Windows Enterprise Design
Departmental Enterprise Product Support Standards

Standard Publication Date: June 24, 2009
Last Review Date: June 24, 2009
Review Cycle: Semiannual

The Enterprise Domain standards apply to all product installations into the Windows Enterprise Domain. These standards apply to colleges, departments or individuals that select products that require action at the Enterprise forest/domain level for deployment and support. Such product installations may include enterprise/domain administrator privileges, Windows Enterprise forest/domain schema extensions, special DNS records, or other Enterprise infrastructure support or modification.

Microsoft Active Directory Built-in Features

Some Microsoft Active Directory features (or products) require actions at the Windows Enterprise level. Many of these issues have already been addressed and simply require "authorization" (or some other action) by an Enterprise/Domain administrator. Examples of such actions may be authorization of "RIS" (Remote Installation Services) servers, group membership for "RAS" (Remote Access Service) servers, or schema extensions required for Exchange servers. However, there will certainly be new Microsoft products available that have never been introduced into our Windows Enterprise domain. To place these products into production may require action at the Enterprise level.

Non-Microsoft Products

Some non-Microsoft "Enterprise class" products may be designed to be managed solely at the Enterprise level and "peer level" shared management may introduce security/usability concerns that preclude any other departmental shared use of the product. It is possible that such requests could be honored but administered at the Enterprise level for the entire university. Products that are designed to do "identity management" (manage user objects) must not interfere with Enterprise account provisioning for university Net-IDs already in place.

Non-Microsoft products will undergo more strenuous research. Non-Microsoft schema changes to Active Directory impact the entire Enterprise domain and must be carefully examined and controlled to protect the proper functioning of Active Directory. Microsoft has designed schema changes so that they can never be "un-installed". Poorly written/tested schema changes may require a complete restore of the Windows Enterprise domain infrastructure from backups, causing considerable disruption of the domain.

As a result of these security, stability, and manageability concerns it may not be possible to approve all requests.

Security and Abuse Issues

This standard precludes products that rely on insecure security protocols (such as LANMAN/NTLMv1 and clear text password exchanges). Products cannot be abusive of Active Directory resources. Examples of abuse are large numbers of repetitive authentication attempts (either successful or failed) or performing repetitive deep-tree LDAP searches on non-indexed values. Such activities impact domain controller performance and domain event log space utilization.

Standards

Standards established by the Enterprise Administrators for any new product introduced at the Windows Enterprise level are:

1. Scope of Benefits. Multiple departments or people should benefit. In general, products that will have "enterprise wide" applicability will meet this consideration even if only one college/department wants the product originally.

2. Impact on AD Size/Replication (Schema Extensions only). Schema Extensions cannot cause AD space requirements to grow beyond current limits. The product should not be designed to cause large amounts of replication activity (i.e. an extremely large number of constant attribute changes to Active Directory objects).

3. Administrative Management. The product must be able to be configured for multiple department use and distributed/decentralized administration. There should be a single set of "Global Settings" and "Management Functions" that can be agreed upon by multiple departments choosing to use the same product.

4. Actions required at Enterprise Level – Microsoft AD Features. Installation functions that need to be performed "one time" by Enterprise/Domain administrators (without continuing activity required at the domain level).

5. Actions required at Enterprise Level – Non-Microsoft products. Installers that require powerful "Domain Administrator" or "Enterprise Administrator" rights to install a product will not be allowed. In addition, no functions of an installed product shall require the departmental IT admin or a service account to be a "Domain Administrator".

6. Authentication Protocols. Active Directory uses Kerberos 5 authentication for domain-member systems. Non-domain-member may authenticate against the domain controllers using NTLMv2. The older LANMAN and NTLMv1 authentication protocols are NOT supported for use on the domain controllers.

7. LDAP searching. Active Directory supports LDAP searches via an LDAPS (LDAP over SSL) protocol. Products should NOT use "simple LDAP binds" as this type of bind is extremely insecure and will be disabled in the future. Searches

should not be abusive (using repetitive searches of the entire LDAP tree on non-indexed values, for example).

8. Cross-Forest Implications. No functions shall require cross-forest trusts to be established (this is a critical security issue).

9. Imbedded Enterprise Services. Other Enterprise services (other than Windows Domain support) that are required to support this product must be outlined for evaluation. Examples are DNS, PKI (digital certificate services), etc.

10. Schedule and Resources (People, Hardware, Time). The desired implementation date and a list of "who provides what" must be submitted.

11. Vendor Reputation and Product Volatility. Products by reputable vendors certified by Microsoft are preferred. New/experimental/unstable products (which may require constant updating during their early versions) will not be viewed favorably for installation into the production forest/domain.

12. Ability to Test in a Laboratory Environment. The ability to test issues such as schema extensions in a stand-alone laboratory environment (provided by the Windows Enterprise administration) during analysis is needed. The department requesting support for the new service may be required to provide some systems specific to the service during the test (special servers, hardware, software, etc).

Select Products with Trial Evaluation Periods

A trial evaluation period for any software is strongly recommended. Because of the distributed management design and security needs of our Active Directory environment, every possible aspect cannot be addressed here. Before buying any product ask for an evaluation copy to verify if it can function in our Active Directory environment. Always check with the Enterprise Admins if you have any question about how a product integrates into our Windows Enterprise Active Directory domain.

How to Request Enterprise Administrative Action for a Product

Requests for action at the Enterprise level for Windows products should be made by sending the request with as much detail as possible to its-ad-admins@iastate.edu. The Windows Enterprise Admins will review the request and work with the department based on the standards listed above. You can expect questions about the product that relate to the security, stability, and manageability of the Windows Enterprise Domain. Any documentation you have available on product requirements, installation procedures, and operational needs will be necessary.

A request for an exemption to these standards may be made via a waiver process. The waiver process can be initiated via an email to the Enterprise Admins at its-ad-admins@iastate.edu. The waiver process will involve review by ITS Security Group,

Networks and Communications teams, and administration. An annual review of waivers will be performed to determine if the waiver is still necessary or should be revoked.