Security Considerations for Trusts: Domain and Forest Trusts

Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2

In this section

The threat scenarios outlined in this section apply only to trusts made between two forests (also known as interforest trusts), including external and forest trusts. All other trusts made within a forest (also known as intraforest trusts), including parent-child, tree-root, and shortcut trusts, are optimally secured by default and do not require further planning to mitigate any known threat. As with intraforest trusts, there are no known threats to realm trusts that require mitigation.

You should be familiar with these threats before you deploy or configure a Windows Server 2003 network environment.

Potential Threats to Interforest Trusts

There are two potential threats to interforest trust relationships in Windows Server 2003. These threats can disrupt or undermine the integrity of interforest trusts.

- **Attack on trusting forest by malicious user in a trusted forest.** A malicious user with administrative credentials who is located in a trusted forest could monitor network authentication requests from the trusting forest to obtain the security ID (SID) information of a user who has full access to resources in the trusting forest, such as a Domain or Enterprise Administrator. SID filtering is set on all trusts by default to help prevent malicious users from succeeding with this form of attack. For more information about how SID filtering works, see “Security Settings for Interforest Trusts.”
- **Attack on shared resources in a trusting forest by malicious users in another organization’s forest.** Creating an external or forest trust between two forests essentially provides a pathway for authentications to travel from the trusted forest to the trusting forest. While this action by itself does not necessarily create a threat to either forest, because it allows all secured communications to occur over the pathway, it creates a larger surface of attack for any malicious user located in a trusted forest. Selective authentication can be set on interforest trusts to help minimize this attack surface area. For more information about how to mitigate this threat, see “Security Settings for Interforest Trusts.”

Security Settings for Interforest Trusts

There are two security settings in Windows Server 2003 that can be used to enhance the integrity of communications made over interforest trusts. SID filtering helps prevent malicious users with administrative credentials in a trusted forest from taking control of a trusting forest. Selective authentication lessens the attack surface by restricting the quantity of authentication requests that can pass through an interforest trust.

SID Filtering

SID filtering is set on all trusts to prevent malicious users who have domain or enterprise administrator level access in a trusted forest from granting (to themselves or other user accounts in their forest) elevated user rights to a trusting forest. It does this by preventing misuse of the attributes containing SIDs on security principals (including inetOrgPerson) in the trusted forest. One common example of an attribute that contains a SID is the SID history attribute (sIDHistory) on a user account object. The SID history attribute is typically used by domain administrators to seamlessly migrate the user and group accounts that are held by a security principal from one domain to another.

When security principals are created in a domain, the domain SID is included in the SID of the principal to identify the domain in which it was created. The domain SID is important because the Windows security subsystem uses it to verify the identity of the security principal, which in turn determines what resources in the domain the principal can access.

How SID History is used to migrate accounts

Domain administrators can simplify account migration by using the SID history attribute to migrate permissions, either automatically by using the Active Directory Migration Tool (ADMT) or manually by adding SIDs from an old user or group account to the SID history attribute of the new, migrated account. With either method, the new account retains the same level of permissions or access to resources as the old account. If domain administrators could not use the SID history attribute in this way, they would have to determine and reapply permissions on each network resource to which the old account had access. For more information about the SID history attribute, see “Trust Security and Other Windows Technologies.”

How SID History can be used to elevate privileges

Although SID history has legitimate and important uses, it can also pose a security threat when used to exploit an unprotected trust. A malicious user with administrative credentials who is located in a trusted forest could monitor network authentication requests from the trusting forest to obtain the SID information of a user, such as a domain or enterprise administrator, who has full access to resources in the trusting forest. After obtaining the SID of an administrator from the trusting forest, a malicious user with administrative credentials can add that SID to the SID history attribute of a security principal in the trusted forest and attempt to gain full access to the trusting forest and the resources within it.

