

## Trust between two forests (Using DNS stub zone):

**NOTE:** Please note that these steps were tried between two forests with root domain in Windows 2012R2 DC and the Forest functional level used is 2012.

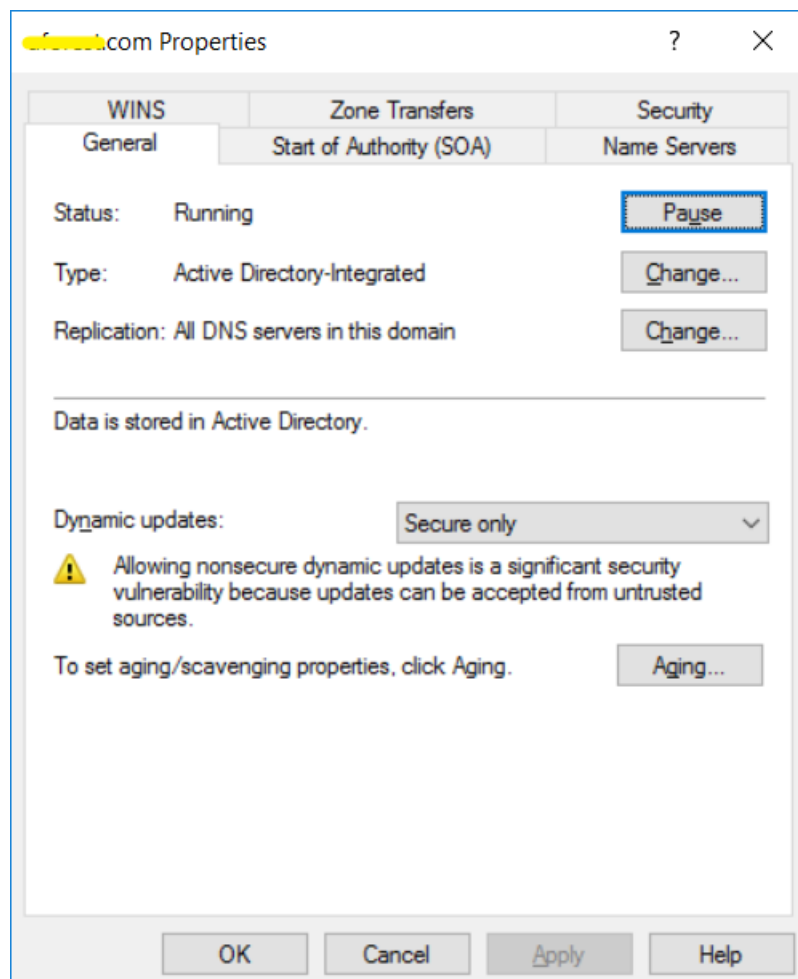
For reference, the forests are named as Forest A and Forest B.

## Configure the source DNS server to allow for zone transfers

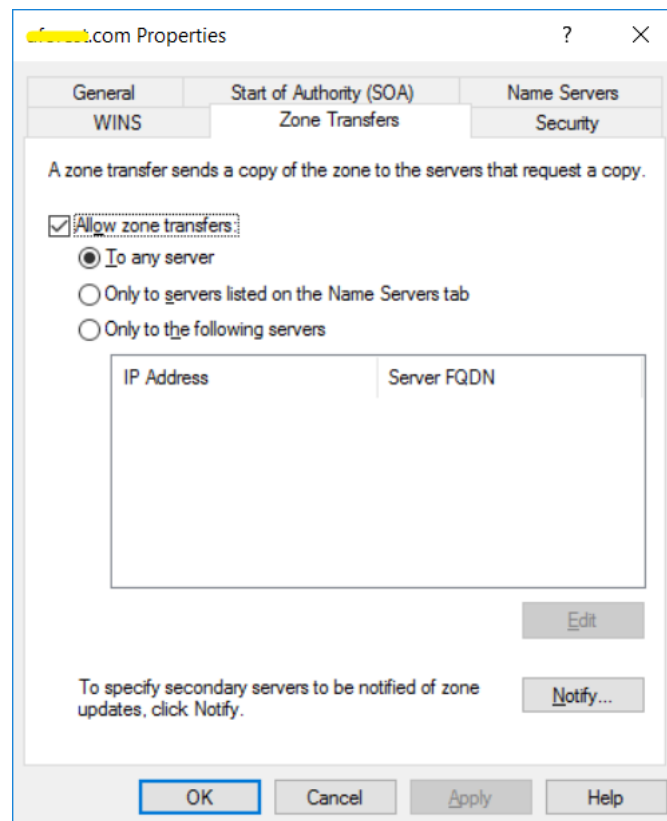
**(These steps will be accomplished on both DNS Servers).**

