Configure Policies

Add a Policy

Procedure

Step 1   Select the **Policy Editor** tab.
The **Policy List** appears to the left and the **Action List** appears at the right of the **Policy** screen.

Step 2   Under **Policy List**select **Add**.
The new policy appears at the top of the list of existing policies.

Step 3   Enter a unique name for the policy.

What to do next

To add actions for this policy, see Add Actions to a Policy, on page 1

Add Actions to a Policy

Procedure

Step 1   Select the **Policy Editor** tab.
The **Policy List** appears to the left and the **Action List** appears at the right of the **Policy Editor** screen.

Step 2   Under **Policy Name** select the policy to which you want to add actions.

Step 3   To add actions, select **Add** under **Action List** on the right of the screen.
The **Action Editor** screen appears.

Step 4   Select a policy action from the **Action Tag Name** list.

| Step 5 | Select **Save**. |
| Step 6 | Repeat Steps 3-5 until all of your policies have actions assigned to them. |

Policy Actions in Webex

By default, a newly provisioned Webex organization has all the capabilities granted to all the users.

Note The end-to-end encryption policy is not enabled by default. The Organization Administrator can enable this policy. Administrators can create policies when specific capabilities for all the users or specific groups of users need to be disabled.

Policy actions cannot be enforced on users using third-party XMPP IM applications.

No more than ten VoIP conference attendees can be connected to the same VoIP conference simultaneously.

External users are users who do not belong to the Webex organization. They can still use Webex to communicate with users who belong to the Webex organization.

Policy Action	Description	Impact
External File Transfer	Controls file transfer in an IM session between organization users and users outside the organization.	**Disabled**—Stops all file transfers be includes multiparty IM sessions wit
Internal File Transfer	Controls file transfer in an IM session between users within the organization.	**Disabled**—Stops all internal file tra **Enabled**—All the users within the o
External IM	Controls IM sessions between users in the organization and users outside the organization.	**Disabled**—Stops all IM sessions be organization. This stops all depende
External VoIP	Controls VoIP communications in IM sessions between users in the organization and users outside the organization	**Disabled**—Stops all VoIP commun organization and users outside the c IM sessions and file transfers are av
Internal VoIP	Controls VoIP communications in IM sessions between users within the organization.	**Disabled**—Stops all VoIP commun organization. However, other servic available. **Enabled**—All the users within the sessions.
External Video	Controls video services in IM sessions between users in the organization and users outside the organization	**Disabled**—Stops all video services and users outside the organization. and file transfers are available.
Internal Video	Controls video services in IM sessions between users within the organization.	**Disabled**—Stops all video services However, other services like text-ba **Enabled**—All the users within the sessions.

Policy Action	Description	Impact
Local Archive	Controls the ability of the user to locally archive IM text messages.	
External Desktop Share	Controls the ability of users within the organization to share their desktop with users outside the organization.	**Disabled**—Prevents users withi users outside the organization. **Enabled**—Users can share thei
Internal Desktop share	Controls the ability of users within the organization to share their desktop with other users within the organization.	**Disabled**—Users within the org the organization. **Enabled**—Users can share thei
Support End-to-End Encryption For IM	Specify support for end-to-end Encryption for IM sessions.	**Enabled**—Support end-to-end End-to-end encryption is not su
Support NO Encoding For IM	Controls whether applications with end-to-end encryption enabled can start an IM session with applications that do not have end-to-end encryption enabled or with 3rd party applications that do not support end-to-end encryption.	**Disabled**—Prevents application IM session with applications or encryption enabled. **Enabled**—Encryption level neg
Internal IM (including White Listed domains)	Controls IM communication between users within the organization and specific domains on the white list.	**Disabled**—Prevents users withi the domains specified in the wh IM with each other. Also disabl File Transfer.
Upload Widgets		
Allow user to edit profile	Controls the ability to restrict users from editing their profile information.	**Disabled**—Prevents users from This policy action impacts the s **Configuration** tab.
Allow user to edit the view profile setting	Controls the ability to restrict groups of users from changing their user profile view settings.	**Disabled**—Prevents users from This policy action impacts the A box in the **Profile Settings** scre The **Allow users to change the** if it is selected.
Internal Screen Capture	Controls users' ability to send a screen capture to users within the organization.	**Disabled**—Prevents users withi the organization.
External Screen Capture	Controls users' ability to send a screen capture to users outside of the organization.	**Disabled**—Prevents users withi of the organization.
Send Internal Broadcast Message	Controls users' ability to send broadcast messages to users within the organization.	**Disabled**—Prevents users withi inside the organization.
Send External Broadcast Message	Controls users' ability to send broadcast messages to users outside of the organization.	**Disabled**—Prevents users withi outside of the organization.

Policy Action	Description	Impact
Allow user to send broadcast to a directory group	Controls users' ability to send broadcast messages to a directory group within the organization.	**Disabled**—Prevents users within th a directory group within the organiz
HD Video	Controls the HD Video feature on computer to computer calls when External Video or Internal Video policies are enabled	**Disabled**—Prevents HD Video for