Managing Active Directory Groups to Access Level Mapping

The SBC Edge (SBC) does not manage individual Active Directory user's SBC permissions directly, instead they are managed by mapping their SBC access level to the Acive Directory (AD) Group(s) to which the user belongs.

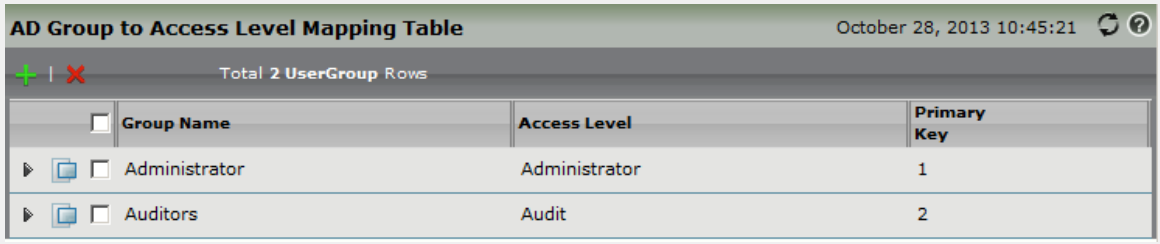
When Active Directory users are authenticated, their permissions on the SBC, will depend on the configured **mapping between their existing Active Directory Group and the SBC Access Level**.

Missing AD Group to SBC Access Level Mapping
If an AD user belongs to a Group which is not mapped to a SBC access level, this user's access will be denied on the SBC.

Working with Active Directory Groups to Access Level Mapping

1. In the WebUI, click **Settings**.
2. In the left navigation pane, go to **Security > Remote Auth Permissions > AD User Group.**

Figure 1: AD User Group



To view an Active Directory Groups to Access Level Mapping's properties:

1. Click the pop-up icon (
   
) next to the entry you want to view.
2. When you are finished, close the window.

To delete an entry, select the checkbox next to the entry and then click the Delete (

) icon.

Creating and Modifying Active Directory Groups Access Level Mapping