Monotype

Kerberos Setup

Configuration Guide for Macintosh and Windows

Version 1.0
March 2016

Copyright and Trademark Information

Disclaimer

How to Use this Guide

This document includes all the necessary steps required to setup and enable Kerberos Authentication for FontExplorer X Server login. If you are new to Kerberos then before you setup Kerberos, we recommend you start by reading the introduction to Kerberos. This chapter includes a brief introduction of Kerberos and its characteristics. See Kerberos Overview.

Before setting up Kerberos, you must ensure that your environment meets the minimum requirements for successful Kerberos setup, see Minimum Requirements.

In order to setup Kerberos, first you need to configure Active Directory. To configure the Active Directory, see Configure Active Directory.

If you have a requirement to use Kerberos Authentication for multiple domains then You should read the chapter Configure Trust Relationship for Cross domain Platform. This chapter includes stepwise procedure to establish the Trust Relationship between multiple domains and configure DNS Settings for cross domain users. It also includes the procedure to edit host file on Server machine.

After configuring Active Directory, the Keytab file should be generated for FontExplorer X Server and the user should be successfully mapped. To perform this process, see Map Domain Service Account with KDC.

If you are using Windows Server than you need to configure FontExplorer X Server for a Window Server. See Configure FontExplorer X Server for a Windows server.

To apply the Kerberos Keytab file and import domain users for Kerberos Authentication, see Configuring FontExplorer X Server for Kerberos Authentication.

Once you setup Kerberos for FontExplorer X, you need to verify the Kerberos Authentication in FontExplorer X Pro. See Verify Kerberos Authentication.

The **Table of Contents** helps you to quickly find the topic you are looking for. In many chapters and sections there are cross-references to other pages with further information on the current topic. They look like this: (see “sample heading”).

To make it easier to find the information you are looking for, we have used the following typographic conventions:

Keyboard shortcuts
Example: Press ⌘ 1

Field names and folder names appear in bold and blue
Example: The **Start** menu

Error Messages, User Interface Controls appear same as they are on UI
Example: The panel will show “Kerberos keytab file is valid.“

If you cannot find the information you need in this guide, please feel free to get in touch with our support team. Further contact information is available at the end of this document.

You are welcome to let us know how to improve this documentation. Please mail your comment to **info@FontExplorerX.com**

Table of Contents

What is Kerberos?

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos authentication has the following characteristics:

— Kerberos Authentication is secured and always sends an encrypted password for the login.

— Only a single login is required per session. Credentials defined at login are then passed between resources without any need of additional logins.

— The concept depends on a secured and trusted third party – a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.

Why Kerberos?

A properly deployed Kerberos infrastructure will help you address problems such as: password sniffing, password file name/database stealing, and the high level of effort necessary to maintain a large number of account databases.

Use of Kerberos will prevent plain text passwords from being transmitted over the network. The Kerberos system will also centralize your username and password information which will make it easier to maintain and manage this data. Finally, Kerberos will also prevent you from having to store password information locally on a machine, whether it is a workstation or server.

Kerberos Setup Prerequisites

To use Kerberos Authentication with FontExplorer X Pro, you need to ensure that your environment meets the minimum requirements for successful authentication.

> **NOTE:** For Kerberos Authentication, It is not recommended to install FontExplorer X Server on a domain controller.

Successful Kerberos Authentication requires the following minimum requirements:

- **FontExplorer X Pro Server 2.0 or later (For Macintosh/ Windows)**
- **FontExplorer X Pro 5.0 (For Macintosh) or later**
- **FontExplorer X Pro 3.0 (For Windows) or later**
- **Windows Server 2008/2012 or later**
- **Microsoft Active Directory**
- **All server and client computers must be a member of the same Active Directory domain**
- **If you have multiple domains to use Kerberos Authentication then a Trust Relationship between domains should be configured**

Create FontExplorer X Service Account in Active Directory

In order for Kerberos Authentication to function, a permanent FontExplorer X service account is required for your domain. This account is used to authenticate users with your domain via FontExplorer X Server.

Connect to a domain controller and create the account as follows:

1) Open **Active Directory Users and Computers**.

2) In the left pane, right-click the OU (Organizational Unit) where you wish to create the service account and select **New > User**.

3) Enter the username of your FontExplorer X service account, for example **FEXService** and click **Next**.

4) Choose a strong password for this account.

5) Uncheck **User must change password at next logon**.

6) Check the **Password never expires** checkbox and click **Next** followed by **Finish**.

