**Advanced AD DS Trust Settings**

**SID Filtering**

By default, when you establish a forest or domain trust, you enable a domain quarantine, which is also known as SID filtering. When a user authenticates in a trusted domain, the user presents authorization data that includes the SIDs of all of the groups to which the user belongs. Additionally, the user's authorization data includes SIDs from other attributes of the user and the user's groups.

AD DS sets SID filtering by default to prevent users who have access at the domain or enterprise administrator level in a trusted forest or domain, from granting (to themselves or to other user accounts in their forest or domain) elevated user rights to a trusting forest or domain. SID filtering prevents misuse of the attributes that contain SIDs on security principals in the trusted forest or domain.

One common example of an attribute that contains a SID is the SID-History attribute (SIDHistory) on a user account object. Domain administrators typically use the SID-History attribute to migrate the user and group accounts that are held by a security principal from one domain to another.

In a trusted domain scenario, it is possible that an administrator could use administrative credentials in the trusted domain to load SIDs that are the same as SIDs of privileged accounts in your domain into the SIDHistory attribute of a user. That user would then have inappropriate levels of access to resources in your domain. SID filtering prevents this by enabling the trusting domain to filter out SIDs from the trusted domain that are not the primary SIDs of security principals. Each SID includes the SID of the originating domain, so when a user from a trusted domain presents the list of the user's SIDs and the SIDs of the user's groups, SID filtering instructs the trusting domain to discard all SIDs without the domain SID of the trusted domain. SID filtering is enabled by default for all outgoing trusts to external domains and forests.

**Selective Authentication**

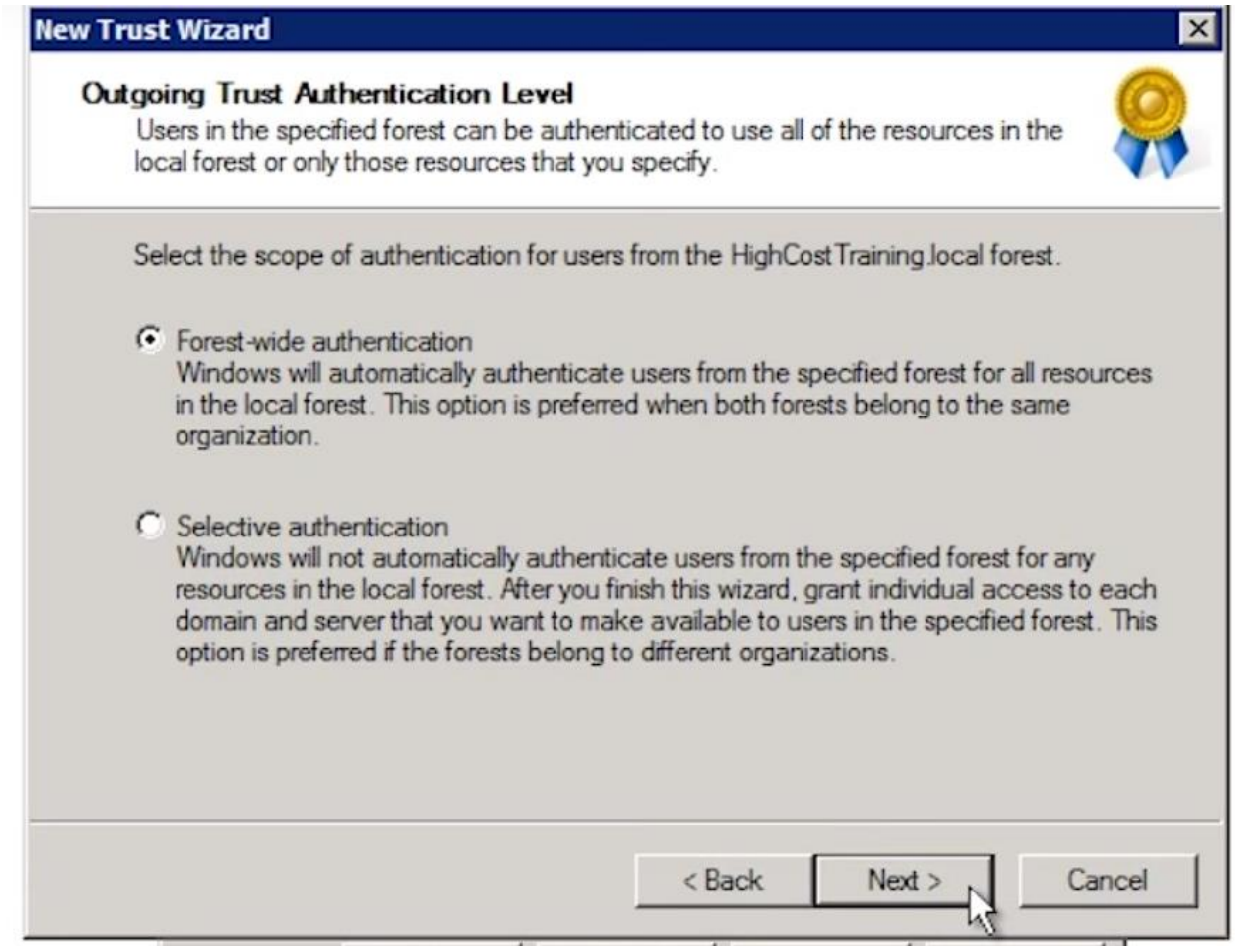
When you create an external trust or a forest trust, you can manage the scope of authentication of trusted security principals. There are two modes of authentication for an external or forest trust:

- Domain-wide authentication (for an external trust) or forest-wide authentication (for a forest trust)
- Selective authentication

If you choose domain-wide or forest-wide authentication, this enables all trusted users to authenticate for services and access on all computers in the trusting domain. Therefore, trusted users can be given permission to access resources anywhere in the trusting domain. If you use this authentication mode, all users from a trusted domain or forest are considered Authenticated Users in the trusting domain. Thus if

you choose domain-wide or forest-wide authentication, any resource that has permissions granted to Authenticated Users is accessible immediately to trusted domain users.

If, however, you choose selective authentication, all users in the trusted domain are trusted identities. However, they are allowed to authenticate only for services on computers that you specify. For example, imagine that you have an external trust with a partner organization's domain. You want to ensure that only users from the partner organization's marketing group can access shared folders on only one of your many file servers. You can configure selective authentication for the trust relationship, and then give the trusted users the right to authenticate only for that one file server.




**Name Suffix Routing**

Name suffix routing is a mechanism for managing how authentication requests are routed across forests running Windows Server 2003 or newer forests that are joined by forest trusts. To simplify the administration of authentication requests, when you create a forest trust, AD DS routes all unique name suffixes by default. A *unique name suffix* is a name suffix within a forest—such as a UPN suffix, SPN suffix,

or DNS forest or domain tree name—that is not subordinate to any other name suffix. For example, the DNS forest name fabrikam.com is a unique name suffix within the fabrikam.com forest.

AD DS routes all names that are subordinate to unique name suffixes implicitly. For example, if your forest uses fabrikam.com as a unique name suffix, authentication requests for all child domains of fabrikam.com (childdomain.fabrikam.com) are routed, because the child domains are part of the fabrikam.com name suffix. Child names appear in the Active Directory Domains and Trusts snap-in. If you want to exclude members of a child domain from authenticating in the specified forest, you can disable name suffix routing for that name. You also can disable routing for the forest name itself

