MSCA group for UW Medicine access

Purpose

This working draft document collects objectives, requirements, and current proposals in a single collaborative document.

REQ2815414 is source.

Objective

In order to provide functionality for UW Medicine, MSCA needs an Exchange Enabled security group.

This group is critical to implement:

- Exchange Admin role delegations via RBAC roles to increase the agility and time to resolution for ITS
- Exchange Admin role delegations via RBAC roles to support UW Medicine compliance needs
- Automatic routing of user reported phishing from Microsoft built in tooling to UW Med CISO
- Other specialized routing rules as needed
- User forwarding controls to comply with UW Medicine forwarding policies.
- SPAM and Phishing policies appropriate for UW Medicine

It can potentially be used for scoping in Cloud App Security.

TBD – decrease the lag time during UW Medicine onboarding

Requirements

The membership should include:

- All UW Medicine Workforce members
- All Clinical Shared UW NetIDs available in Azure AD

The Exchange settings should be:

- TBD – No one, Anyone, Members of a specified group, list of groups or netids

Known constraints

The solution architecture includes the following constraints:

- Solutions that rely on Azure Connect have a 50K limit on group memberships synchronized from AD to AAD (see note)
- Disclosing group membership data to new audiences requires authorization from data owners
- A directly created Azure AD security group can not be Exchange enabled after creation (a synchronized Azure AD security group can be exchange enabled after creation)

Note: we have asked Microsoft to increase their limit, and this ask may be tracked somewhere; Nathan posed something exploratory about this to the AAD govteam.

Group design analysis and proposals

Group memberships

MSCA may have forgotten about some of the groups is this area, which they referenced in REQ1385495 to obtain access to the groups service.

These same groups are also described on this page:

https://wiki.cac.washington.edu/display/infra/UW+Affiliation+Groups

If you click through to the groups themselves, none are larger than 50K. The combined population of target (people) categories is 27,594. Shared UW NetID (non-people) adds just 945 UW NetIDs.

To move forward:

1. We need someone to help MSCA confirm a mapping between the subscription codes you listed in this request and these existing groups:

13: UW Medicine Workforce = uw_affiliation_uw-medicine-workforce (n=27,438)
76: UWP Provider = uw_affiliation_uwp-provider (n=2626)
~~77: UWP Admin Staff = uw_affiliation_uwp-staff~~
80: UWPN Admin Staff = uw_affiliation_uwnc-staff (n=399)
~~104: NWHMC Admin Staff = uw_affiliation_nwh-staff~~
~~105: NWHMC Provider = uw_affiliation_nwh-provider~~

22: UW Medicine Shared UW NetIDs = uw_affiliation_clinicial-shared ?? (n=945)

Note: There is an "Audience RX" product that UWM Marketing was using that introduces a different business and technical definition of UWM workforce tha t includes UWP, UWPN, NWH, Valley, Workday (by box number), but not "Workforce" people as provided to IAM from UWM's Puma database integration.

Note: see also UW Medicine affiliation group transitions 2019-2020

2. There is no reference group for "22: UW Medicine Shared", so we can draft a design proposal here:

Clinical shared UW NetID group design

Note: Above MSCA team refers to "Clinical Shared NetIDs available in Azure AD" which may or may not be the same as "22: UW Medicine Shared".

Provisioning to AAD design proposals

A: Proposed near-term plan - less work, same update latencies*

Assumptions:

1. the desired exchange-enabled group can include other exchange-enabled groups; i.e. it doesn't have to be flat.
2. none of the groups above will exceed 50K direct members any time soon.
3. TBD Azure Connect 50K limit is on direct membership, not effective membership.
4. TBD All Clinical Shared UW NetIDs by definition and design are in Azure AD; any that aren't in AAD should be.
    a. Therefore, Azure AD is a copy of the system of record (Identity Registry)
    b. Therefore, we can use Identity Registry as the data source for maintaining a group of all Clinical Shared UW NetIDs
5. * Once IAM releases real-time updates to uw_affiliation groups, update latencies will be equivalent to what they'd be with Subscriptions (plan B).

Here's a near-term plan, based on the requirements, constraints, and assumptions:

1. MSCA - create a group in the groups service (e.g. u_msca_uwm-exchange-access)
2. IAM - create Clinical shared UW NetID group
    a. e.g. TBD g_clinical-shared-uwnetids
    b. draft and review proposed design: Clinical shared UW NetID group design
    c. implement proposed design
3. MSCA / UWM - confirm which of these groups are fit for purpose:
    a. 13: UW Medicine Workforce = uw_affiliation_uw-medicine-workforce
    b. 76: UWP Provider = uw_affiliation_uwp-provider
    c. ~~77: UWP Admin Staff = uw_affiliation_uwp-staff~~
    d. 80: UWPN Admin Staff = uw_affiliation_uwnc-staff (TBD? maybe?)
    e. ~~104: NWHMC Admin Staff = uw_affiliation_nwh-staff~~
    f. ~~105: NWHMC Provider = uw_affiliation_nwh-provider~~
    g. TBD and/or define any new memberships that are needed.
4. IAM - obtains approval from each group data owner to share UWM group memberships with AAD and Exchange audiences
    a. IAM - remove viewer controls on approved groups
    b. IAM - exchange-enable approved groups
5. MSCA - add other reference groups to the policy group, as desired
    a. Azure Connect - notice and does its thing per current service design
    b. MSCA - confirms everything looks as desired
6. IAM - enable real-time updates to uw_affiliation groups
    a. April/May - complete design and testing
    b. April/May - draft, schedule, and approve change (RFC-0562)
    c. May - release to production

B: Alternative plan using Subscriptions - requires more work from IAM

Here's an alternative plan based on UW Subscriptions like is done to populate Azure AD licensing groups.

Note: this plan will require Ken to develop code, similar to that for AAD licensing groups, that talks to the Graph API.

1. Who – task or step in plan
2. Who – task or step in plan
3. Who – task or step in plan
4. Who – task or step in plan
5. etc.

C: Alternative future contingency plans – as needed

Some contingencies that may play out in the future:

If Microsoft lowers the Azure Connect 50K limit, we scramble a bit.

If any of the groups above show trends of exceeding 50K members in TBD 3-6 months, we transition to an alternate design; e.g. an integration architecture that syncs data from the groups service to AAD through the Graph API (or similar other MS API fit for purpose). Note: the purpose of this current wiki page isn't to explore and describe pros and cons of alternate integration architectures between groups and AAD. We know that can be documented elsewhere.

TBD. Other contingencies can be added here, as needed and if useful.

Data owner/custodian approvals

We need to get authorization to integrate the group membership data into the new target systems (e.g. AD, AAD, Exchange) and therefore disclose data to new data viewers.

1. Nathan (or other?) - identify data owners/custodians for each group.
2. Nathan - identify and document the AD, AAD, Exchange access policies with respect to data disclosure.
    a. We have a good set of subject matter experts who understand the technical controls applied to data in these systems, and we can translate that into an access policy in natural language that data custodians can understand.
3. Nathan (or other?) - request approval(s) from data owners
    a. ensure record of request/approval is created