(See Figure 1 and Figure 2)

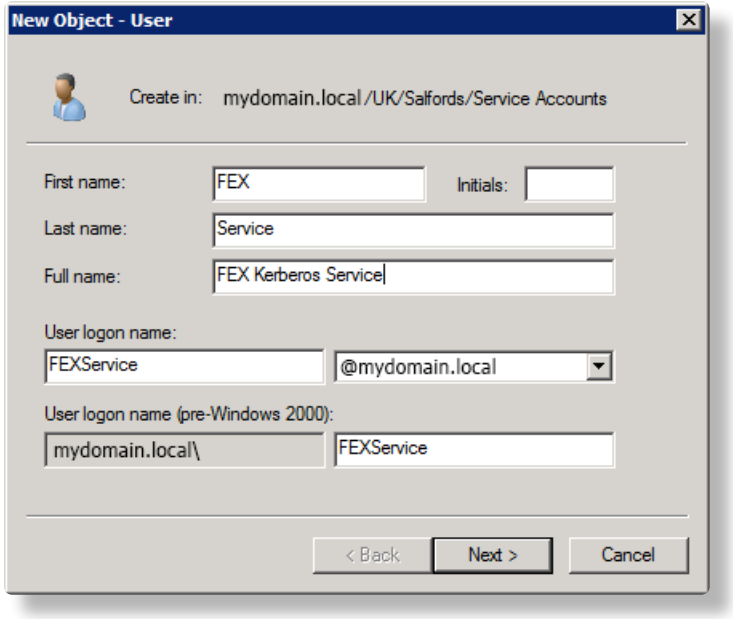

Figure 1

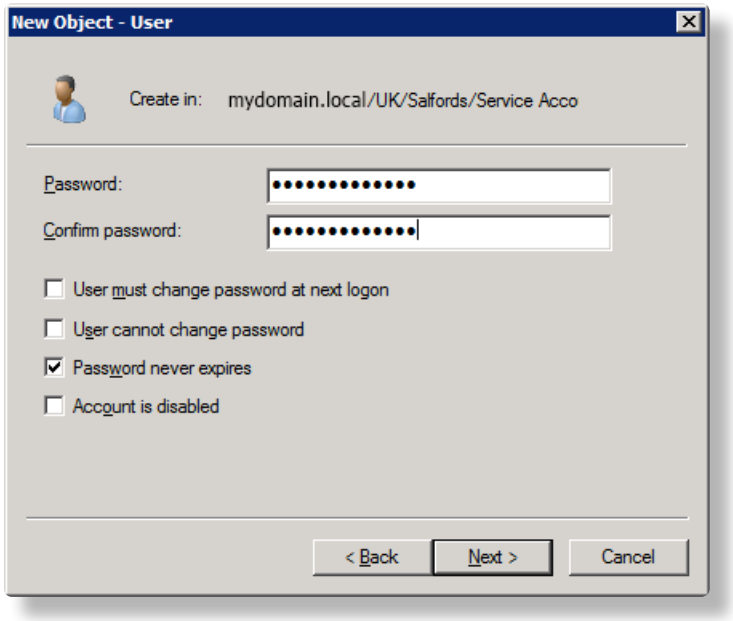

Figure 2

Establish the Trust Relationship between Multiple Domains

To establish the Trust Relationship between multi domains, follow the below steps:

1) On the server machine, open the **Active Directory Domains and Trusts** window.

   To open Active Directory Domains and Trusts, click **Start**, click **Administrative Tools**, and then click **Active Directory Domains and Trusts**.

   OR

   Click **Start**, type **domain.msc**.

2) Select the domain name for trust relationship, right-click and choose **Properties**.

3) Select the **Trust** tab.

4) Now click **New Trust** button to add a new trust relationship and provide name.

5) In the **New Trust** Wizard, select the **Forest trust** radio-button and click **Next**.

6) Select the **Direction of the Trust:** Two-way and click **Next**.

7) Select the **Sides of Trust:** Both this domain and the specified domain and click **Next**.

8) Select **Outgoing Trust Authentication Level-Local Forest:** Forest wide authentication and click **Next**.

9) After configuring the above settings, the specified domain reflects in **Outgoing trusts** and **Incoming trusts** as well.