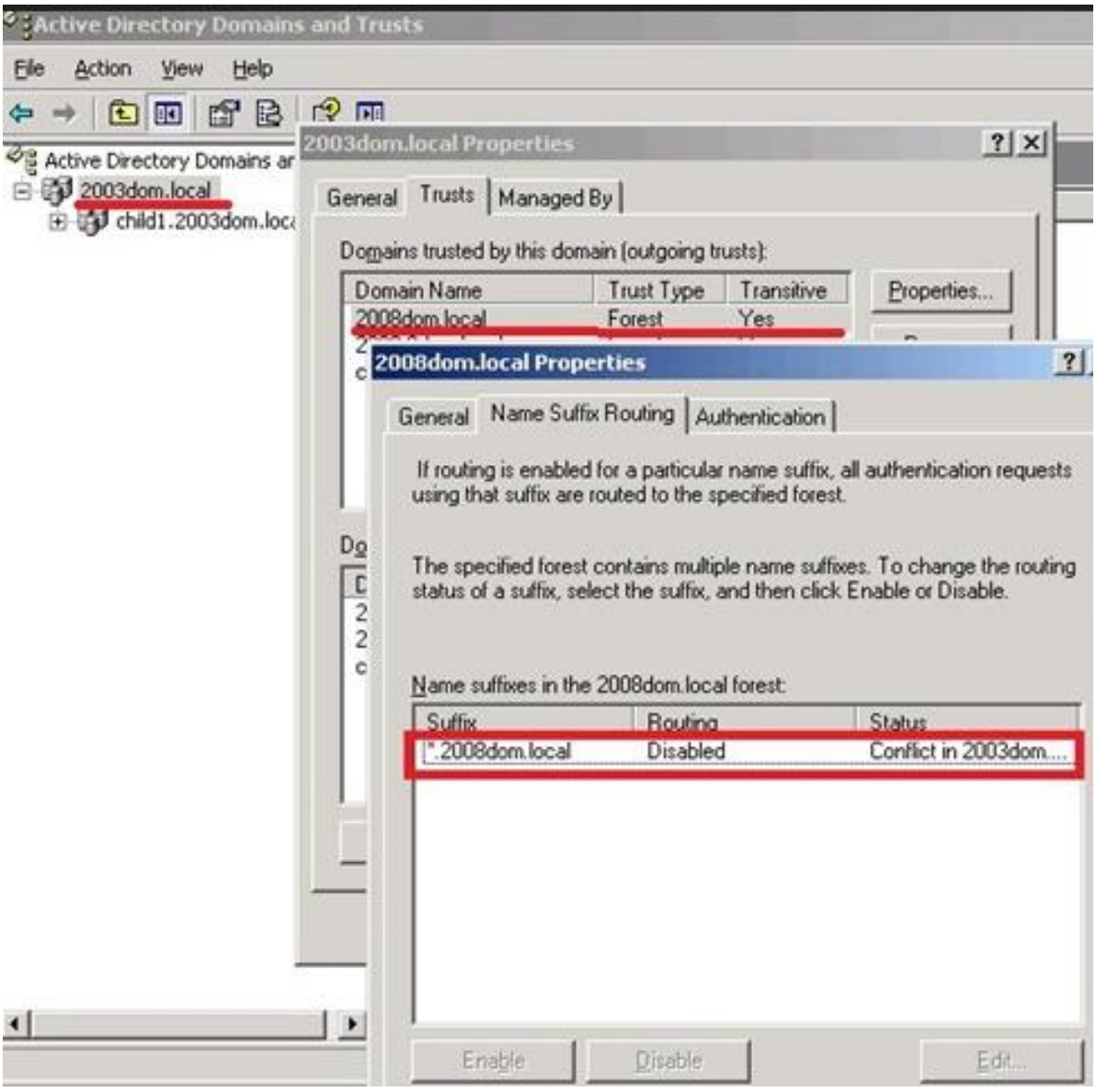
https://www.youtube.com/watch?v=MB4iiqEyr5A

**Trust Properties - Name Suffix Routing Tab**

Updated: March 1, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012

| Item | Details |
| --- | --- |
| **Name suffixes in the <DNS name> forest:** | • **Suffix** : A list of name suffixes in the local forest.<br>• **Routing** : Specifies the routing status of the corresponding name suffix.<br>• **Status** : Specifies the status (conflicts, whether the name suffix is newly created, and so on) of the corresponding name suffix. |
| **Enable** | Click to set the routing status of the selected name suffix to Enabled. |
| **Disable** | Click to set the routing status of the selected name suffix to Disabled. |
| **Refresh** | Click to refresh the list of name suffixes in the local forest. |
| **Edit** | Click to exclude name suffixes from routing to the local forest. |


Active Directory Domains and Trusts
File Action View Help
Active Directory Domains ar
2003dom.local
child1.2003dom.loc
2003dom.local Properties
General Trusts Managed By
Domains trusted by this domain (outgoing trusts):
Domain Name Trust Type Transitive
2008dom.local Forest Yes
Properties...
2008dom.local Properties
General Name Suffix Routing Authentication
If routing is enabled for a particular name suffix, all authentication requests using that suffix are routed to the specified forest.
The specified forest contains multiple name suffixes. To change the routing status of a suffix, select the suffix, and then click Enable or Disable.
Name suffixes in the 2008dom.local forest:
Suffix Routing Status
*.2008dom.local Disabled Conflict in 2003dom....
Enable Disable Edit...

