Installing and Configuring Shibboleth 2.x on Mac OS X 10.6.x Server

Installing and Configuring Shibboleth 2.x on Mac OS X 10.6.x Server

Notes

- Your server must have a static IP address, and valid DNS
- Your server must have the MIT CA installed in it's System Keychain. See the "Install the MIT CA (Certificate Authority)" section on Install and Renew Certificates in Safari on Mac OS X 10.6 for detailed instructions.

Installing an MIT Server Certificate for SSL

1. Obtain a certificate signed by the MIT Certificate authority
2. Launch Server Admin
3. Select the **Server > Certificates > '+' > Import a Certificate Identity**
4. Drag the file containing your private key, https-key.pem from step 1, to the sheet
5. Drag the file containing your certificate, returned by mitcert@mit.edu from step 1, to the sheet
6. Press **Import**
7. Start the Web service if it's not already running
8. Select the Server and press the triangle to list the services
9. Select **Web > Sites** and press **+** to add a new site
10. Enter the server's host name in the host name field
11. Check the Enabled box next to this new site
12. Select the **Security** tab
13. Check "Enable Secure Sockets Layer (SSL)"
14. Press **OK** to the "Site port changed" warning
15. From the Certificate pull down menu, select the certificate you installed above
16. Press **Save**
17. Press **Restart** when asked if you want to restart Web now.
18. Launch Terminal.app
19. Run `sudo -s`
20. Run `cd /etc/apache2`
21. Run `mkdir certs`
22. Run `chmod 700 certs`
23. Copy your private key and certificate, from step 1, into /etc/apache2.
24. Run `chmod -R 600 certs/*`

You should be able to connect to your server via http and https.

Install Shibboleth

1. Install Xcode, found on the Mac OS X 10.6 (Snow Leopard) install DVD
2. Download and run the MacPortsinstaller
3. Launch Terminal.app
4. Run `port selfupdate`
5. Run `sudo -s`
6. Run `port install curl +ssl`
7. Run `port install shibboleth`

Configure Shibboleth

1. Launch Terminal.app
2. Run `sudo -s`
3. Run `cd /private/etc/apache2`
4. Run `echo "Include /opt/local/etc/shibboleth/apache22.config" >> httpd.conf`
5. Run `perl -pi -e 's/UseCanonicalName Off/UseCanonicalName On/' httpd.conf`
6. Run `/usr/sbin/apachectl restart`

7. Run `launchctl load -Fw /Library/LaunchDaemons/org.macports.shibd.plist`
8. Run `touch /opt/local/var/log/httpd/native.log`
9. Run `chown _www /opt/local/var/log/httpd/native.log`
10. Run `cd /opt/local/etc/shibboleth`
11. Run `scp username@athena.dialup.mit.edu:/afs/athena.mit.edu/project/touchstone/config/shibboleth2-sp/. .` where `username` is your Athena username.
12. Run `sh gen-shib2.sh`
13. Press **Return**
14. Enter the full path to your certificate file, found in /etc/apache2/certs.
15. Enter the full path to your private key file, found in /etc/apache2/certs.
16. To get information about authenticated users, you must first register your application as described in the Letting the IdP know about your application section of Touchstone Provisioning Steps.
17. Run `mkdir /Library/WebServer/Documents/secure`. This directory will be restricted to all authenticated users by default. To enable .htaccess files, you'll need to add "AllowOverride AuthConfig" to the "<Location /secure>" section of /opt/local/etc/shibboleth/apache22.config, as well as remove the "require valid-user" line. You'll need to restart apache after making these changes. Once restarted, you can add .htaccess files to limit access to any directory in /Library/WebServer/Documents/secure. To limit access to bob@mit.edu and sue@mit.edu, the .htaccess file would contain "require user bob@mit.edu sue@mit.edu". Note: moira groups are note supported.

Upgrading Shibboleth

1. Launch Terminal.app
2. Run `sudo -s`
3. Run `port sync`
4. Run `port upgrade shibboleth`