(See Figure 3 and Figure 4)

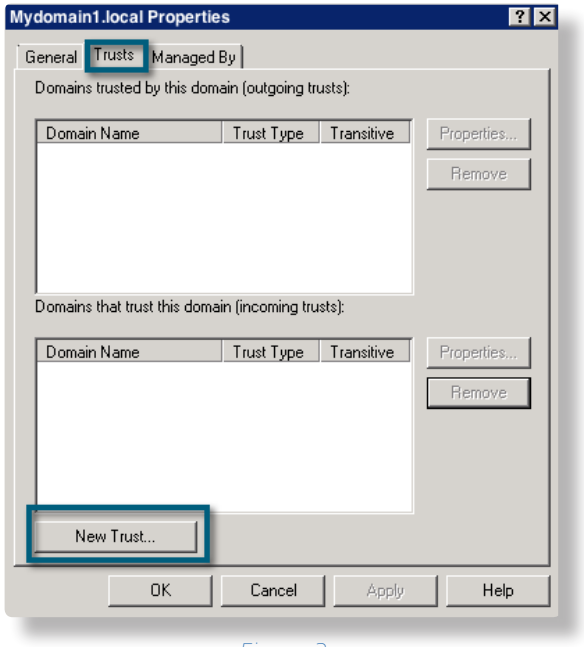

Figure 3

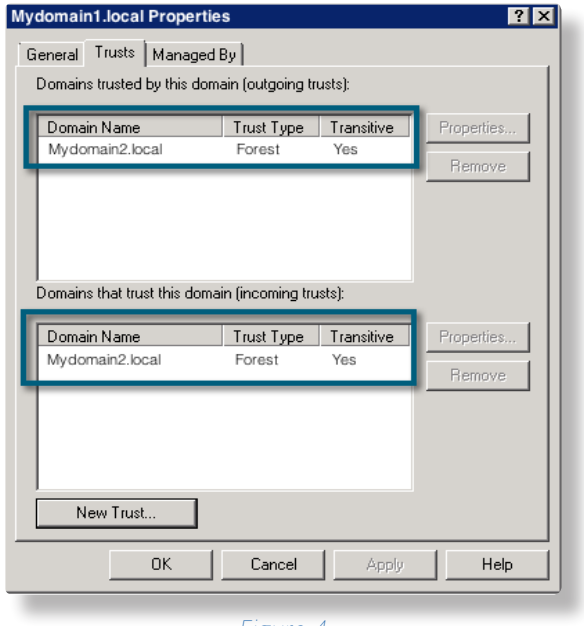

Figure 4

Verify a Trust using the Windows Interface

To verify a trust using the Windows interface:

1) Open **Active Directory Domains and Trusts**.

2) In the console tree, right-click the domain that contains the trust that you want to verify, and then click **Properties**.

3) On the **Trusts** tab, under either Domains trusted by this domain (outgoing trusts) or Domains that trust this domain (incoming trusts), click the trust to be verified, and then click **Properties**.

4) Click **Validate**.

(See Figure 5)

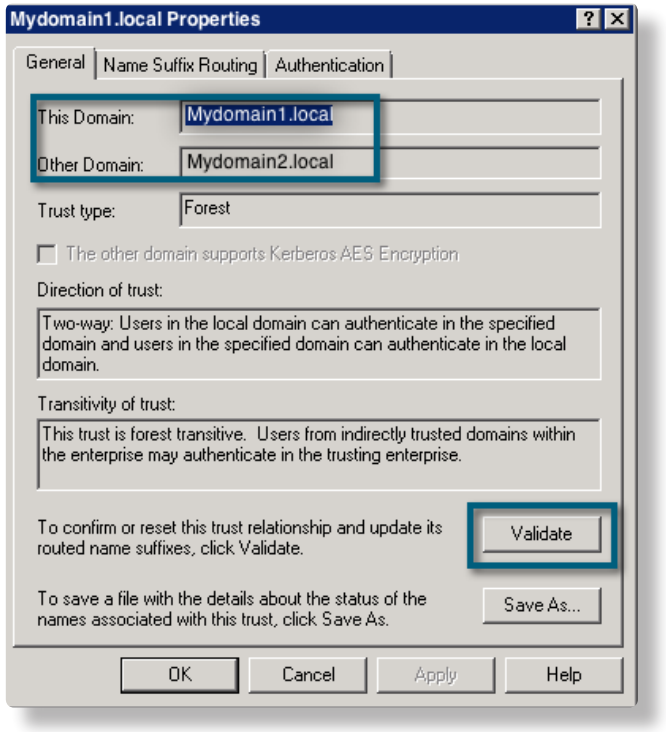

Figure 5

5) In the Active Directory Domain Services, Select **Yes**, validate the incoming trust. Type the user name and password of an account with administrative privileges in the specified domain.

