

How to configure Forest Level Trust in Windows Server

Posted on May 6, 2013 by [Rick Trader](#)
[inShare2](#)

Scenario – Two organizations, USSHQ (USSHQ.Local) and Dulce Base (DulceBase.Local) need to be able to share resources. A forest trust relationship between the two organizations Active Directory Domain Services is desired. Before the trust can be created name resolution needs to be configured and tested for connectivity between the two domains. Once the trust relationship is configured, resource administrators will be able to configure permissions, privileges and rights to the trusted forest users.

Requirements

- Both Forests need to be in Forest Functional Level 2003 or higher
- Name resolution must be in place. Check out the blogs below for more information on how to create.

Conditional Forwarder – [How to configure a Conditional Forwarder in DNS](#)

Stub Zone – [How to configure a DNS Stub Zone in Windows Server](#)

Secondary Zone – [How to configure a DNS Secondary Zone in Windows Server](#)

- Must be a member of the Enterprise Admins Group or the Domain Admins Group in the forest root or delegated the rights to create trusts.

Terms

- Trusted Domain or Forest – is the domain or forest where the users are authenticated.
- Trusting Domain or Forest – is the domain or forest where the resources reside.

Note: Trust**TED** / Trust**ING** – *Ted* has the user, *Ing* has the things.

- Transitive – User are able to traverse through the Parent – Child trust relationship to access resources in the trusting domain.
- Non-transitive – User are not to traverse through the Parent – Child trust relationship to access resources in the trusting domain.

Verifying Name Resolution

If a computer from Dulce Base attempts to contact a computer in USSHQ it should be able to resolve the name to an IP Address.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping usshqsvr1.usshq.local

Pinging usshqsvr1.usshq.local [172.16.10.10] with 32 bytes of data:
Reply from 172.16.10.10: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

If a computer from USSHQ attempts to contact a computer in Dulce Base it should be able to resolve the name to an IP Address.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping dbasesrv1.dulcebase.local

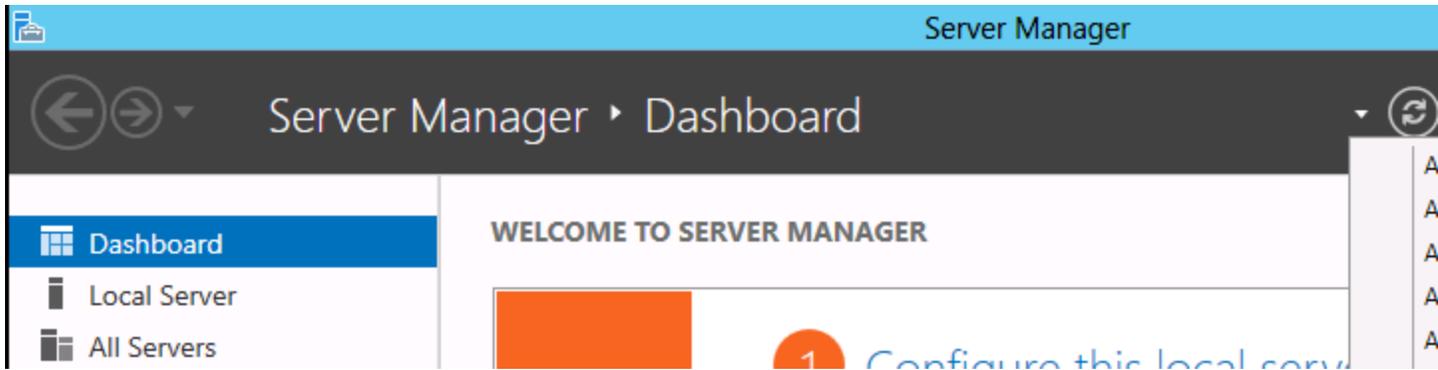
Pinging dbasesrv1.dulcebase.local [172.16.11.20] with 32 bytes of data:
Reply from 172.16.11.20: bytes=32 time=1ms TTL=127
Reply from 172.16.11.20: bytes=32 time<1ms TTL=127
Reply from 172.16.11.20: bytes=32 time<1ms TTL=127
Reply from 172.16.11.20: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.11.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