This method of gaining access by granting unauthorized user rights to a user is known as an elevation of privilege attack. In an elevation of privilege attack, an attacker might apply the SID of a domain administrator located in a trusting forest to the SID history attribute of the attacker’s own account located in a trusted forest, get a ticket that would automatically include the new SID, and then use the ticket to access resources in the trusting forest. When the attacker requests the use of a resource, the access control mechanism considers all SIDs in the authorization data to determine if the principal has the rights to complete the requested action.

In an external trust scenario, a malicious user who has domain administrator credentials in the trusted domain is a threat to the entire trusting forest. In a forest trust scenario, a malicious user who has domain or enterprise administrator credentials in the forest root domain of the trusted forest is a threat to the entire trusting forest. Although the concept of elevating privileges by modifying SIDs is relatively easy to understand, it is quite difficult to implement. Attackers can use various technologies together with SID history to accomplish an elevation of privilege attack.

Application Programming Interfaces (APIs)

Windows includes APIs that facilitate account migration. These APIs are not exposed and can only be accessed on a system that has been patched to allow access to them. In this case, the APIs could be misused to add SIDs for a user from one domain to the SID history of a user in another domain. This is unlikely because these APIs require domain administrative credentials for both domains, including the domain being attacked. In order to overcome that security measure, malicious users would need to get the password of an account with domain administrative credentials before adding the SID. Attackers with access to such an account could more easily use it to accomplish their ultimate goal, rather than having to carry out an elevation of privilege attack to achieve the goal.

Disk Editors

A disk editor, such as the DiskProbe utility included in the Windows Server 2003 support tools, could also be used to mount an attack. A malicious user could boot into another operating system and use a disk editor to modify an offline Active

Directory database. With a disk editor, the user could modify the SID history attribute, modify replication attributes so the change would be replicated, and calculate a new directory checksum so as to prevent Active Directory from detecting that the directory was improperly modified. This attack is difficult not only because it requires physical access to a domain controller, but all of the tasks are technically complex.

Debuggers

Debuggers can also be used maliciously. A user could attach a debugger to a domain controller and use it to modify the copy of the directory loaded in memory. This method is also technically sophisticated. It requires the attacker to have unrestricted physical access, be a domain administrator, and be able to use system APIs to modify system-level code that is not publicly available.

How interforest trusts use SID Filtering

Even though a sophisticated attacker might be able to exploit the SID history attribute to gain unauthorized access to resources, SID filtering can provide an effective countermeasure. An outgoing external or forest trust created from a trusting domain can use SID filtering to verify that incoming authentication requests made by security principals in the trusted domain contain only SIDs of security principals in the trusted domain.

The trust compares the SIDs of the requesting security principal to the domain SID of the trusted domain. Any SIDs from domains other than the trusted domain are removed, or filtered. When this happens the request for authentication will fail and the resource will not be accessed.

A stricter form of SID filtering is SID filter quarantining. When a SID filter quarantine is applied to a trusted domain (using the trust relationship between the two domains), only SIDs from the trusted domain are allowed to traverse the trust relationship. This prevents inbound communications (across the trust relationship) from the trusted domain to claim an identity that belongs to any other domain.

SID filter quarantining was designed to be applied to external trust relationships. It should not be applied to forest trust relationships, trusts within a domain, or trusts within a forest that has a forest functional level of Windows 2000.

External trusts created from domain controllers running Windows 2000 Service Pack 3 (or earlier) do not enforce SID filter quarantining by default. To improve the security of Active Directory forests, domain controllers running Windows Server 2003 and Windows 2000 Service Pack 4 or later enable SID filter quarantining on all new outgoing interforest trusts by default.

Note

- The following restrictions and recommendations apply to using SID filtering to mitigate security threats to external and forest trusts:
- You cannot turn off the default behavior that enables SID filter quarantining for newly created external trusts.
- To further secure your forest, you should consider enabling SID filter quarantining on all existing external trusts that were created by domain controllers running Windows 2000 Service Pack 3 (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 2003 or Windows 2000 Service Pack 4 (or later). Domain controllers running Windows NT Server 4.0 do not take part in the trust creation process when existing domain controllers in the same domain are running Windows 2000 or Windows Server 2003.

