



Configure Policies

- [Add a Policy, on page 1](#)
- [Add Actions to a Policy, on page 1](#)
- [Policy Actions in Webex, on page 2](#)

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 between organization users and users outside the organization. This includes multiparty IM sessions with external users.
Internal File Transfer	Controls file transfer in an IM session between users within the organization.	Disabled —Stops all internal file transfers between users within the organization. Enabled —All the users within the organization can transfer files.
External IM	Controls IM sessions between users in the organization and users outside the organization.	Disabled —Stops all IM sessions between users in the organization and users outside the organization. This stops all dependent services like file transfers and VoIP.
External VoIP	Controls VoIP communications in IM sessions between users in the organization and users outside the organization.	Disabled —Stops all VoIP communications between users in the organization and users outside the organization. IM sessions and file transfers are available.
Internal VoIP	Controls VoIP communications in IM sessions between users within the organization.	Disabled —Stops all VoIP communications between users within the organization. However, other services like text-based chat are available. Enabled —All the users within the organization can have VoIP sessions.
External Video	Controls video services in IM sessions between users in the organization and users outside the organization.	Disabled —Stops all video services between users in the organization and users outside the organization. IM sessions and file transfers are available.
Internal Video	Controls video services in IM sessions between users within the organization.	Disabled —Stops all video services between users within the organization. However, other services like text-based chat are available. Enabled —All the users within the organization can have video 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 within the organization from sharing their desktop with users outside the organization. Enabled —Users can share their desktop with users outside the organization.
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 organization cannot share their desktop with other users within the organization. Enabled —Users can share their desktop with other users within the organization.
Support End-to-End Encryption For IM	Specify support for end-to-end Encryption for IM sessions.	Enabled —Support end-to-end encryption for IM sessions. Disabled —End-to-end encryption is not supported.
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 applications with end-to-end encryption enabled from starting an IM session with applications or devices that do not have end-to-end encryption enabled. Enabled —Encryption level negotiation is supported.
Internal IM (including White Listed domains)	Controls IM communication between users within the organization and specific domains on the white list.	Disabled —Prevents users within the organization from communicating with users in the domains specified in the white list. Enabled —Users can communicate with users in the domains specified in the white list. Also disables File Transfer.
Upload Widgets		
Allow user to edit profile	Controls the ability to restrict users from editing their profile information.	Disabled —Prevents users from editing their profile information. This policy action impacts the Profile Settings tab in the 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 changing their user profile view settings. This policy action impacts the Allow users to change the view profile setting checkbox in the Profile Settings screen. The Allow users to change the view profile setting checkbox is selected by default if it is selected.
Internal Screen Capture	Controls users' ability to send a screen capture to users within the organization.	Disabled —Prevents users within the organization from sending screen captures to other users within the organization.
External Screen Capture	Controls users' ability to send a screen capture to users outside of the organization.	Disabled —Prevents users within the organization from sending screen captures to users outside of the organization.
Send Internal Broadcast Message	Controls users' ability to send broadcast messages to users within the organization.	Disabled —Prevents users within the organization from sending broadcast messages to other users inside the organization.
Send External Broadcast Message	Controls users' ability to send broadcast messages to users outside of the organization.	Disabled —Prevents users within the organization from sending broadcast messages to users 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 the a directory group within the organization
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