Sauce Connect Proxy Certificate Handling

The security of Sauce Connect Proxy communication to both the Sauce Labs API and the virtual machine hosting your tests in the Sauce Labs cloud is managed through public key certificates.

For connection to the API, Sauce Connect Proxy uses certificates issued by certificate authorities, which are are integrated into the operating system of the machine where Sauce Connect Proxy is running.

For connection to the Sauce Labs virtual machines, the certificate presented by the tunnel endpoint is signed by public certificate authorities.

See the following sections for more information:

Setting Revocation Information for SSL Certificate Verification

When securing Sauce Connect Proxy, be sure to whitelist these sites so that the Sauce Connect SSL certificates can be verified:

> **OCSP**: http://gp.symcd.com
>
> **OCSP Servers for VDC/RDC clouds**: http://ocsp.digicert.com, http://status.geotrust.com
>
> **OCSP Servers for Headless**: http://ocsp.int-x3.letsencrypt.org, http://isrg.trustid.ocsp.identrust.com

Sauce Connect Proxy will try to resolve the entire certificate chain at runtime and check if it can reach the OCSP servers in the entire chain. Because the chain is resolved during runtime and certificates change and are constantly renewed, it's possible that the OCSP sites listed in the certification check might change over time as well.

In your log, look for the entries following the `"checking OCSP entry"` line to get the list of certificate authority sites.

In addition to whitelisting these sites, consult the list of domains at the RapidSSL website and add them to your whitelist as well to make sure that Sauce Connect can connect to all appropriate certificate-issuing authorities.

OCSP Tunnel Certificate Validation

This feature lets the Sauce Connect client validate that the tunnel endpoint's public certificate has not been revoked. OCSP relies on Public Key Infrastructure and needs to make additional HTTP requests to OCSP servers associated with the tunnel endpoint’s certificate chain.

You can set your own parameters (e.g., logging, bypassing OCSP checks) by using OCSP command line arguments. In addition to OCSP-specific commands, OCSP supports the following: `--kgp-host, --kgp-port, --proxy, --pac, --no-autodetect, --proxy-tunnel, --tunnel-cainfo, --tunnel-capath`.

Connecting to the Sauce Labs REST API

Connections to the Sauce Labs API go through `https://saucelabs.com`. The way in which Sauce Connect is able to access the certificates to secure the connection depends on the operating system of the machine where Sauce Connect is installed.

Linux

On Linux machines, Sauce Connect will look for the directory where the certificate bundle is installed, typically something like `/etc/ssl/certs`. If it can't find the directory, it will generate an error when trying to connect to the Sauce Labs API.

Windows

On Windows machines, certificates are managed through the Security Support Provider Interface API over SChannel, which requires access to OCSP URL s to verify certificates. If you have set up highly restrictive firewalls or proxies on the machine where Sauce Connect is running and it can't connect to these URLs, you'll get an error when attempting to connect to the Sauce Labs API.

OS X

On OS X machines, certificates are pre-installed as part of the Trust Store and are accessible through the Keychain. If Sauce Connect is installed on an OS X machine, no troubleshooting should be necessary as long as it can access the Keychain.

Tunnel Connection to the Sauce Labs Virtual Machine over SSL/TLS

Sauce Connect Proxy reverses tunnel VM-to-test target traffic through the TLS connection from Sauce Connect-to-tunnel endpoints. Your Selenium and Appium webdriver traffic is sent over `http(80)` or `https(443)` to `ondemand.saucelabs.com`, which has its own TLS certificate that's then passed to the test VM.

Sauce Connect Proxy versions 4.6.0+ will default to the public certificate.

More Information

- Securing Sauce Connect Proxy
- Sauce Connect Proxy and SSL Certificate Bumping