Configuring SID Filter Quarantining: Domain and Forest Trusts; Active Directory

By Archiveddocs

Archived: 2026-04-05 19:58:45 UTC

Applies To: Windows Server 2008, Windows Server 2008 R2

Security principals in Active Directory Domain Services (AD DS) have an attribute, called SID history, to which domain administrators can add users' old security identifiers (SIDs). This is useful during Active Directory migrations so that administrators do not have to modify access control lists (ACLs) on large numbers of resources and users can use their old SIDs to access resources. However, under some circumstances it is possible for attackers or rogue administrators that have compromised a domain controller in a trusted domain to use the SID history attribute (**sIDHistory**) to associate SIDs with new user accounts, granting themselves unauthorized rights. To help prevent this type of attack, SID filter quarantining is automatically enabled on all external trusts that are created from domain controllers running either Windows Server 2003 or later operating systems. External trusts that are created from domain controllers running Windows 2000 Server with Service Pack 3 (SP3) or earlier do not have SID filter quarantining enforced by default. These external trusts must be configured manually to enable SID filter quarantining.

Note

You cannot turn off the default behavior in Windows Server 2003 or Windows Server 2008 that enables SID filter quarantining for newly created external trusts. However, under certain conditions SID filter quarantining can be disabled on such an external trust. For information about conditions for disabling SID filter quarantining, see Disable SID filter Quarantining.

External trusts that are created from domain controllers running Windows 2000 Server with SP3 or earlier do not enforce SID filter quarantining by default. To further secure your forest, consider enabling SID filter quarantining on all existing external trusts that are created from domain controllers running Windows 2000 Server SP3 or earlier. You can do this by using Netdom.exe to enable SID filter quarantining on existing external trusts or by recreating these external trusts from a domain controller running Windows Server 2008, Windows Server 2003, or Windows 2000 Server with Service Pack 4 (SP4).

You can use SID filter quarantining to filter out migrated SIDs that are stored in SID history from specific domains. For example, where an external trust relationship exists so that the one domain, Contoso (running Windows 2000 Server domain controllers), trusts another domain, Cpandl (also running Windows 2000 Server domain controllers), an administrator of the Contoso domain can manually apply SID filter quarantining to the Cpandl domain, which allows all SIDs with a domain SID from the Cpandl domain to pass but all other SIDs (such as those from migrated SIDs that are stored in SID history) to be discarded.

Note

Do not apply SID filter quarantining to trusts within a forest that is not using either the Windows Server 2008 or Windows Server 2003 forest functional level, because doing so removes SIDs that are required for Active Directory replication. If the forest functional level is Windows Server 2008 or Windows Server 2003 and quarantining is applied between two domains within a forest, a user in the quarantined domain with universal group memberships in other domains in the forest might not be able to access resources in nonquarantined domains, because the group memberships from those domains are filtered when resources are accessed across the trust relationship. Likewise, SID filter quarantining should not be applied to forest trusts.

For more information about how SID filtering works, see Security Considerations for Trusts (https://go.microsoft.com/fwlink/?LinkID=111846).

Task requirements

You can use either of the following tools to perform the procedures for this task:

- Active Directory Domains and Trusts
- Netdom.exe

For more information about using the Netdom command-line tool to configure SID filtering settings, see Netdom Overview (https://go.microsoft.com/fwlink/?LinkId=111537).

To complete this task, you can perform the following procedures:

- Disable SID filter Quarantining
- Reapply SID Filter Quarantining
