

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.

Cisco TelePresence Conductor

Status **System** Conference configuration Users Maintenance [Help](#) [Logout](#)

Firewall rules configuration

You are here: [System](#) > [Firewall rules](#) > Configuration

Filter

Service: <all> ⓘ

Description: ⓘ

[Click for more filter options](#)

Filter **Reset**

Records: 4 Page 1 of 1

	Priority	Interface	IP address	Prefix length	Service	Transport	Start port	End port	Action	Description	State	Actions
<input type="checkbox"/>	10	LAN1	172.16.0.0	22	HTTPS	TCP	443	443	✓ Allow	Access from Management Network	Active	View/Edit
<input type="checkbox"/>	11	LAN1	0.0.0.0	0	HTTPS	TCP	443	443	✗ Deny	Deny all out side of Management NW	Active	View/Edit
<input type="checkbox"/>	20	LAN1	172.16.1.60	32	SNMP	UDP	161	161	✓ Allow	SNMP management between TMS	Active	View/Edit
<input type="checkbox"/>	21	LAN1	0.0.0.0	0	SNMP	UDP	161	161	✗ Deny	Deny all SNMP communication	Active	View/Edit

New **Delete** **Undelete** **Activate firewall rules** **Select all** **Unselect all**

Firewall rules are applied in priority order, with 1 being the highest priority

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

The screenshot displays the Cisco TelePresence Conductor interface for Firewall Rules Configuration. At the top, there is a navigation bar with 'System' selected. Below it, a breadcrumb trail shows 'System > Firewall rules > Configuration'. A yellow warning banner states: 'Pending firewall rules exist: There are pending changes to the firewall rules; they have to be activated to take effect.'

Below the banner, a table lists 4 records. The table has columns: Priority, Interface, IP address, Prefix length, Service, Transport, Start port, End port, Action, Description, State, and Actions. The 'State' column for the 3rd and 4th records is highlighted with a red box and labeled 'Pending'.

Priority	Interface	IP address	Prefix length	Service	Transport	Start port	End port	Action	Description	State	Actions
10	LAN1	172.16.0.0	22	HTTPS	TCP	443	443	✓ Allow	Access from Management Network	Active	View/Edit
11	LAN1	0.0.0.0	0	HTTPS	TCP	443	443	✗ Deny	Deny all out side of Management MW	Active	View/Edit
20	LAN1	172.16.1.60	32	SNMP	UDP	161	161	✓ Allow	SNMP management between TMS	Pending	View/Edit
21	LAN1	0.0.0.0	0	SNMP	UDP	161	161	✗ Deny	Deny all SNMP communication	Pending	View/Edit

Below the table, there are buttons: 'New', 'Delete', 'Undelete', 'Activate firewall rules' (highlighted with a red box), 'Select all', and 'Unselect all'. A note states: 'Firewall rules are applied in priority order, with 1 being the highest priority'.

A 'Firewall rules confirmation' dialog is shown below. It contains a 'Warning' box with the text: 'Please confirm these changes - an automatic rollback will occur if you do not accept these changes.' At the bottom of the dialog are two buttons: 'Accept changes' (highlighted with a red box) and 'Rollback changes'.

At the bottom of the screenshot, a yellow banner states: 'Firewall rules activated: Activated Access Control configuration. The system access control lists have been updated with the latest settings.'

Security Enhancement Firewall Rules

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

The screenshot displays the Cisco TelePresence Conductor interface for Firewall rules configuration. The top navigation bar includes 'Status', 'System', 'Conference configuration', 'Users', and 'Maintenance', along with 'Help' and 'Logout' links. The main heading is 'Firewall rules configuration', with a breadcrumb trail: 'You are here: System > Firewall rules > Configuration'. The 'Filter' section contains a dropdown menu for 'Service' set to '<all>' and an empty text input for 'Description'. Below the filter section are 'Filter' and 'Reset' buttons. At the bottom, a table header is visible with columns: Priority, Interface, IP address, Prefix length, Service, Transport, Start port, End port, Action, Description, State, and Actions. The 'New' button in the table's toolbar is highlighted with a red box. The page also shows 'Records: 0' and 'Page 1 of 1'.

