Windows Enterprise Design
Enterprise Design Summary

July 25, 2002
Last Update: June 7, 2013

Forest Design – Single Forest

- The only design that allows a single Exchange organization. This is required to enable enterprise-wide shared calendaring and other online collaboration. Departmental organizations can still be delegated control of their own Exchange servers.
- Collects disperse resources logically into a single management pool for seamless authentication and access
- Common Active Directory Schema, with enterprise-wide policy for schema changes (including review, testing, and application forest-wide)
- Trusted root-domain administrators
    - Domain, Enterprise and Schema Admins at root domain level managed under published enterprise policy
    - Existing departmental and college IT admins will become Organizational Unit admins within their own department or college.

Domain Design – Single Domain

- Best practice as recommended by Microsoft for Windows Active Directory enterprise design
- Single username/password (ISU Net-ID)
- Accounts for people not formally associated with ISU ("exception accounts") will be accommodated better in the future (web-based, not "paper generated")
- Common password policy. Current policy is that enforce by the Acropolis interface:
    - Five character minimum
    - Two character sets required (letters, numbers, special chars)
    - No Expiration (but OU admins can enforce their own expiration on OUs, lists of users, or groups with an AIT-supplied software tool)
    - Cannot use same password twice in a row
- Provides for passwords changes for accounts linked to an ISU NetID to be propagated back up to Acropolis. Changes either by the user changing their password or an OU administrator "setting" their password are "synched". A "bi-directional password synch" is implemented.
- Provides the least amount of enterprise complexity. Makes enterprise trouble-shooting faster/easier.

Site – Single Site (with additional sites as needed for network limitations)

- Currently have one sites (main campus)

- Possible additional sites in the future for Extension Field Office locations

Organizational Unit Design – Departmental OUs

- Delegated full control to departmental admins for their OU
- Faculty/Staff user accounts may be moved into a "Users" container within a college/departmental OU so the departmental admin can reset passwords, maintain roaming profiles, home directories, etc.
- Departmental application/file servers live within departmental OUs.
- Cross-departmental Faculty/Staff reside within one OU based on university records
- Students (inherently cross-departmental users) live within a "generic student" OU managed at the enterprise level. Departmental admins will use standard Windows resource controls to manage what students may access in their department. Work is still being done to determine how departments can still manage roaming profiles and home directories for students on a department-wide basis as needed.

Object Management – Users, OUs, and Groups

- Usernames will come from a single unique namespace, the Acropolis Net-ID pool. Create, Delete, Suspend, Un-Suspend, and Rename operations at the Acropolis level will be instantly replicated in the Windows Active Directory domain. This is key to the accomplishment of a "single sign on" environment for the ISU enterprise.
- Existing departmental faculty/staff may be moved into a departmental OU if the move is coordinated with and enterprise admin (to move them from the general "Users" pool into the departmental OU). After the departmental OU structure exists, new departmental faculty/staff users are automatically placed into a departmental OU (without manual movement).
- It is VERY IMPORTANT that the "security rights" for whatever OU you move NetID-based user objects into be correct. You MUST NOT lock out enterprise "Administrators" access in an OU where university information (and passwords) must be synchronized from the enterprise level. Specifically:
    - The "IASTATE/Administrators" group must have full rights to objects in the "<your OU>/Users" container to add/update/delete the NetID-based user objects that were placed there when your faculty/staff were populated into your OU.
    - If you move NetID-based user objects from "<your OU>/Users" to another OU within your OU, you must remember to grant the "IASTATE/Administrators" group full rights to objects in that container, also, or updates will break.
- Windows OU administrators may create "special purpose" usernames within their Windows OU (for "non-ISU users" or special software application needs). These usernames must follow an "enforced standard" to avoid conflicts with Acropolis Net-IDs that may be created later. The "enforced standard" is that these usernames must be preceded by a "special character" (currently an "!"). Any usernames created by departmental admins that do not have the required "special