How SID filtering impacts operations

SID filtering can affect your existing Active Directory infrastructure in the following two ways:

- Users who use SID history data for authorization to resources in the trusting domain no longer have access to those resources.

Because SID history that contains SIDs from any domain other than the trusted domain is removed from authentication requests made from the trusted domain, the user is denied access to resources that reference the old SID.

- Universal group access control strategy between forests will require changes.

  If you typically assign universal groups from a trusted forest to access control lists (ACLs) on shared resources in the trusting domain, SID filtering will have a significant impact on your access control strategy.

  Because universal groups must adhere to the same SID filtering guidelines as other security principal objects (that is, the universal group object SID must also contain the originating domain SID), you should verify that any universal groups that are assigned to shared resources in the trusting domain were created in the trusted domain.

  If the universal group in the trusted forest was not created in the trusted domain, even though it might contain users from the trusted domain as members, authentication requests made by members of that universal group will be filtered and discarded. Therefore, before assigning access to resources in the trusting domain for users in the trusted domain, you should confirm that the universal group containing the trusted domain users was created in the trusted domain.

  Note

  - The default SID filtering on forest trusts does not prevent migrations to domains within the same forest (intraforest migration) from using SID history, and it will not affect your intraforest universal group access control strategy. You should not apply SID filter quarantining on trusts between forests (that is, forest trusts or interforest trusts).

Disabling SID Filter Quarantining on External Trusts

Although it reduces the security of your forest (and is therefore not recommended), you can disable 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 them access to resources in the trusting domain based on the SID history attribute.

Only domain administrators or enterprise administrators can modify SID filtering settings. To disable SID filter quarantining for the trusting domain, type a command using the following syntax at a command-prompt:

Netdom
trust*TrustingDomainName***/domain:***TrustedDomainName*/quarantine:No/usero:***domainadministratorAcct*/passwordo:***domainadmin

To re-enable SID filtering, set the **/quarantine:** command-line option to **Yes**. For more information about Netdom, see "Domain and Forest Trust Tools and Settings."

Allowing SID History to Traverse Forest Trusts

If users are migrated from one domain to another in different forests, you may want to allow the migrated users to access resources in their original forest using their migrated (SID history) credentials. The default SID filtering applied to forest trusts prevents user resource access requests from traversing the trusts with the credentials of the original domain. If you want to enable users to use the credentials that were migrated from their original domain, you can allow SID history to traverse forest trusts by using the Netdom command.

Only domain administrators or enterprise administrators can modify SID filtering settings. To allow SID history credentials to traverse a trust relationship between two forests, type a command using the following syntax at a command-prompt:

Netdom
trust*TrustingDomainName***/domain:***TrustedDomainName*/enablesidhistory:Yes/usero:***domainadministratorAcct***/passwordo:***domainc*

To re-enable the default SID filtering setting across forest trusts, set the **/enablesidhistory:** command-line option to **No**. For more information about Netdom, see "Domain and Forest Trust Tools and Settings."

Note

- The same security considerations for removing SID filter quarantining from external trusts apply to allowing SID history to traverse forest trusts.

Selective Authentication

Selective authentication is a security setting that can be set on interforest trusts. It provides Active Directory administrators who manage a trusting forest more control over which groups of users in a trusted forest can access shared resources in a trusting forest. This increased control is especially important when administrators need to grant access to shared resources in their organization's forest to a limited set of users located in another organization's forest, because creating an external or forest trust provides a pathway for all authentication requests to travel between forests.

While this action by itself does not necessarily cause a threat to either forest, because all secured communications occur over the pathway, an external or forest trust exposes a larger surface to attack by any malicious user located in a trusted forest. Selective authentication helps to minimize this exposed area by enabling Active Directory administrators to grant a new authentication permission — to computer objects in the resource domain — for specific user accounts located in another organization's forest.