(See Figure 6)

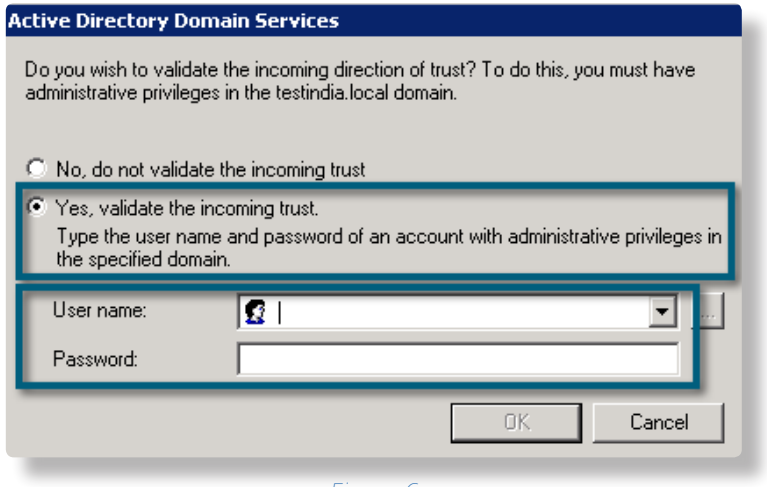

Figure 6

Configure DNS Settings

Perform the following steps:

1) To open Network Connections, click the **Start** button, and then click **Control Panel**. In the search box, type adapter, and then, under **Network and Sharing Center**, click **View network connections**.

2) Right-click the connection that you want to change, and then click **Properties**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

3) Now select either **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

4) To get a DNS server address automatically using DHCP, click **Obtain DNS server address automatically**, and then click **OK**.

(See Figure 7)

5) To change advanced DNS, WINS, and IP settings, click **Advanced** and select **DNS** tab.

6) Examples of different domains: Mydomain1.local, Mydomain2.local and Mydomain3.local

(See Figure 8)

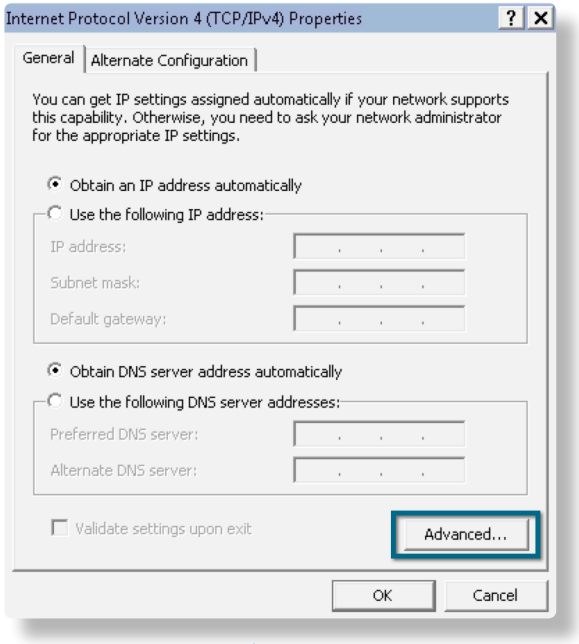

Figure 7

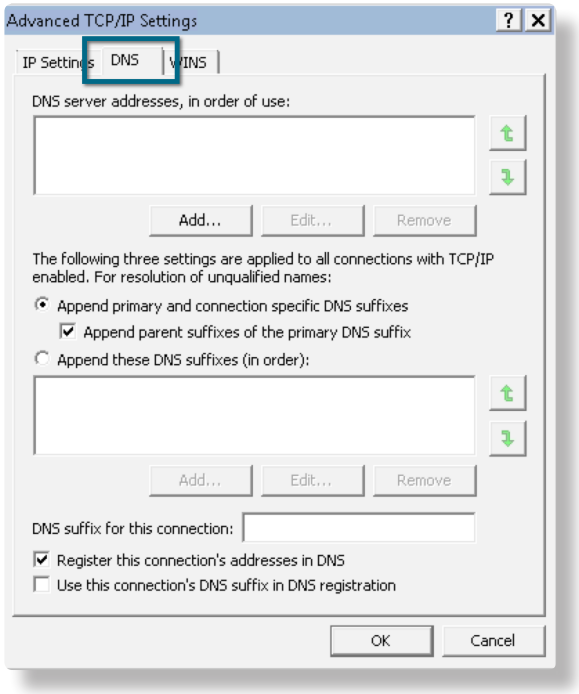

Figure 8

Edit Host file for Trust Relationship

After configuring the Trust Relationship between the multi domains, you need to do some changes in the host file on the server machine.

Perform the below steps to edit host file:

NOTE: These steps need to be followed on LDAP configuration.

