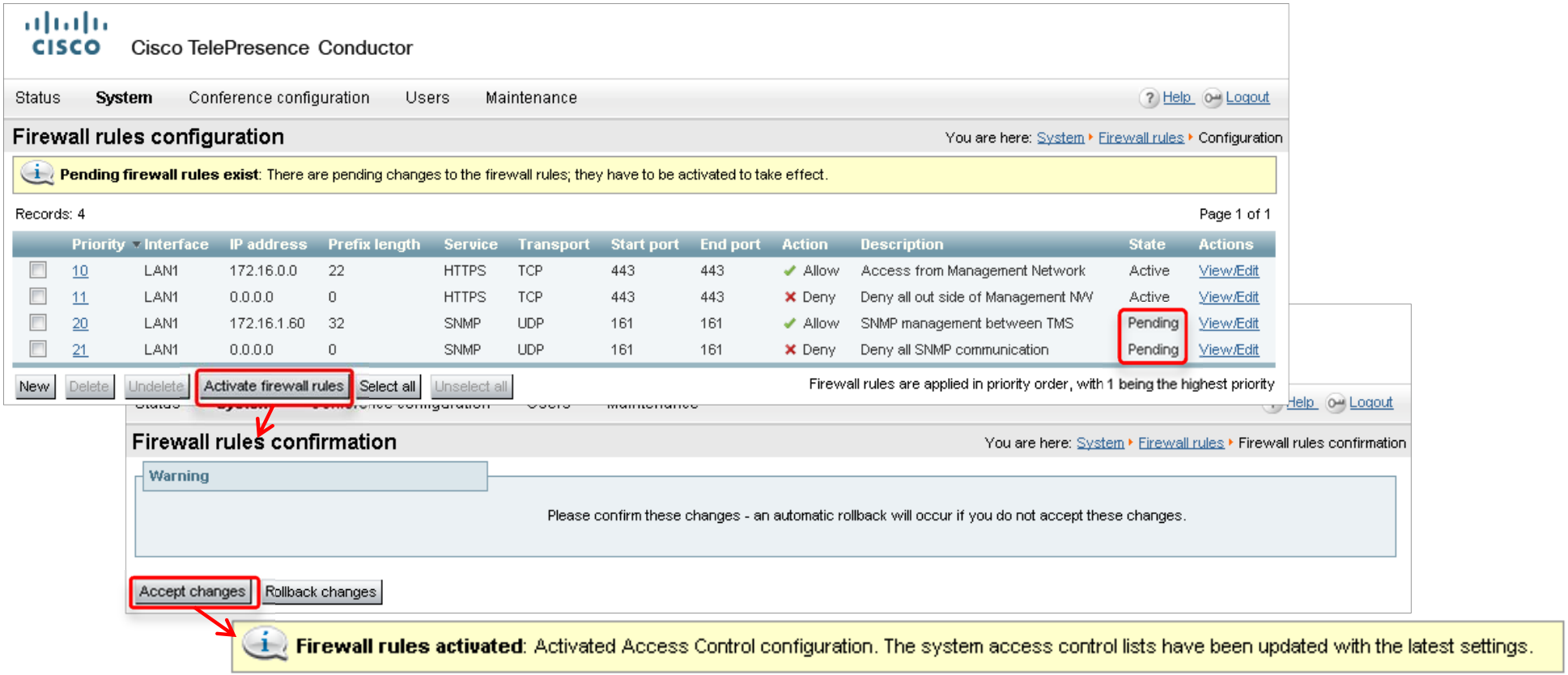
Security Enhancement
Firewall Rules

- Ability to configure rules to control access
  - ✓ Specify the source subnet to allow/deny traffic from
  - ✓ Configure well-known services such as SSH/Telnet, HTTP/HTTPS, SNMP
  - ✓ Custom services based on port range & protocol type
  - ✓ The priority of a rule can be specified and the TelePresence Conductor will then apply the rules in priority order.



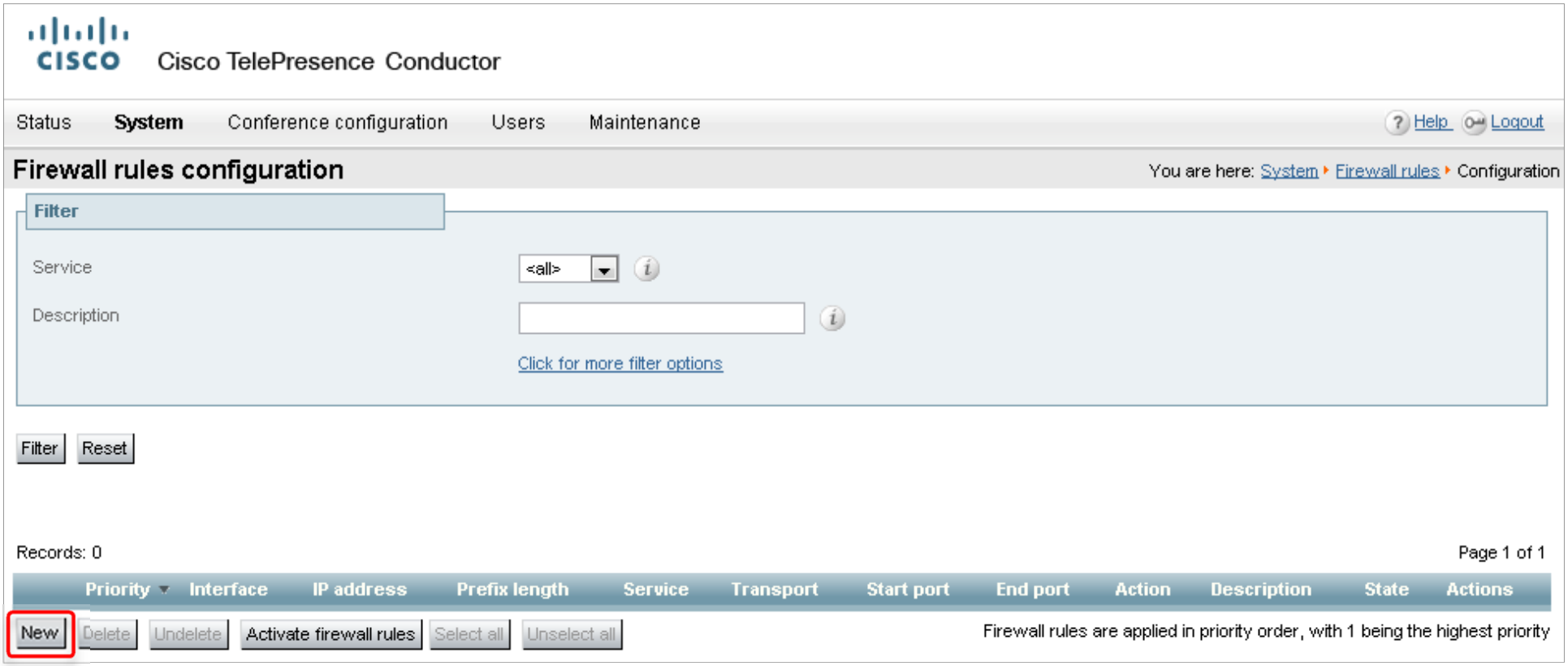
Security Enhancement
Firewall Rules

- Ability to configure rules to control access
  - ✓ Configuration:
    - Safety mechanism - after activating any new rules they have to be positively confirmed - 15 second roll back timer