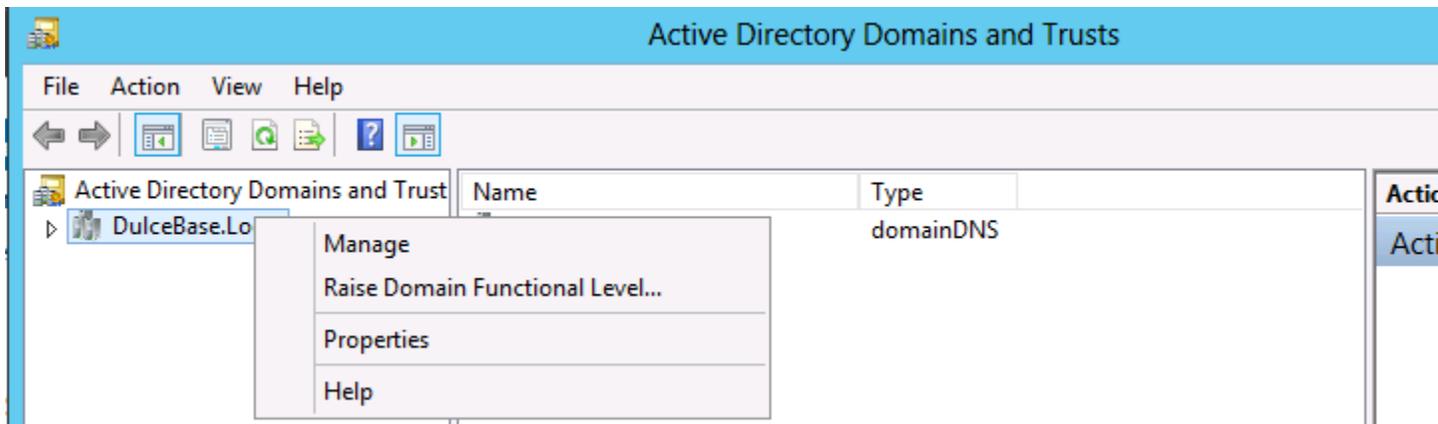
C:\Users\Administrator>
```

Configuring the Forest Trust (steps will be accomplished in both Forest root domains).

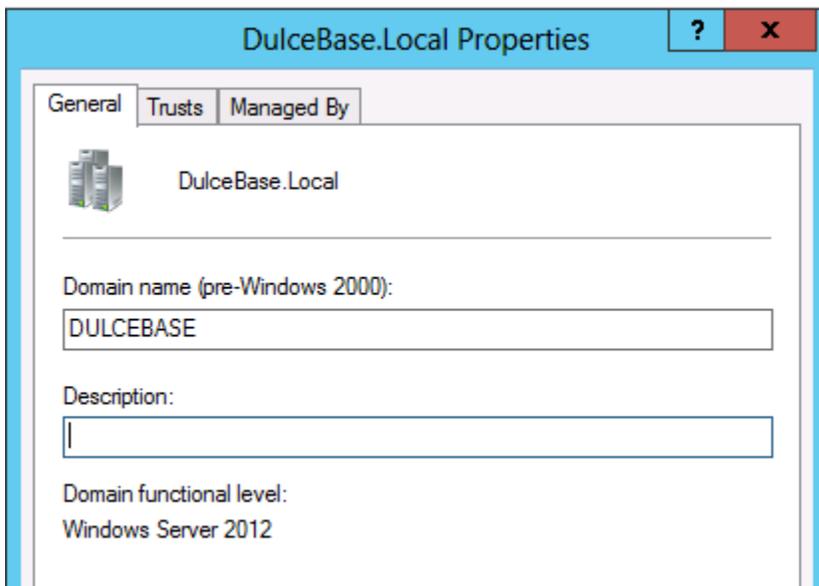
1. Launch Server Manager, using the Tools drop down menu select Active Directory Domain and Trusts.



2. In Active Directory Domains and Trusts, Secondary click on the domain and Click on Properties.

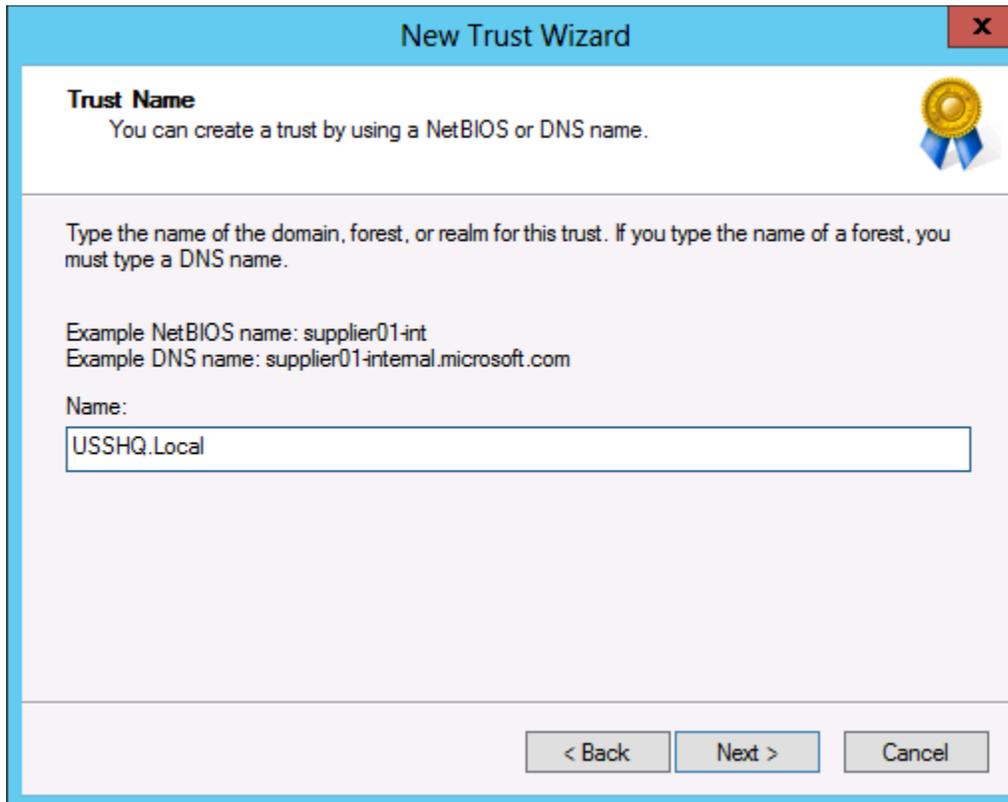


3. On the Domain Properties sheet, click on the Trusts tab.



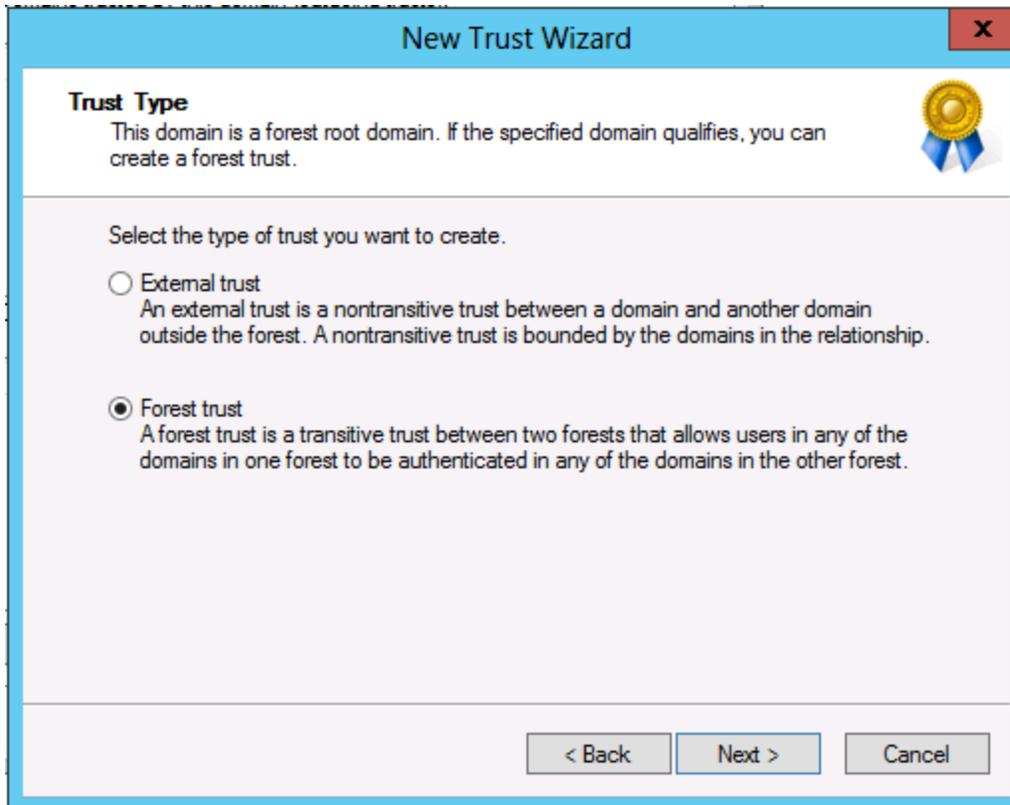
4. Click New Trust, on the Welcome to the New Trust Wizard click Next.