1) Access the path C:\Windows\System32\drivers\etc\hosts and open the file in notepad.

2) Add IP addresses and FQDN (Fully Qualified Domain Name) of all the domain servers in the host file
Example:

   xxx.xx.x.xxx Mydomain1.local
   xxx.xx.x.xxx Mydomain2.local
   where xxx.xx.x.xxx is IP adress
   Mydomain1.local and Mydomain2.local are FQDN

3) Save the host file.

Generate Kerberos Keytab file for FontExplorer X Server

To map the newly created FontExplorer X Service account with the KDC and generate the required keytab file, you must run the built-in windows command **ktpass**. On your Windows Server, open a **Command Prompt** window and run the command. (See right)

Individual components are explained below:

ktpass – is the built in command in windows Server for Kerberos configuration.

-princ – creates a service principal name (SPN) for Kerberos Authentication of the specified user. This is case sensitive.

FEXService – is the AD username created in the previous step.

/mydomain.local – is your domain name.

@mydomain.local – is your Kerberos realm (as above).

-mapuser mydomain\FEXService – specifies the user to map (as above).

-ptype KRB5_NT_PRINCIPAL – specifies Kerberos version 5.

-pass – specifies the current password for the FEX service account.

-out FEX.keytab – is the name of the keytab output file.

After running the command, a keytab file is generated at the command prompt location.

For example: C:\Users\Username>ktpass -princ [...]

In the above scenario, the keytab file would be created at:

C:\Users\Username

Command to generate Kerberos keytab file:

ktpass -princ **FEXService/mydomain.local@mydomain.local** -mapuser **mydomain\FEXService** -ptype KRB5_NT_PRINCIPAL -pass <**yourpassword**> -out FEX.keytab

NOTE: Parameters in **bold** must be replaced with your own values.

IMPORTANT: The -princ parameter is case sensitive.

Merge keytab files (For multiple domains only)

1) Create a keytab file for any of the domains such as Mydomain1 and the keytab file name is FEXkeytabfromstep1. (See right)

2) Merge the Keytab file for working with the cross domain platform. (See right)

   NOTE: This step generates a single merged keytab file for mydomain1 and mydomain2 where keytab file for Mydomain2 will be created from step 2 and merged it with FEXkeytabfromstep1 and the output for the merged keytab file for both domain will be FEX.keytab.

3) Now the merged keytab file FEX.keytab will be used for the cross domain platform.

Command to generate Kerberos keytab file:

ktpass -princ **FEXService/Mydomain1.local@Mydomain1.local** -mapuser **Mydomain1\FEXService** -ptype KRB5_NT_PRINCIPAL -pass <**yourpassword**> -out **FEXkeytabfromstep1.keytab**

Command to merge keytab file:

ktpass -princ **KerberosUser2/Mydomain2.local@Mydomain2.local** -mapuser **Mydomain2\KerberosUser2** -ptype KRB5_NT_PRINCIPAL -pass **<yourpassword>** -in **FEXkeytabfromstep2.keytab** -out **FEX.keytab**

NOTE: Parameters in **bold** must be replaced with your own values.

IMPORTANT: The -princ parameter is case sensitive.

Verify the domain account is mapped

To verify that the user has been successfully mapped, perform the following steps:

1) Open **Active Directory Users and Computers**.

2) Find the **FEXService** user, right-click and select **Properties**.

3) In the **Properties** window, check that the **Delegation** tab is present. (See Figure 9)

   NOTE: The delegation tab should only appear if the user is correctly mapped on Kerberos KDC. If the delegation tab is not present, you should try again to map the user with KDC.

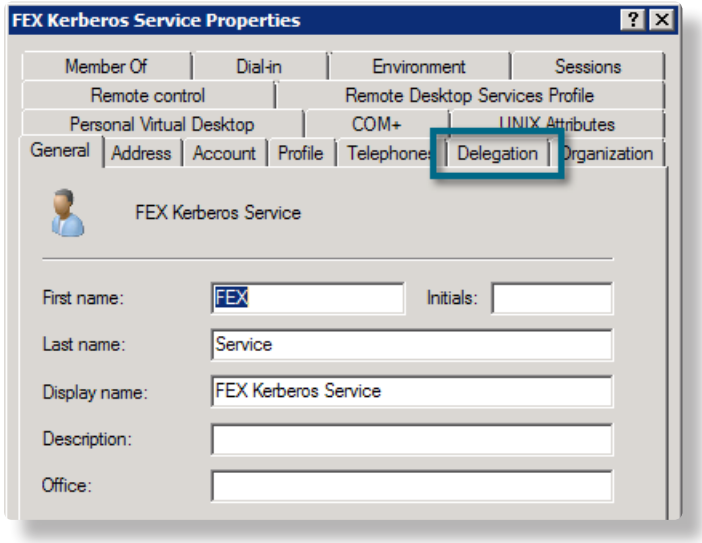

Figure 9

Configure FontExplorer X Server Windows services

> **NOTE:** This configuration step is not required for Macintosh Servers.