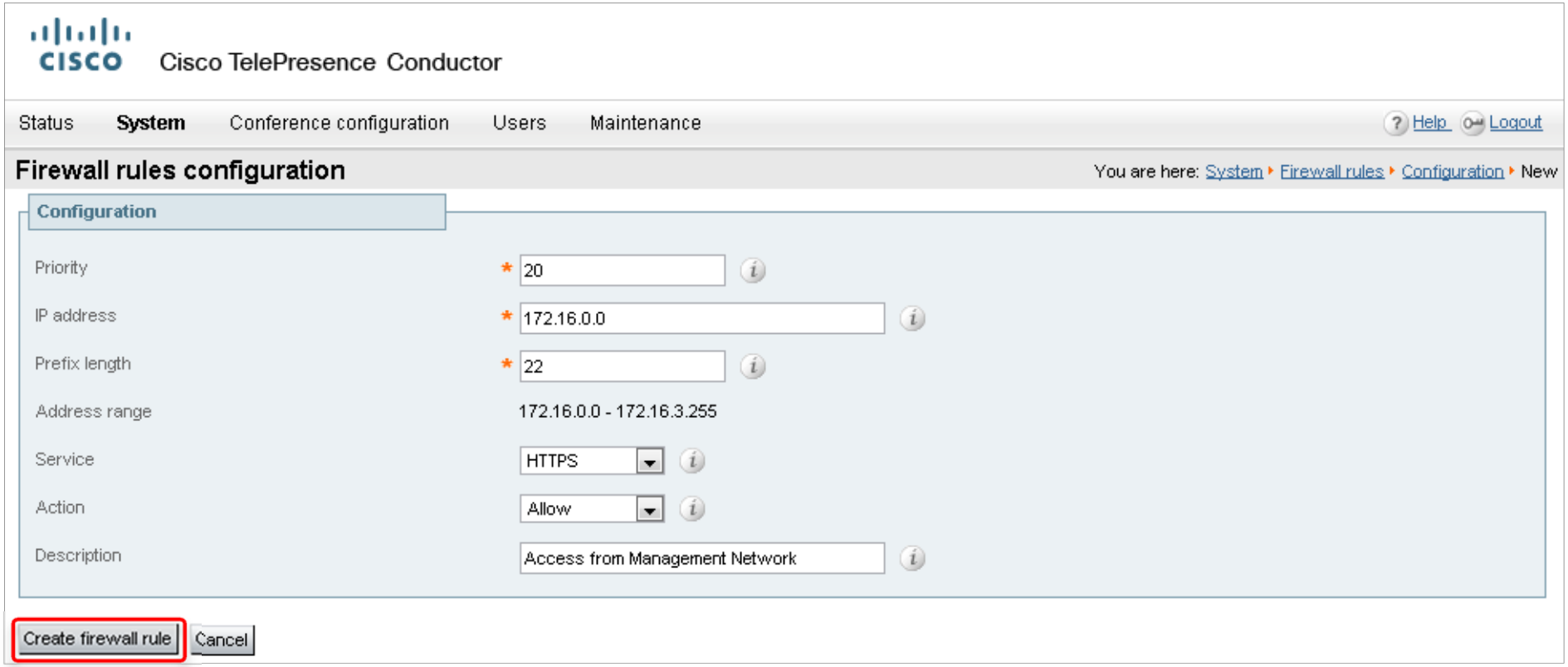
Security Enhancement
Firewall Rules

- Firewall rules configuration
  - ✓ Step 1: Click “New”



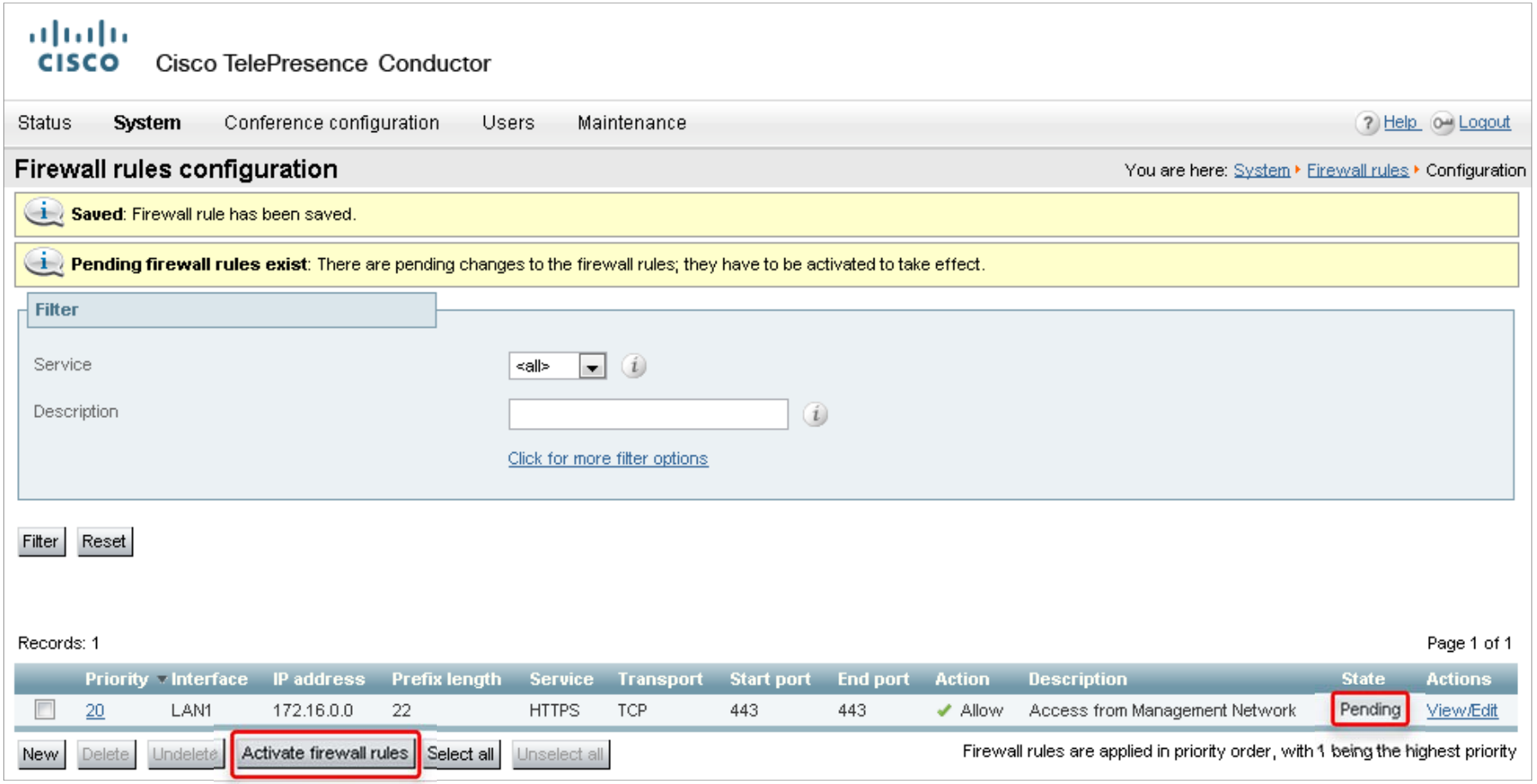
Security Enhancement
Firewall Rules

- Firewall rules configuration
  - ✓ Step 2: Fill out parameter and then click “Create firewall rule”
    - Field with * is mandatory parameter to configure
    - Priority, with 1 being the highest priority



