USE ACTIVE DIRECTORY AND GOOGLE AUTHENTICATOR FOR AUTHENTICATION

The Validation Platform supports using Google Authenticator on Active Directory user accounts. This provides an additional layer of authentication on a per-user basis.

Setting up Active Directory with Google Authenticator for use is a three-step process. First, the administrator configures the platform to use Active Directory and creates Active Directory users. Next, each Active Directory user must configure their own account to use their Google Authenticator app.

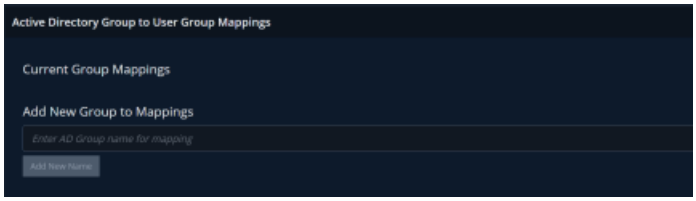
Administrator Setup

CONFIGURE ACTIVE DIRECTORY AS AN ADMIN

1. Go to **Settings** > **User Settings**. The User Settings page opens.
2. Select **Authentication**.
3. Select **Active Directory + Google Authenticator**.
4. Define the authentication fields, which are provided by your Active Directory administrator.
    a. Enter the **AD Server - Address**.
    This is the IP address of your Active Directory server.
    b. Enter the **AD Server - Port**.
    This is the port on which to connect to the Active Directory server (default: 389).
    c. Select the type of encryption you want to use in the **AD Server - Encryption** (default: None).
    d. Enter the **AD Server - Local User**.
    An admin account that always uses local authentication in case of networking or configuration issues. The field defaults to the first user account that is set as Admin.
    e. For Enable Active Directory User Group Sync, select either of the following radio buttons:
        - **True:** Enables the user group sync for users. Upon login, this setting adjusts the user group for the user (based on the Active Directory and group setting and user group mappings).
        When you enable user group sync, the Active Directory Group to User Group Mappings settings display. See **Add New Group to Mappings**.
        If you select False, the mappings settings will not display.
        - **False**: Disables the user group sync.
    f. For Automatically add new users who match group mapping to MSV on first login, select either of the following radio buttons:
        - **True**: Automatically adds the new user to MSV and associates them with the group specified by the AD group/mapping.
        Your Active Directory and Active Directory User Principal Name must be configured.
        - **False:** Disables the user being automatically added to MSV.
    g. Enter the Active Directory Username.
    This is a user account with read access to AD to query users and groups. This is commonly referred to as a “bind” account.
    h. Enter the Active Directory Password.
    This is the Active Directory password for the user.
    i. Enter the Active Directory Tree Root.
    Set the highest common level in the AD tree that contains all users and groups needed for MSV AD

authentication. For information about how to find the Active Directory Tree Root, see **Finding the Active Directory Tree Root**.

5. Click **Update Authentication Settings**.
   If you selected **Enable Active Directory User Group Sync**, the **Active Directory Group to User Group Mappings** settings display.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cec2ee07dc756be50a9cf/n/ad-mappings-add-new-group.png)

Add New Group to Mappings

6. Enter an Active Directory group name in **Add New Group to Mappings**.

> **NOTE:** Any group name you enter in this field must match the corresponding group name in Active Directory exactly.

7. Click **Add New Name**.
8. In the **AD Group <'Group Name'> mapping to User Group** drop-down list, select the user group you want this group to be mapped to.

Select User Group to Map to AD Group

Now when a user, who is part of that AD group, logs in to the , the user group you selected is applied to them.

> If the user is not part of any Active Directory group with a mapping to a user group, they will not be able to login. In addition, if you add multiple group names and select a different user group, the chooses the highest user group level in the list; therefore, any user who is part of those groups will have the highest level of user group permissions after logging in.

> The **AD Login Name** in the dialog box for a user must match the value of the user's `UserPrincipalName` in Active Directory (this is usually the same as the user's email address but this may vary across environments) or the pre-Windows 2000 logon name `DOMAIN\USERNAME`.

9. Reboot the Director in one of the following ways:
   - Go to **Settings > Director Settings**. The Systems Settings page opens. On the System Settings page click **Reboot**, or
   - From the command line, enter `shutdown -r`.

The platform is now ready to use with Active Directory authentication.

Finding the Active Directory Tree Root

An Active Directory forest (AD forest) is the top most logical container in an Active Directory. In an AD forest, domains are arranged in a hierarchy as domain trees, which can be a single domain or a domain with one or more child domains that can also have child domains beneath them.