This new authentication permission is set on the security descriptor of the computer object located in Active Directory, not on the security descriptor physically located on the resource computer in the trusting forest. Controlling authentication in this way provides an extra layer of protection to shared resources by preventing them from being randomly accessed by any authenticated user working in a different organization, unless the user has been granted this permission explicitly by someone with write access to the computer object in Active Directory.

Note

- To enable selective authentication on forest trusts, the trusting forest in which shared resources are located must have the forest functional level set to Windows Server 2003. To enable selective authentication on external trusts, the trusting domain in which shared resources are located must have the domain functional level set to Windows 2000 native.

Authentication Settings for Interforest Trusts

When the forest functional level is set to Windows Server 2003, Active Directory Domains and Trusts recognizes three authentication settings that can be set on interforest trusts: Domain-wide Authentication, Forest-wide Authentication, and Selective Authentication. The following table describes these authentication settings in more detail.

Authentication Settings Used on Interforest Trusts

Authentication Setting	Interforest Trust Type	Description
Domain-wide Authentication	External	Permits unrestricted access by any users in the trusted domain to all available shared resources located in the trusting domain. This is the default authentication setting for external trusts.

Authentication Setting	Interforest Trust Type	Description
Forest-wide Authentication	Forest	Permits unrestricted access by any users in the trusted forest to all available shared resources located in any of the domains in the trusting forest. This is the default authentication setting for forest trusts.
Selective Authentication	External and Forest	Restricts access over an external or forest trust to only those users in a trusted domain or forest who have been explicitly given authentication permissions to computer objects (resource computers) residing in the trusting domain or forest. This authentication setting must be manually enabled.

Domain- and forest-wide authentication settings

Domain and forest-wide authentication provide an unrestricted pathway in which all authentication requests made by users in a trusted forest will be successfully authenticated by a domain controller in the trusting forest where the shared resource is located. The following illustration shows how the domain controller in the trusting forest authenticates and routes authentication requests made by users in the trusted forest.

Authentication Requests Are Authenticated and Routed


Authentication Request is Authenticated and Routed

When domain or forest-wide authentication is enabled, users who are authenticated over an interforest trust are automatically provided the Authenticated Users SID of the trusting forest in their authorization data. The Authenticated Users SID is used to grant many of the default rights for users in a forest.

Because the Authenticated Users group is a computed group, and its SID is added on the server to which the user authenticates, you cannot change the membership of the group. Because of this, after you set up a interforest trust, users from the other forest receive some default rights to all of the resources in the trusting forest that are accessible by the Authenticated Users group. Consequently, you might not want to use the domain-wide or forest-wide authentication setting if the trust is set up only to allow access to a small subset of users who are in the trusted forest.

Once an authentication request made to a resource in a trusting forest is validated by the trusted forest, it is routed to the targeted resource computer, which determines, based on its access control configuration, whether to authorize the specific request made by the user, service, or computer in the trusted forest. In this way, interforest trusts provide the mechanism by which validated authentication requests are passed to a trusting forest, while access control mechanisms on the resource computer determine the final level of access granted to the requestor in the trusted forest.

Once the authentication request reaches the resource computer, that computer must determine whether the user who initiated the authentication request is authorized to access the shared resource it is hosting. It does this by comparing the SIDs provided in the access token of the authentication request with the SIDs in the security descriptor that has been granted access to the shared resource.

Selective authentication setting

Unlike domain and forest-wide authentication, selective authentication provides a more restrictive pathway in which only authentication requests made from users in a trusted forest, who have been granted access to the Active Directory objects hosting the resources in a trusting forest, can be authenticated by the domain controller in the resource domain. The following illustration shows how the domain controller in the trusting forest can restrict the flow of authentication requests made by users in the trusted forest to shared resources in the trusting forest when those users have not been granted the appropriate permissions.