5. On the Trust Name page, enter the name of the forest you want to establish the trust with, click Next.



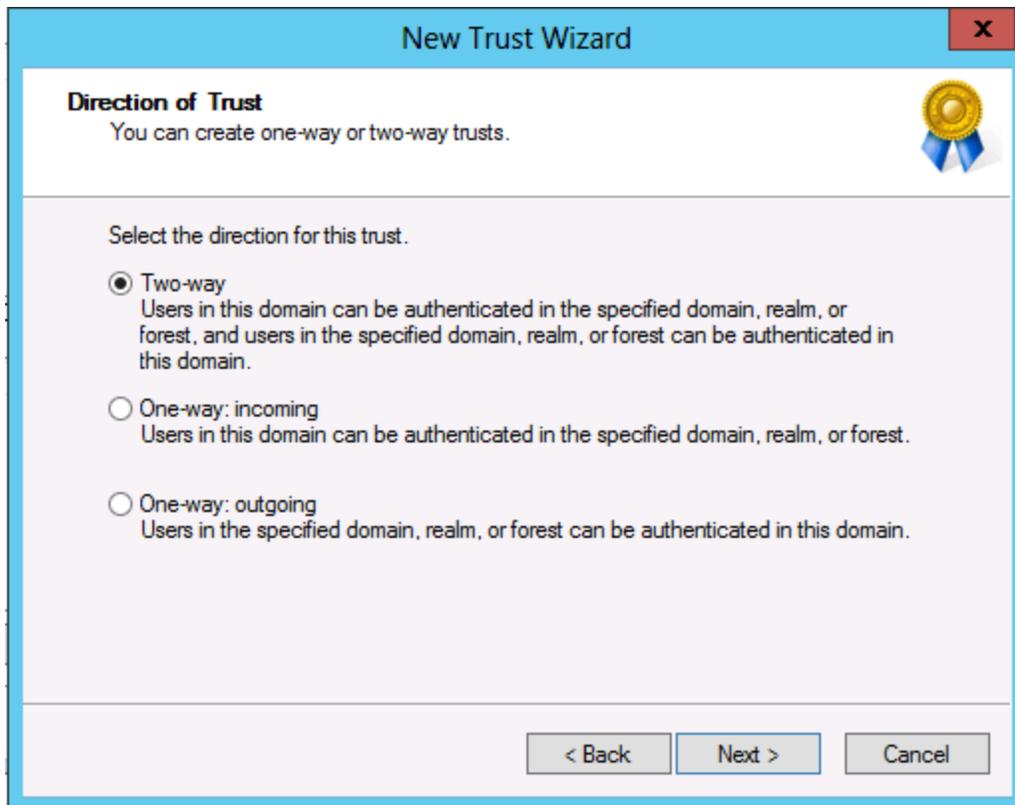
The screenshot shows a Windows dialog box titled "New Trust Wizard" with a close button (X) in the top right corner. The main heading is "Trust Name" with a gold medal icon to the right. Below the heading is the instruction: "You can create a trust by using a NetBIOS or DNS name." A larger text block follows: "Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name." Below this are two example lines: "Example NetBIOS name: supplier01-int" and "Example DNS name: supplier01-internal.microsoft.com". A label "Name:" is positioned above a text input field containing "USSHQ.Local". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

