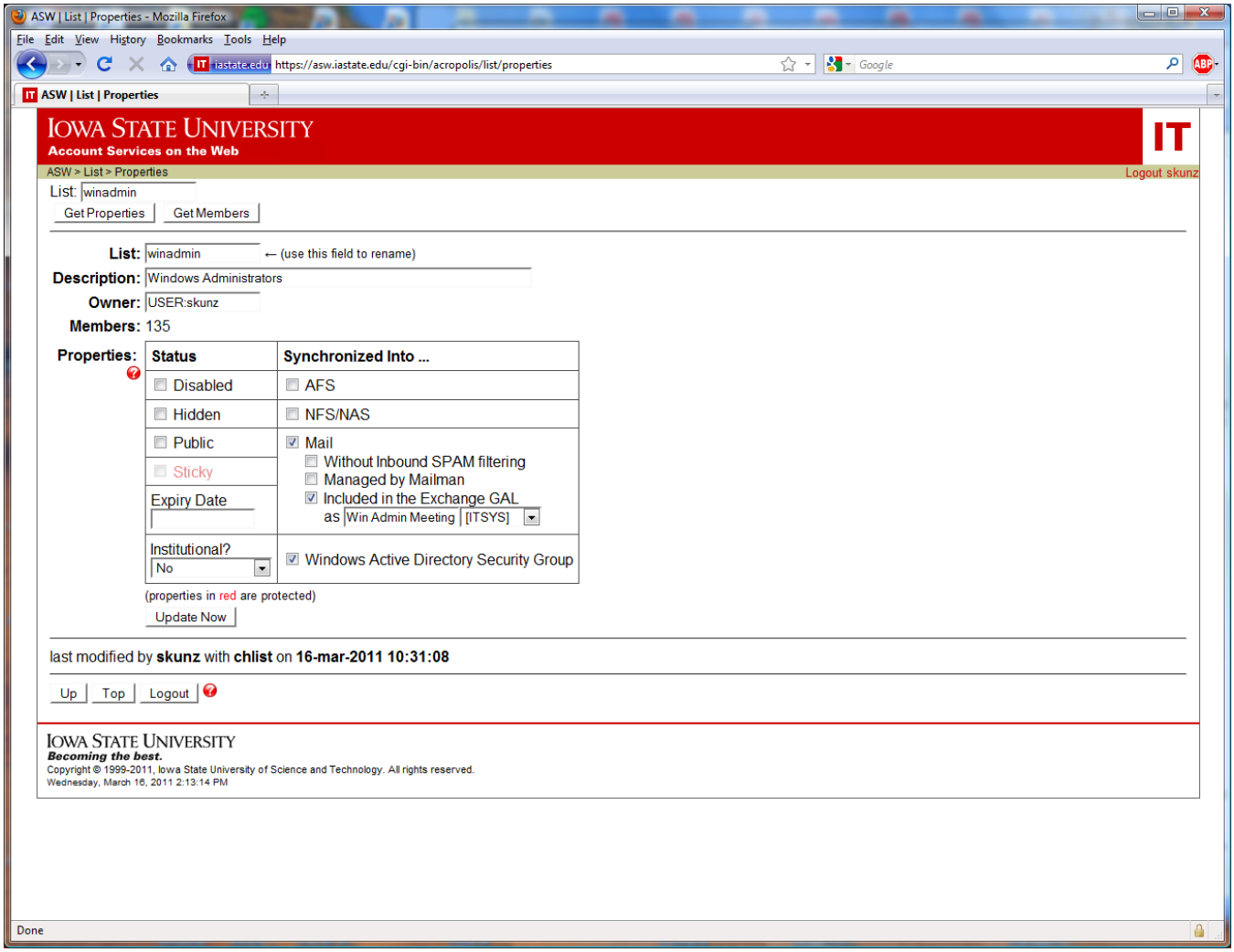
Windows Enterprise Design
ListSync
User Requested Lists as Universal Security Groups

September 14, 2009
Updated: December 8, 2015

ASW List owners can request any ASW list to synchronize into Windows Active Directory as a Universal Security Group. List synchronization is established by the list owner using Acropolis Secure Web utility (ASW) at https://asw.iastate.edu by altering the list properties. Two properties (selected by checkboxes) relate to Windows synchronization – "Hidden" and "Windows Active Directory Security Group".