When installing FontExplorer X Server (For Windows), two Windows services are installed:

— FontExplorer X Server

— FontExplorer X Server Controller

(See Figure 10)

For Kerberos Authentication, both services must be started using the FontExplorer X Service account created earlier. To run the services under the required domain account, perform the following steps:

1) On the server machine, open the **Services** window. (services.msc)

2) Right-click on **FontExplorer X Server** and choose **Properties**.

3) From the **FontExplorer X Server Properties** window, select the **Log On** tab. (See Figure 11)

4) In the **Log On as** section, select the **This account** radio-button.

5) Enter the account details as created previously. (for example: mydomain\FEXService).

6) Click **OK**.

7) Perform the same steps with the **FontExplorer X Server Controller** service. (perform steps 2 to 6)

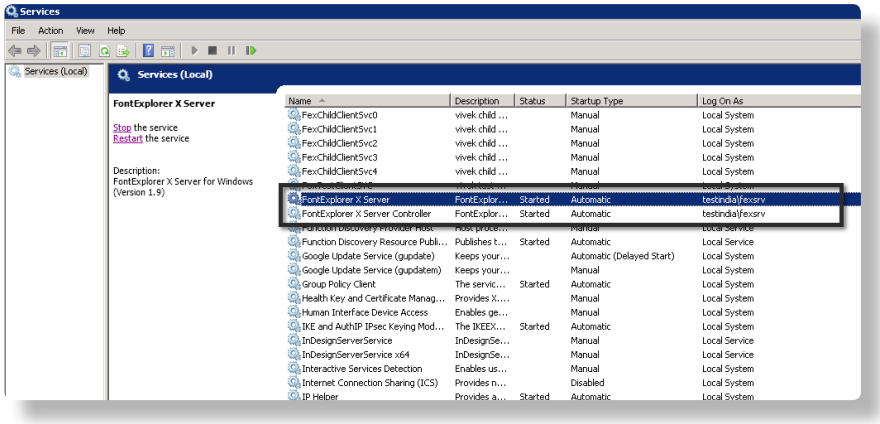

Figure 10

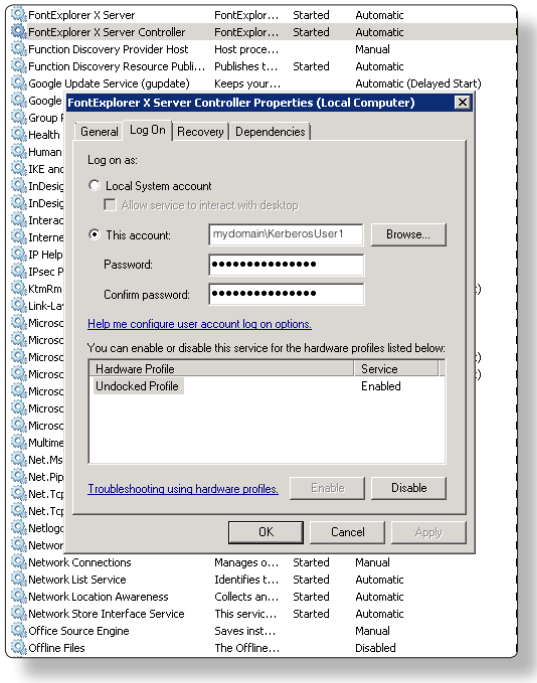

Figure 11

Configure user permissions

> **NOTE:** This configuration step is not required for Macintosh Servers.

In order to access the FontExplorer X Server files, the domain account used to start the FontExplorer X Server services must be added to the local “Administrators” user group on the server machine.

To apply the required rights, perform the following steps:

1) On the server machine, open the **Local Users and Groups** window (lusrmgr.msc). (See Figure 12)

2) Select the **Groups** folder.

3) Right click the **Administrators** group and choose **Properties**

4) Click **Add** and select the domain account used for the FontExplorer X Server services in the previous step (For example: mydomain\FEXService).

5) Click **OK**.