To forward lookup zone properties,

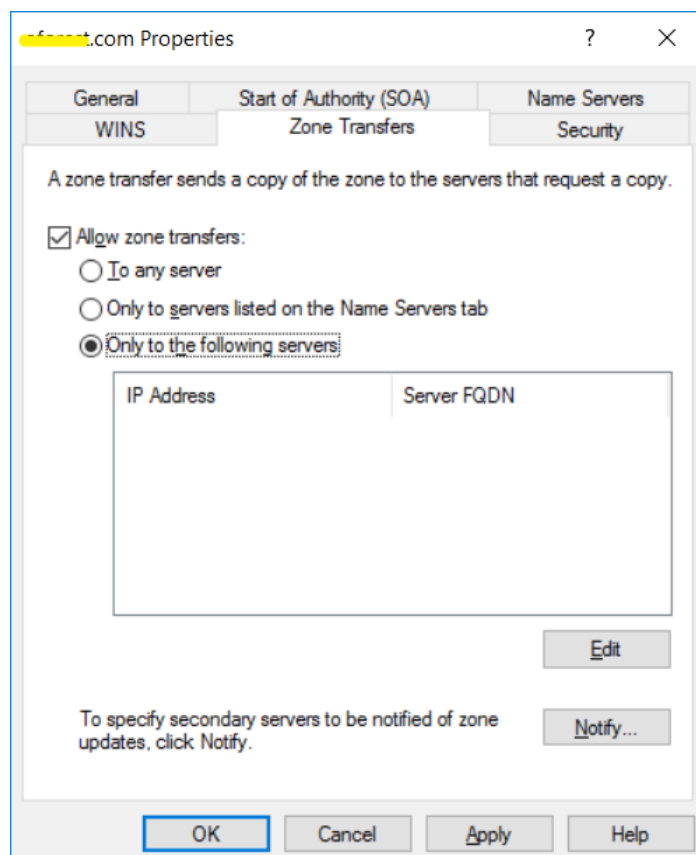
1. Launch the **DNS console**.
2. Click on the **Forward Look Zone** that you desire so configure.
3. Click on **Properties**.



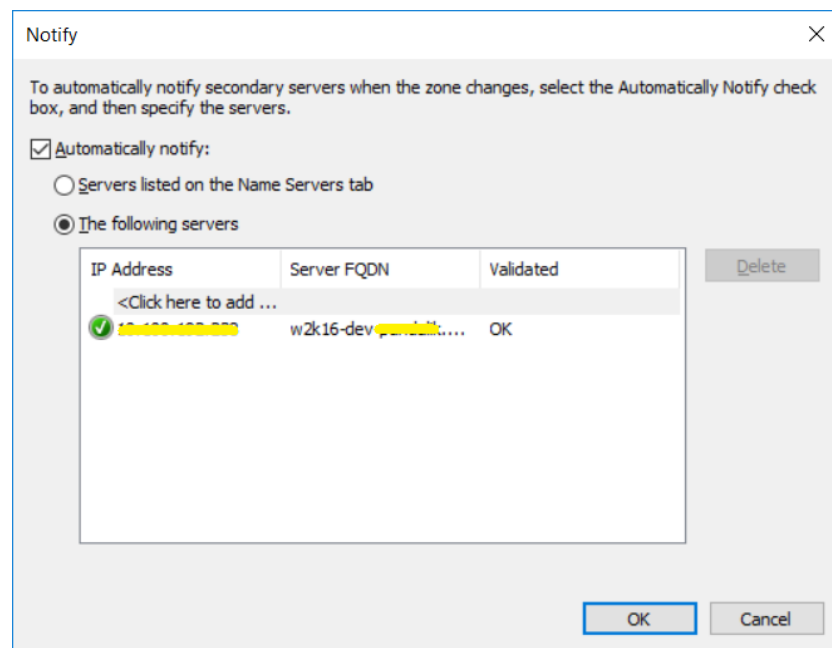
4. Select the **Zone Transfers** tab.



