
JNUC
2019

Daniel MacLaughlin

Implementation Engineer
Jamf

MDM Not Working? Was It the Proxy?

Presentation agenda:

What do we mean when we say “Proxy”

Different “Proxy” configurations

How does it impact MDM and Apple

Who’s Security is better?

Troubleshooting, Takeaways and Q’s maybe A’s

Whats in a Name?

proxy *noun*

\ ˈpräk-sē \

plural **proxies**

Definition of *proxy*

1 : the agency, function, or office of a deputy who acts as a substitute for another

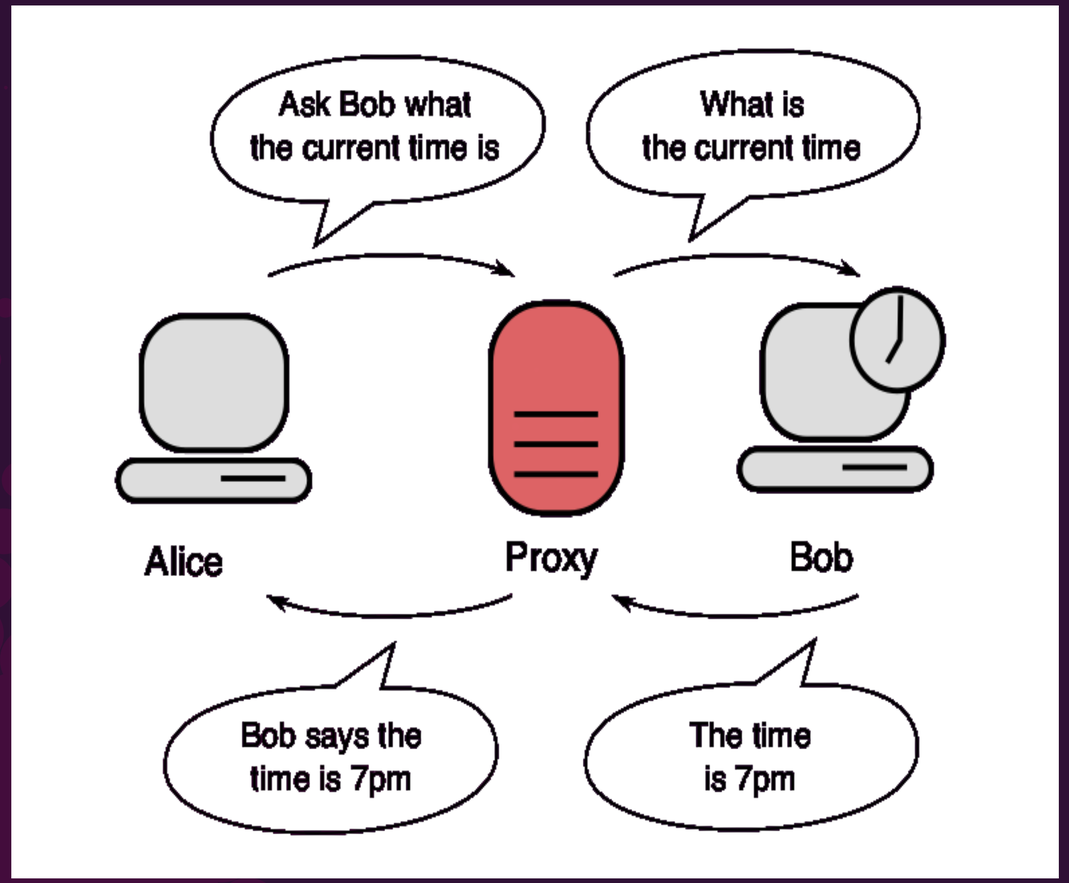
2 **a** : authority or power to act for another

b : a document giving such authority

specifically : a power of attorney authorizing a specified person to vote corporate stock

3 : a person authorized to act for another : PROCURATOR

Proxy in a Tech Sense

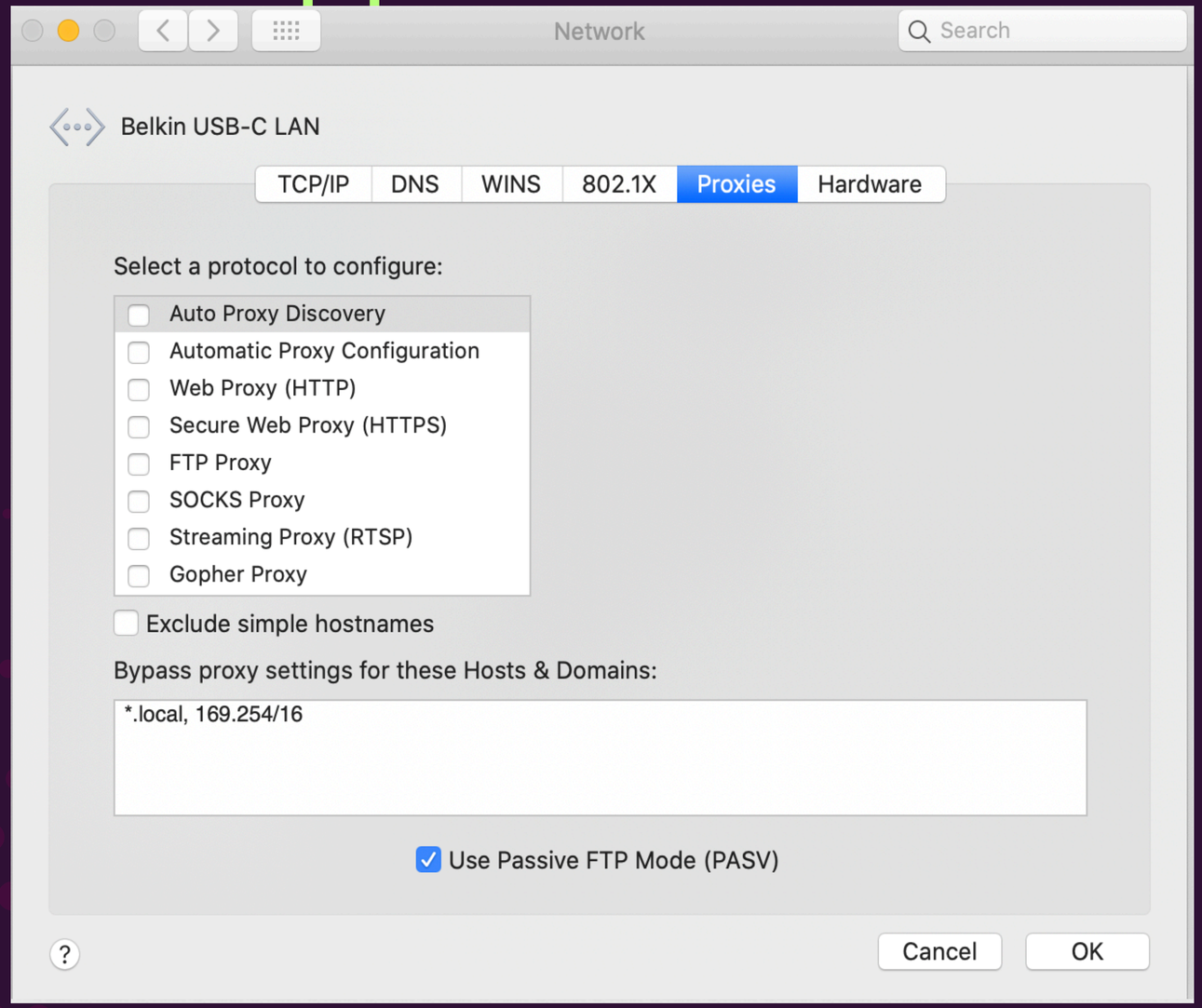


Alice isn't talking to Bob directly.