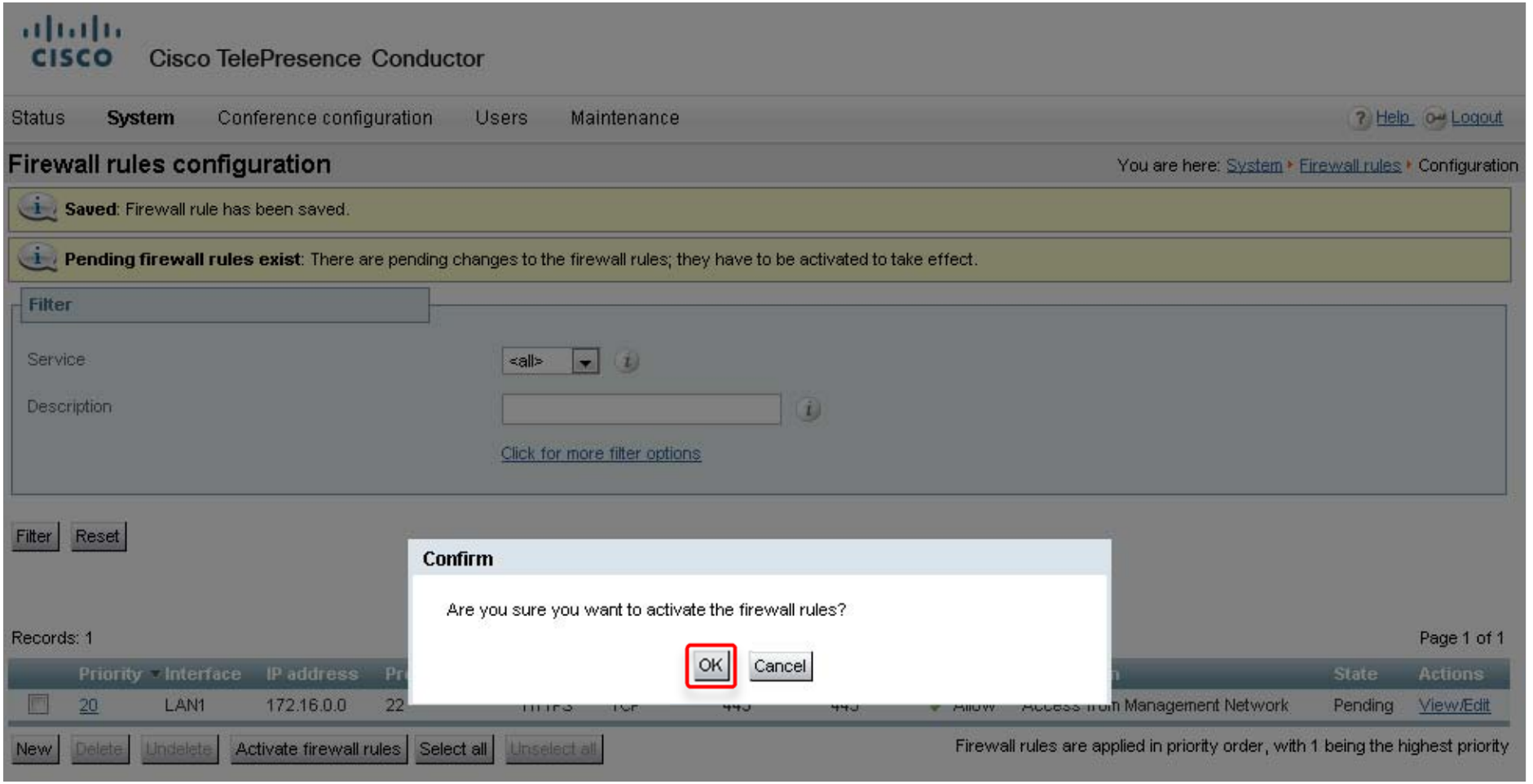
Security Enhancement
Firewall Rules

- Firewall rules configuration
  - ✓ Step 3: Confirm newly configure firewall parameters (status = pending) and then click “Activate firewall rules”



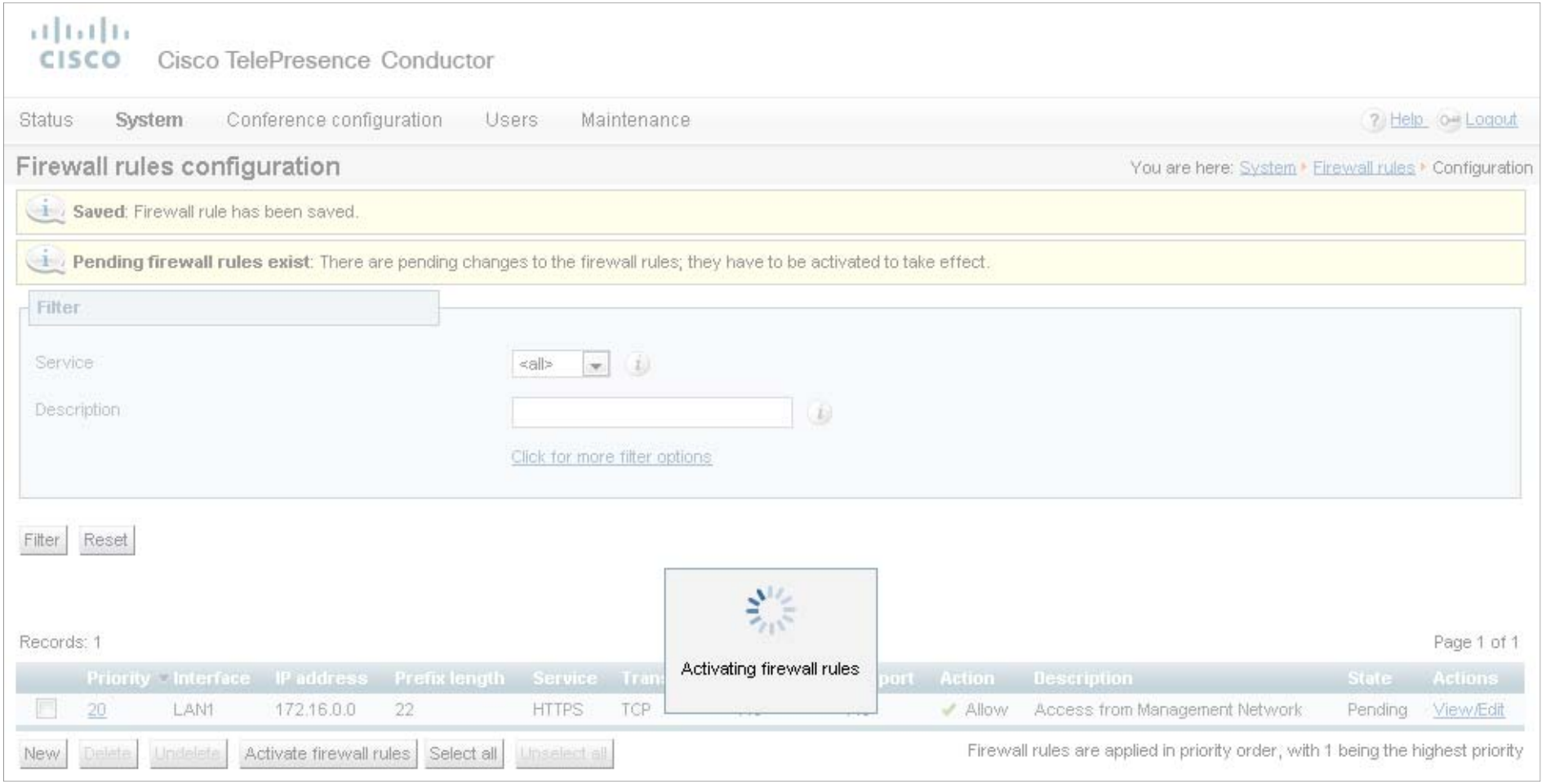
Security Enhancement
Firewall Rules

- Firewall rules configuration
  - ✓ Step 4: click “OK” to proceed firewall rules activation



