Portal URL Overview

Last Modified on 07/30/2024 1:10 pm EDT

Overview

The **Portal Settings: Portal URL** feature allows administrators to use a single account to grant multiple users limited access to Core. This is done by generating a URL that displays only the Confidential Submission form (e.g., an incident report) or selected activity, without requiring login credentials. This feature is useful for organizations that occasionally require third parties or front-line employees to confidentially create or edit Core data.

Tip:
Are you an incident management application user? Read more here: Confidential Portal Overview.

All changes made via a Portal URL are captured in the Audit Trail. Therefore, when creating a new Portal URL, administrators must first create a non-administrative user account and assign that account to a role with access to the applicable object type(s) and activity from the confidential submission.

Note:
By creating a Portal URL, you are accepting the Terms of Service on behalf of the users who will be accessing the link.

IP Authorization Control

IP authorization control helps administrators control who's accessing specific orgs based on the IP address of users logging into Core and users accessing it through a Portal URL.

If enabled on a Portal URL, the IP address of the user accessing the URL will be validated against the entries in the org's IP allow list. If the IP address doesn't match any of the entries, a 403 error is displayed. This is captured in the User Audit Trail as an **Unsuccessful Portal URL Login** event.

Before this option can be enabled on a URL, IP authorization must be enabled on the org by a member of Resolver Support. For more information, including functionality for additional login scenarios, see the IP Authorization Control section.