Mail Express Windows Authentication Configuration

Contents

Configuring Mail Express Server and the Outlook Add-in to Use Windows Authentication

This document explains how to correctly configure Mail Express so that Outlook Add-in users can authenticate with the Mail Express Server using integrated Windows Authentication. The benefits of using Windows Authentication as it pertains to Mail Express include:

- The Add-in does not need to store any credentials for authenticating, which is more secure.
- Aside from ensuring that each user has a domain account, an organization does not need to create and maintain additional credentials for each Mail Express user.
- The credentials are not passed between the Add-in and the Mail Express Server, which is more secure.

1. Configure Active Directory

To configure the Mail Express Server to use Windows Authentication, launch the Mail Express Administration Web Site and navigate to the **Active Directory** page. Complete the form as it pertains to your environment.

The table below provides a description of the major fields on the form, a description, and an example value.

Field	Description	Example
Active Directory Host	The name of the active directory server.	adserver.globalscape.com
Active Directory Port	The port where Active Directory listens for LDAP communication.	389
Authentication Mode	Dictates whether a pre-auth user account's credentials are used to authenticate with Active Directory.	
Pre-auth user DN	An Active Directory domain account with privileges to search the directory.	CN=mepreauthuser,CN=Users,DC=globalscape,DC=com Or GLOBALSCAPE\mepreauthuser
Pre-auth user password	The pre-auth user's password.	
Confirm pre-auth user password	The pre-auth user's password.	

Field	Description	Example
Search base	The base active directory container that is searched by Mail Express to find users that it will try to authenticate. Searches are recursive.	CN=Users,DC=globalscape,DC=com Note: In this example all objects from the com\globalscape\users node and below in Active Directory will be included in the search.
Search filter	The search filter that is used to find accounts under the search base. Mail Express will match the username against the result returned from the search via the {0} argument in the filter.	(&(objectclass=user)(sAMAccountName={0})) Note: In this example the filter matches any "User" class of object and matches the username provided to Mail Express Server against the value of the "sAMAccountName" property of the Active Directory object.

After configuring the settings on the **Active Directory** page, make sure that the settings are accurate by completing the **Test Configuration** fields (**Test username**, **Test user password**, and **Confirm test user password**) and clicking **Test**. Be sure to click **Save** to save your settings before leaving the page.

2. Configure Kerberos

If the Active Directory settings test was successful, then proceed to the **Add-in Settings** page, select the **Enable Single Sign On (Kerberos)** checkbox, complete the **Single Sign On** fields, then click **Save**.

The table below provides a description of each field, a description, and an example value.

Field	Description	Example
KDC host	The KDC host name. A KDC for a domain is located on a domain controller. If a domain has a single domain controller the KDC host will be the same as the Active Directory server host.	adserver.globalscape.com
KDC port	The port that the KDC is listening on.	88
Domain name	The name of the domain.	globalscape.com
KDC pre-auth username	The username of an Active Directory account that will be used to authenticate with the KDC. This account will be configured so that it may participate in Kerberos in the "Service Principal Names" section below.	mepreauthuser
KDC pre-auth user password	The password of the account that will be used to authenticate with the KDC.	
Confirm KDC pre-auth user password	The password of the account that will be used to authenticate with the KDC.	

3. Configure the Service Principal Names

Using the Windows "setspn" utility, create Service Principal Names (SPN), which is necessary for Kerberos to function correctly for Mail Express. The SPN is a name by which the Add-in can uniquely identify the Mail Express Server service. The SPN will be associated with the Active Directory domain account used in the **KDC pre-auth username** field of the Mail Express Server **Kerberos Configuration**.

The "setspn" utility is typically installed by default on Active Directory server computers. The command must be run using an account with Active Directory administration rights. Typically it is easiest to perform these steps on the domain's primary Active Directory server.

To create the SPNs, execute the following at a command prompt:

```
setspn –A HTTP/<MailExpressServerHostName> <PreAuthUsername>

setspn –A HTTP/<MailExpressServerFullyQualifiedHostName>
<PreAuthUsername>
```

Where:

- <MailExpressServerHostName> is the host name of the machine running the Mail Express Server. This is the host name that workstations would use internally to communicate with the Mail Express Server machine.
- <MailExpressServerFullyQualifiedHostName> is the fully qualified host name of the machine running the Mail Express Server. This is the full host name that workstations would use internally to communicate with the Mail Express Server machine.
- <PreAuthUsername> with the username of Active Directory domain account used in the "KDC pre-auth username" field of the Mail Express Server Kerberos Configuration.

Do not type "HTTP://" -- the proper prefix is "HTTP/". For example, type:

```
setspn –A HTTP/meserver mepreauthuser

setspn –A HTTP/meserver.globalscape.com mepreauthuser
```

These SPNs should work regardless of the account the Mail Express Server Windows Service is running as.

To view the SPNs to verify that they were created successfully, run the following command after substituting `<PreAuthUsername>` with the username of the pre auth user account:

```
setspn -l <PreAuthUsername>
```

4. Configuring the Outlook Add-in

When the Outlook Add-in is installed, end users can choose between Windows or Manual Authentication. If Windows Authentication is specified, the Service Principal Name created earlier must be specified. For instance, if a Service Principal Name was created with the command "`setspn –A HTTP/meserver mepreauthuser`" then type **HTTP/meserver** in the **Service Principal Name** field of the installation wizard. Again, ensure you use the prefix "HTTP/" and not "HTTP://".

- If the Outlook Add-in is installed silently, then the SPN must be provided as an installation parameter. The installation parameter name is "SERVICEPRINCIPALNAME."
- If the Outlook Add-In has already been installed using alternate authentication settings, then the settings can be changed after installation either by:
  - Re-running the installation in silent mode and specifying a different value for the SERVICEPRINCIPALNAME installation parameter

  –or-

  - Changing the **ServicePrincipalName** registry setting directly and then restarting Outlook. This registry setting resides under the following registry key:

    HKEY_CURRENT_USER\Software\GlobalSCAPE\Mail Express Outlook Addin\Settings