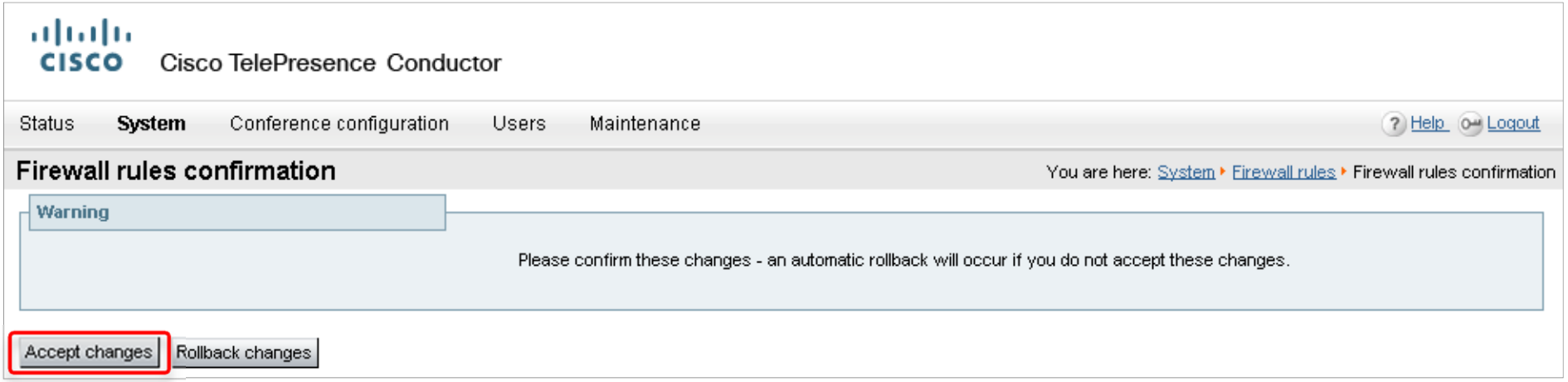
Security Enhancement
Firewall Rules

- Firewall rules configuration
  - ✓ Step 5: Wait while the firewall rules are activated



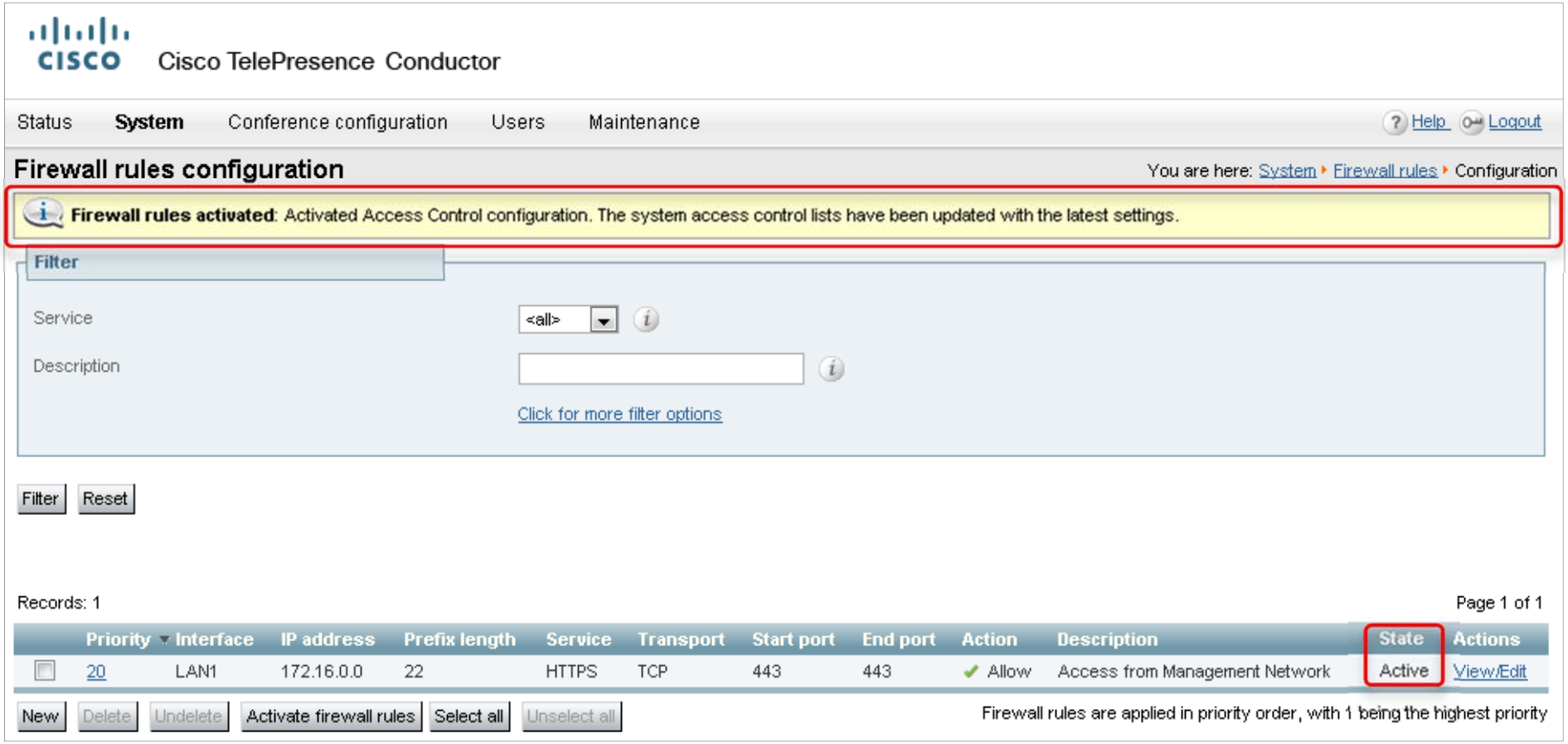
Security Enhancement
Firewall Rules

- Firewall rules configuration
  - ✓ Step 6: Confirm new firewall changes by clicking “Accept changes” to activate firewall rules permanently



