Configuring Cross-Forest SMTP Authentication

An Exchange organization can span more than one forest, but some additional setup is required to make this work and allow messages to flow between the two forests. This article walks through how to configure cross-forest SMTP authorization using two forests: Sherwood and Black.

The basic setup requires setting up connectors in each forest using an authorized account. When an email is sent between the two forests, it is sent from an authorized user and can be transferred across. Without setting up these connectors, Exchange would bounce any mail sent to the forest because it would not know where it came from.

The setup process is simple and should take no more than 10 minutes to configure. First, you need to create a user account in the Sherwood forest with Send As permissions. This user needs to have Send As permissions for everyone within your Exchange organization who is connected to that forest.

Second, you need to perform the same operation in the Black forest, ensuring that the user account has Send As permissions for everyone in the Black forest.

NOTE
Because this is a "slave" account to be used solely for cross-forest authentication, you will want to set a strong password that is difficult to crack. Using simple or standard passwords for this type of account can lead to compromised security.

You can test these two accounts by logging in as the nominated user and attempting to send an email on someone else's behalf. If this operation works, you'll know that this part of the cross-forest setup was successful.

Next, to configure the Exchange connector in the Sherwood forest (and then the Black forest), you need to use the Exchange System Manager to create a new SMTP connector by right-clicking on Connectors and selecting New, SMTP Connector.

Enter a name for your connector and select the option Forward All Mail Through This Connector to the Following, and then enter the name of the Exchange server you want to connect to in the other forest.

Then, click Add to specify the name of the server in your forest you want to send mail from and select the SMTP server where this connector will reside. You also need to switch over to the Address Space tab and click Add, SMTP and then enter the name of the domain you want to connect to (such as `www.black.com`).

Finally, on the Advanced tab, click on Outbound Security and then click on Modify the Properties Associated with Integrated Windows Authentication.

In Outbound Connection Credentials, you need to specify the user account and password that you created earlier with the Send As permissions for everyone in the originating forest. When you are finished, click OK.

After you have configured the connector for the Sherwood forest, you need to repeat these steps for the Black forest. When you are finished, you should be able to send messages between the two forests without error.

Some of the most common errors that can occur with the setup include not checking the account before you use it in the connector, and existing network security that won't allow a server from one forest to "see" the Exchange bridgehead server in the other forest.