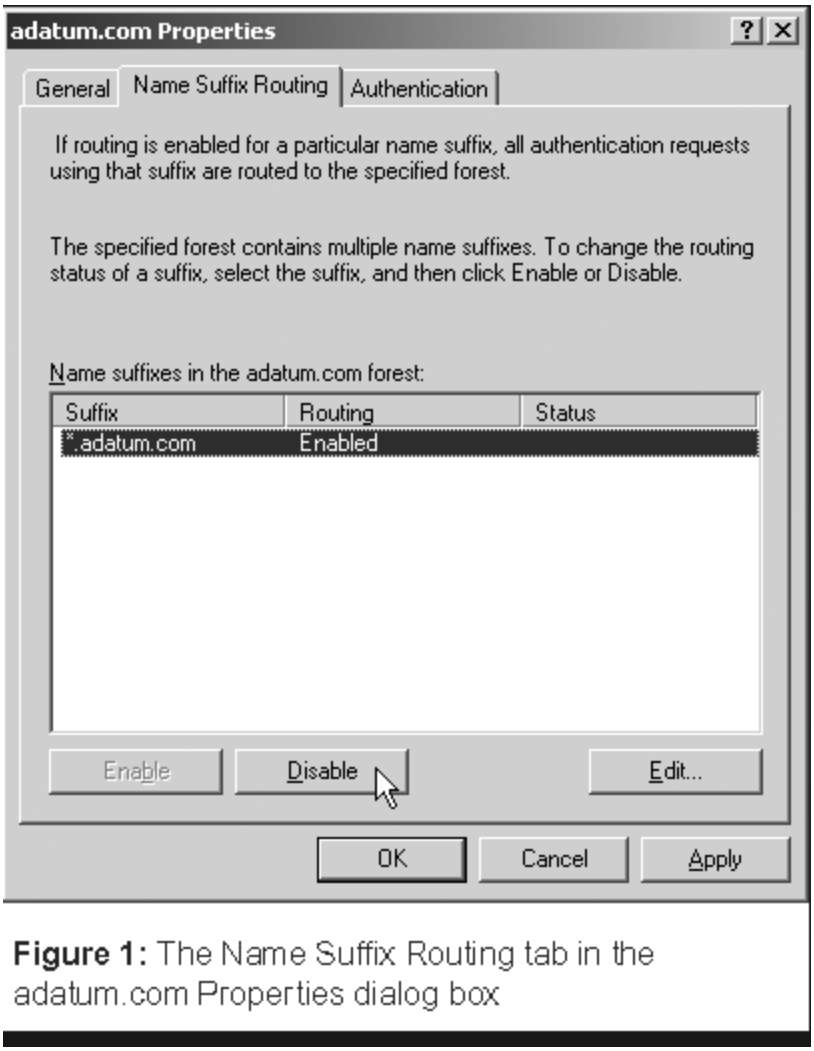
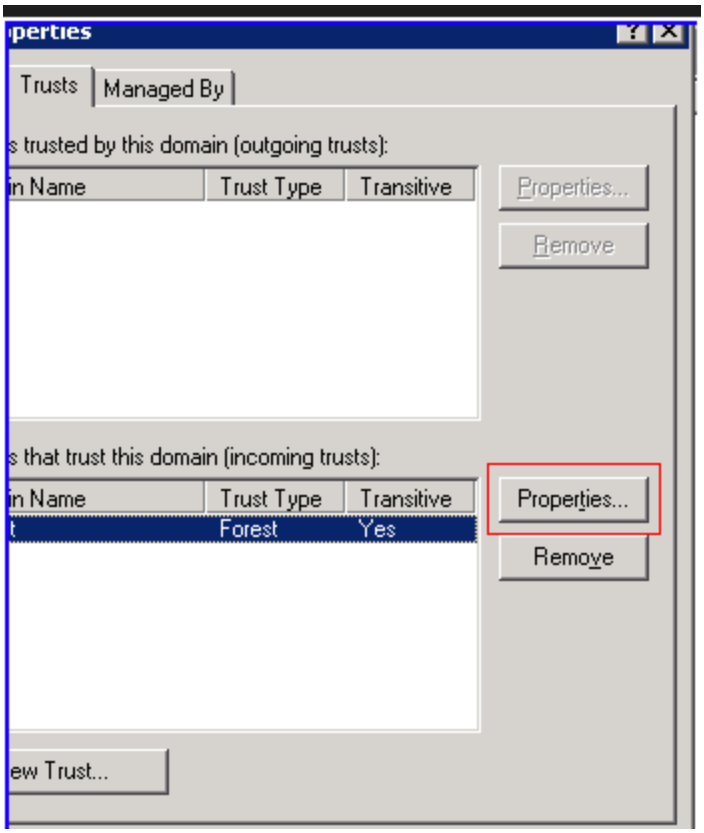