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

The screenshot shows the Cisco TelePresence Conductor interface for configuring a firewall rule. The page title is "Firewall rules configuration" and the breadcrumb trail is "System > Firewall rules > Configuration > New". The "Configuration" tab is active. The form contains the following fields:

Priority	* 20	i
IP address	* 172.16.0.0	i
Prefix length	* 22	i
Address range	172.16.0.0 - 172.16.3.255	
Service	HTTPS	i
Action	Allow	i
Description	Access from Management Network	

At the bottom of the form, there are two buttons: "Create firewall rule" (highlighted with a red box) and "Cancel".

Security Enhancement Firewall Rules

- Firewall rules configuration

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

Filter

Service: <all> ⓘ

Description: ⓘ

[Click for more filter options](#)

Filter Reset

Records: 1 Page 1 of 1

Priority	Interface	IP address	Prefix length	Service	Transport	Start port	End port	Action	Description	State	Actions
20	LAN1	172.16.0.0	22	HTTPS	TCP	443	443	✓ Allow	Access from Management Network	Pending	View/Edit

New Delete Undelete **Activate firewall rules** Select all Unselect all

Firewall rules are applied in priority order, with 1 being the highest priority

Security Enhancement Firewall Rules

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

The screenshot shows the Cisco TelePresence Conductor interface for Firewall Rules Configuration. At the top, there is a navigation bar with 'Status', 'System', 'Conference configuration', 'Users', and 'Maintenance'. Below this, the page title is 'Firewall rules configuration' and the breadcrumb trail is 'You are here: System > Firewall rules > Configuration'. A message bar indicates 'Saved: Firewall rule has been saved.' and 'Pending firewall rules exist: There are pending changes to the firewall rules; they have to be activated to take effect.' The main configuration area includes a 'Filter' section with a dropdown menu set to '<all>' and a 'Description' field. Below the configuration area, there are 'Filter' and 'Reset' buttons. A confirmation dialog box is overlaid on the page, asking 'Are you sure you want to activate the firewall rules?' with 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a red square. Below the dialog box, a table shows one record with columns for Priority, Interface, IP address, and State. The record has a priority of 20, interface LAN1, IP address 172.16.0.0, and state Pending. At the bottom, there are buttons for 'New', 'Delete', 'Undelete', 'Activate firewall rules', 'Select all', and 'Unselect all'. A footer note states 'Firewall rules are applied in priority order, with 1 being the highest priority'.

Records: 1

Priority	Interface	IP address	Port	Protocol	Source	Destination	Action	Access from Management Network	State	Actions
20	LAN1	172.16.0.0	22	TCP	172.16.0.0	172.16.0.0	Allow	Access from Management Network	Pending	View/Edit

Page 1 of 1

Firewall rules are applied in priority order, with 1 being the highest priority

Security Enhancement Firewall Rules

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

The screenshot shows the Cisco TelePresence Conductor interface for Firewall rules configuration. At the top, the Cisco logo and 'Cisco TelePresence Conductor' are visible. Below the navigation bar, the page title is 'Firewall rules configuration'. A yellow message box indicates 'Saved: Firewall rule has been saved.' and another yellow message box states 'Pending firewall rules exist: There are pending changes to the firewall rules; they have to be activated to take effect.' The main configuration area includes a 'Filter' section with a 'Service' dropdown set to '<all>' and a 'Description' text input field. Below this are 'Filter' and 'Reset' buttons. A table of records is shown with one entry: Priority 20, Interface LAN1, IP address 172.16.0.0, Prefix length 22, Service HTTPS, and Action Allow. A modal dialog box with a loading spinner and the text 'Activating firewall rules' is overlaid on the table. At the bottom, there are buttons for 'New', 'Delete', 'Undelete', 'Activate firewall rules', 'Select all', and 'Unselect all'. A footer note states 'Firewall rules are applied in priority order, with 1 being the highest priority'.