Authentication Requests Are Not Authenticated or Routed

How selective authentication affects domain controller behavior

When selective authentication is enabled, all authentication requests made over a trust to the trusting forest are tagged with an identifier that subjects the request to closer scrutiny by the domain controllers in the domain where the target resource is located. This is important because the mere presence of this identifier triggers the domain controller in the resource domain to first check whether the user requesting the access has been given explicit permissions to the Active Directory object where the resource is hosted. The appropriate permission to the resource object in Active Directory is verified before the domain controller sends a service ticket back to the requesting workstation in the trusted forest. The following illustration summarizes how domain controllers in the trusting forest are affected when selective authentication is enabled.

Effect of Selective Authentication on Domain Controllers in the Trusting Forest

The steps by which domain controllers process authentication requests when selective authentication is enabled are as follows:

1. **All domain controllers in the domain where the trust is established detect authentication requests made from the other organization.**

   When selective authentication is enabled all domain controllers in the forest root domain of a trusting forest (with a forest trust) or all domain controllers in a resource domain in the trusting forest (with an external trust) are aware that all authentication requests coming in over that trust are coming from a different organization. This means that when a user from a different organization authenticates across a trust with the selective authentication option enabled, the domain controller that receives the request in the trusting domain recognizes this user as other than an authenticated user located in the trusting forest.

2. **Receiving DC in the domain where trust is established tags an identifier to the authorization data of the trusted user.**

   Once a domain controller receives the request it adds an identifier to the authorization data of the trusted user. This identifier is known as the Other Organization SID. The Other Organization SID is used to identify users making requests across a trust with selective authentication enabled.

3. **All domain controllers in the resource domain detect requests originating from the other organization, and the receiving domain controller in the resource domain performs an access check.**

   When a domain controller in a resource domain detects an Other Organization SID in the authorization for the trusted user, the domain controller is alerted to first check whether the requesting user has been granted explicit permissions to the Active Directory object where the resource is hosted. The appropriate permission to the resource object in Active Directory must be verified before the domain controller can authenticate the access request and send a service ticket back to the requesting workstation in the trusted forest.

   This verification process works by checking the access permissions set on the Allowed to Authenticate permission on the discretionary access control list (DACL) on the computer object in Active Directory. When you set selective authentication on an outgoing interforest trust, you need to manually assign access to the Allowed to Authenticate permission on each computer object, which physically represents a member server to which you want users in the trusted forest to authenticate.

   You must grant access to this permission in order for users located in a trusted forest to authenticate to the shared resources hosted by the server computer. If this permission has not been granted to a user whose authorization data contains the Other Organization SID, the service ticket to the server hosting the shared resource is not granted and the authentication process fails.

   Note

- The following restrictions apply to the Allowed to Authenticate authorization permission:
- By default, only members of the Account Operators, Administrators, Domain Administrators, Enterprise Administrators, and SYSTEM security groups located in the trusting domain can modify the Allowed to Authenticate authorization permission.
- When Kerberos is used for authentication, the Allowed to Authenticate permission should be enabled on computer accounts when the service that hosts the resource is running as Local System or Network Service. If the service that hosts the resource is running as a Domain Service account, the permission should be configured on that account. For example, if the SQL service is running under the account SQLServer, the SQL Server account has to have the Allowed to Authenticate permission enabled for users to be able to authenticate to that account across trusts that have selective authentication enabled.
- When NTLM is used for authentication, the Allowed to Authenticate permission should be granted to the computer account, even if the service that you want to connect to is using a domain user account.

When a Windows NT 4.0, Windows 2000 Server, or Windows Server 2003 member server receives an authentication request from a user, regardless of whether that user is identified with the Other Organization SID, the member server automatically adds the Authenticated Users SID for the trusting forest to the authorization data for that user.

How selective authentication affects Windows Server 2003 member server authentication

When users who are located in a domain within the trusting forest (or in a trusted domain that does not have selective authentication enabled) authenticate to local Windows Server 2003 member servers, the Authenticated Users SID and a new identifier indicating that they belong to the same organization are placed in their authorization data. This new identifier is known as the This Organization SID. Only the Other Organization SID or the This Organization SID can be present in the authorization data of an authenticated user along with the Authenticated Users SID. The following table describes the SIDs that can be added to the authorization data of a user throughout the entire selective authentication process and shows when they are added.