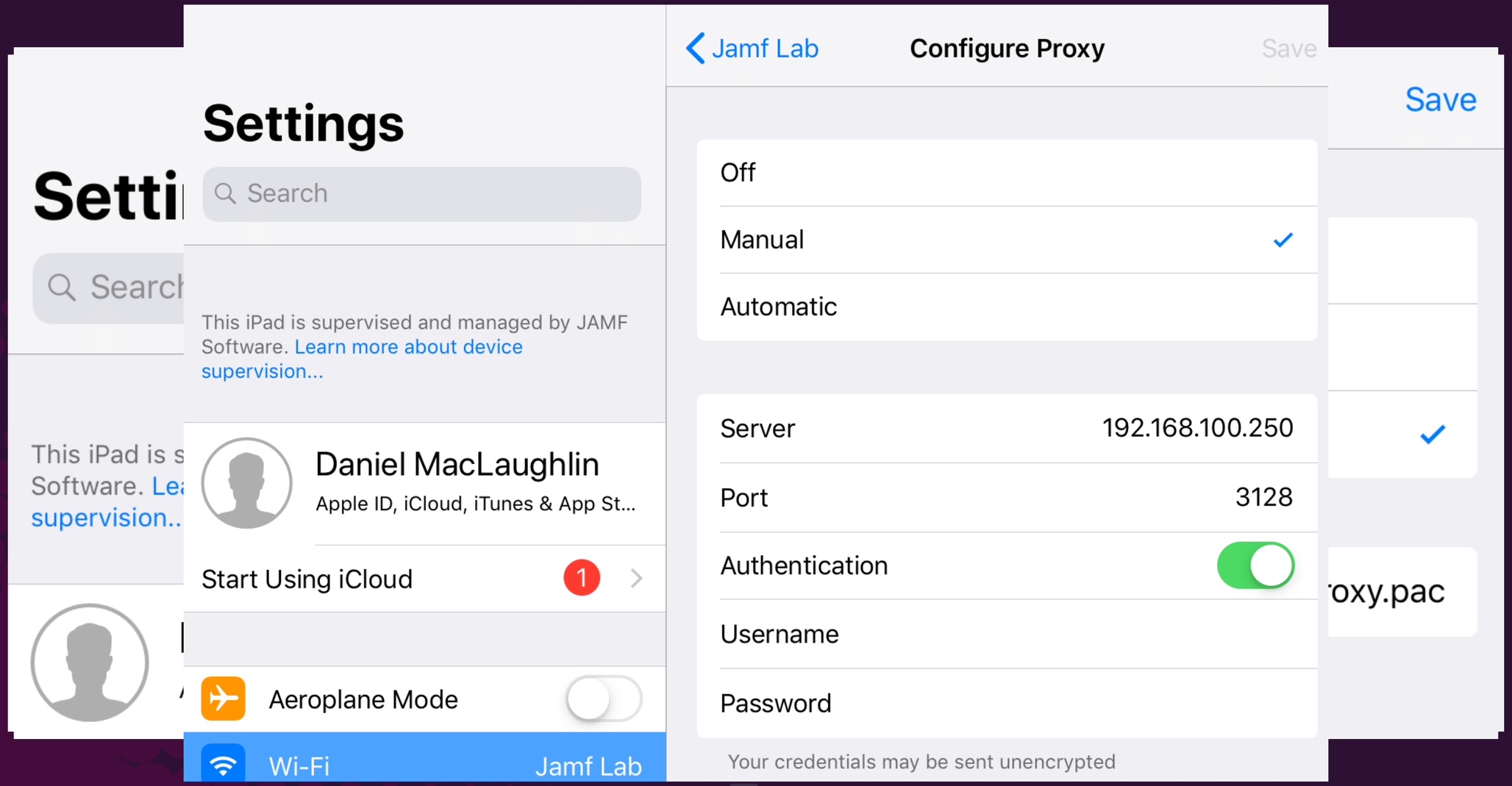
Bob doesn't see a request from Alice.

The Proxy is acting like a relay.

Proxies and Apple



Proxies and Apple



Proxies and Apple

Proxies and Apple

```
function FindProxyForURL(url, host) {

// If the hostname matches, send direct.
    if (dnsDomainIs(host, "intranet.domain.com") ||
        shExpMatch(host, "(*.abcdomain.com|abcdomain.com)"))
        return "DIRECT";

// If the protocol or URL matches, send direct.
    if (url.substring(0, 4)=="ftp:" ||
        shExpMatch(url, "http://abcdomain.com/folder/*"))
        return "DIRECT";

// If the requested website is hosted within the internal network, send direct.
    if (isPlainHostName(host) ||
        shExpMatch(host, "*.local") ||
        isInNet(dnsResolve(host), "10.0.0.0", "255.0.0.0") ||
        isInNet(dnsResolve(host), "172.16.0.0",  "255.240.0.0") ||
        isInNet(dnsResolve(host), "192.168.0.0",  "255.255.0.0") ||
        isInNet(dnsResolve(host), "127.0.0.0", "255.255.255.0"))
        return "DIRECT";

// If the IP address of the local machine is within a defined
// subnet, send to a specific proxy.
    if (isInNet(myIpAddress(), "10.10.5.0", "255.255.255.0"))
        return "PROXY 1.2.3.4:8080";

// DEFAULT RULE: All other traffic, use below proxies, in fail-over order.
    return "PROXY 4.5.6.7:8080; PROXY 7.8.9.10:8080";

}
```

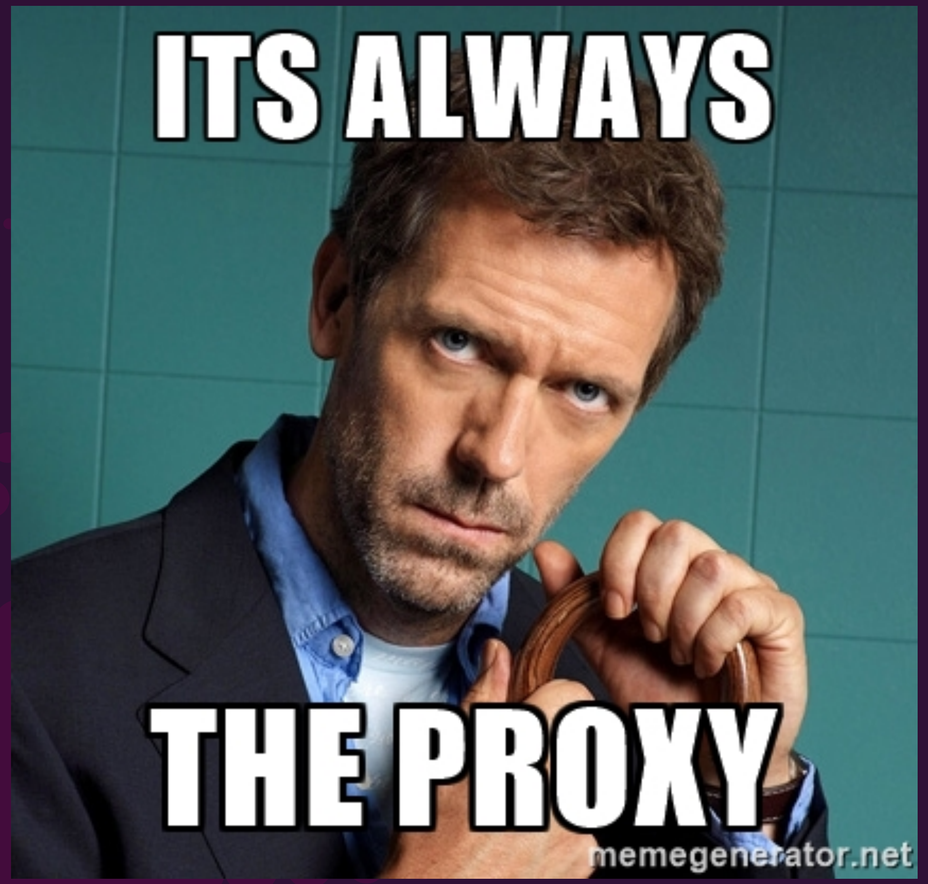
So Whats the Problem?

Did we miss something?

Why are there options?

Is it or Isn’t it Supported?