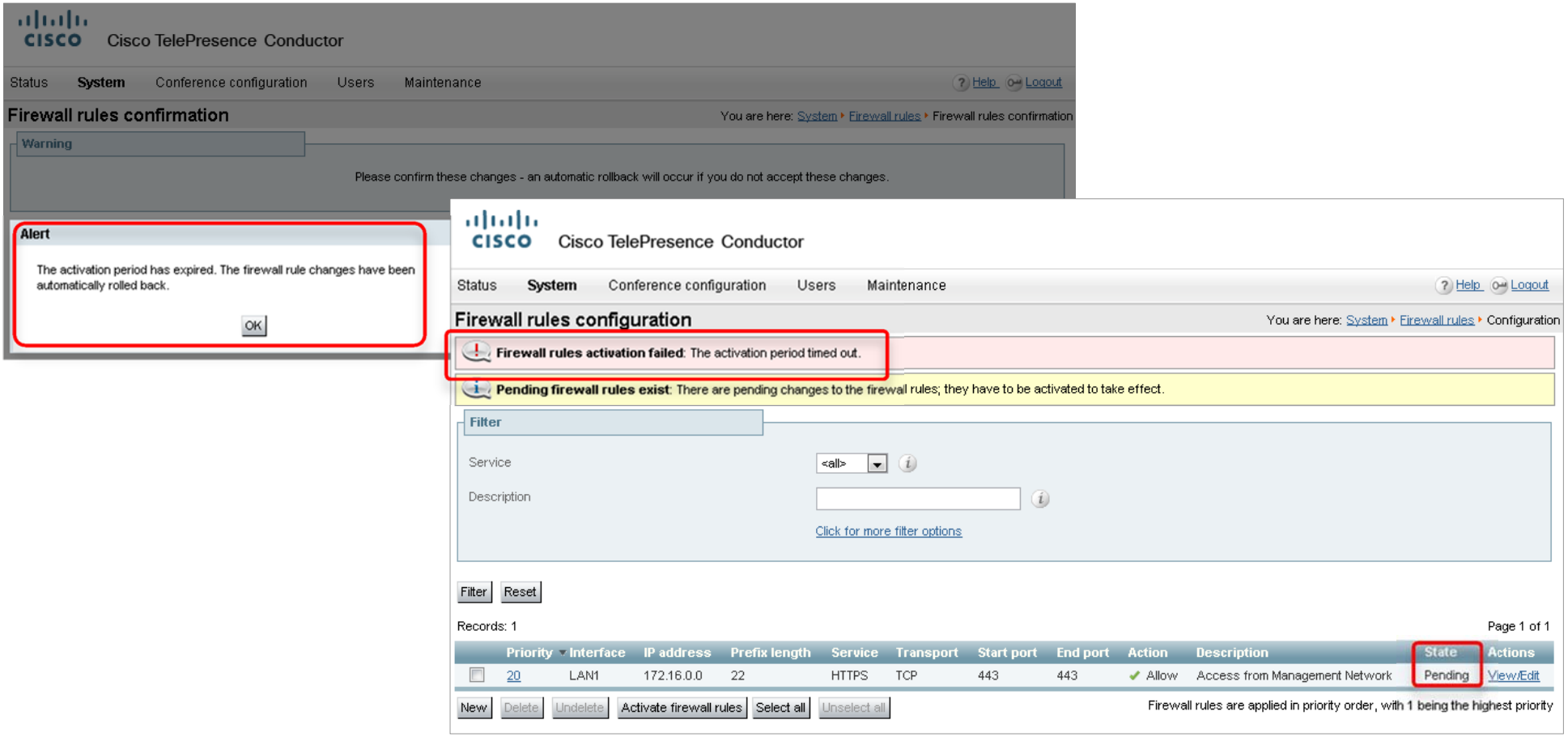
Security Enhancement
Firewall Rules

- Firewall rules configuration
  - ✓ Firewall rules now activated. Check status which should show “Active”



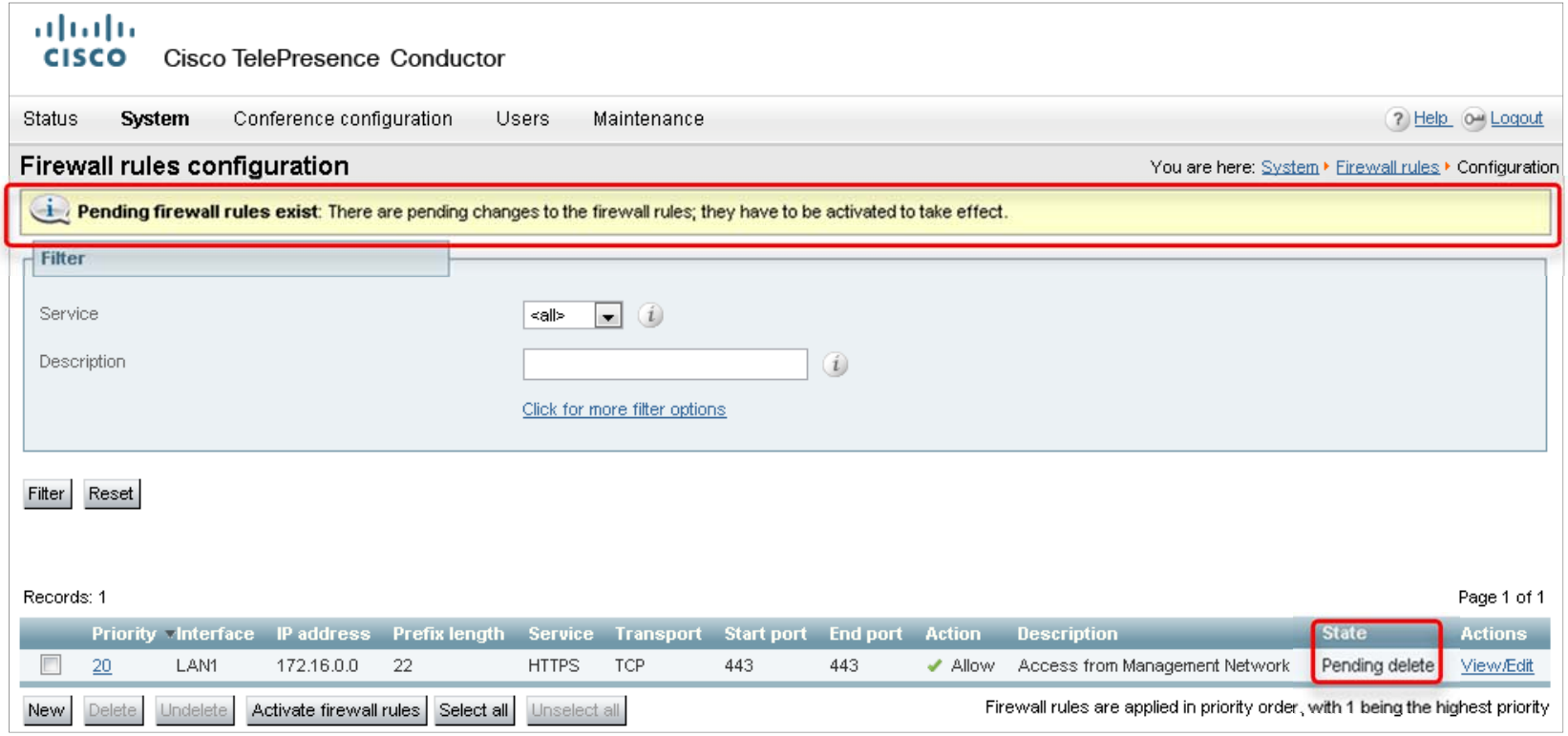
Security Enhancement
Firewall Rules

- Firewall rules configuration
  - ✓ If changes are not accepted in Step 6 within 15 seconds, firewall rule is automatically rolled back and placed into “Pending” status”



Security Enhancement
Firewall Rules

- Firewall rules configuration - deleting the rule(s)
  - ✓ Same “Activate firewall rules” -> “Accept changes” steps will require for deleting any firewall rule which in active status.
  - ✓ Select firewall rule(s) and click “Delete” will bring those firewall rule to be State = “Pending Delete” but rules(s) are not yet deactivate/delete.