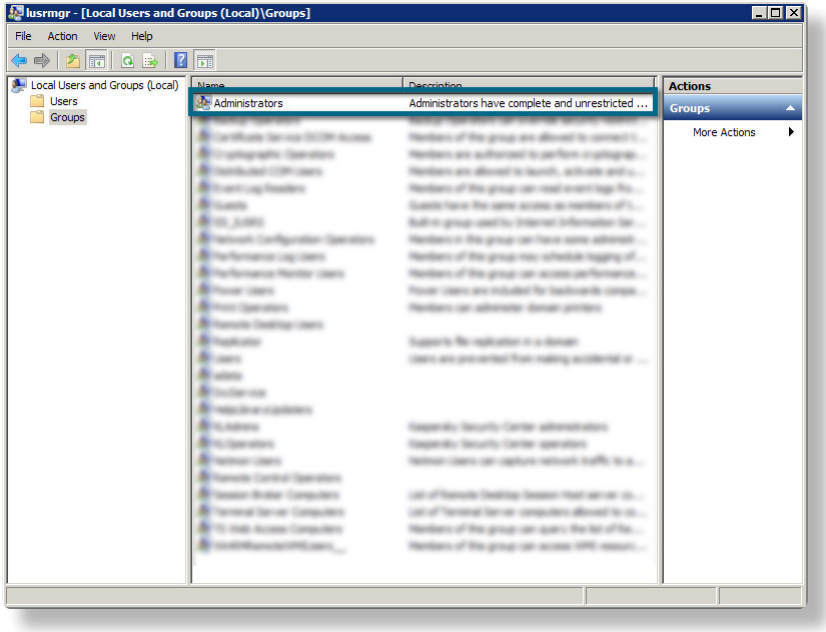

Figure 12

Apply the Kerberos keytab file

To configure the FontExplorer X Server to use Kerberos Authentication, you must apply the previously generated Kerberos keytab file via the FontExplorer X Server Control Panel (For both Mac and Windows Servers).

To apply the keytab file, perform the following steps:

1) Open the FontExplorer X Pro Server Control Panel and select the **Kerberos** tab.

2) Stop the FontExplorer X Server. (if already running)

3) Click **Select** and choose the Keytab file, generated previously. (FEX.keytab)

4) If successful, the panel will show "Kerberos keytab file is valid." and the Select option will now show "Remove". (See Figure 8)

5) Start the FontExplorer X Server.

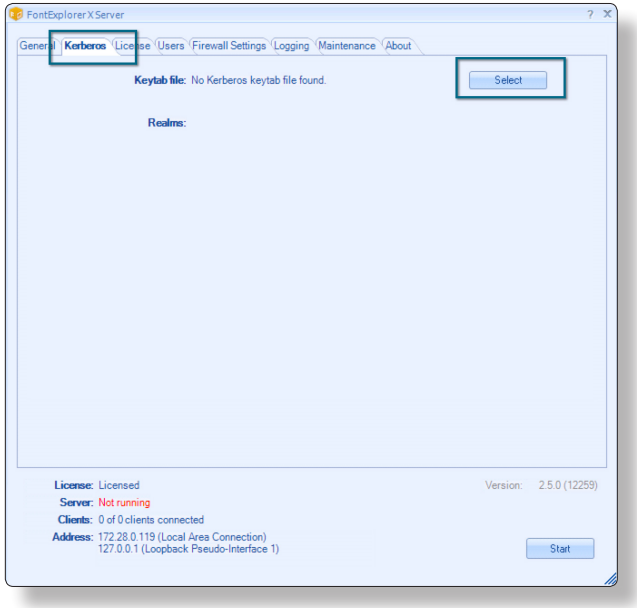

Figure 13

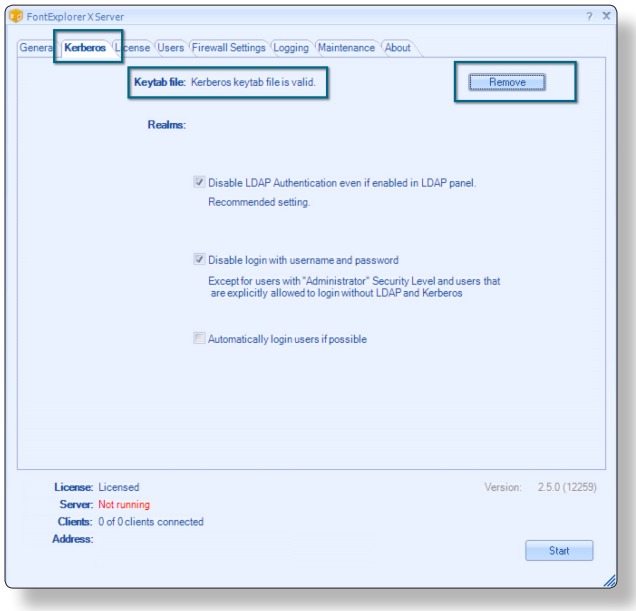

Figure 14

Import domain users for Kerberos Authentication

NOTE: If you have already imported users via LDAP, you can skip this step.