It’s Always the Proxy

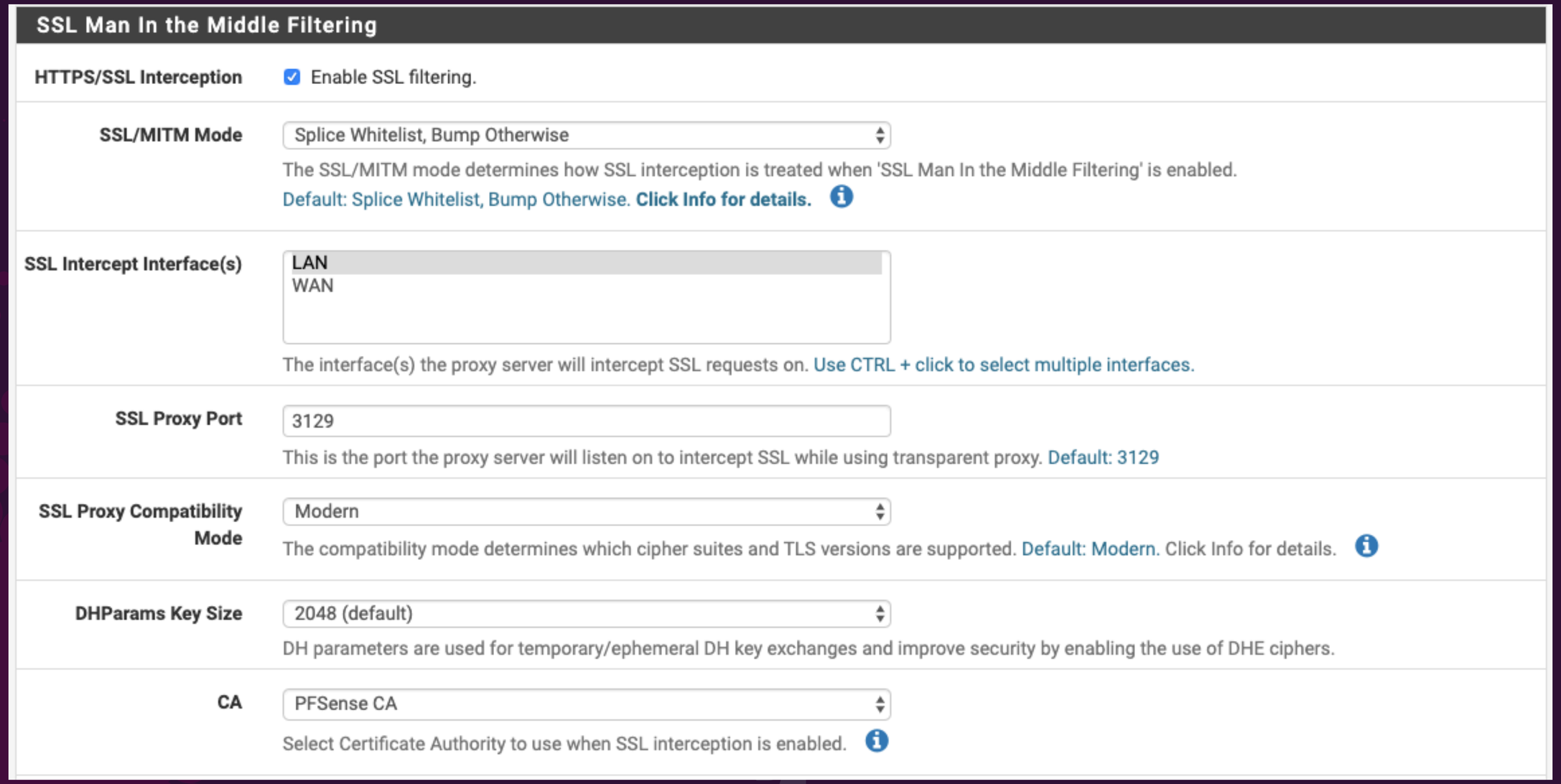


Well there is something

Its called SSL inspection

It’s not supported!

It’s Always the Proxy



Proxies and Apple

Check required ports

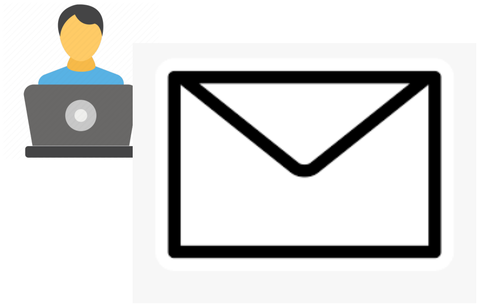
If you use Wi-Fi behind a firewall, or private Access Point Name for cellular data, connect to specific ports.

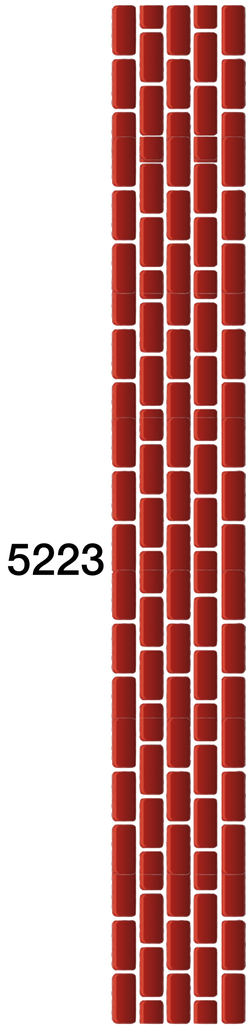
I have received an answer from Firebase support team about this question. The answer is below:

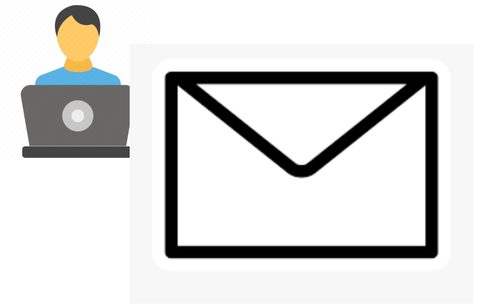
> Please note that FCM do not support Proxy at the moment, however we will take a note of this and we could consider it moving forward. I can't give you a definite timeline for this, rest assured your feedback has been acknowledged. We are constantly working on providing developers a more friendly experience hence your inputs are greatly appreciated.

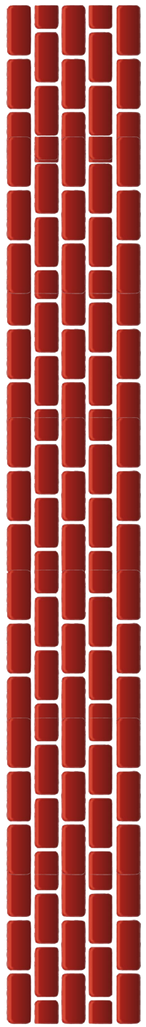
The APNs servers use load balancing, so your devices don't always connect to the same public IP address for notifications. It's best to let your device access these ports on the entire 17.0.0.0/8 address block, which is assigned to Apple.

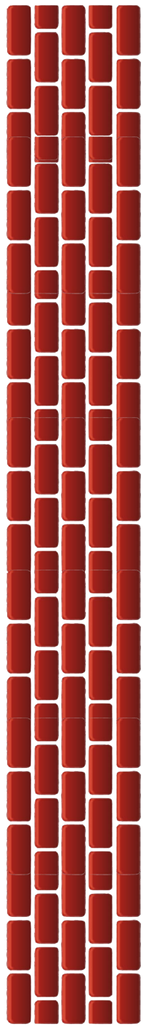
Windows clients **do not** support all proxies, the connection to WNS must be a direct connection.