5. Select "**Only to the following servers**".



6. Click on **Automatically notify** and add the IP of the Forest B. Make sure the IP is resolved and the green check mark appears.
7. Click **OK**.



## Configure a Stub Zone

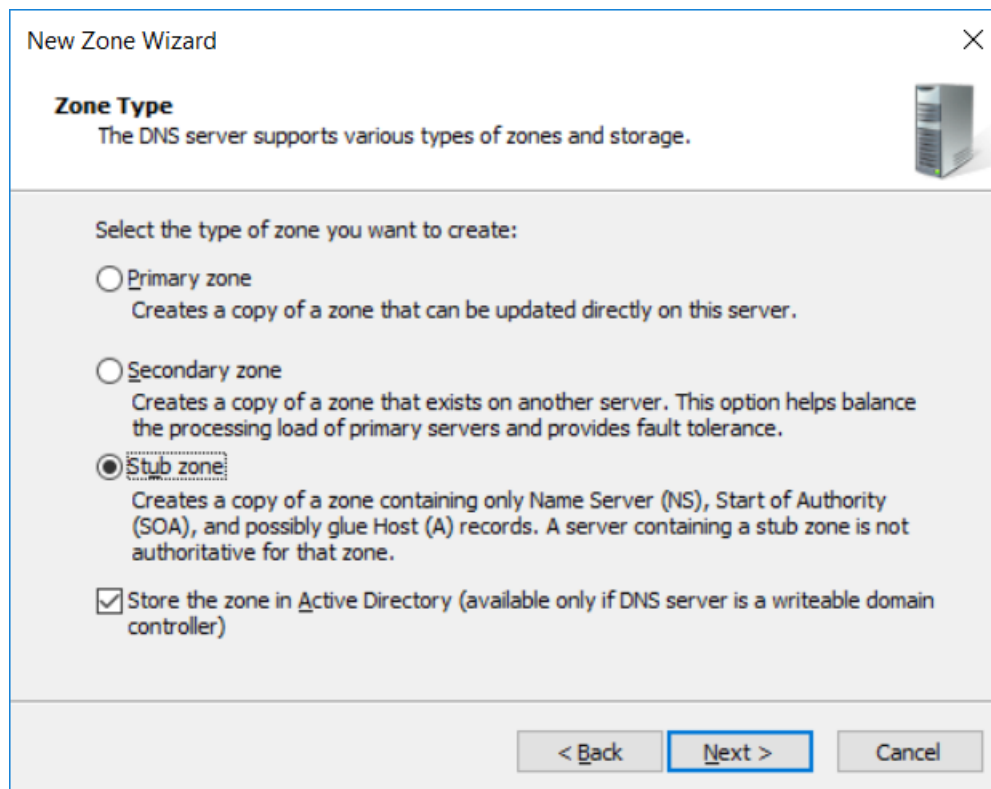
**(These steps will be accomplished in both DNS servers).**

To create a new forward lookup zone for Forest B in Forest A,

1. Launch the **DNS Console**.
2. Click on **Forward Lookup Zone** and choose **New Zone**.
3. In the **Welcome to the New Zone Wizard**, click **Next**.