6. On the Trust Type page click on Forest trust, click Next.



Note: If one of the forest were not at Forest Functional Level 2003 or higher, an external trust relationship would be the default and the above screen would not have appeared.

7. On the Direction of Trust page choose the direction of the trust, click Next.



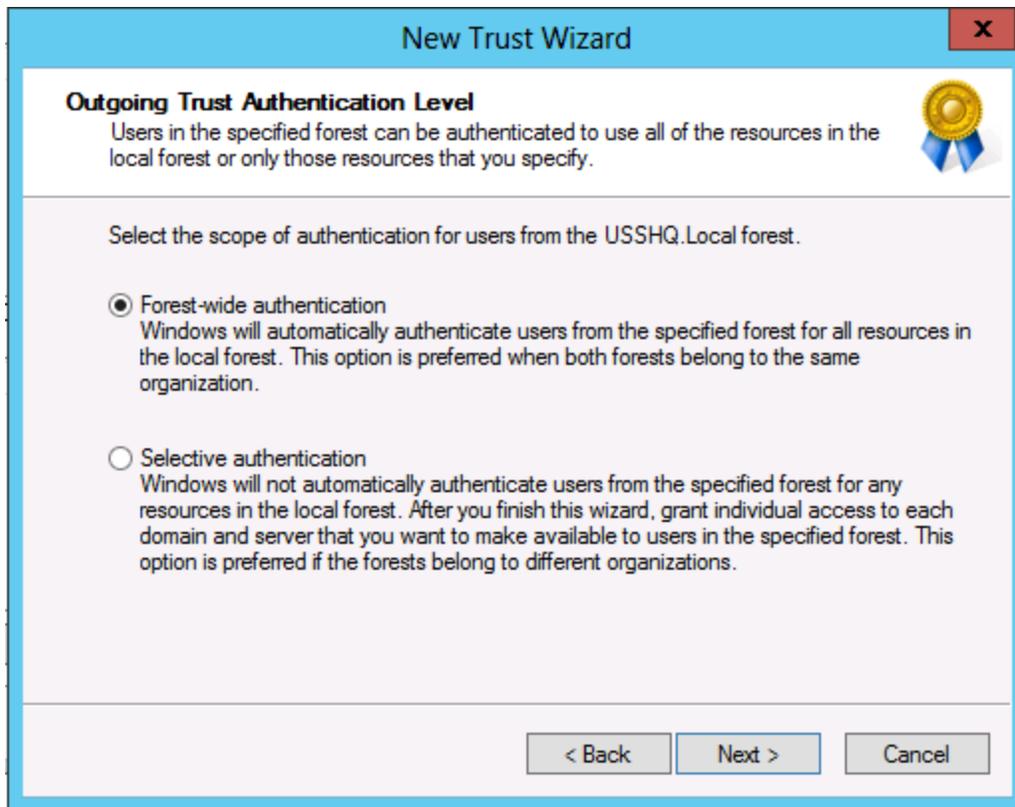
8. On the Sides of Trust page, in order to set the trust up for both domains you will need the administrative privileges or know the administrator account and password for both domains. In this demo I will choose **This Domain Only**, click Next.