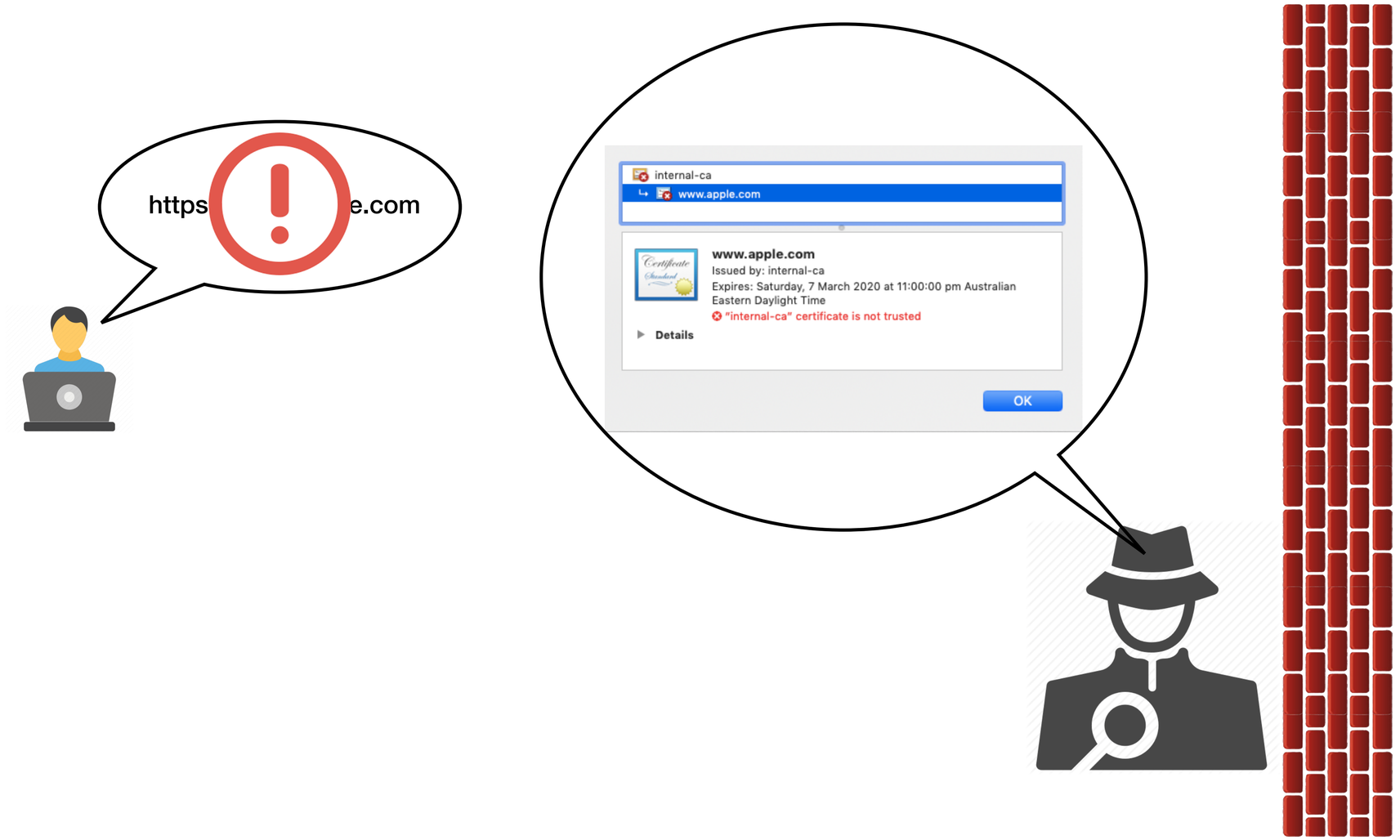




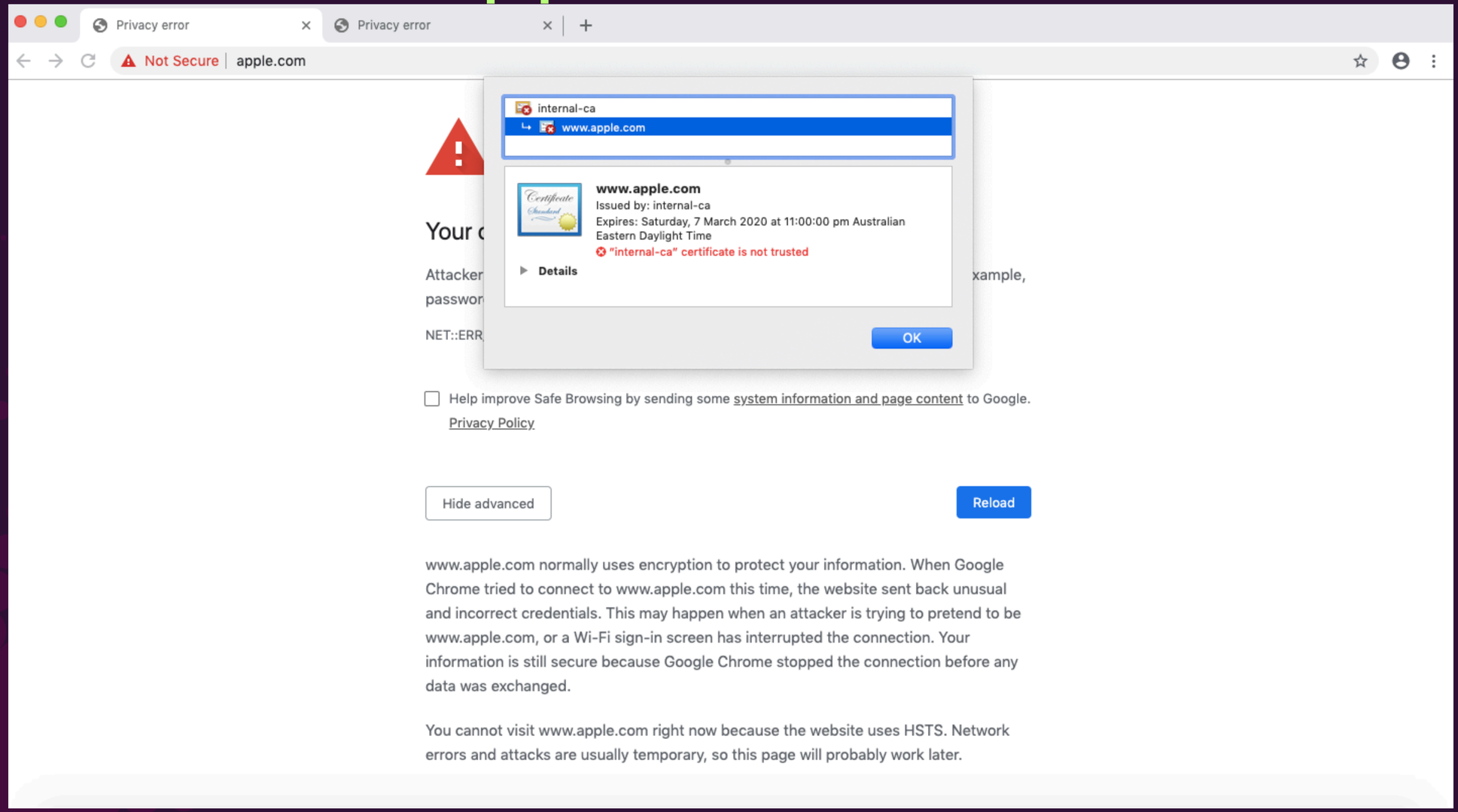


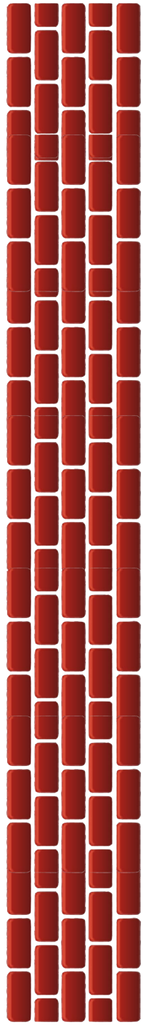




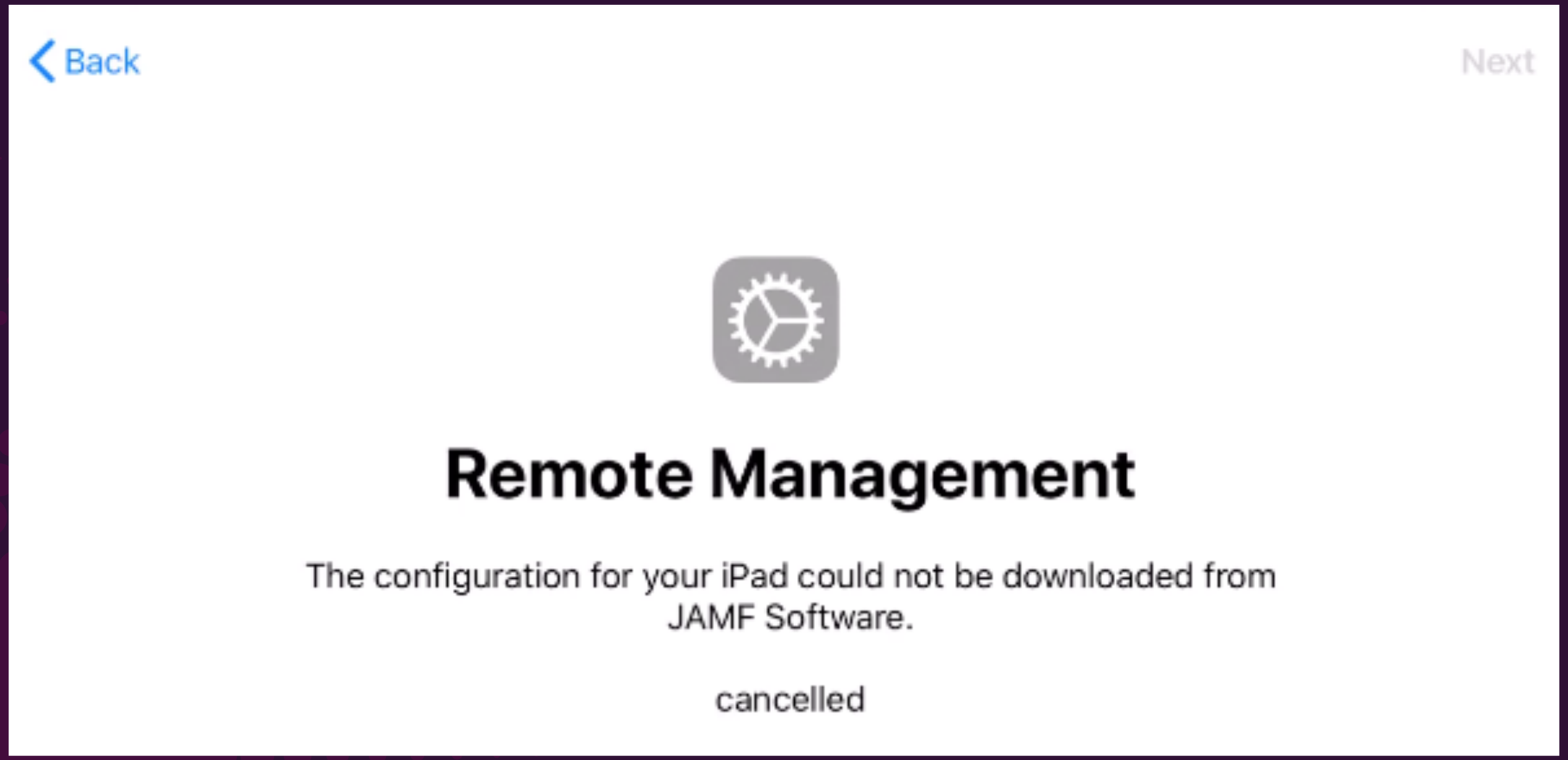


Proxies and Apple



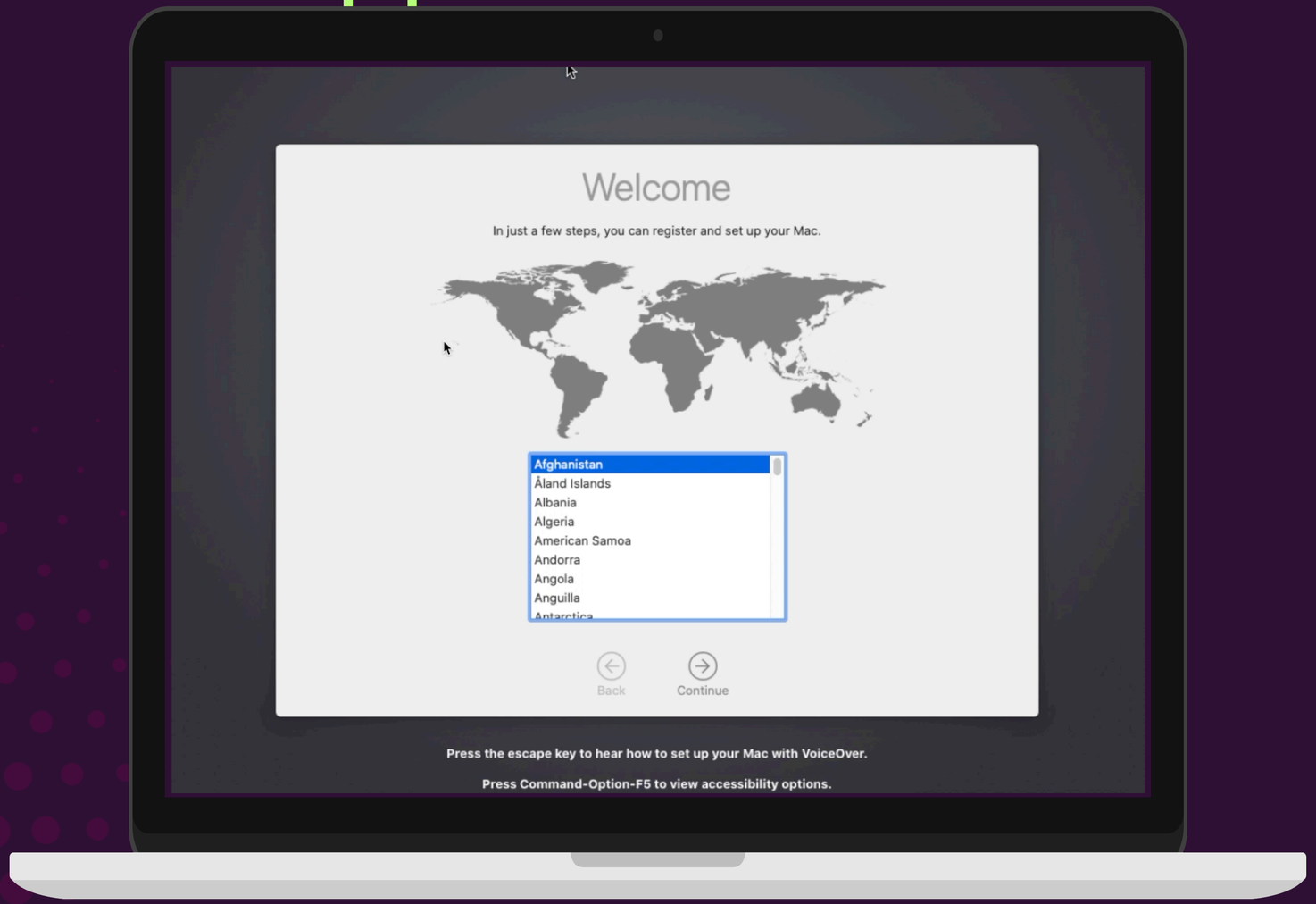


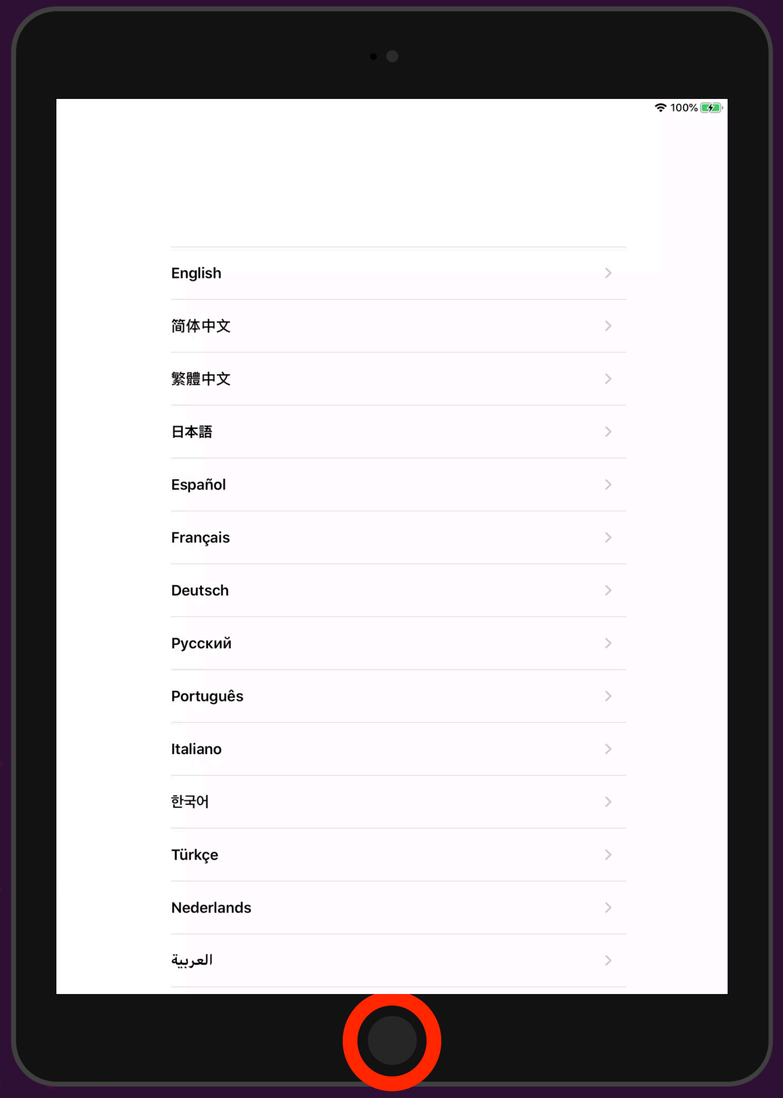
