Managing Authorized Users

Agent OS is the program Spectrum call center agents use while troubleshooting customer issues. One of the tasks an agent can assist a customer with is managing the authorized users on their account.

My role: Content design, UX design

Collaboration: Accessibility, Design Systems, Engineering, Customer Operations

Focus: Using the best component and interaction for the action; crafting understandable copy for the related alert

Challenges: Ensuring designs followed two-factor authentication flow; focusing on specific project ask vs. overall improvements

Collaboration

Collaborating with various teams allowed us to incorporate two-factor authentication into the user flow.

Accessibility: Sharing best practices for using disabled CTAs and hiding certain elements from the UI.

Design Systems: Selecting the right components for an intuitive flow.

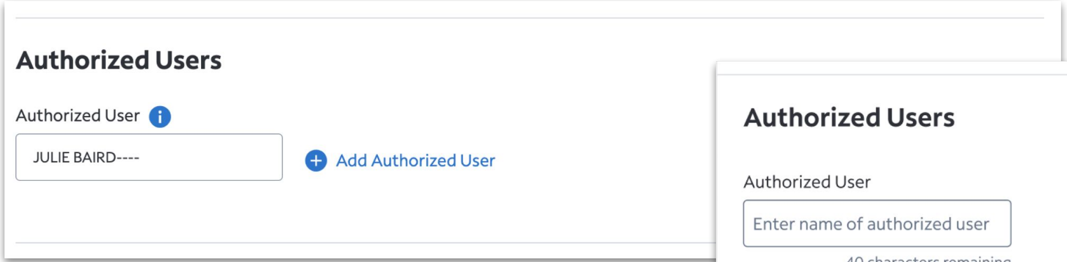
Engineering: Explaining the backend limitations and capabilities.

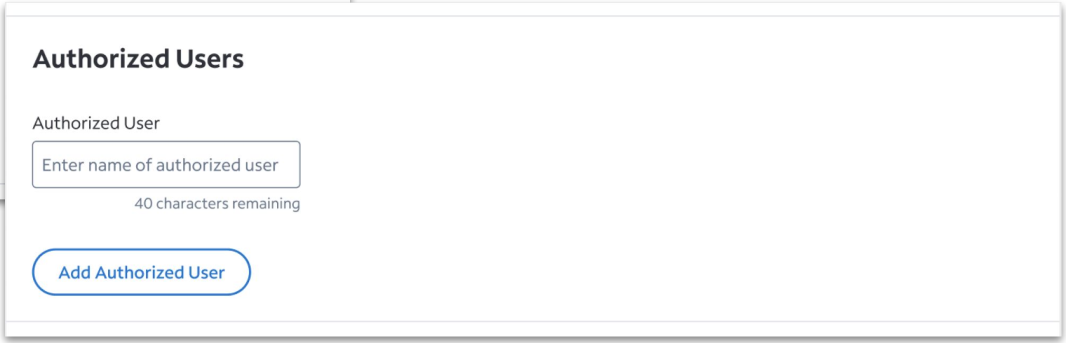
Customer Operations: Defining the identification actions and pointing out the necessary improvements.

Component Selection – Match Design System

Left: This is what exists in Agent OS today. The info icon hides the character limit information and the CTA is next to the field, rather than under it.

Right: We could update this section to our current design system specifications, but that doesn't clarify the actions available to the agent – do they click the CTA to save the information they added to the input field? What if the account already has an authorized user, how can it be edited or removed?