In order for domain users to login to the FontExplorer X Server using Kerberos Authentication, an administrator must first select and import those users.

To import users, perform the following steps:

1) Open the FontExplorer X Pro and login to your FontExplorer X Server using an account with the Administrator security level. (for example, the built-in 'admin' account).

2) In the left pane, select **Account Management** and choose the **LDAP** tab.

3) If not already configured, you will need to add your domain by entering your domain name, DSN and login details.

4) Select the **Import Users and Groups** tab and select your domain from the **Connection** menu.

5) Locate your users and check the box next to the accounts you wish to import.

6) If required, change the desired security level and click **Save** to import the selected users. (See Figure 15)

NOTE: Any domain users that are not imported to the Users tab will be unable to login to the FontExplorer X Server.

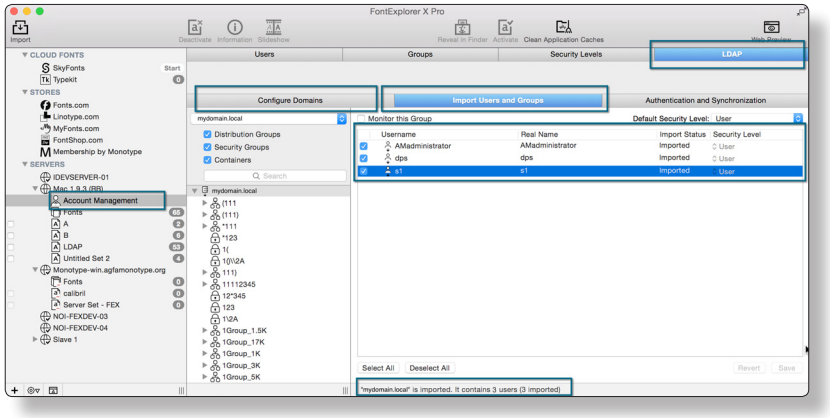

Figure 15

Test Kerberos Authentication in the FontExplorer X Pro

Having configured your server for Kerberos, you can perform the following steps to check that authentication is working correctly:

1) Start the FontExplorer X Pro.

2) Select your server on the left to reveal the **Summary and Login** panel.

3) Select the **Kerberos** radio button. The username field should be automatically populated with the username of the user currently logged on to the machine. (See Figure 16)

4) If desired, check **Login automatically to this server**.

5) Click **Login**.

NOTE: In order for Kerberos to function, the client computer must be a member of your domain and the user account selected for login must have been imported to your FontExplorer X Server.

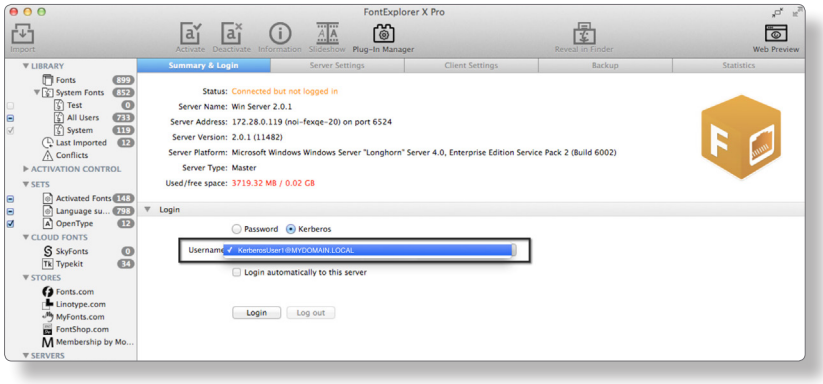

Figure 16

Support and Additional Information

Should you have questions regarding FontExplorer X Products, you will find further information on the FontExplorer X website at: (See right)

http://www.fontexplorerx.com

Or just contact us by email at: (See right)

support@fontexplorerx.com

Imprint

Monotype GmbH
Werner-Reimers-Strasse 2-4
61352 Bad Homburg
Germany

E-mail: info@fontexplorerx.com

Phone: +49 61 72 484-423
Fax: +49 61 72 484-499

Registered in Bad Homburg, commercial register no. HRB10375

Tax no. 03 238 18023
Local revenue office: Bad Homburg, Germany
VAT reg.no. DE250989316
Managing Director: Christopher Kollat