Security principals in Active Directory have an attribute, called SID history, to which domain administrators can add users' old security identifiers (SIDs). This is useful during Active Directory migrations because administrators do not need 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, Windows Server 2003 automatically enables SID filter quarantining on all external trusts that are created by a Windows Server 2003 domain controller. External trusts that are created using domain controllers running Windows 2000 Server with Service Pack 3 (SP3) or earlier must be manually configured to enable SID filter quarantining.

Note

You cannot turn off the default behavior in Windows Server 2003 that enables SID filter quarantining for newly created external trusts. External trusts that are created from domain controllers running Windows 2000 Server with SP3 or earlier do not enforce SID filter quarantining by default.

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 such 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.

Disable SID filter quarantining

Updated: March 2, 2005

Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

Although it is not recommended, you can disable security identifier (SID) filter quarantining for an external trust by using the Netdom.exe tool. You should consider disabling SID filter quarantining only in the following situations:

- You have an equally high level of confidence in the administrators who have physical access to domain controllers in the trusted domain and the administrators with such access in the trusting domain.
- You have a strict requirement to assign universal groups to resources in the trusting domain, even when those groups were not created in the trusted domain.
- Users have been migrated to the trusted domain with their SID histories preserved, and you want to grant those users access to resources in the trusting domain based on the **SIDHistory** attribute.

For more information about how SID filtering works, see "Security Considerations for Trusts" in the Windows Server 2003 Technical Reference on the Microsoft Web site (http://go.microsoft.com/fwlink/?LinkId=35413).

You can disable SID filter quarantining by using the Netdom command-line tool. For more information about the Netdom command-line tool, see "Netdom.exe: Windows Domain Manager" in the Windows Server 2003 Technical Reference on the Microsoft Web site (http://go.microsoft.com/fwlink/?LinkId=41700).

Administrative credentials

To complete this procedure, you must be a member of the Domain Admins group or the Enterprise Admins group in Active Directory.

To disable SID filter quarantining

1. To disable SID filter quarantining for the trusting domain, open a Command Prompt.
2. Type the following command, and then press ENTER:

   Netdom trust *TrustingDomainName*
   /domain:*TrustedDomainName*
   /quarantine:No
   /userD:*domainadministratorAcct*
   /passwordD:*domainadminpwd*

Value	Description
TrustingDomainName	The Domain Name System (DNS) name (or network basic

	input/output system (NetBIOS) name) of the trusting domain in the trust that is being created.
TrustedDomainName	The DNS name (or NetBIOS name) of the domain that will be trusted in the trust that is being created.
domainadministratorAcct	The user account name with the appropriate administrator credentials to modify the trust.
domainadminpwd	The password of the user account in *domainadministratorAcct.*

Note

You can enable or disable SID filter quarantining only from the trusting side of the trust. If the trust is a two-way trust, you can also disable SID filter quarantining in the trusted domain by using the domain administrator's credentials for the trusted domain and reversing the *TrustingDomainName* and *TrustedDomainName* values in the command-line syntax

SID NOTES

- SID Filtering is also known as Quarantine, Domain Quarantine, or SID Filtering Quarantine.
- SID Filtering only applies to trusts, it cannot be enabled within a domain.
- SID Filtering, by default, is not active on automatically created trusts within a forest. You can enable it, but not if the forest functional level is below Windows Server 2003. Doing so on any trust within a forest breaks replication. Additionally, if the forest functional level *is* Windows Server 2003 or higher; users with universal group memberships from other domains in the forest may loose access to resources if you enable SID Filtering on any of your trusts.
- You can check the status of SID Filtering with the **netdom.exe** (Windows Domain Manager) command:
    - To verify the status of SID Filtering between two **domains**:
      netdom trust <TrustingDomainName> /domain: <TrustedDomainName> /quarantine
      Example output:
      SID filtering is not enabled for this trust. All SIDs presented in an authentication request from this domain will be honored.
      This is the default setting between domains in the same forest.
    - To verify the status of SID Filtering between two **forests**:
      netdom trust <TrustingDomainName> /domain: <TrustedDomainName> /enablesidhistory
      Example output:
      SID history is disabled for this trust.
      This is the default setting between trusting forests.
    - As you can see the two commands are nearly identical, but **/quarantine** applies only to domain trusts and **/enablesidhistory** is only valid for an outbound forest trust. They also output totally different messages making it hard to see that they actually apply to the same thing