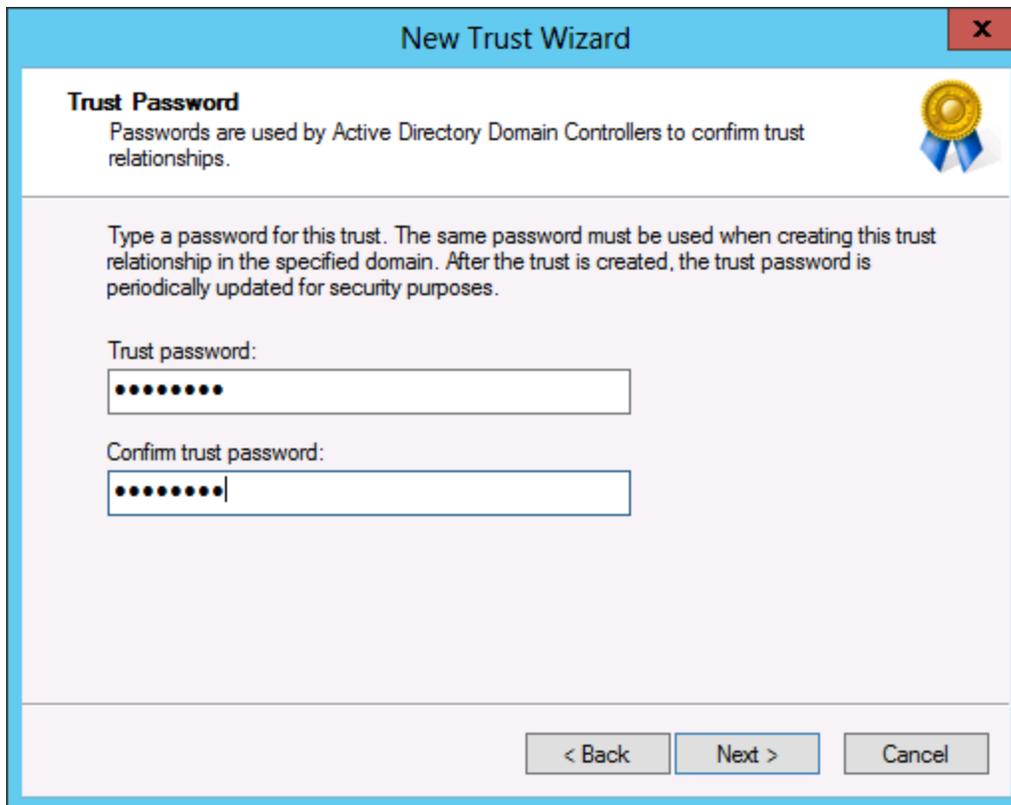
9. On the Outgoing Trust Authentication Level page, choose the appropriate authentication level, click Next.

Forest-wide will allow any authenticated user from the trusted forest to access any resource in the trusting forest that they have the permissions, privileges or rights. They will also be able to log onto computers in the trusting forest.

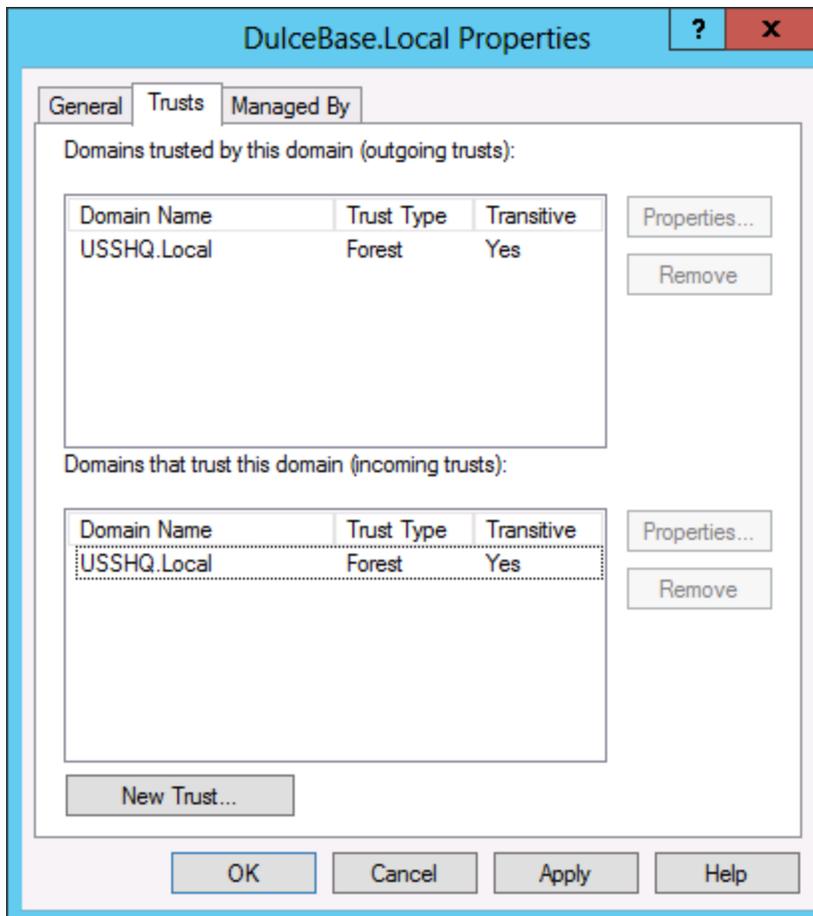
Selective will allow the administrator in the trusting forest to specify which resources and domain the users from the trusted forest.



10. On the Trust Password page, enter a password that the administrators from both forests have agreed upon as the trust password, click Next.



11. On the Trust Selections Complete page click Next.
12. On the Trust Creation Complete page click Next.
13. On the Confirm Outgoing Trust page and the Confirm Incoming Trust page click Next.
14. On the Completing the New Trust Wizard page click Finish
15. On the Domain Properties page, click Apply.



Once the Forest Trust has been created in the other forest the two-way trust will be completed. User will then be able to access resources across the transitive trust between the forests. Use the Sharing and Security tabs to give the appropriate permissions to folders and/or files.