

Windows Enterprise OU Administrator Tips Using the Enterprise WSUS Server

April 25, 2012

General Information on Using the ITS WSUS Server at “sus.iastate.edu”

The ITS Enterprise WSUS server with the hostname of “sus.iastate.edu” is a "local mirror" of Microsoft's update services. It exists solely for "bandwidth conservation", keeping several thousand ISU systems from creating update traffic off-campus to Microsoft's servers.

This server automatically “approves for installation” all updates received from Microsoft daily. **There is no testing of the updates, nor is there any delay or filtering of updates other than the “client-side target group” support outlined below.** IT admins who want more granularity on what and when Microsoft updates are approved would be advised to look at managing their own WSUS server for their specific needs.

The Enterprise WSUS server checks for updates from Microsoft three times a day (starting at 8:05 AM). You cannot exactly predict when a synchronization begins or completes due do a random offset controlled by the WSUS server and the amount of updates available.

To Configure a Windows Client to Use the Enterprise WSUS Update Server

Using either “local security policy” or “OU Group Policy”, find the following settings:

Local Computer Policy
Computer Configuration
Administrative Templates
Windows Components
Windows Update

Use the following settings in the “Windows Update” area:

- "Configure Automatic Updates" should be “Enabled”.
- "Specify intranet Microsoft update service location" should be “Enabled” with “http://sus.iastate.edu” supplied for both server values.
- "Enable client-side targeting" should be enabled only if you want to choose a group other than the default (which receives all updates except “Drivers”). See below for a definition of the WSUS groups.
- Choose the other Automatic Updates configuration options as you prefer.
- Do NOT configure your clients to check for updates more than once or twice a day. Currently the Enterprise WSUS server synchronizes with Microsoft three times a day. It

is pointless (and an unnecessary load on the WSUS server) to check for updates multiple times a day.

Microsoft documentation on configuring a client (either joined to the Enterprise domain or not) is available here:

<http://technet.microsoft.com/en-us/library/cc708599%28v=ws.10%29.aspx>

A good overview of the entire WSUS process is available here:

<http://www.microsoft.com/technet/technetmag/issues/2005/11/HandsOn/default.aspx>

Who Can Use the Enterprise WSUS Server

You do not have to be a member of the Enterprise Windows Domain to use the Enterprise WSUS server – but you do have to be on an on-campus subnet. Local security policy settings can be used to point a non-member system to the Enterprise WSUS server (as per the above instructions) and it will receive updates. However, in order to provide the best service for the ISU community only certain “on campus” subnets are allowed to connect. These are:

129.186.0.0/16	(ISU Main Campus)
147.155.0.0/16	(Ames Lab)
192.188.159.0/24	(ISU res-halls)
192.188.160.0/22	(ISU res-halls)
64.113.64.0/19	(ISU res-halls)
65.110.224.0/19	(ISU res-halls)
10.0.0.0/8	(Non-routable internal)

Definition of Client-Side Targeting Groups

- “Unassigned Computers” (the default group if client-side targeting not used) -- Receives all updates EXCEPT "Drivers".
- "All" -- Receives all possible updates (including "Drivers")
- "SC" -- Receives only "Critical", "Security", "Service Packs", "Update Rollups", and "Definitions" updates. No “Drivers” or optional updates.