Records: 1

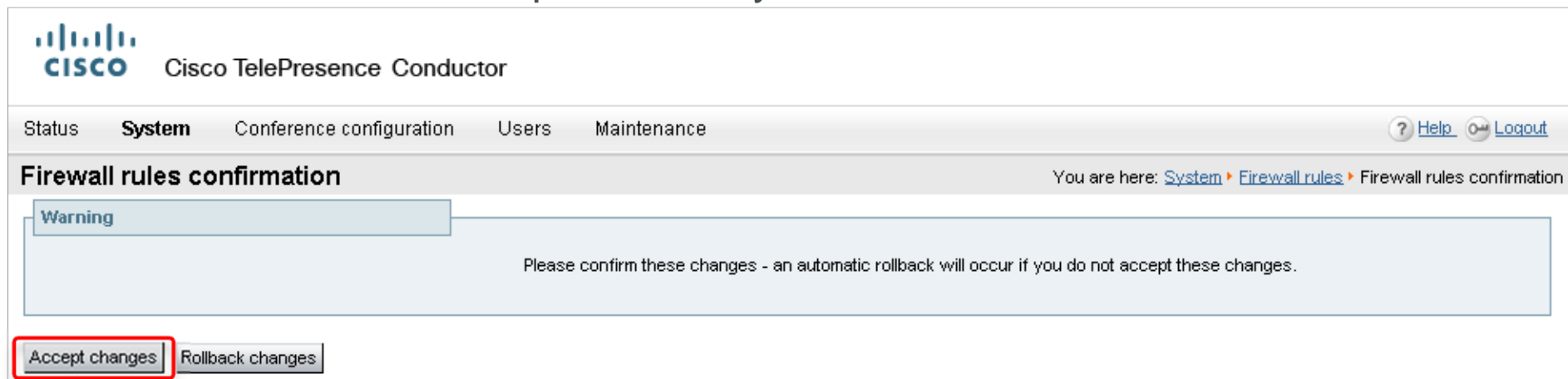
Priority	Interface	IP address	Prefix length	Service	Trans	Port	Action	Description	State	Actions
20	LAN1	172.16.0.0	22	HTTPS	TCP		Allow	Access from Management Network	Pending	View/Edit

Activating firewall rules

Firewall rules are applied in priority order, with 1 being the highest priority

Security Enhancement Firewall Rules

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



The screenshot shows the Cisco TelePresence Conductor interface. At the top left is the Cisco logo and the text "Cisco TelePresence Conductor". Below this is a navigation bar with tabs for "Status", "System", "Conference configuration", "Users", and "Maintenance". The "System" tab is selected. In the top right corner, there are links for "Help" and "Logout". The main content area is titled "Firewall rules confirmation" and includes a breadcrumb trail: "You are here: System > Firewall rules > Firewall rules confirmation". A warning message is displayed in a light blue box: "Warning" followed by "Please confirm these changes - an automatic rollback will occur if you do not accept these changes." At the bottom of the page, there are two buttons: "Accept changes" (highlighted with a red box) and "Rollback changes".

Security Enhancement Firewall Rules

- Firewall rules configuration

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

Firewall rules configuration You are here: [System](#) > [Firewall rules](#) > Configuration

Firewall rules activated: Activated Access Control configuration. The system access control lists have been updated with the latest settings.

Filter

Service: <all> [i](#)

Description: [i](#)

[Click for more filter options](#)

Filter Reset

Records: 1 Page 1 of 1

Priority	Interface	IP address	Prefix length	Service	Transport	Start port	End port	Action	Description	State	Actions
<input type="checkbox"/> 20	LAN1	172.16.0.0	22	HTTPS	TCP	443	443	✓ Allow	Access from Management Network	Active	View/Edit

New Delete Undelete Activate firewall rules Select all Unselect all

Firewall rules are applied in priority order, with 1 being the highest priority

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”

The screenshot displays the Cisco TelePresence Conductor interface for Firewall rules configuration. It is divided into two main sections: 'Firewall rules confirmation' and 'Firewall rules configuration'.

Firewall rules confirmation: This section shows a 'Warning' box with the text: 'Please confirm these changes - an automatic rollback will occur if you do not accept these changes.'

Firewall rules configuration: This section shows a red-bordered 'Alert' box with the text: 'The activation period has expired. The firewall rule changes have been automatically rolled back.' Below this, a red-bordered message states: 'Firewall rules activation failed: The activation period timed out.' A yellow message below that says: 'Pending firewall rules exist: There are pending changes to the firewall rules; they have to be activated to take effect.'

The configuration area includes a 'Filter' section with a dropdown menu set to '<all>' and a search box for 'Description'. Below the filter are 'Filter' and 'Reset' buttons.

At the bottom, there is a table of records. The table has columns: Priority, Interface, IP address, Prefix length, Service, Transport, Start port, End port, Action, Description, State, and Actions. The first record is highlighted:

Priority	Interface	IP address	Prefix length	Service	Transport	Start port	End port	Action	Description	State	Actions
20	LAN1	172.16.0.0	22	HTTPS	TCP	443	443	Allow	Access from Management Network	Pending	View/Edit

Below the table are buttons for 'New', 'Delete', 'Undelete', 'Activate firewall rules', 'Select all', and 'Unselect all'. A note at the bottom right states: 'Firewall rules are applied in priority order, with 1 being the highest priority'.