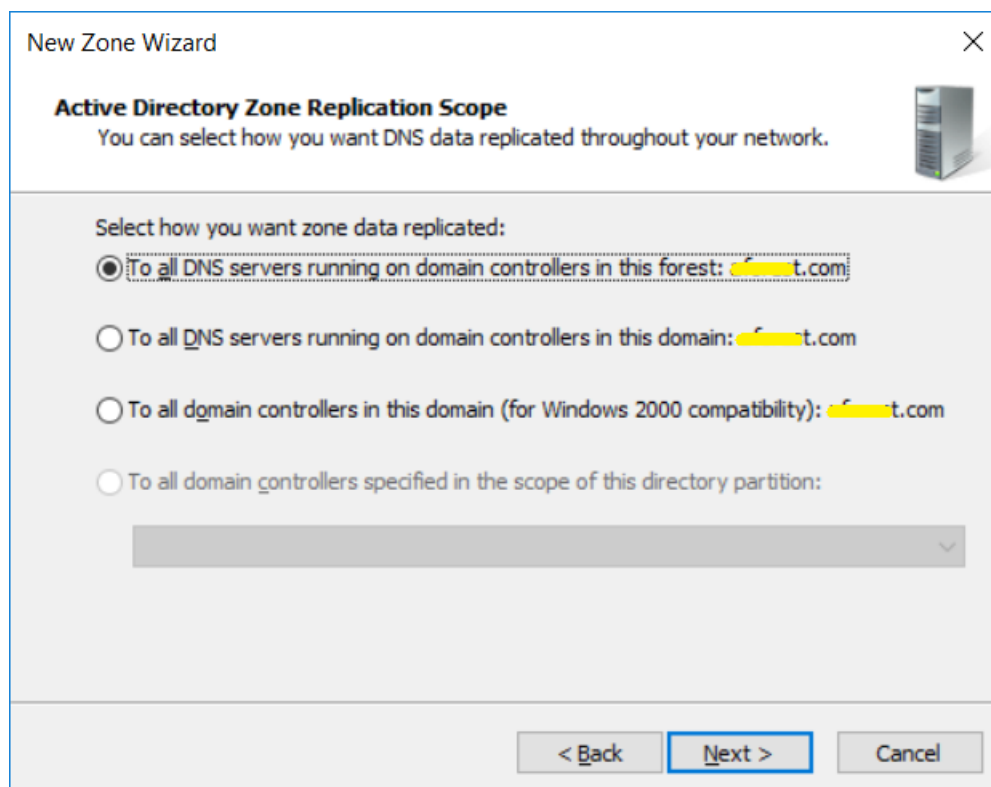


4. Click on **Next** and select the Zone type.



The screenshot shows the 'New Zone Wizard' dialog box with the 'Zone Type' step. The title bar reads 'New Zone Wizard' and there is a close button (X) in the top right corner. Below the title bar, the text 'Zone Type' is followed by the instruction 'The DNS server supports various types of zones and storage.' and a server icon. The main area contains the instruction 'Select the type of zone you want to create:' followed by four radio button options: 'Primary zone' (unselected), 'Secondary zone' (unselected), 'Stub zone' (selected), and 'Store the zone in Active Directory (available only if DNS server is a writeable domain controller)' (checked). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

5. In the next step, select "To all DNS servers running on domain controller in this forest".



The screenshot shows the 'New Zone Wizard' dialog box with the 'Active Directory Zone Replication Scope' step. The title bar reads 'New Zone Wizard' and there is a close button (X) in the top right corner. Below the title bar, the text 'Active Directory Zone Replication Scope' is followed by the instruction 'You can select how you want DNS data replicated throughout your network.' and a server icon. The main area contains the instruction 'Select how you want zone data replicated:' followed by four radio button options: 'To all DNS servers running on domain controllers in this forest: [domain.com]' (selected), 'To all DNS servers running on domain controllers in this domain: [domain.com]' (unselected), 'To all domain controllers in this domain (for Windows 2000 compatibility): [domain.com]' (unselected), and 'To all domain controllers specified in the scope of this directory partition:' (unselected). Below the last option is a dropdown menu. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

- On the **Zone Name** page, enter the desired zone to transfer from, click **Next**.

The screenshot shows the 'New Zone Wizard' dialog box with the 'Zone Name' step selected. The title bar reads 'New Zone Wizard' and there is a close button (X) in the top right corner. Below the title bar, the section is titled 'Zone Name' and asks 'What is the name of the new zone?'. A server icon is visible in the top right. The main text explains: 'The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.' Below this, there is a label 'Zone name:' followed by a text input field containing 'newzone.microsoft.com'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

- Add the IP of Forest B DC and hit **Enter**. Make sure the IP is resolved.

The screenshot shows the 'New Zone Wizard' dialog box with the 'Master DNS Servers' step selected. The title bar reads 'New Zone Wizard' and there is a close button (X) in the top right corner. Below the title bar, the section is titled 'Master DNS Servers' and says 'The stub zone is loaded from one or more master servers.' A server icon is visible in the top right. The main text explains: 'Specify the DNS servers from which you want to load the zone. A stub zone is loaded by querying the zone's master server for the SOA resource record, the NS resource records at the zone's root, and glue A resource records.' Below this, there is a label 'Master Servers:' followed by a table. The table has three columns: 'IP Address', 'Server FQDN', and 'Validated'. The first row is a blue link: '<Click here to add an IP Address or DNS Name>'. The second row contains a green checkmark, the IP address '10.10.10.10', the FQDN 'WIN-1010101010', and 'OK'. To the right of the table are three buttons: 'Delete', 'Up', and 'Down'. Below the table, there is a checkbox labeled 'Use the above servers to create a local list of master servers' which is currently unchecked. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

IP Address	Server FQDN	Validated
<a href="#">&lt;Click here to add an IP Address or DNS Name&gt;</a>		
10.10.10.10	WIN-1010101010	OK

- Click **Finish** and perform the same steps in Forest B DNS for Forest A.