Security Enhancement
Firewall Rules

- Firewall rules configuration
  - ✓ Note:
    - The default setting for the Firewall rules will be to allow everything
    - Need to configure rules to lock down the TelePresence Conductor as required

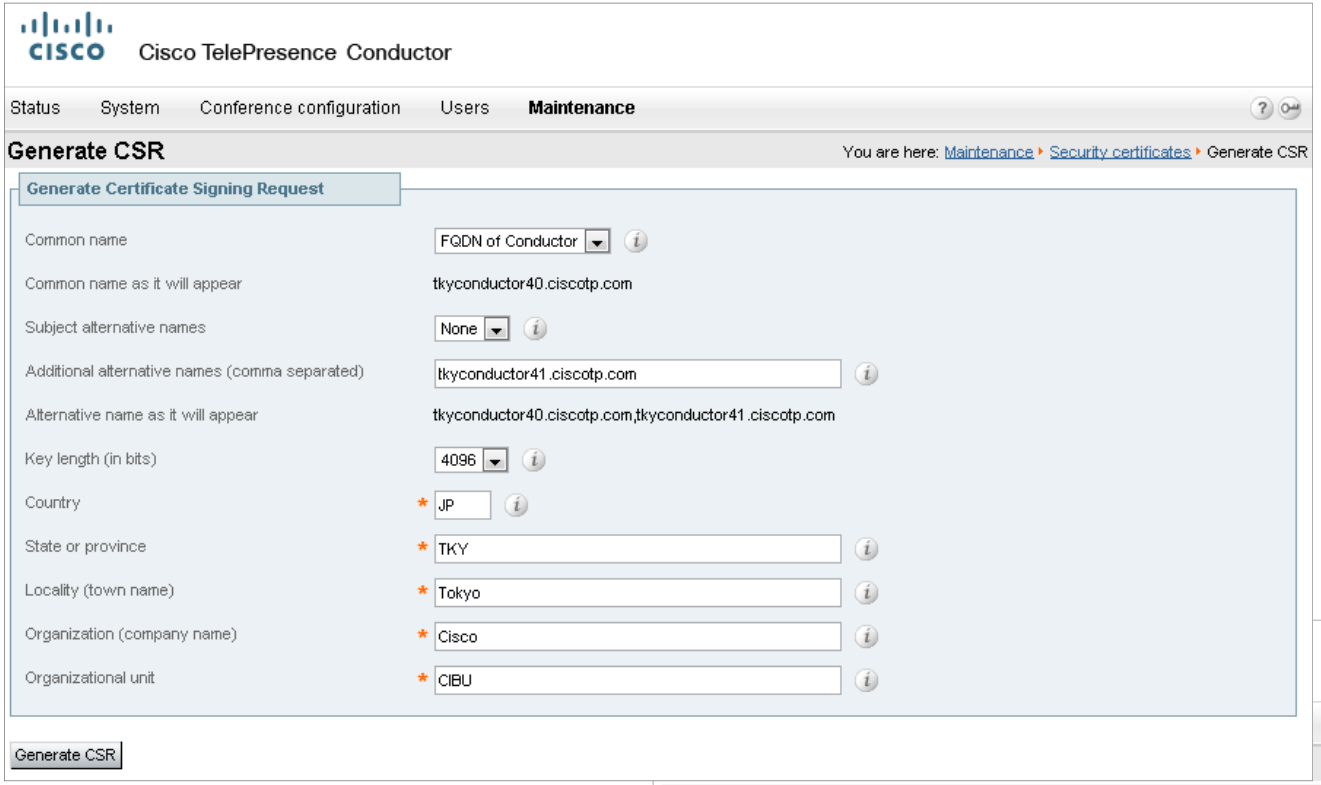
Security Enhancement

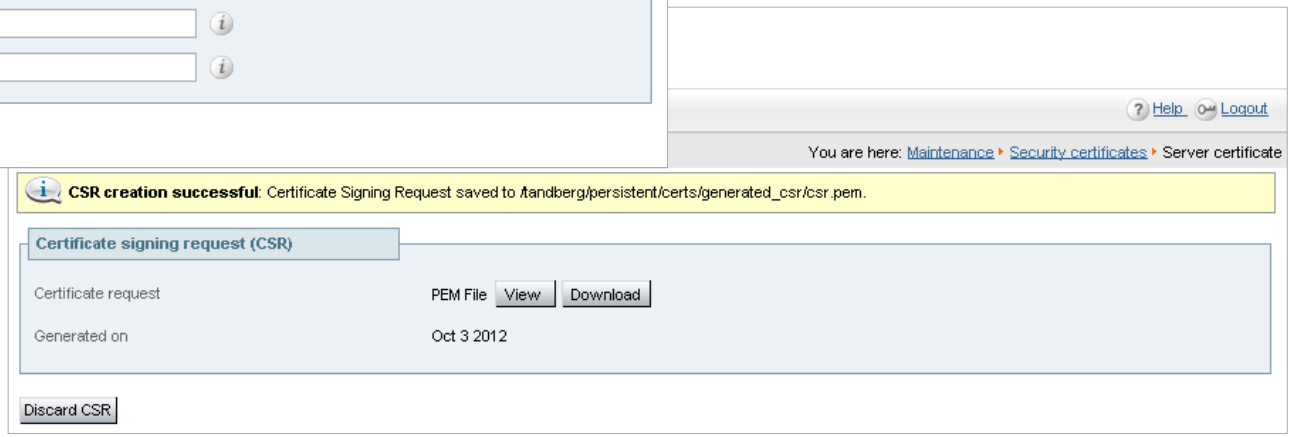
Certificate Signing Request (CSR)

- New mechanism to generate a certificate signing request
  - ✓ TelePresence Conductor now has separate pages for uploading the trusted CA certificate, and for the server certificate loading/requests
  - ✓ Simplify the process of creating CSR, e.g.
  - ✓ Removing the need for external/out-of-band steps to generate certificate requests

Security Enhancement
Certificate Signing Request (CSR)

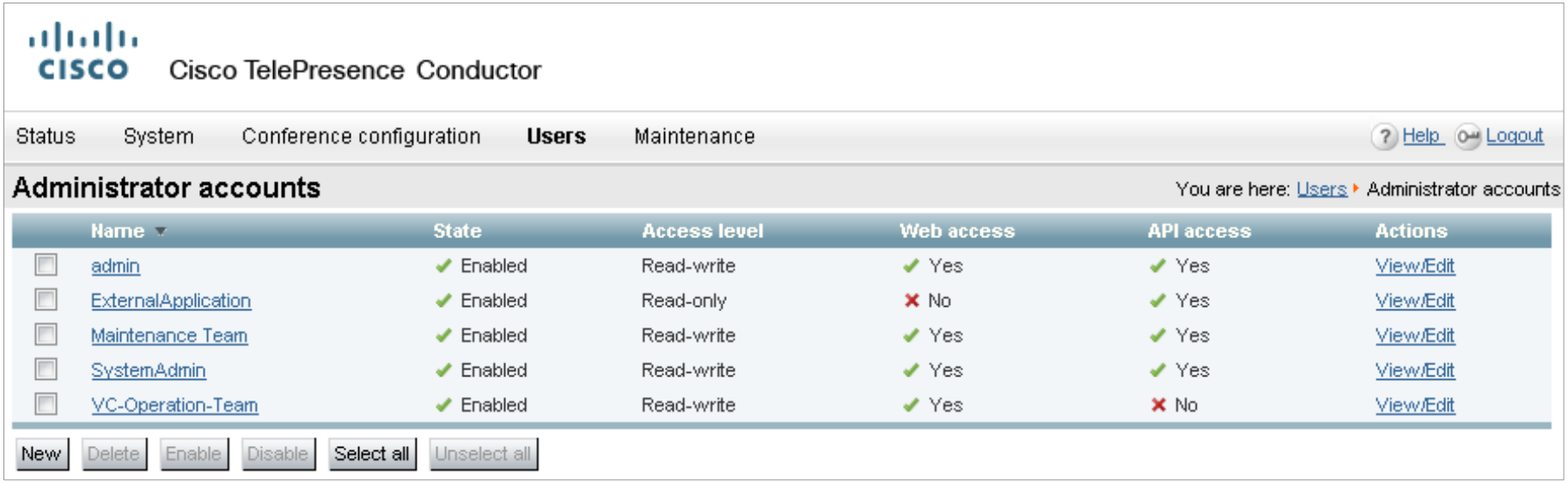
- Generate a certificate signing request