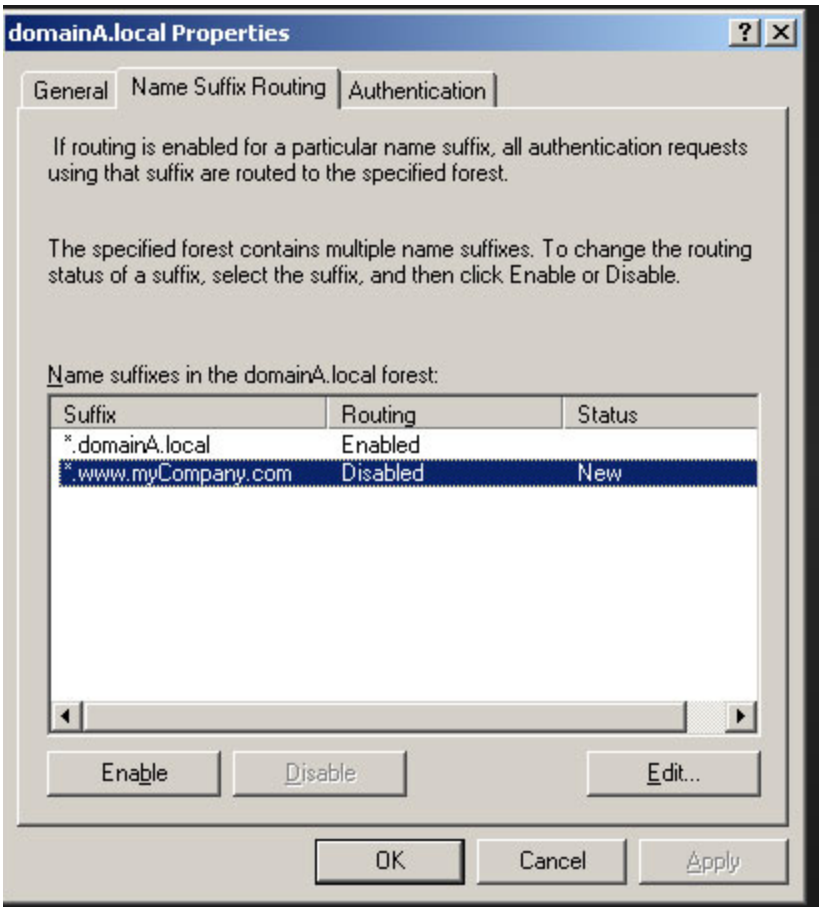
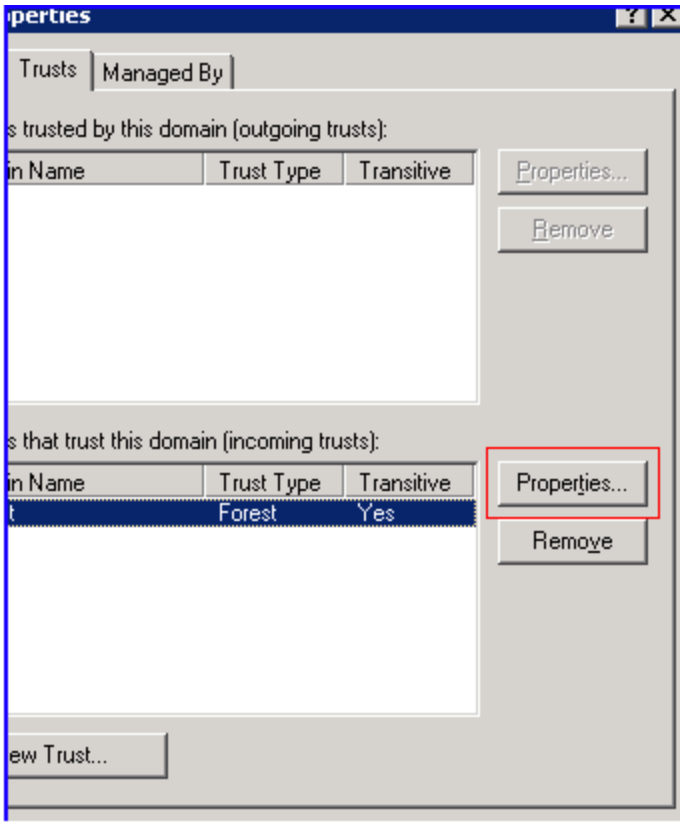