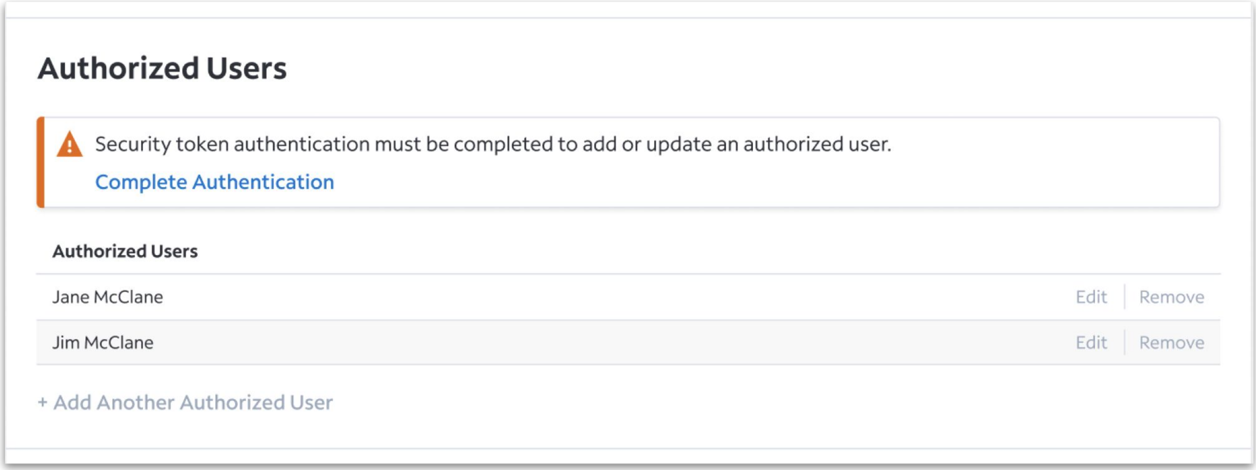




Component Selection – Include All Actions

By changing the input field to a table, we're able to show existing authorized users and related actions. We explored keeping the input field inline when an agent adds a new user, but in working with our Accessibility and Design System partners, we determined that each of the actions in this section should surface a dialog.

Including the alert message and disabling the actions in this section by default follows the two-factor authentication process.



Alert Copy – Common Word Choices

The first drafts of this messaging were a direct translation of the requirements for this action. While the message is clear, both versions use words that are typically avoided, as per our voice and tone guidelines.

⚠ Security token authentication must be completed to add or update an authorized user.

Complete Authentication

⚠ Security token authentication required to add or update an authorized user.

Complete Authentication

Other Common Word Choices

- Use **let** in place of **allow** (condescending, paternalistic; "This option lets you save…").
- Use **affect** in place of **impact** ("The storm may have affected your services…").
- Use **issue** in place of **problem** ("We'll resolve the issue soon").
- Avoid the words **must**, **need** and **required** when possible (can sound heavy-handed), and instead rephrase to indicate the required action ("To get started, review and accept these terms and conditions" instead of "You must accept…").

Alert Copy – Accuracy, Clarity, Brevity

After further drafting the copy into a more conversational tone, I considered our “ACBs”:

- ❑ Is the message **accurate**? Yes, based on the back end requirements.
- ❑ Is it **clear**? Yes, especially when the verb “complete” is mirrored in the body copy as well as the CTA.
- ❑ Is it **brief**? Yes, especially the version using “manage”.

⚠ Complete security token authentication to add or update an authorized user.

Complete Authentication

⚠ Complete security token authentication to manage authorized users.

Complete Authentication

Remember Your ACBs

We apply many well-established UX writing principles when drafting content for our products. Some of these include being clear and concise, using plain language, adhering to established guidelines for consistency, avoiding ambiguity and others (ask a content designer to tell you more!). But above all, we remember our ACBs: **Accuracy**, **Clarity**, **Brevity**.

To help our users complete the tasks they need to do, the content we write needs to be—*in this order*—accurate, clear and brief. It’s not useful, for example, to be as brief as possible if that means that accuracy and clarity suffer.

Security Requirements

As a measure to limit fraudulent activity, two-factor authentication is required for a customer to manage their authorized users.

It was important to understand the difference between verification and authentication and what an agent is able to do for a customer at each stage of identification.

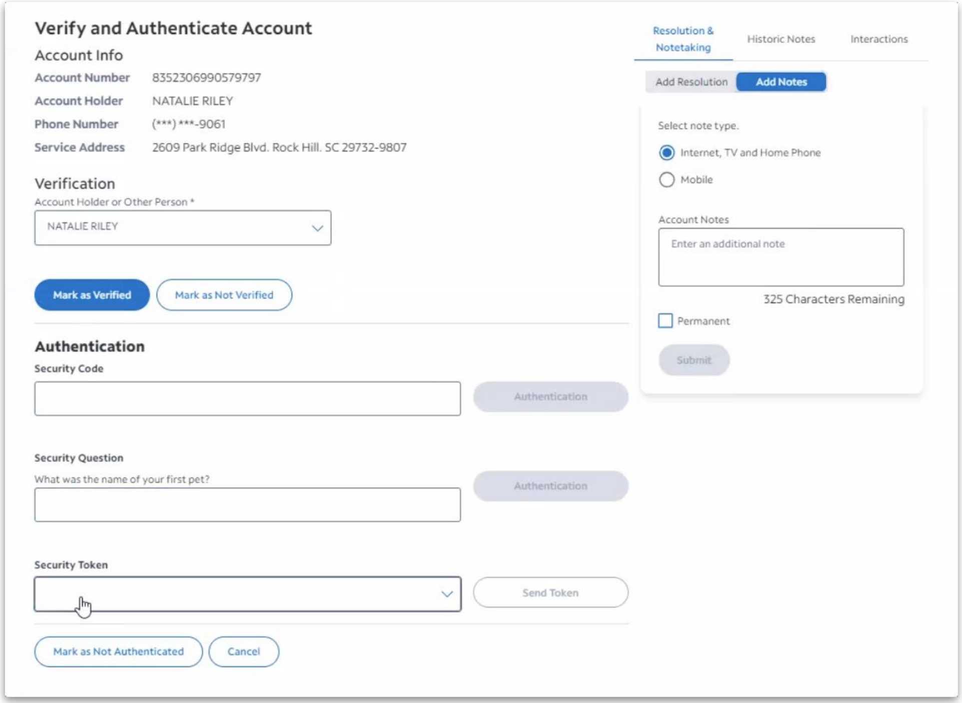
Since actions like managing authorized users are only accessible after a customer has been both verified *and* authenticated, it was important for the UX to reflect this.

