What do I need to know before approving an OpenID Connect site?

Q: What do I need to know before approving an OpenID Connect site?

On this page:

Answer
- Information Access
- Temporary vs Permanent
- Client Registration
- Site Information

Answer

OpenID Connect is a new pilot service allowing website owners to authenticate members of the MIT community, without having to manage certificates or passwords. When you visit an OpenID Connect enabled site for the first time, you will be prompted to authorize this site, with a screen similar to this one:

The screen gives you all the information you need to decide whether or not to authorize the application. Once you have made your decision, click the green **Authorize** button at the bottom of the page, or click the **Deny** button to cancel the authentication process.

Information Access

At the top right of the page, you see a list of what information ("scopes") the site is requesting. If you hold your mouse cursor over the question mark icon next to each piece of information, you will see a popup telling you what data will be sent:

Access checkboxes	Access checkboxes (with explanation popup)

If you do not wish to share some information with a site, you may un-check some of the boxes. For example, you may un-check the box next to "telephone number" if you do not wish to share your phone number with the site. **Note:** If you un-check the box next to **log in using your identity** or **basic profile information**, the site may not function correctly.

Temporary vs Permanent

Below the "Access to" box, you'll find a box dictating how OpenID Connect should handle future visits to this site:

By default, OpenID Connect will remember your decision until [you revoke it]. You can also choose to remember the decision for an hour, or to prompt again next time.

- The "decision" being remembered includes both the site *and* the information you choose to share with it. In the example screenshots on this page, the site you're trying to access has asked OpenID Connect for your identity information, name, e-mail address, and telephone number. If you choose to share everything except your telephone number, the server will remember your choice. However, you **will** be prompted on the next access, because the site is still asking for all 4 pieces of information, and needs your approval again.
- A "Deny" decision is not remembered. If you choose "Deny", you will be prompted again if you access the site in the future. In general, however, if you Deny access to a site, it is expected that you are unlikely to visit that site again voluntarily.

Client Registration

At the top left of the page, you'll see a box indicating whether or not the client was dynamically registered, how long ago, and whether or not it has been previously approved.

The box may be a different color depending on how recently the client was registered, and whether it was previously approved. Because a web

application can dynamically register with the server (e.g. no human interaction is required for a site to choose to accept OpenID Connect), this warning box is displayed.

Site Information

At the left side of the page is the site logo. If you click the triangle next to **more information**, you will be presented with links to the site's home page, its terms of service, usage policy, and administrative contact. You can use this information to help you decide whether or not to authorize the site.