A domain tree is a contiguous namespace, meaning that the child domains are a continuation of the naming hierarchy. For example, a domain with the name comp.com (or DC=comp,DC=com) can have a child domain with the name mydivision (mydivision.comp.com or DC=mydivision,DC=comp,DC=com), which could then have a child domain with the name mydev (mydev.mydivision.comp.com or DC=mydev,DC=mydivision,DC=comp,DC=com).

TO FIND THE ACTIVE DIRECTORY TREE ROOT

From your Active Directory server:

1. Select **Start > Administrative Tools > Active Directory Users and Computers** .
2. In the Active Directory Users and Computers tree, locate and select your domain name.
3. Expand the tree to locate the path through your Active Directory hierarchy.
4. Domain name components have the following format:
    - `DC=domain name component`

> **NOTE:** Domain name components are appended to the end of the search base string and are comma-delimited.

5. You must include a separate domain name component in your Active Directory search base for each level in your domain name. For example, if your domain name is prefix.example.com, the domain name component in your search base is:
    - `DC=prefix,DC=example,DC=com`

Create Active Directory Users

1. Go to **Settings** > **User Settings**. The User Settings page opens.
2. Select **Users**.
3. Click **Add User**.
4. Enter the following information for the user.
    a. Email: Their Active Directory email address
    b. First name: Their first name
    c. Last name: Their last name
    d. AD Login Name: The login name of their Active Directory

    > **NOTE:** You can enter either DOMAIN\USERNAME or username@domain in this field.

    e. AD User Principal Name: The UPN of their Active Directory

    > **NOTE:** This name must match the AD UPN that's in the Active Directory.

5. Select a **User group** from one of the following roles:
    - System Admin
    - Power Users
    - Users
    - Reporting

- Custom

  For information about user roles, see **Security Validation User Groups and Permissions (https://docs.mandiant.com/home/msv-user-groups-and-permissions)**.

6. Select **Approve Endpoint Actions** if this user will be permitted to approve Host CLI Actions after the Action is created.
7. Select **Approve on Action Creation** if this user will be permitted to approve Host CLI Actions while creating the Action.
8. Select **Approve File Library Restrictions** if this user will be permitted to designate a file as safe during upload to the file library or to approve uploaded files that are in a Pending Approval state. See **Approving Files for Use in the File Library (https://docs.mandiant.com/home/msv-approving-files-for-use)** for more information
9. Click **Create User**.

   The new user can log in using their AD email and password.

End user setup

Configure Google Authenticator

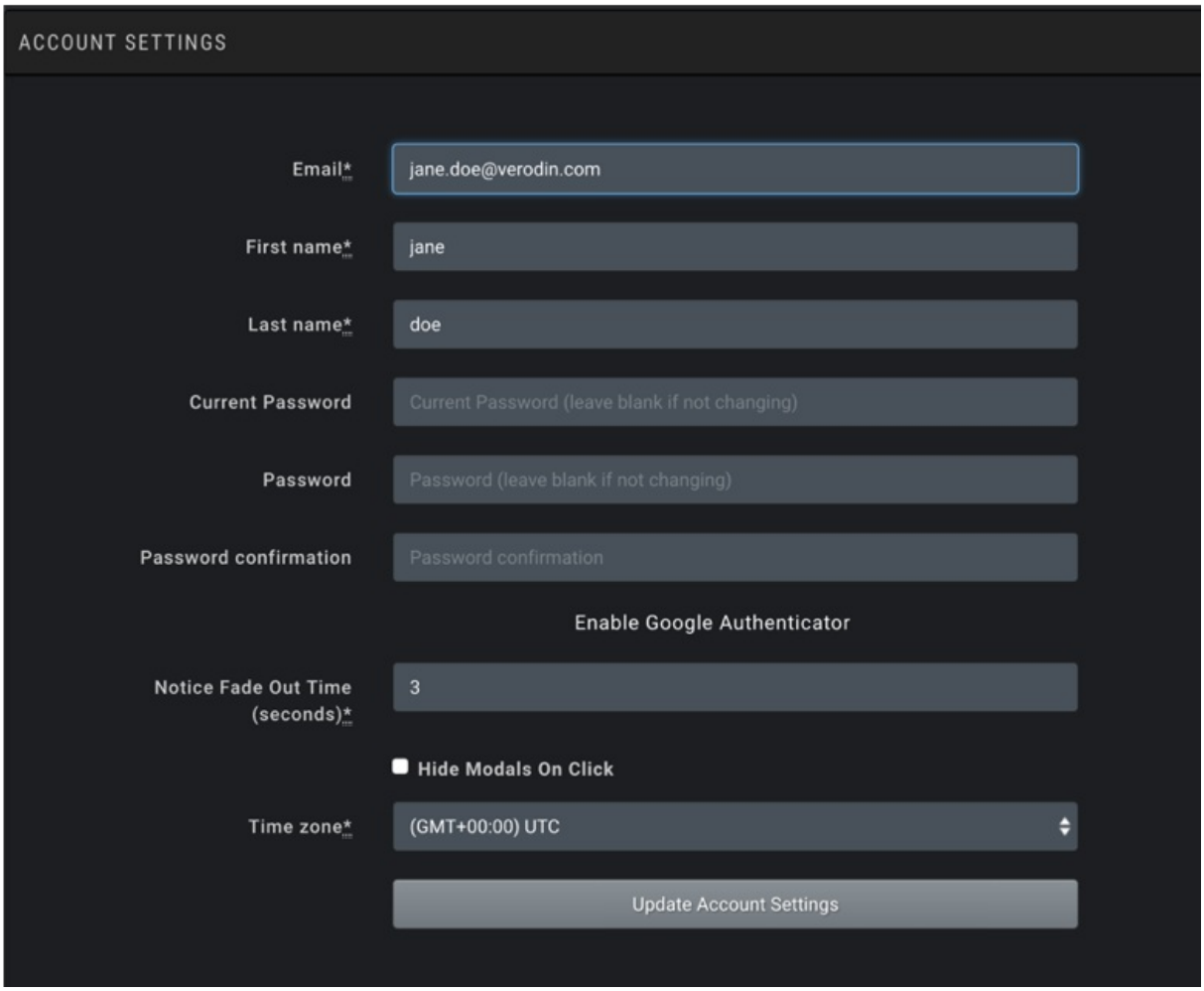
After an administrator enables Active Directory authentication, each user with an Active Directory email address can configure their account to use Google Authenticator.

