Setting Up Your Privacy Policies

Setting Your Default Privacy Policy

Privacy policies allow you to determine which users can see your availability status, and send you instant messages (IM). This release of IM and Presence supports the contact list rule whereby anyone in your contact list (being watched by you) is able to see your availability status by default *unless* you explicitly deny that person permission to view your status.

You use privacy policies, therefore, to allow and block users and domains. The following options allow you to configure privacy policy either as a default setting at the organizational level or by specific request to the user.

- Allow—Users/domains are allowed to see your availability status and are able to send you instant messages by default. unless you explicitly add the user/domain to your Blocked list. You can set the Allow privacy policy for internal users and domains only. This option is *not* available for external (federated) users/domains.
- Block—Users/domains that you block cannot see your availability status and cannot send you instant messages. Users that you block always see your status as Unavailable. You can set the Block privacy policy for internal and external (federated) users and domains.
- Ask Me—Ask Me privacy policy prompts users (via a request) to either explicitly block or allow the exchange of availability status and IM from specific users/domains. The client application prompts the user to authorize or reject the subscription. You can set the Ask Me privacy policy for external (federated) users and domains only, and only if the external contact or domain is *not* in either the Allowed or Blocked list for the user.

Procedure

Step 1 Select **User Options > Privacy Policies**.

Step 2 Select one of these options:

If You Want To...	Do This
Allow all internal users to see your availability and send you instant messages (except those internal users/domains that you explicitly add to your blocked exception list). **Note** See the exception to this policy setting in the Troubleshooting Tips section of this topic. This policy will not allow external users to see your availability.	**1** Select **Allow** from the Internal users (within your company/organization): drop-down menu. **2** (Optional) Add internal users to your blocked exception lists following the procedures described in this module. See What To Do Next.
Block all internal users from seeing your availability and sending you instant messages (except those internal users that you explicitly add to your allowed exception list). **Note** This policy will not block external users from seeing your availability.	**1** Select **Block** from the Internal users (within your company/organization): drop-down menu. **2** (Optional) Add internal users to your allowed exception list following the procedures described in this module. See What To Do Next.
Block all external users from seeing your availability and sending you instant messages (except those external users that you explicitly add to your allowed exception list). **Note** This policy will not block internal users from seeing your availability.	**1** Select **Block** from the External users (all others): drop-down menu. **2** (Optional) Add external users to your allowed exception list following the procedures described in this module. See What To Do Next.
Prompt all users (with an Ask Me request) to set their own Allow/Block policy for external users (except those external users that you explicitly add to your allowed/blocked exception list). **Note** This policy will not block internal users from seeing your availability.	**1** Select **Ask Me** from the External users (all others): drop-down menu. **2** (Optional) Add external users to your allowed/blocked exception list following the procedures described in this module. See What To Do Next.

Step 3 Select **Save Defaults**.

Troubleshooting Tips

The IM and Presence server automatically authorizes a user that is on the contact list of another user to view their availability status. Note this exception to the *Allow all internal users* policy setting if you turn *off* automatic authorization on the IM and Presence server and both the global and local domain default is set to Allow - the user will be prompted to either approve or reject the subscription request. This is the Ask Me scenario for the local domain. For more information about the automatic authorization setting on IM and

Presence, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* (on Cisco.com).

What to Do Next

- If you want to override the default Allow/Block privacy policy set for internal/external users at organizational level, see the following topics that describe how to configure exception lists for users.

Adding Internal Users to Your Allowed or Blocked Exception Lists

This procedure allows you to manage the exceptions to the general privacy policy in the form of Allow and Block lists. Depending on the default privacy policy that you set at organizational level, either the allowed or blocked list is available for you to edit. In this way, you can override the default policy behavior to add specific people within your organization to your allowed or blocked list.