All lists synchronized to Windows will exist as Universal Security Groups in one of two containers in Active Directory:

- AutoLists/UserReqLists (for groups with visible membership)
- AutoLists/UserReqHMLists (for groups with hidden membership)

Checking "Windows Active Directory Security Group"

- Causes the list to begin synchronization to Windows Active Directory as a Universal security group.
- If "Hidden" is not checked, the membership will be visible and the group will be created in the "AutoLists/UserReqLists" container.
- If "Hidden" is checked, the membership will be hidden and the group will be created in the "AutoLists/UserReqHMLists" container.

Unchecking "Windows Active Directory Security Group"

- Causes the security group to be deleted in Windows Active Directory
- IMPORTANT! If you have Windows resources that use this security group (shared files, etc) use caution here. Unchecking "Windows Active Directory Security Group" means that any resources with access controls to the Windows Universal Security Group are lost and need to be reconstructed if the "Windows Active Directory Security Group" box on the list is checked again (since the GUID of the group will be different). Make sure you are aware of *where* the Universal Security Group is used before unchecking the "Windows Active Directory Security Group" checkbox.

Changing "Hidden" with "Windows Active Directory Security Group" Checked

- Causes the existing group to be move to the appropriate container and the membership make hidden or visible as appropriate.
- Any Windows resources that use the security group retain their correct access control list (only the membership visibility of the group changes).

General Notes

- Name conflicts within the domain will be detected. Conflicts are not allowed (i.e. if a security group with the same name exists within a college/departmental OU the sync request will not be allowed). Due to the design of the ASW web page and the ListSync infrastructure, an immediate web popup with an error message is not possible. An email will be sent with a "name conflict" message to the NetID of the owner of the list (the person initiating the request). An ASW web page "refresh" will result in the "Windows Active Directory Security Group" checkbox being "unchecked".
- Membership in hidden lists can only be viewed on the list via ASW. Membership of hidden security groups for "user requested" lists cannot be viewed with Windows Active Directory (even by the owner).
- Membership in the Windows Universal Security Groups can only be changed by changing the membership in the ASW list. User-requested groups are always mastered from ASW.
- Changes in the list properties related to Windows Active Directory synchronization occur within a few minutes (with the list and its current membership being pushed into Windows AD).

- Only members that are “users” (NetIDs) or “lists” are pushed down to Windows. Other values (such as “strings” of external email addresses) are NOT pushed down (since they have no meaning in a security group context within Windows).

Nested Lists (“Lists of Lists”)

- Nested lists are supported ("lists of lists and users" on ASW become "groups of groups and users" on Windows).
- For a list containing nested lists you must check the “Windows Active Directory Security Group” box for EACH “member list” you want have pushed down to Windows. Simply checking the “Windows Active Directory Security Group” box on a list containing other lists will NOT cause the “member lists” to be automatically pushed down. However, the order in which you select the lists to be pushed down is not important. If you select the “top” list first, then select the “member lists”, they will appear as members of the owning lists. Likewise, if you select the “member lists” first, then select the “owning” list, the owning list will contain the “member lists” previously pushed down.

Important Implications of This Design

- Provisioning of lists occurs at the master (ASW) level. Within ASW “lists” are owned by the creator/owner. However, when synchronized to Windows Active Directory the Universal Security Group is owned by an Active Directory administrative account. If the creator/owner of a list leaves the university and ownership is not transferred to an existing valid NetID, the list will eventually be deleted by automatic provisioning. At that time the Windows Universal Security Group will also be deleted. Lists that perform longtime functions should be owned by a non-expiring administrative account (available through the Solution Center) or have “group ownership”.