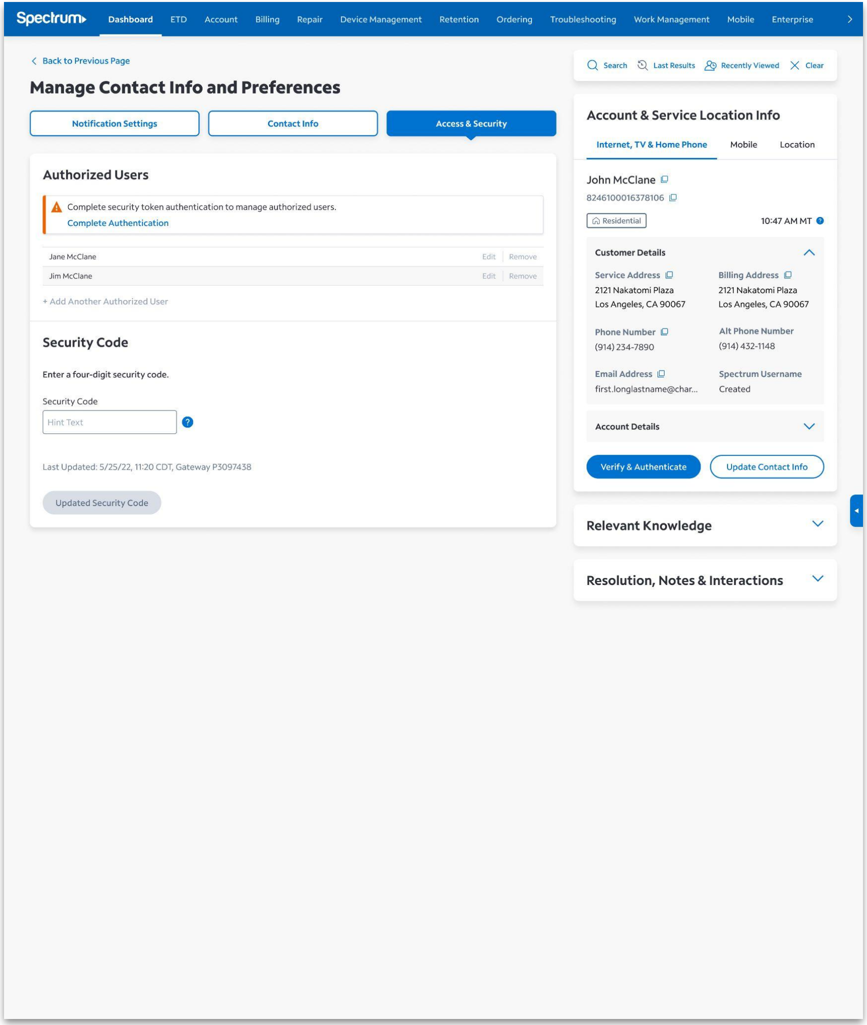
Definitions

Verification: A way of identifying the customer based on their voice prompts during the call-in process.

Authentication: A second step taken to confirm the customer's identity (also known as two-factor authentication or 2FA).

Authorized User: A trusted person the customer adds to their account who can access information and make decisions.





Final Design and Prototype

After finalizing the content for this section, we were able to work with our Customer Operations partners to relocate it. Now, all of the items that require two-factor authentication are located on the same tab.

Figma prototype

We'll partner with our UX research team in the future to determine the best agent experience for these settings. This will potentially affect the page title, tab order, and CTA used to navigate to this part of Agent OS.