- Setting the Allow policy for specific users enables them to be able to see your availability and send you instant messages even if the general policy blocks them.
- Setting the Block policy for specific users prevents them from viewing status and exchanging IM when they are using Cisco clients (Cisco Jabber Version 8) - even if the general policy allows them. Users on the Contact list are always allowed unless explicitly blocked on the Exception list. Note that some third-party XMPP clients will still send and receive IMs regardless of the policy that you set.

Before You Begin

Set your default privacy policy.

Procedure

Step 1 Select **User Options > Privacy Policies**.

Step 2 Select **Add User** in the User Settings frame on the Privacy Policy window.

Step 3 Perform one of these actions:

- Select **Allow** to allow the user to see your availability.
- Select **Block** to block the user from seeing your availability.

Step 4 Enter a valid User ID for the internal user. The User ID must exist in your internal network in the format<*userid@domain*>.

Step 5 Select **Local domain**.

Step 6 Select **Add** to add the internal user to the local domain.

Troubleshooting Tips

- Federated users can add a local user using either an emailid or a standard JID. The choice depends on whether the Administrator has enabled or disabled the emailid for the domain.

- Once you **Add** a user to your Allowed/Blocked list, the details display in the table on this window. To remove any user from your Allowed/Blocked list, check the check box for the user and select **Delete Selected**.

Adding External Users to Your Allowed or Blocked Exception Lists

This procedure allows you to manage the exceptions to the general privacy policy in the form of Allow and Block lists. Depending on the default privacy policy that you set at organizational level, either the allowed or blocked list is available for you to edit. In this way, you can override the default policy behavior to add specific people outside of your organization to your allowed or blocked list.

- Setting the Allow policy for specific users enables them to be able to see your availability and send you instant messages even if the general policy blocks them.
- Setting the Block policy for specific users prevents them from seeing your availability and sending you instant messages even if the general policy allows them (via a positive response to an Ask Me request).

Before You Begin

Set your default privacy policy.

Procedure

Step 1 Select **User Options > Privacy Policies**.

Step 2 Select **Add User** in the User Settings frame on the Privacy Policy window.

Step 3 Perform one of these actions:

- Select **Allow** to allow the user to see your availability.
- Select **Block** to block the user from seeing your availability.

Step 4 Enter a valid User ID for the internal user. The User ID must exist in your internal network in the format (*<userid@domain>*.

Step 5 Select one of these domains to which the user belongs:

- **Federated domain**.
- **Custom domain** - a custom domain is an external domain that is not in the federated domain list.

Step 6 Complete one of these actions:

If you selected...	Do this:
Federated domain	Select the domain with which you are federating from the drop-down list.

If you selected...	Do this:
Custom domain	Enter the domain for the user. **Note** An example of a custom domain is 'mycompany.com'.

Step 7 Select **Add**.

Troubleshooting Tips

Once you **Add** a user to your Allowed/Blocked list, the details display in the table on this window. To remove any user from your Allowed/Blocked list, check the check box for the user and select **Delete Selected**.

Adding External Domains to Your Allowed or Blocked Exception Lists

Before You Begin

You can allow or block a whole external domain. If you block an external domain, any requests to see your availability from users in that domain are blocked, provided you have not added those external users to your allowed list.

Procedure

Step 1 Select **User Options > Privacy Policies**.

Step 2 Select **Add Domain** in the User Settings frame on the Privacy Policy window.

Step 3 Perform one of these actions:

- Select **Allow** to allow the user to see your availability.
- Select **Block** to block the user from seeing your availability.

Step 4 Select one of these domains to allow or block:

- **Federated domain**
- **Custom domain** - a custom domain is an external domain that is not in the federated domain list.

Step 5 Complete one of these actions:

If you selected...	Do this:
Federated domain	Select the domain with which you are federating from the drop-down list.

If you selected...	Do this:
Custom domain	Enter the domain for the user. **Note** An example of a custom domain is 'mycompany.com'.

Step 6 Select **Add**.

Troubleshooting Tips

Once you **Add** a domain to your Allowed/Blocked list, the details display in the table on this window. To remove any domain from your Allowed/Blocked list, check the check box for the domain and select **Delete Selected**.