**Figure 1:** The Name Suffix Routing tab in the adatum.com Properties dialog box


perties
Trusts
Managed By
s trusted by this domain (outgoing trusts):
in Name
Trust Type
Transitive
Properties...
Remove
s that trust this domain (incoming trusts):
in Name
Trust Type
Transitive
Forest
Yes
Properties...
Remove
ew Trust...


domainA.local Properties
General
Name Suffix Routing
Authentication
If routing is enabled for a particular name suffix, all authentication requests using that suffix are routed to the specified forest.
The specified forest contains multiple name suffixes. To change the routing status of a suffix, select the suffix, and then click Enable or Disable.
Name suffixes in the domainA.local forest:
Suffix
Routing
Status
*.domainA.local
Enabled
*.www.myCompany.com
Disabled
New
Enable
Disable
Edit...
OK
Cancel
Apply


perties
Trusts
Managed By
s trusted by this domain (outgoing trusts):
in Name
Trust Type
Transitive
Properties...
Remove
s that trust this domain (incoming trusts):
in Name
Trust Type
Transitive
Forest
Yes
Properties...
Remove
ew Trust...

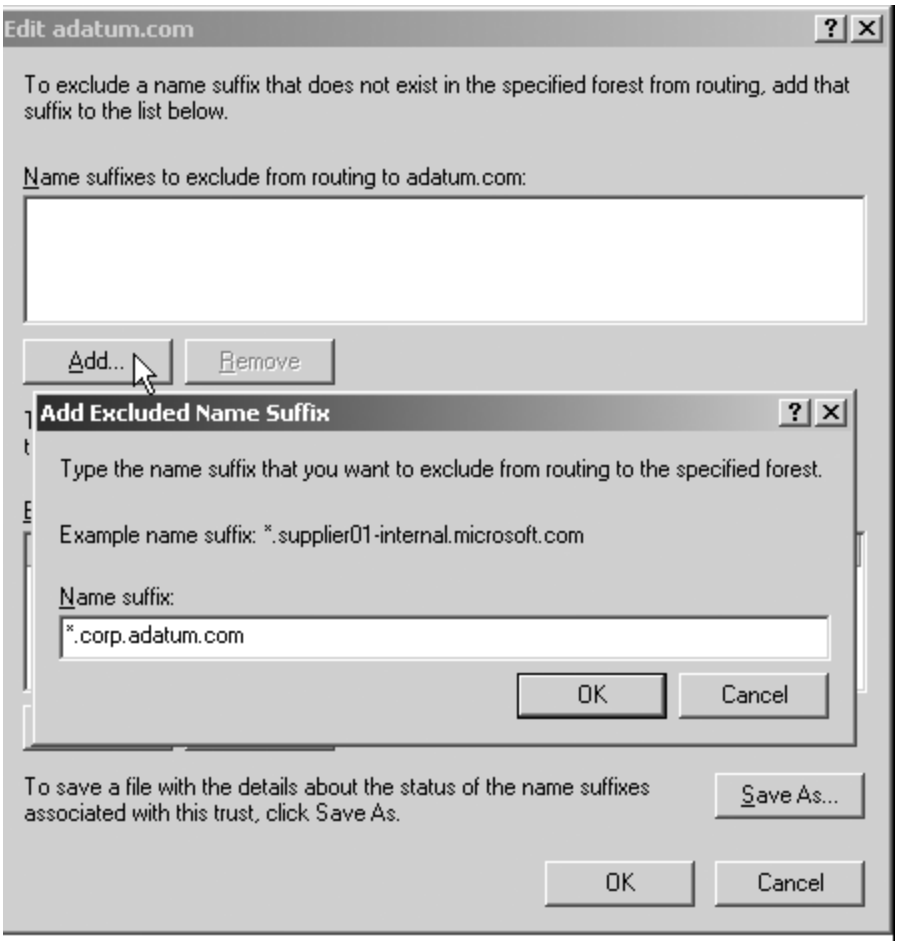



**Figure 2:** Adding a specific name-suffix exclusion to a forest