Proxies and Apple



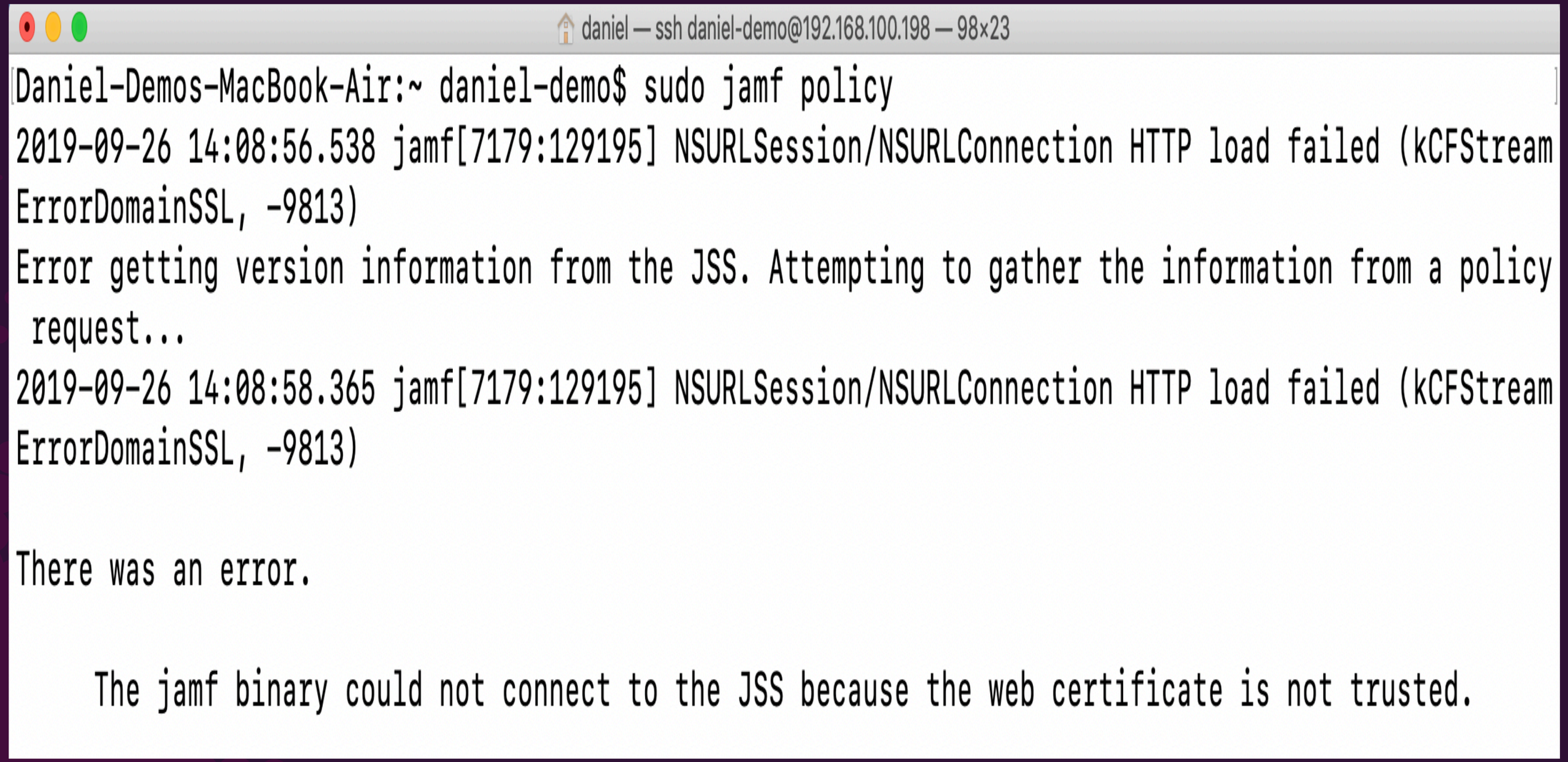
Proxies and Apple

Proxies and Apple





Proxies and Apple

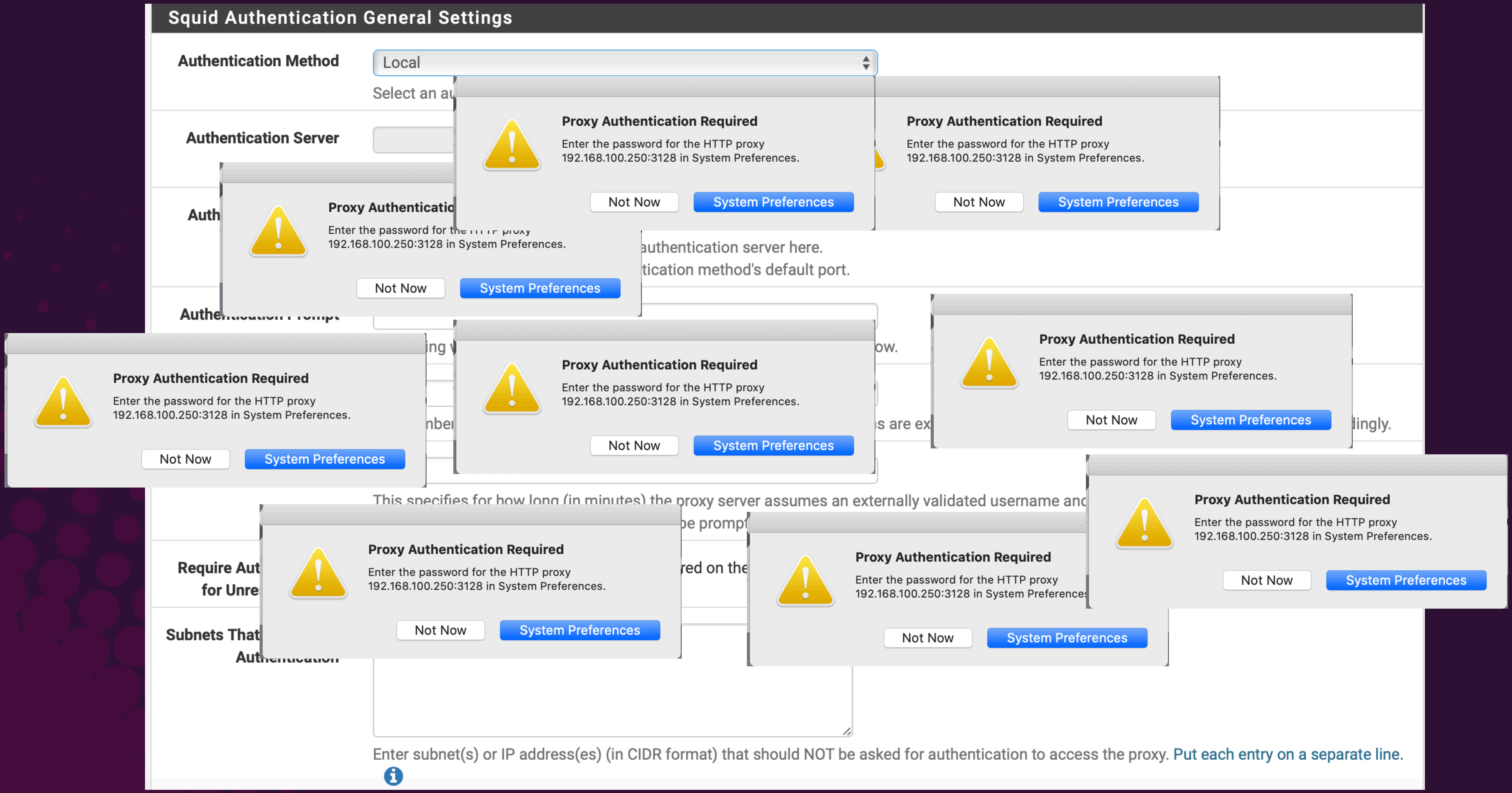


Proxies and Apple

Ok Network admin has whitelisted Apple to bypass SSL inspection

Why is it still not working?

