Okta - Recent Sign-in Activity

Purpose: Use this document as a reference for identifying recent sign-in activity for your account in ctcLink.

Audience: College Faculty, Staff and Students.

The **myaccount Sign-In** page can by located by navigating to https://myaccount.ctclink.us.

Recent Sign-in Activity

Recent Activity provides end users with information about sign-in and security event activity.

- Sign-ins provides end users with increased visibility into their account by summarizing a list of their most recent sign-in activity to Okta.
- Security Events provides end users with a summarized list of recent security events from their Okta account.

> ❗ Strange or unusual activity should be reported to campus help desk.

## Sign-ins and Security Events Details

- Sign-ins feature relies on a System Log event called user.authentication.verify. This event is fired when an end user completes authentication to sign in to Okta.
- Security Events logs primary and secondary email updates, password change events, factor enroll and reset events from the most recent days.
- Sign-ins and Security Events features are only supported in the new Okta End-User Dashboard, which is currently a self-service Early Access feature. If end users revert to the old dashboard, these features will not be available.

Recent Sign-ins

Sign-ins provides end users with a summarized list of their most recent sign-in to Okta. When enabled, this feature:

- shows up to the last 100 sign-in attempts or activity up to the last 30 days.

- groups information by the device used to sign in to Okta.
- provides end users with a device link for viewing recent sign-in details.
- shows an approximate location for recent sign-in activity.
- provides end users with a button to report suspicious activity to their Okta admin directly.
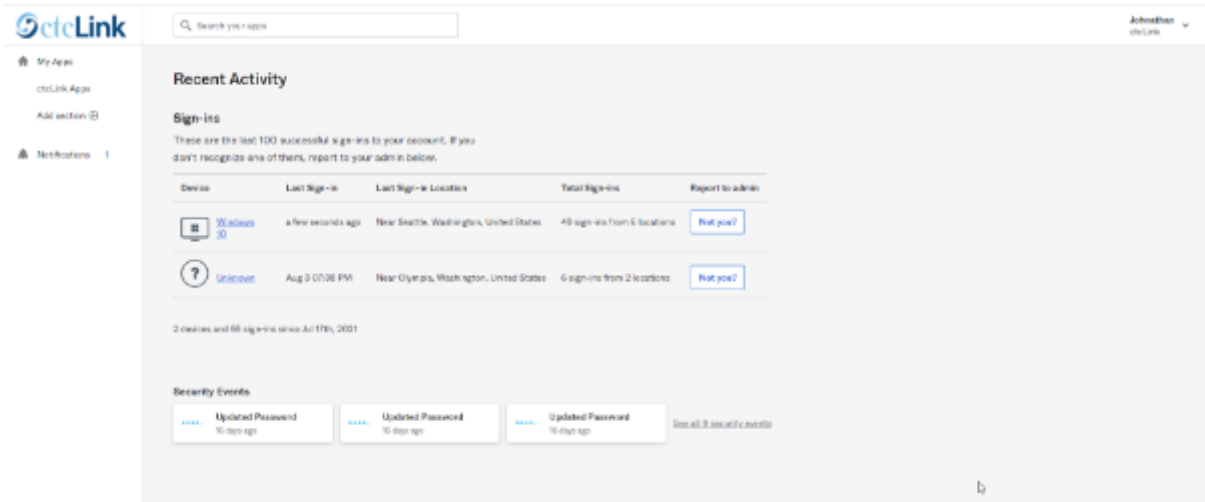
Sign-ins Information

After this feature is enabled, there are no additional settings to configure.

