

Virginia Tech Active Directory Child Domain Usage Requirements Addendum

Acronyms

EA	= Enterprise Administrators
DC	= Domain Controller
MIG	= Microsoft Implementation Group
IMS	= Identity Management Services (formerly IRM)
AD	= Active Directory
ITSO	= IT Security Office
SETI	= Secure Enterprise Technology Initiatives
IAD	= Internet Application Development

Alternative terminology

While the term “child domain” accurately reflects the programmatic relationship between the Active Directory root and child domains (one to many), the phrase may be misconstrued as politically insensitive. To eliminate this unintended implication, future revisions of the VT AD Child Domain Usage Requirements document will replace the term “child domain” with “member domain”.

Additional benefit of participation

- Usage of the development and test AD forests. Member domains may utilize the development and test forests to test hotfixes, applications, security and interoperability functions, providing they have the necessary hardware and software to maintain a member domain within this environment. MIG maintains the root domain for this pilot environment and the ECCT-WAS group maintains a test Exchange environment within the forest.

Patch schedule

The Windows patching schedule is based upon Microsoft’s patching release schedule. Currently, Microsoft releases new patches cumulatively on the second Tuesday of each month. Once released publicly, the MIG group analyzes new Windows 2000/2003 hotfixes for applicability and criticality for Domain Controller operations. Once identified internally, notification of intent to test is sent to the w2k_admin listserv (typically the same day as the patches are released). At this point, member domains are encouraged to test the patches in their own pre-production environments to ensure correct function.

MIG receives and reviews inputs regarding patch stability/suitability from many sources, such as:

- Member domains

- Microsoft Premier Support Services
- Windows related public listservs (ex, NTBUGTRAQ, Secunia, WIN-HIED, etc)

Based on these inputs, MIG certifies a patch release and issues a statement via the w2k_admin listserv requiring all member domains within the forest to apply the patches. The statement includes a timeline for the patches to be properly installed. At the end of the allotted timeframe, all DCs are audited by the EA for compliance. Failure to comply results in the initiation of the resolution procedures as identified on page seven of the Usage Requirements document.

Enforced group policy

While the EA reserves the right to apply group policies to member domain controllers and member domain workstations, it should be noted this would only occur under *abnormal* circumstances. GPOs (Group Policy Objects) have never been forced at a forest or individual member domain level. The only theoretical reason to force GPOs is because of a security compromise or crisis situation. If it became necessary to enforce a GPO across domains within the forest, signoff is required from all available levels of MIG's management (see contact section). These GPOs would be removed as soon as feasible once steps to remediate the crisis have been implemented.

Remediation process

If a department or member domain admin has an issue, concern or problem with the operations, policy or interaction within the AD forest they should identify the appropriate primary contact (see contact section) and contact them as soon as possible. Policy or application exceptions can be considered on a case-by-case basis with full management involvement required by both parties. The department heads of both parties are required to sign off on any exceptions that may impact the security, stability or scalability of the AD forest.

Contacts and escalation pathway

[For hardware, software, policy and security questions]

(Primary)

MIG (Root Domain and Enterprise Administrators)

Marc DeBonis (marcd@vt.edu | 540-231-2728)

Steve Warrick (swarrick@vt.edu | 540-231-2634)

(Secondary)

SETI (Department Head)

Mary Dunker (dunker@vt.edu | 540-231-9327)

SETI (Administrative contact)

Sue Stewart (sustew@vt.edu | 540-231-7553)

[For OU and account management questions]

(Primary)

IMS

Rhonda Randall (randelr@vt.edu | 540-231-4245)

Doug Atwater (datwater@vt.edu | 540-231-1866)

(Secondary)

IMS

Karen Herrington (kmherrin@vt.edu | 540-231-3614)

(Tertiary)

ITSO (Chief Security Officer)

Wayne Donald (wdonald@vt.edu | 540-231-7694)