Kerberos Client Configuration

> ⚠ **Work in progress**
>
> This site is in the process of being reviewed and updated.

All Kerberos clients, including the Java Krb5LoginModule, require client configuration. Unfortunately, this is platform specific. This HOWTO covers configuration of Kerberos clients on various operating systems.

*NIX /etc/krb5.conf Configuration

On most UNIX platforms Kerberos clients look for the /etc/krb5.conf file. This file contains configuration settings for both servers and clients however we're only concerned with client configuration.

Minimum config file

At a minimum, you must configure your host so that it knows where to get Kerberos tickets. The minimum config file must list the default Kerberos realm and the location of at least one key distribution center (KDC).

Note that these configuration examples assume hostnames such as kdc.example.com will resolve on your network. If kdc.example.com is not found, you may see the error *Error getting credentials: Cannot resolve network address for KDC in requested realm*. Assuming you are running Kerberos on IP address '10.0.0.2', you can correct this with the following /etc/hosts entry.

```
10.0.0.2       kdc.example.com
```

In the [libdefaults] section the most important parameter to configure is the default_realm.

In the [realms] section you want to configure the EXAMPLE.COM realm. Remember case makes a difference and realm names need to be in all uppercase. In this section you can configure the server and port for the KDC. Apache Directory is the KDC and Kerberos by default runs on port 88.

In the [domain_realm] section we map the DNS domain name to the Kerberos realm name. Note that the first line has a '.' in front of the domain name.

Below is a minimal example krb5.conf configuration file from a Linux workstation setup for the EXAMPLE.COM realm:

```
[libdefaults]
 default_realm = EXAMPLE.COM

[realms]
 EXAMPLE.COM = {
  kdc = kdc.example.com
 }

[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
```

Slightly more advanced configuration

The [realms] section here demonstrates a few configuration options. First, you can adjust the service ports to connect to. Second, you can configure a **kpasswd_server**. This is for the Change Password protocol service which also runs on Apache Directory. The default port for the Change Password protocol is 464. The last parameter in this section is the **default_domain**. This is the DNS domain name to use to locate the **kdc** and the **kpasswd_server** if they cannot be resolved by the non-qualified host name specified.

```
[libdefaults]
 default_realm = EXAMPLE.COM

[realms]
 EXAMPLE.COM = {
  kdc = kdc.example.com:88
  kpasswd_server = kdc.example.com:464
  default_domain = example.com
 }

[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
```

Most advanced Linux configuration

You shouldn't have to get more advanced than this. While you can configure many parameters of tickets, like various times and encryption types, you shouldn't ever have to. You are better off setting realm-wide configuration on the KDC.

This example demonstrates how to configure resolution of KDC's in 2 realms. You would use a client configuration like this when you have configured cross-realm authentication, aka a "trust relationship."

```
[libdefaults]
 default_realm = EXAMPLE.COM

[realms]
 EXAMPLE.COM = {
  kdc = kdc.example.com
  kpasswd_server = kdc.example.com
 }

 EU.EXAMPLE.COM = {
  kdc = kdc.eu.example.com
 }

[domain_realm]
 .example.com = EXAMPLE.COM
 .eu.example.com = EU.EXAMPLE.COM
```

Some Kerberos clients

You can install kerberos clients from the apt repositories. A working GUI client is gnome-kerberos and the command-line tools can be found as krb5-workstation.

```
$ apt-get install gnome-kerberos
```

or

```
$ apt-get install krb5-workstation
```

When you run the gnome-kerberos client (/usr/bin/krb5) after a fresh install, you will see that the EXAMPLE.COM domain is already configured.

Windows krb5.ini Configuration

Windows uses the same exact file format as does *NIX platforms (meaning syntax) except the name of the file is different and the file paths inside are Windows file paths. Other than this you can use the same information above for configuring Windows Kerberos client settings.

Even though different Windows versions have different system directories (i.e. C:\Windows or C:\WINNT) the krb5.ini file is always expected to be present within the C:\WINNT directory even if there exists a C:\Windows directory and no WINNT directory. If the C:\WINNT directory does not exist just create it and add this file.

MacOSX Kerberos Configuration

The Kerberos configuration on MacOSX is stored in a plist configuration file named edu.mit.Kerberos.KerberosLogin.plist. It contains imilar settings as the krb5.conf file however it is located in specific places. More details on how to configure MacOSX for Kerberos consult the following page:

http://web.mit.edu/macdev/KfM/Common/Documentation/preferences-osx.html

There is however a fallback to use a krb5.conf file in /etc for UNIX compatibility mode.