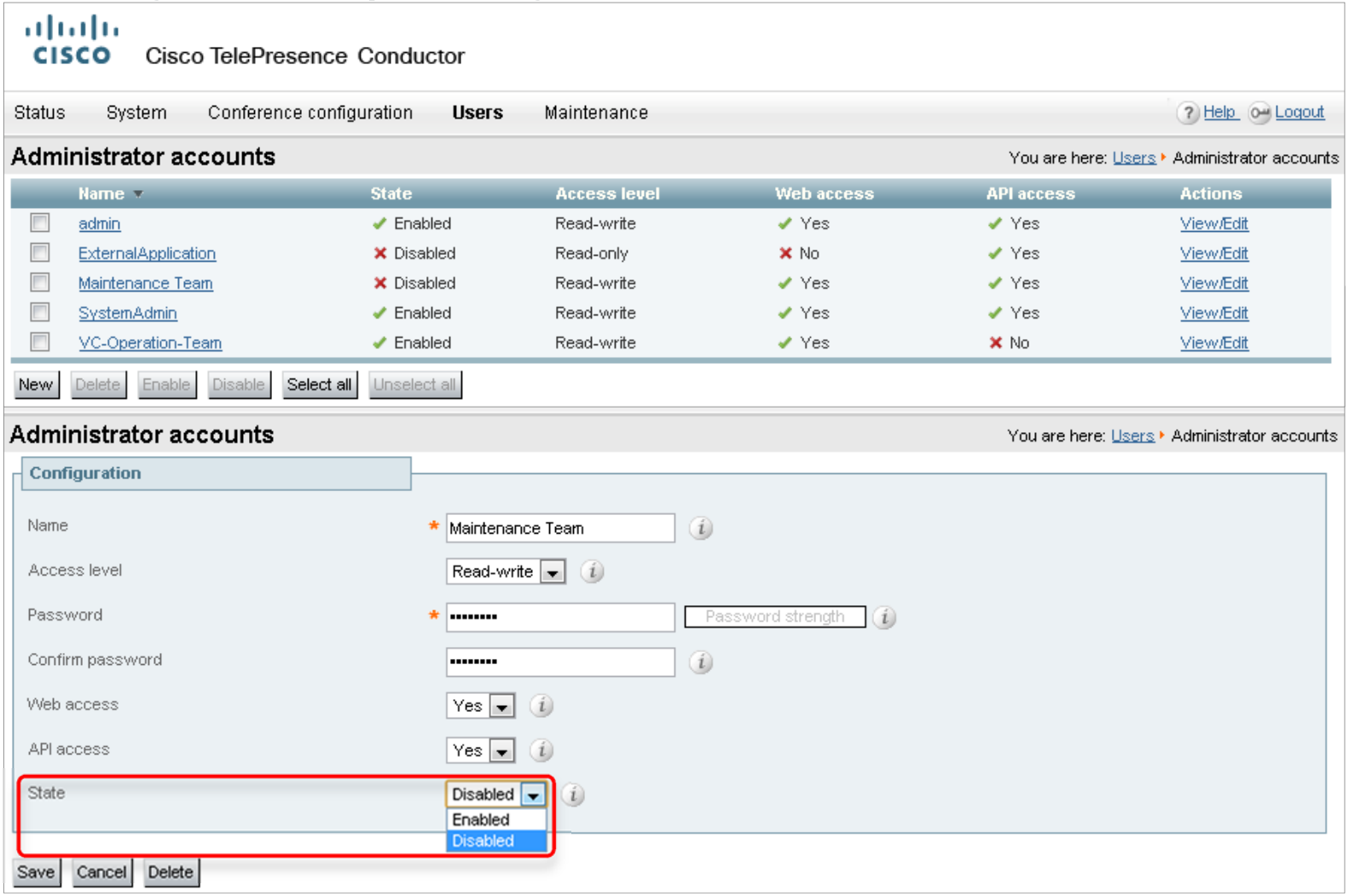
Security Enhancement
Administrator Account Management

- Addition of multiple administrator accounts
  - ✓ It is now possible to add multiple administrator accounts with pre-determined access level settings.



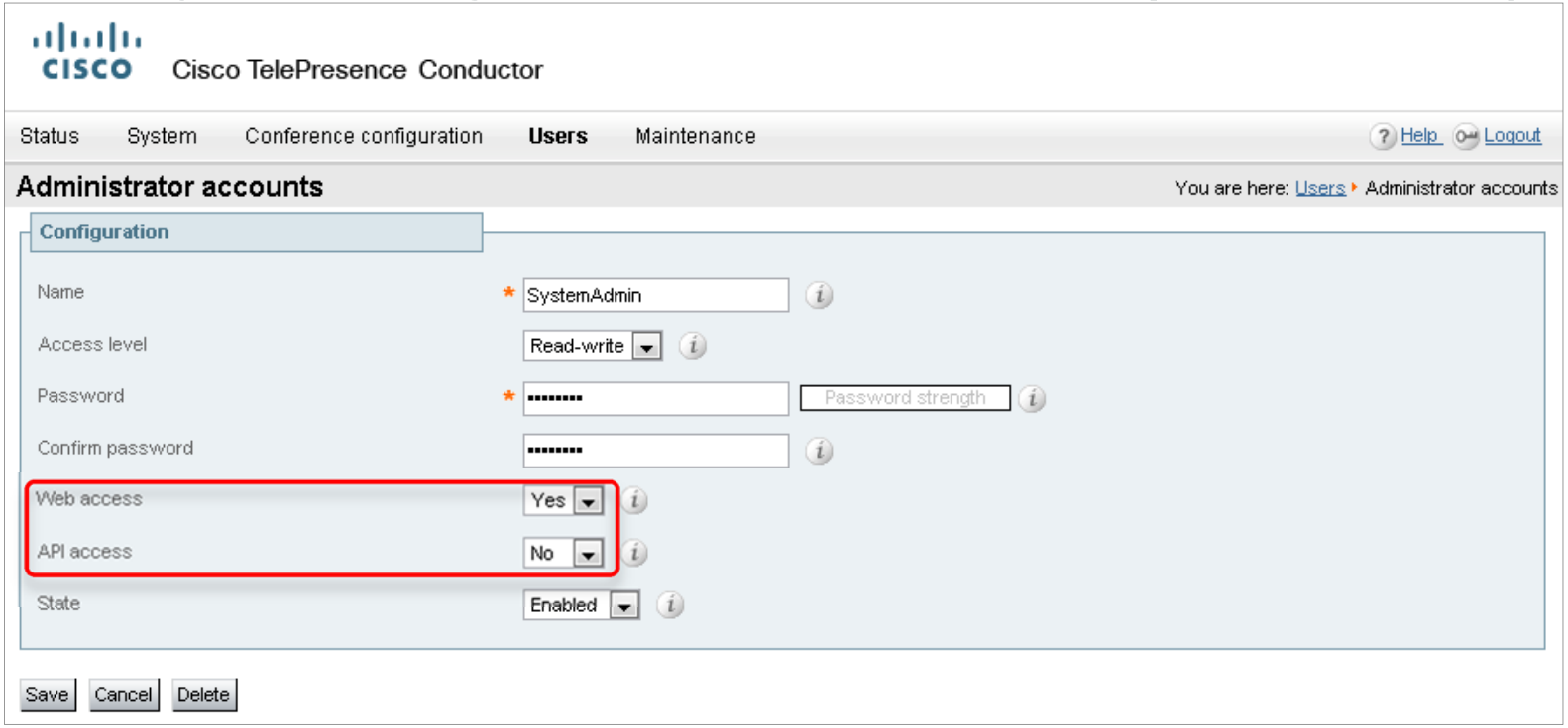
Security Enhancement
Administrator Account Management

