Security Awareness Training

Azure Active Directory Sync - Simple Setup

Telesystem IT's About Trust | #HackersSuck

The Azure Active Directory Synchronization feature allows you to manage users for Security Awareness Training (SAT) with ease. Add, Modify, or Deactivate users as soon as they are in your system so they can get up to speed on cybersecurity, without a hitch.

Create Azure AD Sync Security Groups

This step defines the portal access for each employee by adding them to groups.

Create the following Groups:

1. **BSN-Employees –** Defines the users that will be enrolled in SAT as standard employees.
2. **BSN-Managers –** Defines users in the manager role, supersedes BSN-Employees. Managers get access to reporting and employee data inside the SAT portal.

NOTE: **When entering the above security groups, spaces are NOT permitted before, after, or within the string.**
Important: If Azure AD Sync is enabled and these groups are note defined after the initial synchronization, there is a risk of users becoming deactivated in the portal and the users will be notified.

Set Group Parameters

For the BSN-Employees group use the following parameters:

- Group Name: BSN-Employees
- Group Type: Security
- Group Description: PII/PHI Protect Standard Users

For the BSN-Managers group use the following parameters:

- Group Name: BSN-Managers
- Group Type: Security
- Group Description: PII/PHI Protect Manager Role

An Option Group may be created for Manager Admins. This group would be given to select managers with the ability to manage phishing campaigns as well as the bulk manage user functionality. Standard manger accounts do not have this functionality.

For the Manager Admins group, use the following parameters:

- Group Name: BSN-ManagerAdmins
- Group Type: Security
- Group Description: PII/PHI Protect Manager Admin Role

Assign Users to Groups

Assign users to the appropriate groups that have been created. Anyone setup in the BSN-Managers group will also have an employee account.

Be sure not to assign non-user accounts to these groups as portal accounts will be created for all users assigned. Any user assigned to the BSN-Employees group and the BSN-Managers group will have the manager roll take precedence.

Create Tag Groups (Optional)

Tags are used for creating specific groups, typically to separate users by department, to create groups you'd like to send specific phishing email to, or to simplify tracking in the portal.

If you would like to use Tag Group, please create them using the following parameters:

- **Group Type** – Security
- **Group Name** – BSN-TAG-*tagname*
  - "tagname" will be the tag you want the users associated with
  - Examples: BSN-TAG-ExecutiveTeam, BSN-TAG-Finance, etc…
- **Group Description** – Optional field if you would like to add details on the tag you created.

Assign users to the group accordingly.

NOTE: For those using on-premise along with Azure Sync to synchronize with the free tier of Azure AD; nested group memberships are not supported for group-based assignment at this time.

Completing Directory Sync

The Telesystem ThreatProtector team will need valid credentials for an account that is designated as a Global Admin within your tenant to complete the setup. This will provide the SAT portal with access to the following:

- Sign in and read user profile
- Read all users full profiles
- Read all groups
- Read directory data
- Read all group memberships

Depending on the user count within your Office 365 tenant, the users should begin appearing with the User tab in the SAT portal in approximately 5 minutes.