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.

Cisco TelePresence Conductor

Status **System** Conference configuration Users Maintenance [? Help](#) [Logout](#)

Firewall rules configuration You are here: [System](#) > [Firewall rules](#) > Configuration

Pending firewall rules exist: There are pending changes to the firewall rules; they have to be activated to take effect.

Filter

Service: <all> ⓘ

Description: ⓘ

[Click for more filter options](#)

Filter Reset

Records: 1 Page 1 of 1

Priority	Interface	IP address	Prefix length	Service	Transport	Start port	End port	Action	Description	State	Actions
20	LAN1	172.16.0.0	22	HTTPS	TCP	443	443	✓ Allow	Access from Management Network	Pending delete	View/Edit

New Delete Undelete Activate firewall rules Select all Unselect all

Firewall rules are applied in priority order, with 1 being the highest priority

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

The screenshot displays the Cisco TelePresence Conductor web interface. At the top left is the Cisco logo and the text 'Cisco TelePresence Conductor'. Below this is a navigation menu with 'Status', 'System', 'Conference configuration', 'Users', and 'Maintenance' (highlighted). To the right of the menu are 'Help' and 'Logout' links. The main content area is titled 'Server certificate' and includes a breadcrumb trail: 'You are here: Maintenance > Security certificates > Server certificate'. A sub-section titled 'Certificate signing request (CSR)' is visible, containing a text area with the message 'There is no certificate signing request in progress' and a 'Generate CSR' button.

Security Enhancement Certificate Signing Request (CSR)

- Generate a certificate signing request

The screenshot displays the Cisco TelePresence Conductor web interface. At the top, the Cisco logo and 'Cisco TelePresence Conductor' are visible. A navigation bar includes 'Status', 'System', 'Conference configuration', 'Users', and 'Maintenance'. The 'Maintenance' tab is active, and the breadcrumb path is 'You are here: Maintenance > Security certificates > Generate CSR'.

The main content area is titled 'Generate CSR' and contains a form for creating a Certificate Signing Request. The form fields are as follows:

Common name	FQDN of Conductor
Common name as it will appear	tkyconductor40.ciscotp.com
Subject alternative names	None
Additional alternative names (comma separated)	tkyconductor41.ciscotp.com
Alternative name as it will appear	tkyconductor40.ciscotp.com,tkyconductor41.ciscotp.com
Key length (in bits)	4096
Country	* JP
State or province	* TKY
Locality (town name)	* Tokyo
Organization (company name)	* Cisco
Organizational unit	* CIBU

Below the form is a 'Generate CSR' button. To the right, there are 'Help' and 'Logout' links.

Below the main form, a yellow notification bar states: 'CSR creation successful. Certificate Signing Request saved to /tandberg/persistent/certs/generated_csr/csr.pem.' Below this is a section titled 'Certificate signing request (CSR)' with a table:

Certificate request	PEM File	View	Download
Generated on	Oct 3 2012		

At the bottom of this section is a 'Discard CSR' button.

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.

The screenshot shows the Cisco TelePresence Conductor web interface. At the top left is the Cisco logo and the text "Cisco TelePresence Conductor". Below this is a navigation bar with tabs for "Status", "System", "Conference configuration", "Users", and "Maintenance". The "Users" tab is selected. In the top right corner, there are links for "Help" and "Logout".

The main content area is titled "Administrator accounts" and includes a breadcrumb trail: "You are here: Users > Administrator accounts". Below the title is a table with the following columns: Name, State, Access level, Web access, API access, and Actions.

Name	State	Access level	Web access	API access	Actions
<input type="checkbox"/> admin	✓ Enabled	Read-write	✓ Yes	✓ Yes	View/Edit
<input type="checkbox"/> ExternalApplication	✓ Enabled	Read-only	✗ No	✓ Yes	View/Edit
<input type="checkbox"/> Maintenance Team	✓ Enabled	Read-write	✓ Yes	✓ Yes	View/Edit
<input type="checkbox"/> SystemAdmin	✓ Enabled	Read-write	✓ Yes	✓ Yes	View/Edit
<input type="checkbox"/> VC-Operation-Team	✓ Enabled	Read-write	✓ Yes	✗ No	View/Edit

At the bottom of the table, there is a row of action buttons: "New", "Delete", "Enable", "Disable", "Select all", and "Unselect all".