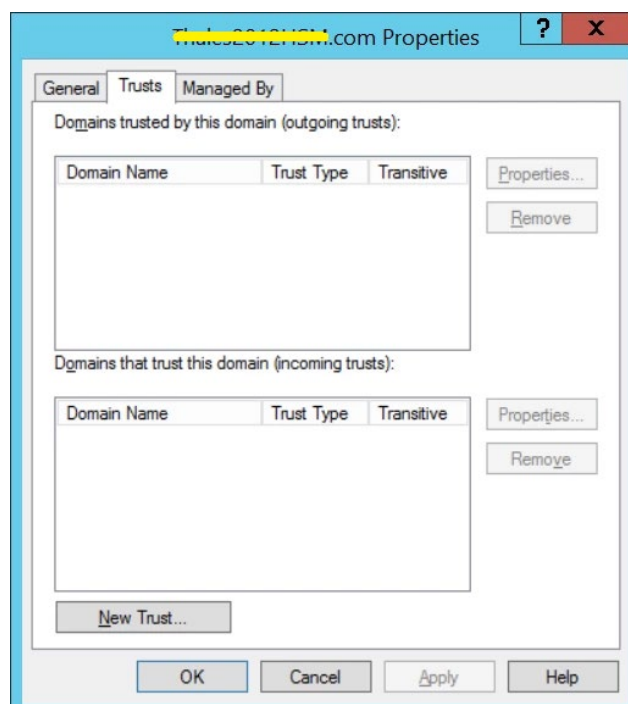


**NOTE:** nslookup should work from Forest A to Forest B and vice-versa without adding IPs of the domain in Host file.

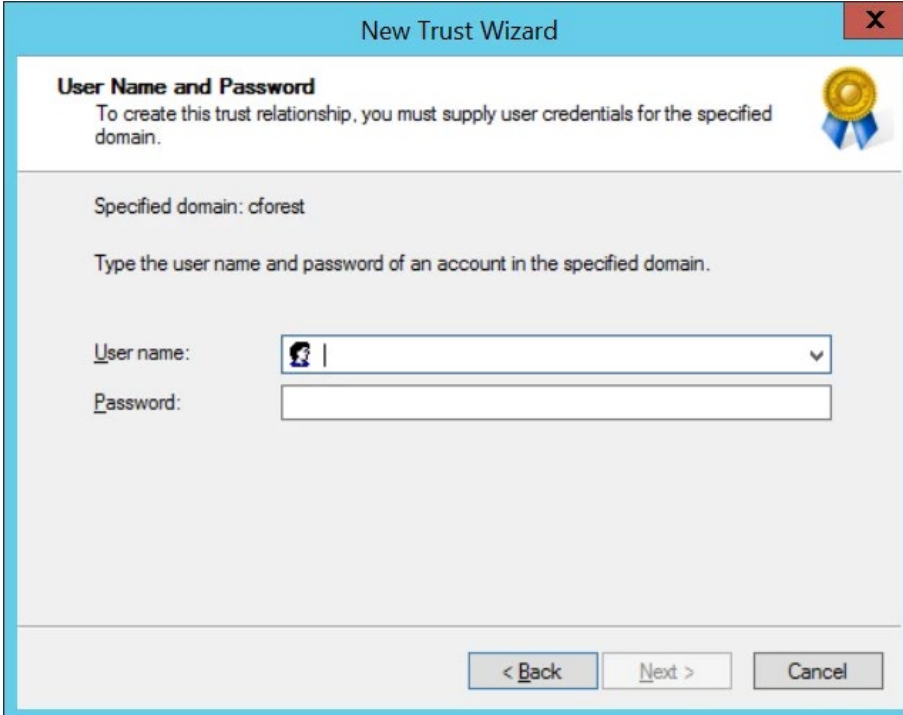
## Create a cross-forest trust

For Active directory domains and trust,

- Go to property of root domain in Forest A. Navigate to **Trusts** tab and add a new trust.