Is it always the proxy?

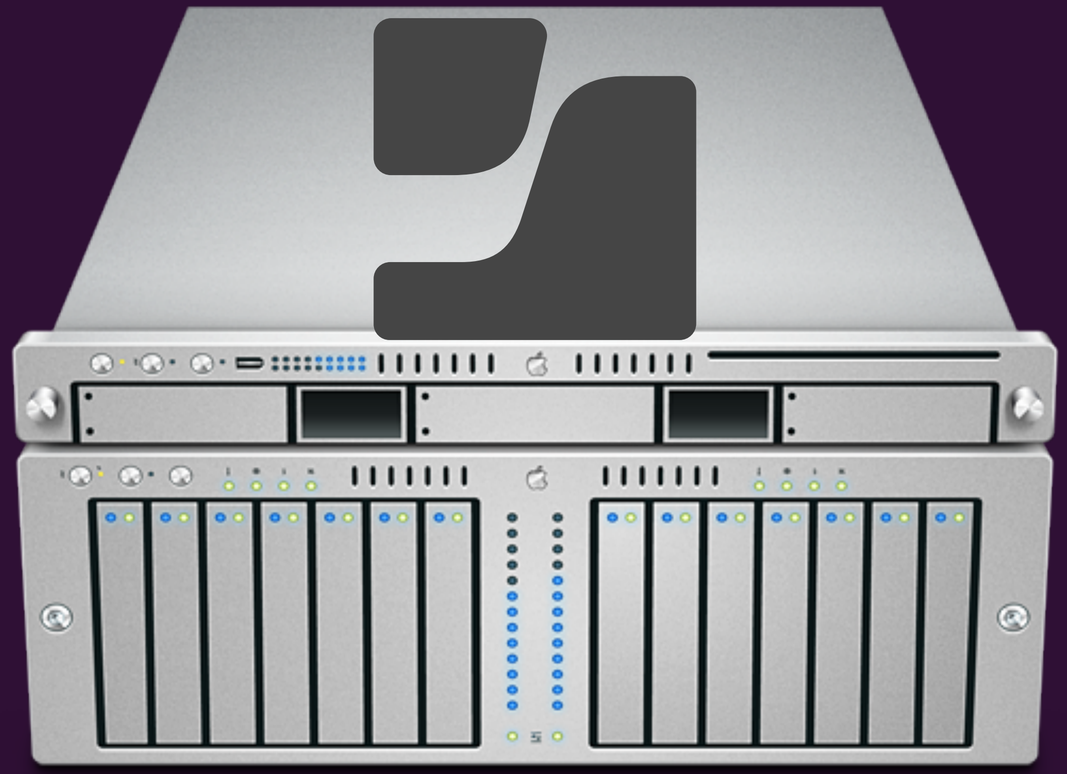


Proxies and MDM

What about the MDM

My Server is On-Prem

Will I still have issues?



Proxies and MDM

Configuring Jamf Pro to use an HTTP Proxy Server for Communications with Automated Device Enrollment and Volume Purchasing

Posted: 10/3/2014 at 3:13 PM CDT

Modified: 10/29/2019 at 11:44 AM CDT

Jamf Pro, DEP

Overview

This article explains how to configure Jamf Pro to use an HTTP proxy server for communications with Automated Device Enrollment (formerly DEP) and Volume Purchasing (formerly VPP).