> **NOTE:** Each user must complete this process the first time they sign into the Validation Platform. They will not be able to access the platform until they do.

1. Sign into the Director as a user created with Active Directory credentials.

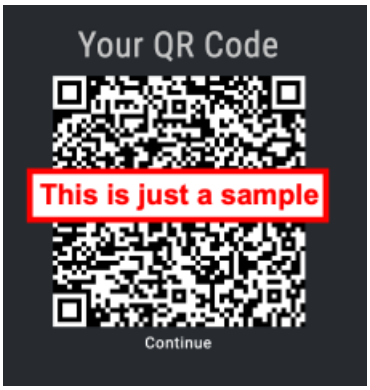
   > **NOTE:** Do not enter anything in Two factor code field. The field becomes required after completing this procedure.

   The User Preferences page automatically opens.



User Preferences

2. Click **Enable Google Authentication**.
   This step brings up a QR code that's specific to your Validation Platform account.



Google Authenticator QR Code

3. Open Google Authenticator, select add **+**, select **scan barcode**. The code is created in Google Authenticator tied to your Validation Platform user name.
4. Click **Continue** under the QR Code to return to User Preferences.

The next time you sign-in, you are required to enter the Google Authenticator token. If you do not, you will receive an Invalid Username or Password message.

Restore Two-Factor Authentication access for a user

Use the following steps if a user is no longer able to authenticate to MSV (on-prem) using two-factor authentication (2FA). For example, the user lost their mobile device, got a new mobile device, or accidentally deleted the MSV entry in their authenticator app.

> These steps require assistance from an MSV user with administrative privileges.

Temporarily enable local authentication for the user (admin)

1. Sign into the on-prem Director as a user with administrative privileges, and then go to **Settings > User Settings**.
2. Click the pencil icon under the Actions column associated with the user and then select **Local User Authentication**. This allows the user to sign in locally and then reestablish their 2FA connection.

Reconfigure two-factor authentication (user)

1. As the user who lost 2FA access, from the on-prem Director sign-in page, go through the forgot password steps and set a new password.

   > If you're not sure about where to sign in, work with your administrator.

2. When signed in, access `https://DIRECTOR_IP/two_factor`, where *DIRECTOR_IP* is the IP address of the Director you're already signed into. You should see a QR code.
3. Using your mobile device, scan the QR code and go through the steps to enroll in two-factor authentication.
4. Sign out from the Director session.

Disable local authentication for the user (admin)

1. As a user with admin privileges, sign into the on-prem Director and go to **Settings > User Settings**.
2. Click the pencil icon under the Actions column associated with the user and then deselect **Local User Authentication**. The user can sign in again using 2FA.