- Ability to temporarily disable administrator account



Security Enhancement
Administrator Account Management

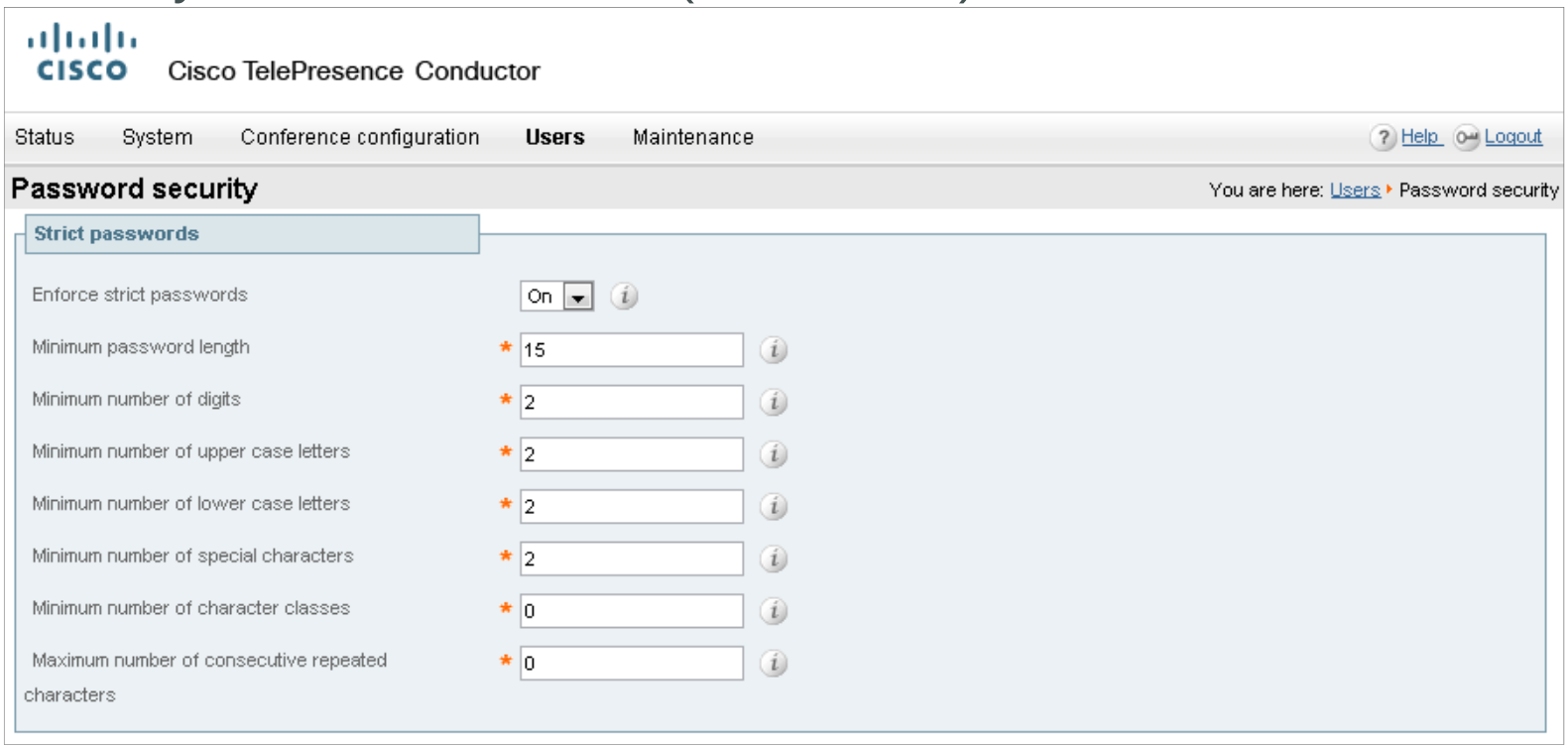
- Ability to configure Web/API access permission per account



Parameter	Definition
Web access	Determines whether this user is allowed to log onto the TelePresence Conductor using the web interface.
API access	Determines whether this user is allowed to access the TelePresence Conductor status and configuration using the Application Programming Interface (API).

Security Enhancement
Administrator Account Management

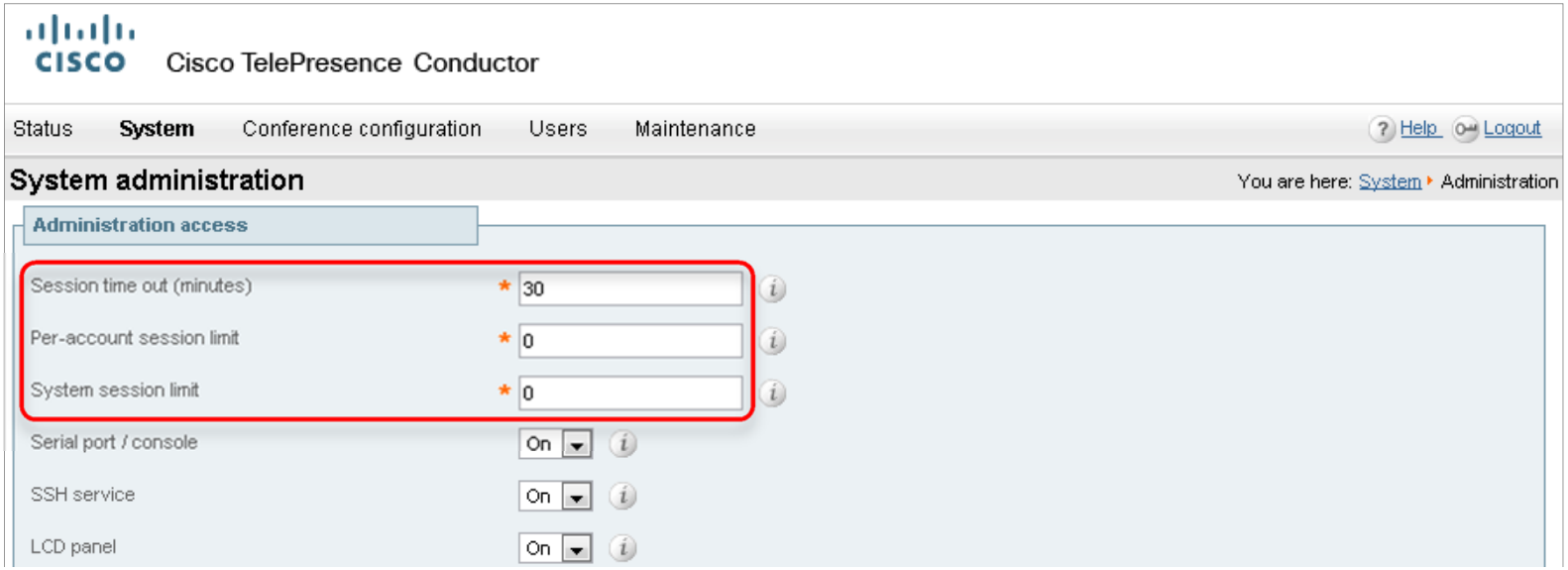
- Support strict password checking
  - ✓ Ability to define strict level (Default: Off)



  - ✓ Account won't create if password does not meet configured strict level

Security Enhancement
Session Management

- System Administration session timeout and limits
  - ✓ It is now possible to set a session time out, as well as limits for concurrent sessions and concurrent logins per administrator account for web, SSH and serial sessions.



Parameter	Definition
Per-account session limit	The number of concurrent sessions that each individual administrator account is allowed on the system. This includes web, SSH and serial sessions.
System session limit	The maximum number of concurrent administrator sessions allowed on the system. This includes web, SSH and serial sessions.


cisco