SIDs Added to Authorization Data During the Selective Authentication Process

SID	Purpose	When Added to User Authorization Data
Authenticated Users	Adds default access rights to resources in the trusting forest. Because this SID is mandatory for all incoming authentication requests, it prevents all anonymous access to resources in the trusting forest.	Added when any incoming authentication request to a member server is made from a user who has been identified with the Other Organization SID. This SID is always applied by the member server to the authorization data of an incoming user, in addition to one of the other SIDs in this table.
This Organization	Identifies users who access resources locally within a trusting forest or across a trust that is not marked for selective authentication.	Added when users who are located in any of the domains within a trusting forest authenticate to a local Windows Server 2003 member server. This SID and the Authenticated Users SID are added by the member server. The Other Organization SID cannot be added to this authorization data of this user.
Other Organization	Identifies users coming across a trust that is marked for selective authentication.	Added when any incoming authentication request is made from a user located in a trusted forest to a domain controller in the domain in the trusting forest where the trust is established. This SID is added by the domain controller that initially receives the authentication request. The

SID	Purpose	When Added to User Authorization Data
		Authenticated Users SID is not added to the authorization data of the user until the member server has authenticated the user.

Note

- The Allowed to Authenticate permission can be set on computer objects that represent member servers running Windows NT Server 4.0, Windows 2000 Server, and Windows Server 2003. However, only member servers running Windows Server 2003 can provide the This Organization SID to the authorization data of a user.

Processing authentication requests made over forest trusts with selective authentication enabled

Before an authentication request made with the Kerberos version 5 authentication protocol can follow the forest trust path, the service principal name (SPN) of the resource computer must be resolved to a location in the other forest. A SPN is a multicomponent name that is used to identify a service that is associated with a computer account. When a workstation in one forest attempts to access data on a resource computer in another forest, the Kerberos authentication process contacts the domain controller for a service ticket to the SPN of the resource computer. Once the domain controller queries the global catalog and determines that the SPN is not in the same forest as the domain controller, the domain controller sends a referral back to the workstation for its parent domain. The workstation queries its parent domain for the service ticket and continues to follow the referral chain until it reaches the domain where the resource is located.

Once the workstation reaches a domain controller in the root domain of the resource forest where selective authentication is enabled, the domain controller adds the Other Organization SID to the authorization data for the user. After the Other Organization SID is added, the domain controller in the resource domain checks the Allowed to Authenticate permission on the computer object (located in Active Directory) that is hosting the resource. If the user has been granted access the domain controller issues a service ticket back to the workstation. This is an important part of the selective authentication process, because if the user does not have permission to authenticate to the computer object, a service ticket will not be granted and access to the target resource computer fails. In this way, the selective authentication setting restricts what authentication requests can pass through a trust and obtain a ticket for a target resource computer.

The following figure and corresponding steps provide a detailed description of the Kerberos authentication process that is used when computers running Windows 2000 Professional, Windows XP Professional, Windows 2000 Server, or Windows Server 2003 attempt to access resources from a computer located in another forest when selective authentication is enabled.

Kerberos authentication process over a forest trust with selective authentication enabled

 Kerberos authentication over a forest trust

This illustration incorporates images from Active Directory Users and Computers in the Microsoft Management Console to help you better understand at what point during the authentication process a domain controller queries the Allowed to Authenticate permission for the resource object.

1. Acctuser1 logs on to Workstation1 using credentials from the Sales.tailspintoys.com domain. The user then attempts to access a shared resource on FileServer1 located in the WingtipToys forest. Acctuser1 is also a member of the Accounting global group in the Sales.tailspintoys.com domain.

