Understanding Slack membership roles on the MIT Enterprise Grid

Understanding Slack membership roles on the MIT Enterprise Grid

Enterprise Slack is now available to members of the MIT community. All faculty, staff and students are eligible to request a workspace. Affiliates are eligible to participate in workspaces. All MIT users can join the MIT workspace at https://mit.slack.com, where you can learn about getting started with MIT's Slack Enterprise Grid.

Many members of the MIT community may already be familiar with Slack as it's free for anyone to use with a valid email address. But it's important to be aware that membership roles on MIT's Enterprise Slack Grid function differently than they do on a Free or Paid Slack workspace.

Below you will find important information on how membership roles function on MIT's Enterprise Slack Grid and workarounds for common problems users can encounter when trying to utilize different roles on their workspaces.

Understanding each role

Primary Owners

This role is not available to the community on MIT's Enterprise Slack Grid. The primary owner role for all workspaces is administered by IS&T.

Workspace Owners

There can be multiple Workspace Owners. Similar to a Primary Owner, this role also holds the highest level of permissions, but can't delete or transfer ownership of a workspace.

Workspace Admins

There can be multiple Workspace Admins. This role helps manage members, channels, and other administrative tasks.

Members

Members are the people that join your Slack workspace. They can use Slack to communicate and collaborate with other Members.

To become a Member of a workspace on the MIT Slack Enterprise Grid a user **must** have a kerberos account. The Enterprise Grid uses SSO authentication with Touchstone, which means that access for Members is only granted by means of their Kerberos credentials.

Guests

Guests are people that join your workspace, but have limited access. Multi-Channel Guests can use specific channels, and Single-Channel Guests can only use one channel. Guests can only collaborate with the members they share channels with.

Guests don't authenticate with SSO and Touchstone, instead they use Slack's standard username and password authentication method. No one with a kerberos account should ever be invited to the role of Single or Multi-Channel guest.

Why Kerberos accounts should only ever hold the role of Member

No one with a kerberos account should ever be invited to a workspace on the MIT Enterprise Slack Grid as a Single or Multi-Channel guest. The reason for this is two-fold. First, once a user's membership role is established on a workspace on the Enterprise Grid, that role is now locked for said individual grid-wide.

For example: If a member of the MIT community with an active kerberos account is invited to a workspace as a Multi-Channel guest, they are now unable to join any other workspace on the Enterprise Grid in any role other than Multi-Channel Guest. So if a different colleague were to invite this individual to a totally separate workspace, they'd be unable to join in any role other than Multi-Channel Guest. This would also prevent them from a requesting a workspace for themselves.

Second, this is also problematic because members of the MIT Community with kerberos accounts are intended to be able to enjoy the full benefits afforded to those in the Member role on MIT's Slack Enterprise Grid. Adding a user in the role of Single or Multi-Channel guest removes their ability to do so.

If you have users on your workspace with kerberos accounts in roles of Single or Multi-Channel Guest, you should take steps to upgrade them to Member as soon as possible.

How do I limit a colleague's access to specific channels on my workspace, without being able to invite them to my workspace as a Guest?

The most common reason we see users with kerberos accounts invited to the role of Single or Multi-Channel Guest is because the owner/admin of a workspace wants to invite another member of the MIT community to their workspace with limited access to one or several channels.

It's still possible to limit a Member's access to your workspace and specific channels, but you will need to use a workaround to achieve it.

The most common workaround we recommend is to make all of the channels on your workspace private. When a Member joins your workspace, they only have the ability to join public channels on their own. To join a private channel, they need to be invited to it by someone who's already in the channel. This will allow you to limit access to your channels without having a Member of the MIT community on your workspace in a Guest role.

Another option is to have a colleague join your workspace using a non-MIT email address, which will allow you to invite them as a Single or Multi-Channel Guest. We don't recommend this workaround, as it requires the person using it to manage two separate Slack accounts and prevents their message data from being unified under one account. But some individuals may find it to be a good solution for them.

We're aware that neither of these workarounds are necessarily ideal and we've provided the feedback to Slack.

If you have any questions about Slack membership roles, converting kerberos users from Guest to Member, or Slack in general, please contact the Service Desk: 617-253-1101 or servicedesk@mit.edu.