character" will be renamed automatically (with the special character pre-pended) by an overnight process.
- Sub-OUs may be created/rename/deleted/moved by Windows OU administrators.
- Official university "department", "college", "major", and "class" lists are automatically synchronized down into Active Directory as "Global Security Groups". Membership in these lists is controlled by official university data sources (the Personnel and Registrar's offices) and can be used but not manipulated within Windows Active Directory. Membership in certain groups (such as class-list based groups) is hidden for FERPA compliance.
- Private Acropolis lists (managed by ASW) can be synchronized to Windows as security groups. Both hidden and visible membership is supported.
- Private Acropolis mail-lists (managed by ASW) can by synchronized to Windows as Exchange contacts. This causes them to appear in the GAL for selection to mail to with Outlook clients.
- Windows OU administrators may create departmental security groups. Like usernames, the Acropolis namespace is given priority. Departmental list must be created with a "special character" preceding it (currently an "!") to make sure the name does not conflict with an Acropolis list. Any groups created by departmental admins that do not have the required "special character" will be asked to be renamed.

Domain Controller Infrastructure – Enterprise Capacity Planning
- Domain controller capacity currently adequate for needs (five root domain controllers)

Time Services
- Domain controller network time synchronized from existing campus time standards.

DNS Architecture - BIND
- Existing BIND/DNS servers are suitable for all Windows functionality
- Dynamic DNS registration of hostname records will not be supported (use of upcoming NetReg expansion for campus-wide DNS registration will provide a similar function).

DHCP Architecture
- Existing DHCP server are suitable for nearly all Windows functionality
- Exception is the "network discovery" capability of Systems Management Server 2.0. Using this feature of SMS 2.0 that queries Microsoft DHCP servers for a list of all known registered devices for SMS client agent installation.. This functionality is of limited use in an enterprise such as ISU with many thousands of registered DHCP devices.

Naming Conventions
- Username - Existing Acropolis naming convention
- Hostname – Existing Acropolis naming convention

- Group name – Existing Acropolis naming convention

Acropolis Extensions Related to Windows Active Directory Integration

Several modifications/extensions have been implemented to accommodate departmental needs in the integrated environment. Some of these are:

- Automatic population of departmental OUs with Faculty/Staff user accounts (via existing enterprise directory information).
- Two-way password sync. Changing the ISU NetID password changes it in Windows Active Directory. Changing the password on Windows Active Directory changes it for the Acropolis ISU NetID.
- ASW list to Active Directory security group sync.
- ASW mail-list to Active Directory contact sync.

Possible Future Acropolis Extensions

Several modifications/extensions are being looked at to accommodate departmental needs in the integrated environment. One such idea is the automated creation of exception accounts via a secure web page (asw.iastate.edu). This will be used to create "Acropolis-wide" usernames for "non-ISU" staff that can be used on multiple operating systems (not just Windows).

Exchange 2000/2003/2007/2010

Exchange 2000 was a major design change from the old Exchange 5.5 system. Exchange 5.5 had a separate directory system for email and scheduling of people and resources. Starting with Exchange 2000 a separate Exchange directory was eliminated and Windows Active Directory became the single integrated directory for all users.

The university has implemented an enterprise "Exchange organization". This "root level" Exchange architecture encompasses all existing departmental Exchange servers for message flow and overall integration. Departments can still manage their own departmental Exchange servers, though a strong focus is being placed on central provisioning of Exchange.

Central Exchange provisioning continues. Schema updates to support Exchange 2003 were added March 6, 2004. Schema updates to support Exchange 2007 were added July 2009. ITS currently supports Exchange 2007 and is looking ahead to Exchange 2010. Schema updates to support Exchange 2010 were added April 19, 2011.

SMS 2003 and SCCM 2007

SMS and SCCM are used for system management of groups of machines. The university currently provides support for SCCM 2007 (the schema extensions for SCCM 2007 were installed March 2011).

OCS and Lync

Microsoft Office Communications Server was place in production in 2010. This product integrates with Active Directory and Exchange to combine instant messaging, presence, conferencing, desktop sharing, and voice telephone. OCS was later upgraded to Microsoft Lync. See http://www.it.iastate.edu/services/lync for more information on this offering.