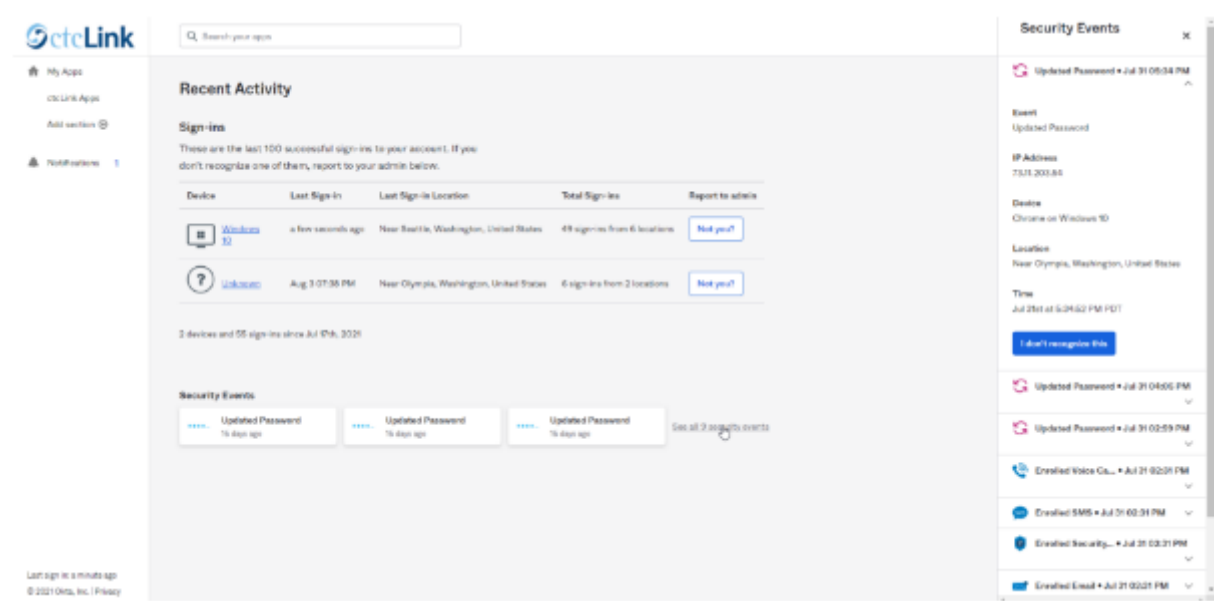End users will have access to the following Sign-ins information about their account:

Device	The device used by the end user to sign in to Okta. When a user clicks this link, detailed information is displayed for each sign-in activity: • IP Address • Location • Time • Browser • I don't recognize this sign-in: Users can click the button to report unrecognized activity directly to their org admin.
Last Sign-in	The most recent time that the device was used to sign in.
Last Sign-in Location	The best effort or approximate location where the user signed in.
Total Sign-ins	A summary of the total sign-in activity and location activity.
Report to Admin	Provides an option for the user to report potential suspicious activity directly to their admin.

Security Events

Security Events provides end users with a summarized list of recent security events from their Okta account. Security Events provides information about updates to primary and secondary email accounts, account password changes and MFA Factor reset and enrollment. When enabled, this feature:

- shows up to the last three most recent security events and when they occurred.
- provides end users with more security events when they click the See more link.
- provides end users with a button to report suspicious activity to their Okta admin directly.
- provides end users with a message when no security events information is available.

> ⚠ When an account gets created, you may see Oregon as the first entry when checking your Okta login activity within the Okta portal; myaccount.ctclink.us. Do not be alarmed! This is the AWS region our PeopleSoft environments are in. Okta will log the account creation from PeopleSoft, Activate Your Account (AYA) for 90 days. Ninety days is the length a user can see their login activity.

Security Events Information

After this feature is enabled, there are no additional settings to configure.

End users will have access to the following Security Events information:

Security Events	When a user clicks a security event, detailed information is displayed for each security event:

- Event
- IP Address
- Device
- Location
- Time
- I don't recognize this sign-in: Users can click this button to report unrecognized activity directly to their org admin

ℹ️ Device, IP and Location events can display with **Unknown**, when the original event does not capture enough log information.

💡 *Information taken from Okta Help Center user documentation.*

The process to review recent sign-in activity is now complete.