How to Create a GroupWise Trusted Application Key

https://campus.barracuda.com/doc/3229/

This article refers to the Barracuda Message Archiver firmware version 5.0 or higher, and Novell® GroupWise® versions 6.5, 6.5.3, 7.0, 8.0, 2012, and 2014.

A Trusted Application Key is created at the Domain database level. To create this key, you need the following:

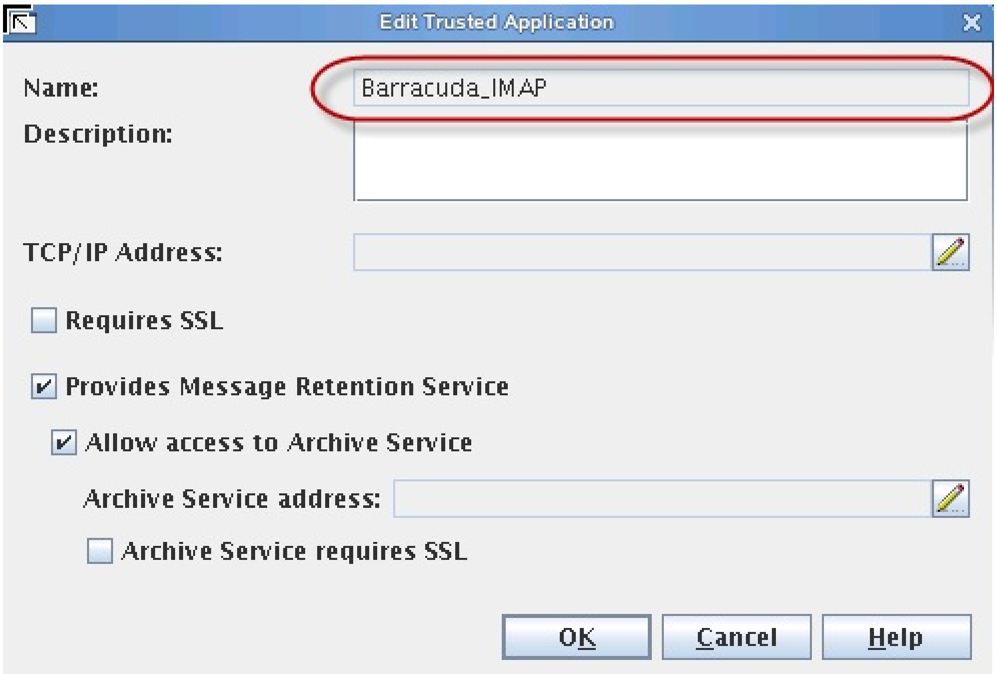
- An application capable of creating the Trusted Application Key such as the GroupWiseavailable on the **USERS > Client Downloads** page of the Barracuda Message Archiver
- Administrator access to the GroupWise wpdomain.db database
- Administrator privileges to the Domain object within eDirectory

As with the majority of GroupWise administration, information is written to the Domain database, which is then propagated throughout the system. Information is replicated to other Domain databases which in turn push this information to the Post Office database. Therefore, it is critical when creating a Trusted Application Key that all Domains are communicating and show OPEN status in the Message Transfer Agents (MTAs).

Note that propagation of the Trusted Application Key to the Post Office database is based on the size of the GroupWise system; allow the Trusted Application Key to fully propagate before attempting to log in.

Name the Trusted Application Key for the Barracuda Message Archiver

You must name the Trusted Application Key Barracuda_IMAP


Edit Trusted Application

Name: Barracuda_IMAP

Description:

TCP/IP Address:

□ Requires SSL

☑ Provides Message Retention Service

☑ Allow access to Archive Service

Archive Service address:

□ Archive Service requires SSL

Validate the Trusted Application

If the application is having difficulty running, or if the Trusted Application Key does not generate properly, review the Post Office Agent (POA) log files for the Post Office database you are trying to access using the Trusted Application Key. Locate the log entry for the login attempt:
TRUSTED APP login attempt

If the login attempt fails, there may have been issues encountered during the creation of the Trusted Application Key. Use the following steps to troubleshoot the Trusted Application Key:

1. Validate that the key lists the Trusted Application Key in eDirectory. The actual key is a 64-byte alpha-numeric string, for example:
   B346A421039D0000803225001F008000B346A422039D0000803225001F008000
   If the key does not look similar to this example, or if it contains non alpha-numeric characters, such as ¬, it is likely due to insufficient rights to the domain object in eDirectory when creating the object.
2. If the key structure is valid, it may be that the key credentials did not propagate to the Post Office database; perform a database rebuild on the Post Office database, and restart the POA.
3. The SINGLE-SIGNON setting on the Novell Client can also cause issues with the Trusted Application Key. If this property is activated, then the Trusted Application Key cannot log in to any account on the server unless the workstation is authenticated to eDirectory using that *same* account. If you can run the application when using the same GroupWise account as the account with which you are logged into eDirectory but you cannot access any other accounts, then run the GroupWise Client on the station and ensure that Single Sign-On is

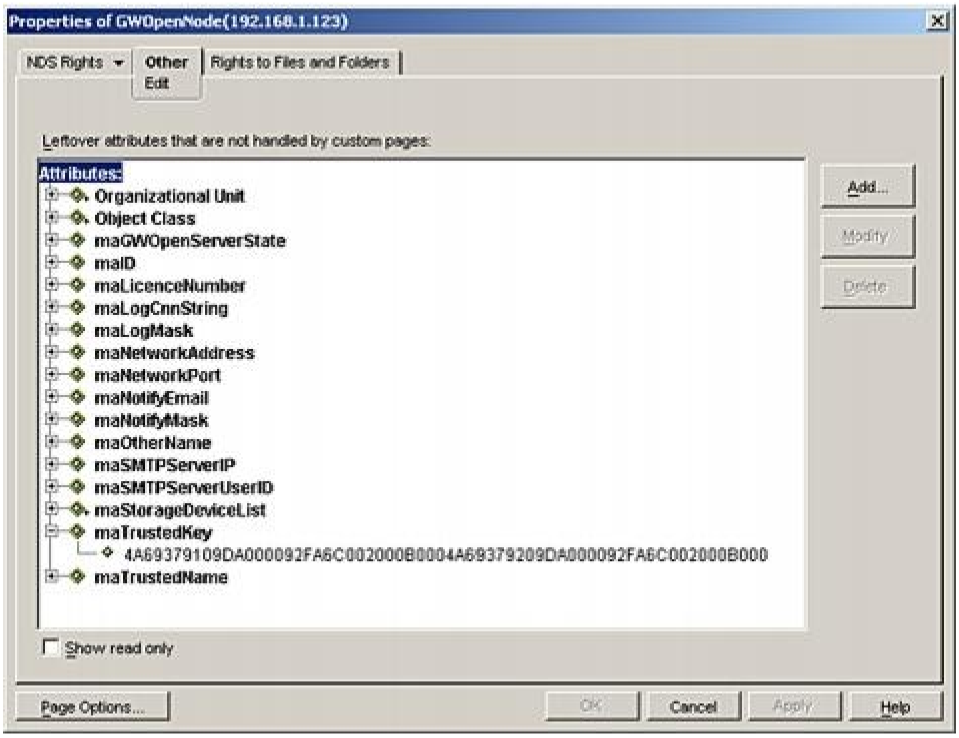
turned *off*.

4. If you are still unable to log in, delete the TRUSTED APP from ConsoleOne and regenerate using the GroupWise Trusted Application Key Maker available from the **USERS > Client Downloads** page in the Barracuda Message Archiver.

Locate the Trusted Application Key

If the Trusted Application Key is not properly regenerating in ConsoleOne, use the following steps to delete the Trusted Application Key from the eDirectory Configuration Container of the GroupWise POA:

1. To locate your Trusted Application Key, launch ConsoleOne, and then locate the **Group Wise Node** object.
2. Right-click on the **GW POA** object, and select **Properties**.
3. In the **Properties** dialog box, click the **Other** tab.
4. Under **Attributes**, expand the tree under **Trusted Application Key**:



Properties of GWOpenNode(192.168.1.123)

Leftover attributes that are not handled by custom pages:

```
Attributes:
 Organizational Unit
 Object Class
 maGWOpenServerState
 maID
 maLicenceNumber
 maLogCnnString
 maLogMask
 maNetworkAddress
 maNetworkPort
 maNotifyEmail
 maNotifyMask
 maOtherName
 maSMTPServerIP
 maSMTPServerUserID
 maStorageDeviceList
 maTrustedKey
   4A69379109DA000092FA6C002000B0004A69379209DA000092FA6C002000B000
 maTrustedName
```

☐ Show read only

Figures