Shelterly Quick Reference
User Management

Summary

Shelterty user management is performed by a Shelterly administrator with User Permissions.

Key concepts:

- A Shelterly User is someone who has a Shelterly account (login credentials) for a given organization.
- A Shelterly User can have access to more than one organization. They use the same login credentials for all organizations they have access to. When they login, they are prompted to pick an organization.
- A Shelterly User can have either permanent or temporary edit access to an organization's Shelterly data.
    - Typically, trusted and trained members of your organization are given permanent access.
    - When you bring in additional Shelterly help from outside your organization during an incident, these Shelterly Users should be given temporary access only. Temporary access is also useful for Shelterly trainings.

Startup

User management features are accessed by selecting **User Administration** or **Access Tokens** on the **Select Incident** page.

- The **Select Incident** page appears after the **Login** page (and also after the **Select Organization** page if you are a Shelterly User in multiple organizations).
- If you are already logged into Shelterly, you can return the **Select Incident** page by selecting the incident name under the Shelterly logo.

Adding Shelterly Users

You can create new Shelterly Users individually (**Create New User**), or you can share an **Access Token** that allows existing Shelterly Users to access your organization.

Create New User – use to add new members to your organization's Shelterly team

- Select **User Administration** on the **Select Incident** page.
- Select the **Create New User** icon.
- Use **Use Existing User** to check if the user already has a Shelterly account.
    - This is important to avoid creating duplicate accounts for the same user.
    - If you find the user in the pull-down menu, select to prefill the fields.
- If the user does not already have an account, fill in first/last name, email, and phone.
- **Agency ID** can be left blank, or can be used for your organization name or an individual organization ID number for this user.
    - Note that this field is not organization-specific, so use with caution for Shelterly Users who are with multiple organizations.
- Grant edit access
    - **Access Expires In**: Choose between **Never**, a specific number of days, and **Custom**.
    - The expiration date (if any) will appear in the edit box (greyed out). If you select **Custom**, the edit box is ungreyed and you can enter any date.

- Grant permissions
    - See Shelterly Admin Permissions below for details.
- Select **Save**. The user will receive an email inviting them to set up their password.
    - The link in the email will expire after 24 hours.
    - The sender of the email will be DoNotReply@shelterly.org.

Access Tokens – use to quickly grant Shelterly Users access to your organization during an incident or for a training, usually with temporary access only. Note that Access Tokens only work for users who already have a Shelterly login.

- Select **Access Tokens** on the **Select Incident** page.
- Select **Create Access Link.**
    - **Access Expires In:** Enter an expiration date for the Shelterly User's edit access to your organization (Never, 1, 3, 5, 7, or 30 days)
    - **Link Expires In:** Enter an expiration date for the link in the email (1, 3, or 7 days).
        - This helps to limit unauthorized access due to email forwarding. Consider setting this to just one day.
- Select **Save** to create the Access Token – you will see a link and an icon to access a QR code.
- Share the link and/or QR code with the Shelterly Users you want to have access to your organization.
    - The user clicks the link to login to Shelterly. They will see your organization added to the pull-down menu on the **Select Organization** page.
    - If the person already has Shelterly access to your organization, the link will just update their access expiration date.
- It is a good practice to cancel old Access Tokens when they are no longer needed. Select **Access Tokens** on the **Select Incident** page, then select the X to cancel each one.

Data Security Considerations When Creating New Users

- Shelterly data in real incidents includes a variety of sensitive data (owner contact information, location of valuable animals, gate codes, etc.) Your organization should manage Shelterly access accordingly.
- As a general guide, don't grant permanent access when temporary will suffice. Especially, consider carefully before granting permanent access via Access Tokens.
- Conduct regular reviews of your organization's Shelterly Users to remove access as appropriate.

Managing Shelterly Users

- Select **User Administration** on the **Select Incident** page.
- Find the user and select the appropriate Action icon:
    - **Edit User**: Update name, email, phone, access expiration, and permissions. See Create New User above for details on these fields.
    - **Remove User**: Removes the user's edit access to your organization's Shelterly data.
        - The Shelterly User's access to other organizations (if any) is not affected.
    - **Reset User Password**: The user will receive an email with a link to the **Forgot Password** workflow.

Shelterly Admin Permissions

Any Shelterly user can be given one or more Admin Permissions. Typically only a few leaders/experts in your organization should have these permissions. See Managing Shelterly Users above for details on changing these permissions for a user.

- **User Permissions**: Allows the Shelterly User to create and edit other Shelterly Users, including the granting of Admin Permissions.
- **Incident Permissions**: Allows the Shelterly User to create, edit, hide, and remove Shelterly incidents (both training and real). Refer to ***Shelterly Quick Reference – Incident Management*** for details.
- **Veterinary Permissions**: Allows the Shelterly User to make edits in the **VetMed** module. Typically granted to DVMs (veterinarians) and RVTs (vet techs) during an incident.
    - Veterinary Permissions allow the user to create, update, and remove the following: Veterinary Requests, Medical Records, Treatments, Procedures, Diagnostics, and Procedures.
    - All users have read-only access to veterinary data, and can create or update Veterinary Requests (i.e. they do not need Veterinary Permissions for these tasks).

Common User Issues

Forgotten password

- Shelterly allows users to do their own password resets via **Forgot Password** on the **Login** page. (See Managing Shelterly Users above for how to reset a password for a user.)

Duplicate accounts

- A user may forget that they already have a Shelterly account with your organization or a different organization, and mistakenly set up a new account for your organization.
- Multiple accounts for a single user are allowed by Shelterly, but it is better for the accounts to be merged so that the user does not have to remember which user account has which permissions.
    - If the user has duplicate accounts for your organization (and does not have access to any other organizations), you can simply delete the unwanted account (see **Managing Shelterly Users** above).
    - If the user has multiple accounts and has access to multiple organizations, contact the Shelterly team to resolve.

Multiple organizations

- Shelterly Users who have access to multiple organizations must be careful to select the appropriate organization in order to access a given incident. (Users sometimes login into their home organization as usual, and then wonder why they cannot see the incident they are doing mutual aid for, which belongs to a different organization.)