2. Workstation1 contacts the Key Distribution Center (KDC) on a domain controller in its domain (TailspinDC1) and requests a service ticket for the FileServer1 SPN. FileServer1 is located in the Mktg.wingtiptoys.com domain and is a member server.

3. TailspinDC1 does not find the SPN in its domain database and queries the global catalog to see if any domains in the TailspinToys forest contain this SPN. Because a global catalog is limited to its own forest, the SPN is not found. The global catalog then checks its database for information about any forest trusts that are established with its forest, and, if any are found, it compares the name suffixes listed in the forest trust trusted domain object (TDO) to the suffix of

the target SPN to find a match. Once a match is found, the global catalog provides a routing hint back to TailspinDC1.

4. Using the information in the routing hint, TailspinDC1 sends a referral for a domain controller located in the forest root domain of the WingtipToys forest back to Workstation1.

5. Workstation1 contacts a domain controller in the forest root domain (WingtipDC1) of the Corp.wingtiptoys.com forest and requests a service ticket to the Fileserver1 resource computer.

6. WingtipDC1 contacts its global catalog to find the SPN, and the global catalog finds a match for the SPN and sends it back to WingtipDC1.

7. Because the authentication request originated from the TailspinToys forest and selective authentication is enabled WingtipDC1 applies the Other Organization SID to the user's authorization data and then sends a referral for the mktg.wingtiptoys.com domain back to Workstation1.

8. Workstation1 contacts the KDC on WingtipDC2 and attempts to negotiate a ticket for Acctuser1 to gain access to FileServer1.

9. WingtipDC2 detects the Other Organization SID in the authorization data of Acctuser1, which requires the domain controller to first locate the computer object of the resource computer (Fileserver1) before providing a ticket back to the requesting computer.

10. Once the computer object is located, the domain controller must check whether the user requesting access to the resource computer has been explicitly granted the **Allowed to Authenticate** permission on the Fileserver1 computer object located in the Mktg.wingtiptoys.com domain. This process must complete successfully before WingtipDC1 can provide a ticket back to the requesting computer.

    Note

    - In this example, Acctuser1 is a member of the Accounting group in the TailspinToys forest and that group has been explicitly granted the **Allowed to Authenticate** permission to this computer object residing in Active Directory.

11. After WingtipDC1 determines that Acctuser1 has the required permission to Filerserver1, it sends a service ticket back to Workstation1 permitting it to gain access to FileServer1.

12. Now that Workstation1 has a service ticket, it sends the server service ticket to FileServer1, which reads the security credentials for Acctuser1 and constructs an access token accordingly.

Impact of Selective Authentication

Because all verification of incoming interforest authentication requests is done locally on the receiving domain controller in the trusting forest, access to resources in the trusting forest is likely to be extremely limited for a broad set of users on the network (which is the purpose of this security setting). Consequently, implementing selective authentication might require user education, particularly due to the following reasons:

- Users browsing network resources through My Network Places to resources located in a trusting forest might get access denied messages when attempting to access those resources.

- Resources in the trusting forest that were once available to users in a trusted forest might no longer be available.

Note

- As a security best practice it is recommended that resource administrators in a trusting forest remove the default access rights granted to the Authenticated Users group in all of the shared resources in the trusting forest. This practice will help to further minimize the possibility of authenticated users inside and outside of a forest from accessing protected resources.

Enabling and Disabling Selective Authentication

Selective authentication must be manually enabled or disabled by using Active Directory Domains and Trusts or the Netdom.exe tool. To enable selective authentication for the trusting domain, type a command using the following syntax at a command-prompt:

Netdom
trust*TrustingDomainName***/domain:***TrustedDomainName*/SelectiveAuth:Yes/usero:***domainadministratorAcct***/passwordo:*****domainad

To disable selective authentication, set the **/SelectiveAuth:** command-line option to **No**. For more information about the Netdom tool, see "Domain and Forest Trust Tools and Settings."

