# 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 Cisco Webex

By default, a newly provisioned Cisco 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 Cisco Webex organization. They can still use Cisco Webex to communicate with users who belong to the Cisco Webex organization.

| Policy Action | Description | Impact | Default Value |
|---|---|---|---|
| External File Transfer | Controls file transfer in an IM session between organization users and users outside the organization. | **Disabled**—Stops all file transfers between the organization users and external users. This includes multiparty IM sessions with at least one external user. | **Enabled** |
| Internal File Transfer | Controls file transfer in an IM session between users within the organization. | **Disabled**—Stops all internal file transfers.<br>**Enabled**—All the users within the organization can exchange files with the internal users. | **Enabled** |
| 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 voice, video, and VoIP. | **Enabled** |

| Policy Action | Description | Impact | Default Value |
|---|---|---|---|
| External VoIP | Controls VoIP communications in IM sessions between users in the organization and users outside the organization | **Disabled**—Stops all VoIP communications in IM sessions between users in the organization and users outside the organization. However, other services like text-based IM sessions and file transfers are available | **Enabled** |
| Internal VoIP | Controls VoIP communications in IM sessions between users within the organization. | **Disabled**—Stops all VoIP communications in IM sessions between users within the organization. However, other services like text-based IM sessions and file transfers are available.<br>**Enabled**—All the users within the organization can use VoIP communications in IM sessions. | **Enabled** |
| External Video | Controls video services in IM sessions between users in the organization and users outside the organization | **Disabled**—Stops all video services in IM sessions between users within the organization and users outside the organization. However, other services like text-based IM sessions and file transfers are available. | **Enabled** |
| Internal Video | Controls video services in IM sessions between users within the organization. | **Disabled**—Stops all video services in IM sessions between users within the organization. However, other services like text-based IM sessions and file transfers are available.<br>**Enabled**—All the users within the organization can use video communications in IM sessions. | **Enabled** |

| Policy Action | Description | Impact | Default Value |
|---|---|---|---|
| Local Archive | Controls the ability of the user to locally archive IM text messages. | | **Enabled** |
| 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 (local) desktop with users outside the organization.<br>**Enabled**—Users can share their (local) desktop with users outside the organization. | **Enabled** |
| 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 can't share their desktop with other users within the organization.<br>**Enabled**—Users can share their desktop with other users inside the organization. | **Enabled** |
| 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.<br>End-to-end encryption is not supported for logged users. | **Disabled** |
| 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 initiating an IM session with applications or 3rd party applications that do not have end-to-end encryption enabled.<br>**Enabled**—Encryption level negotiated is the highest level that the other party supports. | **Enabled** |

| Policy Action | Description | Impact | Default Value |
|---|---|---|---|
| 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 being able to IM users within the domains specified in the white list. However, users within the domain can start an IM with each other. Also disables other dependent services such as VoIP, Video, and File Transfer. | **Enabled** |
| Upload Widgets | | | **Enabled** |
| Allow user to edit profile | Controls the ability to restrict users from editing their profile information. | **Disabled**—Prevents users from editing their profile information.<br>This policy action impacts the settings in the **Profile Settings** screen under the **Configuration** tab. | **Enabled** |
| 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.<br>This policy action impacts the **Allow users to change their profile view settings** check box in the **Profile Settings** screen under the **Configuration** tab.<br>The **Allow users to change their profile view settings** check box has no impact even if it is selected. | **Enabled** |
| 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 within the organization. | **Enabled** |
| 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 outside of the organization. | **Enabled** |

| Policy Action | Description | Impact | Default Value |
|---|---|---|---|
| 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 inside the organization. | **Enabled** |
| 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 outside of the organization. | **Enabled** |
| 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 organization from sending broadcast messages to a directory group within the organization. | **Enabled** |
| 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 all computer to computer calls. | **Enabled** |