How do I configure SSH to always delegate my Kerberos tickets?

Q: How do I configure SSH to always delegate my Kerberos tickets?

Answer

> **Delegation and athena.dialup.mit.edu**
> When using Kerberos over SSH, you can choose to merely use Kerberos to authenticate yourself, or you can choose to use Kerberos to delegate your tickets in addition to authentication. While some workstations may let you log in without delegation, `athena.dialup.mit.edu` does not. The reason for this is that without delegation, `athena.dialup.mit.edu` cannot obtain Kerberos tickets for you to use once logged in, and cannot obtain AFS tokens necessary to access your files. Rather than let you end up logged in without access to your files, athena.dialup.mit.edu requires that you delegate tickets, use traditional password-based authentication, or explicitly opt-in to public-key authentication.

Most ssh client configurations (such as those on MacOS X and Ubuntu) do not delegate (forward) Kerberos tickets by default, to avoid inadvertently exposing your Kerberos tickets to a malicious machine. Normally, you must use **ssh -K** to delegate your tickets on a per-connection basis. For example, instead of typing:

```
ssh athena.dialup.mit.edu
```

you would now type:

```
ssh -K athena.dialup.mit.edu
```

NOTE for Mac OS X: Kerberos Extras will configure your ssh client to delegate kerberos tickets.

Delegating by default

If you wish to delegate your tickets by default, you can add a line like the following to your `~/.ssh/config` file:

```
Host athena.dialup.mit.edu
    GSSAPIDelegateCredentials yes
```

That will cause ssh to delegate your credentials when connecting to athena.dialup.mit.edu (but not when connecting to other machines). You can specify multiple hosts like so:

```
Host athena.dialup.mit.edu some-other-machine.mit.edu
    GSSAPIDelegateCredentials yes
```

You can even specify wildcards, though we do not recommend you do this:

```
Host *.mit.edu
    GSSAPIDelegateCredentials yes
```

On MacOS Big Sur, if you want to use kinit on the command line, you need to explicitly configure where the ticket cache is; in .bashrc, either

```
export KRB5CCNAME=KCM:uid
```

or

```
export KRB5CCNAME=/tmp/tkt_username (a valid file name)
```

It will also work if you use the ticket viewer application to get tickets, and leave KRB5CCNAME unset.