You can enable or disable selective authentication only from the trusting side of a trust. If the trust is a two-way trust, you can also enable or disable selective authentication in the trusted domain by using the credentials of the domain administrator for the trusted domain and reversing the values of TrustingDomainName and TrustedDomainName in the command.

Note

- You can further increase security in a forest by enabling selective authentication on all external and forest trusts used to connect forests that are not managed by the IT department in your organization.

Minimum Administrative Credentials for Securing Trusts

The following table lists the minimum administrative credentials necessary to enable or disable the SID filtering and selective authentication security settings in Active Directory.

Minimum Administrative Credentials Necessary To Secure Trusts

SID Filter Quarantining - External Trusts	Allowing SID History - Forest Trusts	Selective Authentication - External Trusts	Selective Authentication - Forest Trusts
You must be a member of the Domain Admins group in the trusting domain or the Enterprise Admins group in the trusting forest.	You must be a member of the Domain Admins group in the forest root domain or the Enterprise Admins group in the trusting forest	You must be a member of the Domain Admins group in the trusting domain or the Enterprise Admins group in the trusting forest.	You must be a member of the Domain Admins group in the forest root domain or the Enterprise Admins group in the trusting forest

Trust Security and Other Windows Technologies

Trust security can be affected or enhanced by other technologies built into the Windows operating system. These include SID history and the Lightweight Directory Access Protocol (LDAP).

SID History

SID History is used to store the former SIDs of moved objects such as users and security groups. Prior to Windows 2000, restructuring a domain generally meant the creation of new accounts that needed to be placed in the same groups the old accounts were placed in. Since Windows 2000, domain restructuring is considerably easier because of SIDHistory, which is an attribute of Active Directory security principals.

As part of the move operation for the user or group, Application Programming Interfaces (APIs), or tools and support utilities built from these APIs, update the SIDHistory attribute of the object, representing it in Active Directory with its former SID. When the user next logs on to the system, not only the new SID, but also the old SID retrieved from the SIDHistory attribute is added to the user's access token and serves to determine the user's group memberships. The SIDs of

the groups of which the user is a member (through either the new SID or the old SID) are also added to the access token, together with any SIDHistory those groups might have.

Groups have a SIDHistory attribute because they also can be moved. The system retrieves the SIDHistory attributes of all the groups of which the user is a member and adds these attributes to the user's access token. Because these SIDHistory entries in the token look to the operating system like normal group memberships during authorization checks, the token can grant appropriate access even on earlier versions of the operating system.

Because old SIDs can be stored in SIDHistory, the user can continue to access resources after a move without requiring administrators to modify ACLs. Once a migration is complete, if all needed resources are in the new domain, use of SIDHistory can be phased out if desired.

Note

- The SIDHistory attribute can be updated only in native mode Windows 2000 or Windows Server 2003 domains, which requires all migration operations relying on SIDHistory to have a native mode target.

For more information about the security threat that exploits SID history, see "Security Settings for Interforest Trusts."

LDAP Sign and Encrypt

When using Windows Server 2003, secure LDAP traffic is enabled so that Active Directory administrative tools sign and encrypt all LDAP traffic by default. In this way, secured LDAP traffic enhances the security of communications that can occur between trusts.

Active Directory Domains and Trusts signs and encrypts all LDAP traffic by default. Signing LDAP traffic guarantees that the packaged data comes from a known source and that it has not been tampered with. Active Directory administrative tools in Windows 2000 do not sign and encrypt all LDAP traffic by default. In order to maintain a secure network, it is strongly recommended that you upgrade all domain controllers running Windows 2000 to Service Pack 3 or later.

You can use the corresponding Active Directory administrative tools in Windows 2000 to manage Windows 2000 domain controllers that do not have the Windows 2000 Server Service Pack 3 or later installed. However, traffic is not signed and encrypted by LDAP on domain controllers running Windows 2000.

The following resources contain additional information that is relevant to this section.

- Domains and Forests Technical Reference
- Kerberos Authentication Technical Reference
- Security Identifiers Technical Reference
- Security Principals Technical Reference