2. Enter NetBIOS name of Forest B, on the next screen and enter the admin credentials for Forest B.



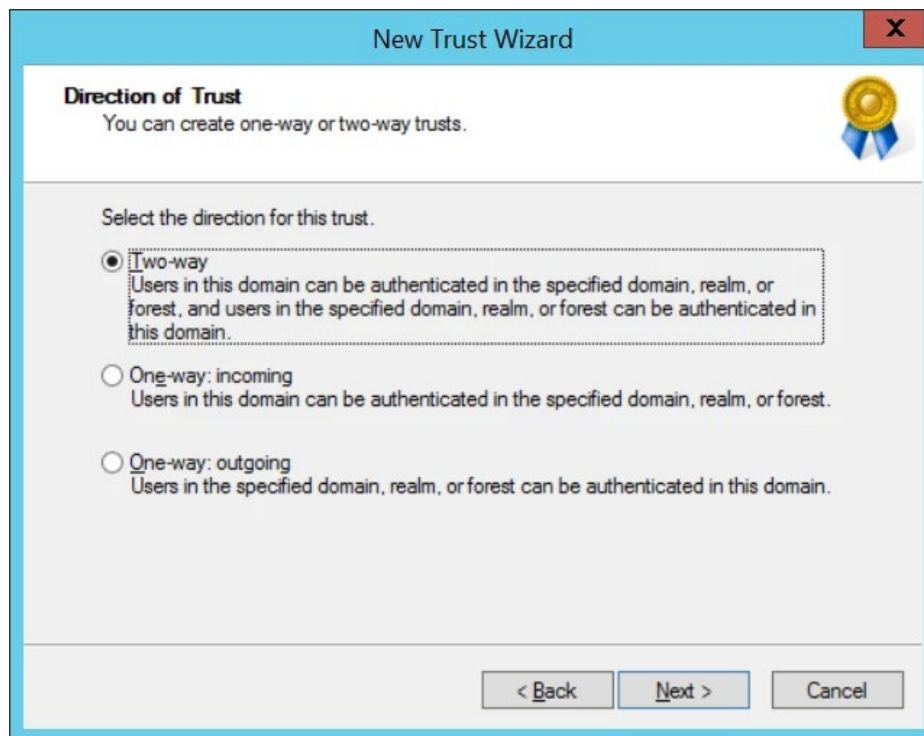
The screenshot shows the 'New Trust Wizard' window, specifically the 'User Name and Password' step. The window title is 'New Trust Wizard' with a close button (X) in the top right corner. Below the title bar, there is a section header 'User Name and Password' followed by the instruction: 'To create this trust relationship, you must supply user credentials for the specified domain.' A gold medal icon with a blue ribbon is positioned to the right of this text. Below the instruction, it says 'Specified domain: cforest' and 'Type the user name and password of an account in the specified domain.' There are two input fields: 'User name:' with a dropdown menu showing a user icon and a vertical bar, and 'Password:' with an empty text box. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

