Vertiv™ Avocent® ADX MP1000 Management Platform and Vertiv™ Avocent® ADX RM1048P Rack Manager

Resolving Log In Issues with External Authentication Provider Users

Technical Note

SEPTEMBER 2023

Technical Note Section Outline

1. Overview

The Vertiv™ Avocent® ADX MP1000 Management Platform and Vertiv™ Avocent® ADX RM1048P Rack Manager allow users from an external authentication provider group to log into the Vertiv™ Avocent® ADX platform. (External authentication providers include Active Directory or LDAP, for example.) For this feature to work, the following pre-requisites must be met:

- An external authentication provider must already be added and configured.
- An internal user group must already be created and have a system role assigned to it.
- Then, the external authentication provider group must be assigned or mapped to an existing internal user group.

NOTE: For additional information, see the Authentication Providers, User Management, and Roles and Permissions sections of the Vertiv™ Avocent® ADX MP1000 Management Platform Installer/User Guide (available at www.vertiv.com/ADX-Management-Platform) or the Vertiv™ Avocent® ADX RM1048P Rack Manager Installer/User Guide (available at Vertiv™ Avocent® ADX Rack Manager). When the product page links open, the documents are listed under the *Documents & Downloads* tab.

2. Issue and Workaround

When you create an internal user group, if you do not assign a system role to it, then users from the external authentication provider group are unable to log in to the Vertiv™ Avocent® ADX platform. In this section, we will demonstrate how to replicate this issue for reference and then provide you with a workaround to resolve it. In order to replicate and resolve this issue, you must be able to access the list of internal user groups in the appliance web User Interface (UI).

Accessing the Internal User Groups List

To access the list of internal user groups:

1. Log into your Vertiv™ Avocent® ADX platform appliance web UI with an administrator user account.
2. In the UI sidebar, select *Administration – User Management*.
3. When the User Management page opens, select the *Groups* tab to access the list of internal user groups.

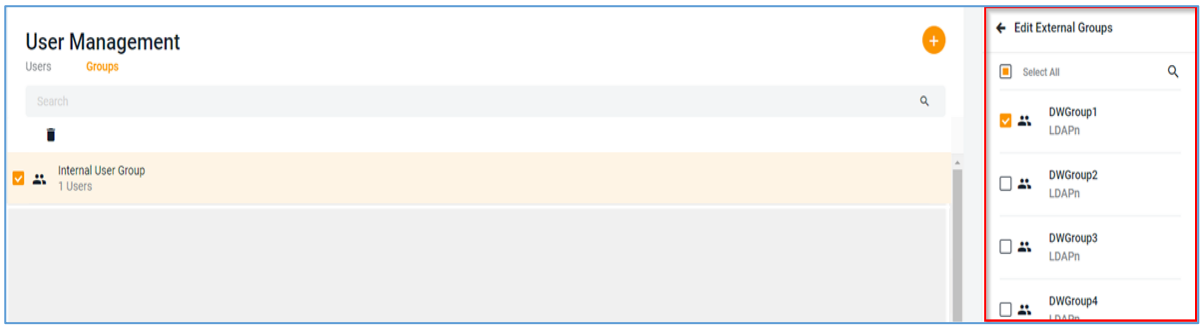
Replicating the Issue

To demonstrate how users from an external authentication provider group cannot log in if a system role is unassigned:

1. Access the list of internal user groups in the Vertiv™ Avocent® ADX platform appliance web UI.
2. Select the applicable internal user group.
3. Under the Internal User Group section on the right-hand side of the screen, click the Edit (pencil) icon next to Group Properties.

4. Verify that no system role is assigned to the internal user group.

5. Click the Edit (pencil) icon next to External Groups.
6. Select the external authentication group to assign or map to the internal user group.



7. Log out from the web UI, then log in again with a user from the external authentication provider group. The login screen stays frozen, does not show any error messages to the user, and does not allow the user to log into the web UI.

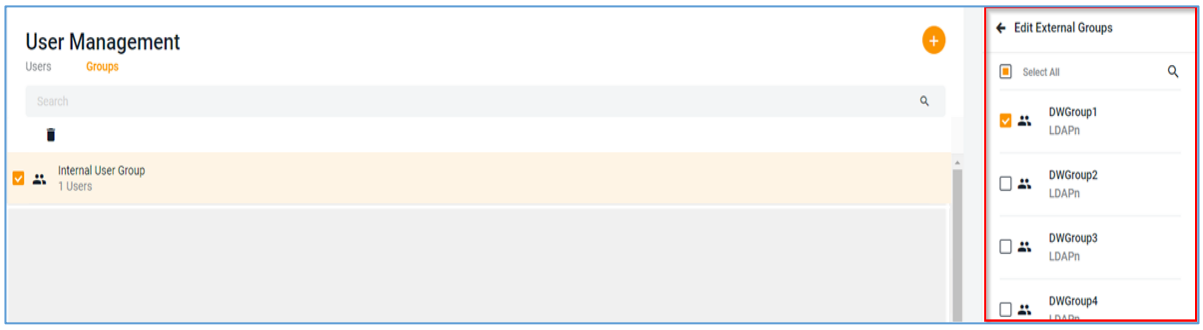
Resolving the Issue

To workaround the log in issue:

1. Access the list of internal user groups in the Vertiv™ Avocent® ADX platform appliance web UI.
2. Select the applicable internal user group.
3. Under the Internal User Group section on the right-hand side of the screen, click the Edit (pencil) icon next to Group Properties.
4. Select at least one System Role from the list to assign it to the internal user group.

5. Click the Edit (pencil) icon next to External Groups.

6. Select the external authentication group to assign or map to the internal user group.



7. Log out from the web UI, then log in again with a user from the external authentication provider group. The user is now properly logged into the web UI.