Security Enhancement Administrator Account Management

- Ability to temporarily disable administrator account

The screenshot displays the Cisco TelePresence Conductor interface for managing administrator accounts. The top navigation bar includes 'Status', 'System', 'Conference configuration', 'Users', and 'Maintenance'. The 'Users' section is active, showing a breadcrumb path: 'You are here: Users > Administrator accounts'.

Administrator accounts table:

Name	State	Access level	Web access	API access	Actions
<input type="checkbox"/> admin	✓ Enabled	Read-write	✓ Yes	✓ Yes	View/Edit
<input type="checkbox"/> ExternalApplication	✗ Disabled	Read-only	✗ No	✓ Yes	View/Edit
<input type="checkbox"/> Maintenance Team	✗ Disabled	Read-write	✓ Yes	✓ Yes	View/Edit
<input type="checkbox"/> SystemAdmin	✓ Enabled	Read-write	✓ Yes	✓ Yes	View/Edit
<input type="checkbox"/> VC-Operation-Team	✓ Enabled	Read-write	✓ Yes	✗ No	View/Edit

Below the table are buttons: New, Delete, Enable, Disable, Select all, Unselect all.

Administrator accounts configuration form:

The configuration form for the 'Maintenance Team' account is shown. The 'State' dropdown menu is highlighted with a red box, showing the following options: Disabled (selected), Enabled, and Disabled.

Configuration fields include:

- Name: Maintenance Team
- Access level: Read-write
- Password: [Redacted]
- Confirm password: [Redacted]
- Web access: Yes
- API access: Yes
- State: Disabled

Buttons at the bottom: Save, Cancel, Delete.

Security Enhancement Administrator Account Management

- Ability to configure Web/API access permission per account

The screenshot shows the Cisco TelePresence Conductor web interface for configuring an administrator account. The page title is 'Cisco TelePresence Conductor' and the navigation menu includes 'Status', 'System', 'Conference configuration', 'Users', and 'Maintenance'. The current page is 'Administrator accounts', with a breadcrumb trail 'You are here: Users > Administrator accounts'. The 'Configuration' tab is active, showing fields for Name (SystemAdmin), Access level (Read-write), Password (masked), Confirm password (masked), Web access (Yes), API access (No), and State (Enabled). A red box highlights the 'Web access' and 'API access' dropdown menus. At the bottom, there are 'Save', 'Cancel', and 'Delete' buttons.

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).

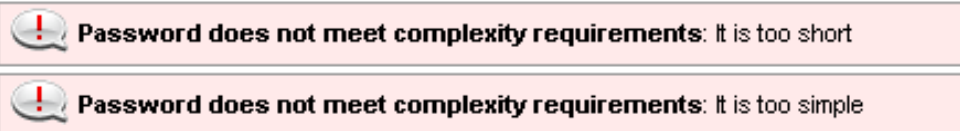
Security Enhancement Administrator Account Management

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

The screenshot shows the Cisco TelePresence Conductor Administrator interface. At the top, there is a navigation bar with tabs for Status, System, Conference configuration, **Users**, and Maintenance. A 'Help' link and a 'Logout' button are also present. Below the navigation bar, the page title is 'Password security' and the breadcrumb trail is 'You are here: Users > Password security'. The main content area is titled 'Strict passwords' and contains several configuration options:

Configuration Option	Value
Enforce strict passwords	On
Minimum password length	15
Minimum number of digits	2
Minimum number of upper case letters	2
Minimum number of lower case letters	2
Minimum number of special characters	2
Minimum number of character classes	0
Maximum number of consecutive repeated characters	0

- ✓ 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.

The screenshot shows the Cisco TelePresence Conductor interface. The top navigation bar includes 'Status', 'System', 'Conference configuration', 'Users', and 'Maintenance'. The 'System' tab is active. The main content area is titled 'System administration' and contains a sub-section 'Administration access'. This section has three input fields: 'Session time out (minutes)' with a value of 30, 'Per-account session limit' with a value of 0, and 'System session limit' with a value of 0. Each input field has an information icon (i) to its right. Below these are three dropdown menus: 'Serial port / console' (On), 'SSH service' (On), and 'LCD panel' (On), each also with an information icon.

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.