3. Select the **Forest trust** for trust type.

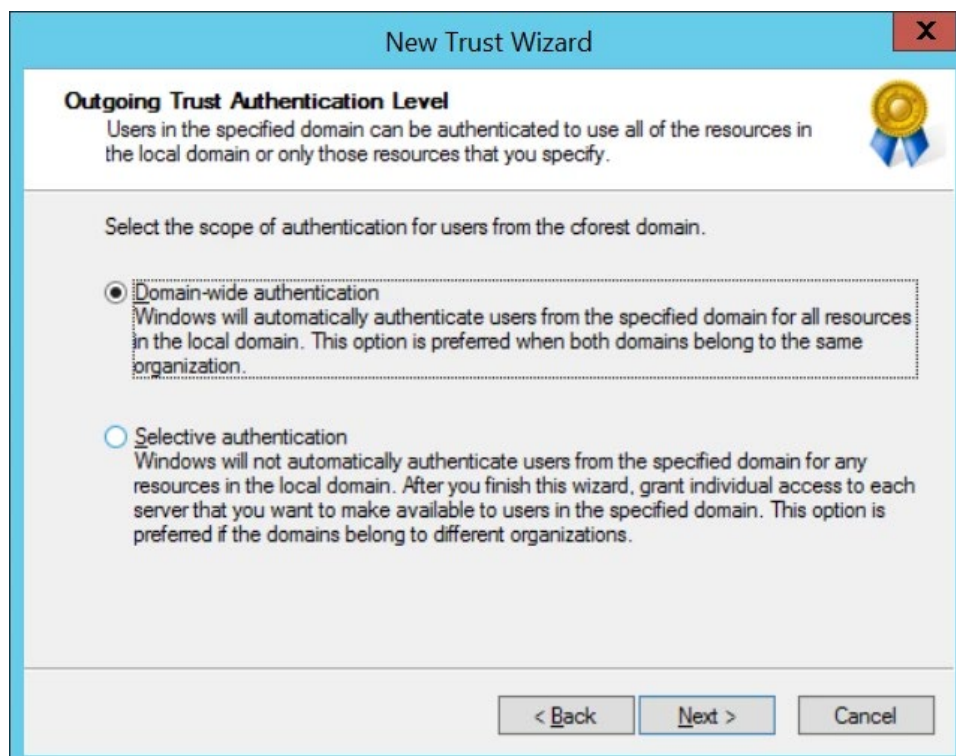


The screenshot shows the 'New Trust Wizard' window, specifically the 'Trust Type' step. The window title is 'New Trust Wizard' with a close button (X) in the top right corner. Below the title bar, there is a section header 'Trust Type' followed by the instruction: 'This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.' A blue icon of two hands shaking is positioned to the right of this text. Below the instruction, it says 'Select the type of trust you want to create.' There are two radio button options: 'External trust' with the description 'An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.' and 'Forest trust' with the description 'A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.' The 'Forest trust' option is selected. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

4. Select the **Two-way** direction for this trust.

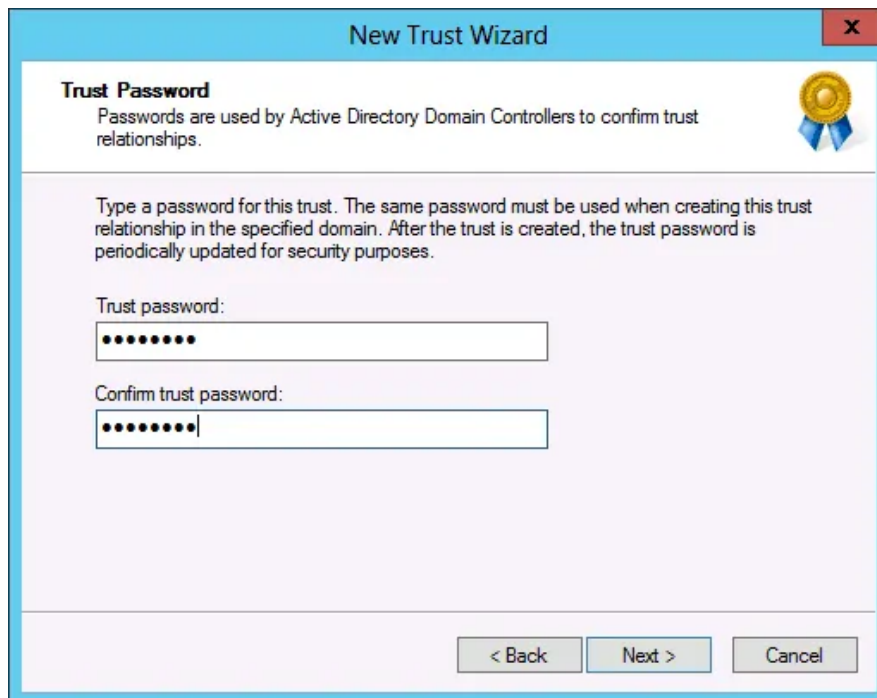


5. For Outgoing Trust Authentication Level, select **Domain-wide authentication**.





6. Provide a trust password. This is required for creating the trust in Forest B.
7. Proceed with the wizard and complete it.



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 Password" in bold. Below it, a subtitle reads: "Passwords are used by Active Directory Domain Controllers to confirm trust relationships." To the right of this text is a gold medal icon with a blue ribbon. The main instruction text says: "Type a password for this trust. The same password must be used when creating this trust relationship in the specified domain. After the trust is created, the trust password is periodically updated for security purposes." There are two text input fields: the first is labeled "Trust password:" and contains seven black dots; the second is labeled "Confirm trust password:" and contains seven black dots. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".