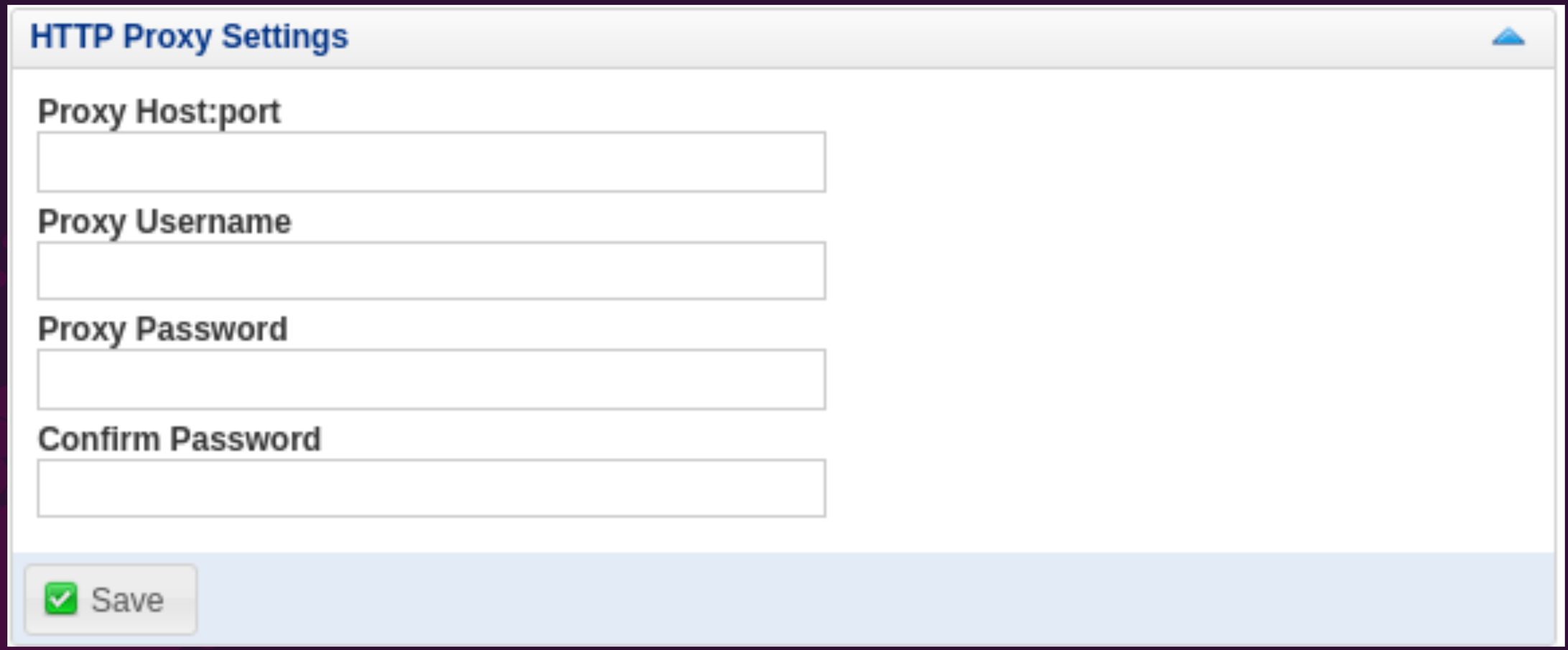
Versions Affected

Jamf Pro 9.52 or later

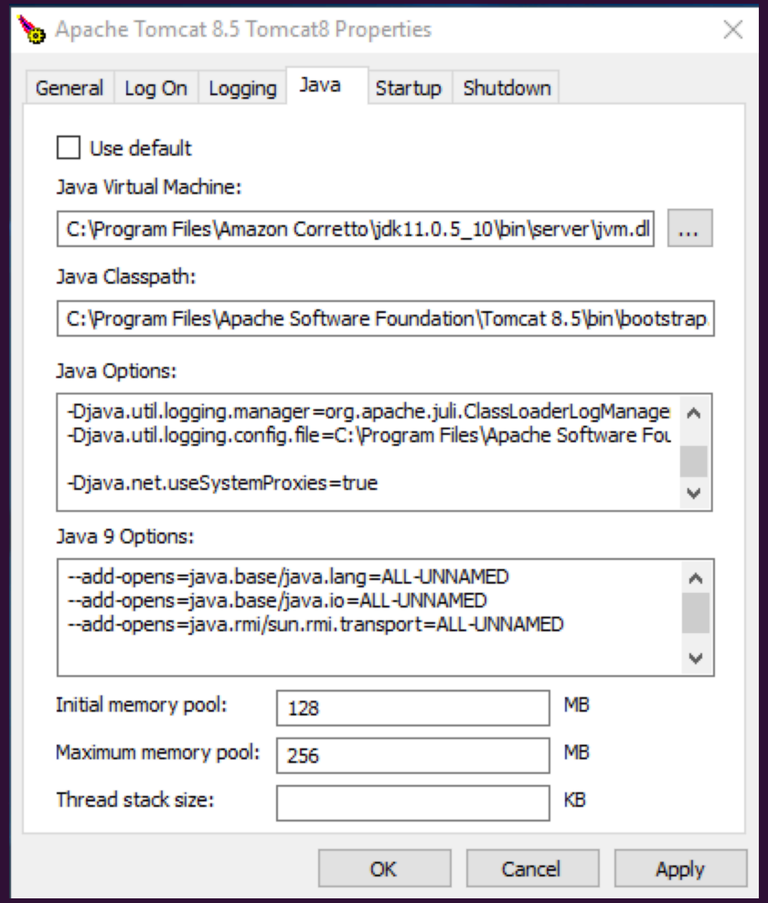
Procedure

There are two ways to configure Jamf Pro to use an HTTP proxy server for Automated Device Enrollment and Volume Purchasing. Jamf Pro can either use HTTP proxy server settings stored in the jamfsoftware database or use settings specified in the JVM (Java Virtual Machine) properties. Follow the procedure below for your desired method.

Proxies and MDM



Proxies and MDM



Certificate Security

OCSP Stapling

Cert Trust Anchors

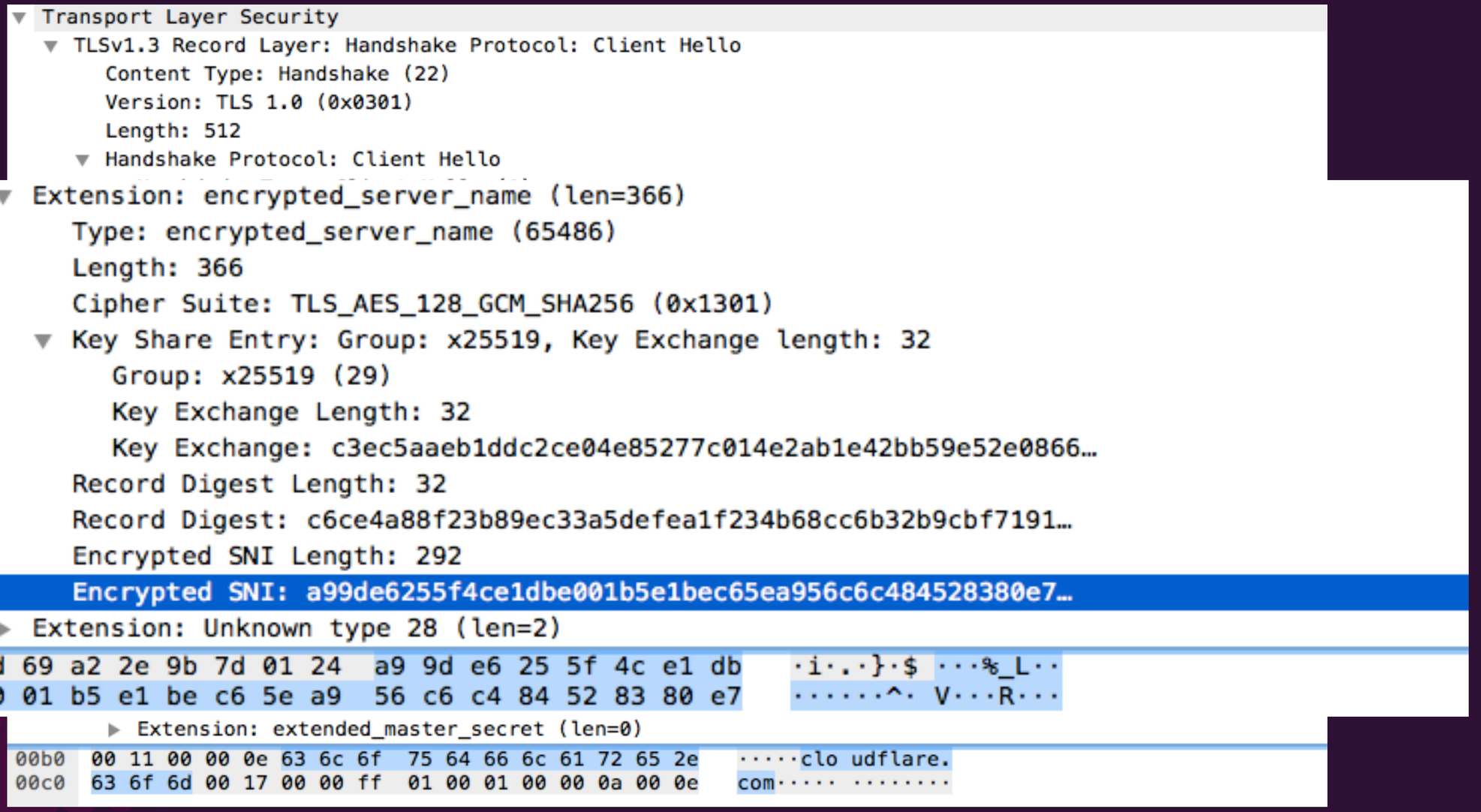
More Certificate Security

Transparent Proxies

Explicit Proxies

There’s this thing called

TLS 1.3 and SNI or ESNI



Prove its the Proxy

You have to get some logs

Packet captures

Even from the proxy server

Getting Packet Captures

For MacOS we can use 3rd party tools like:

Charles Proxy and WireShark

Local Tools:

tcpdump

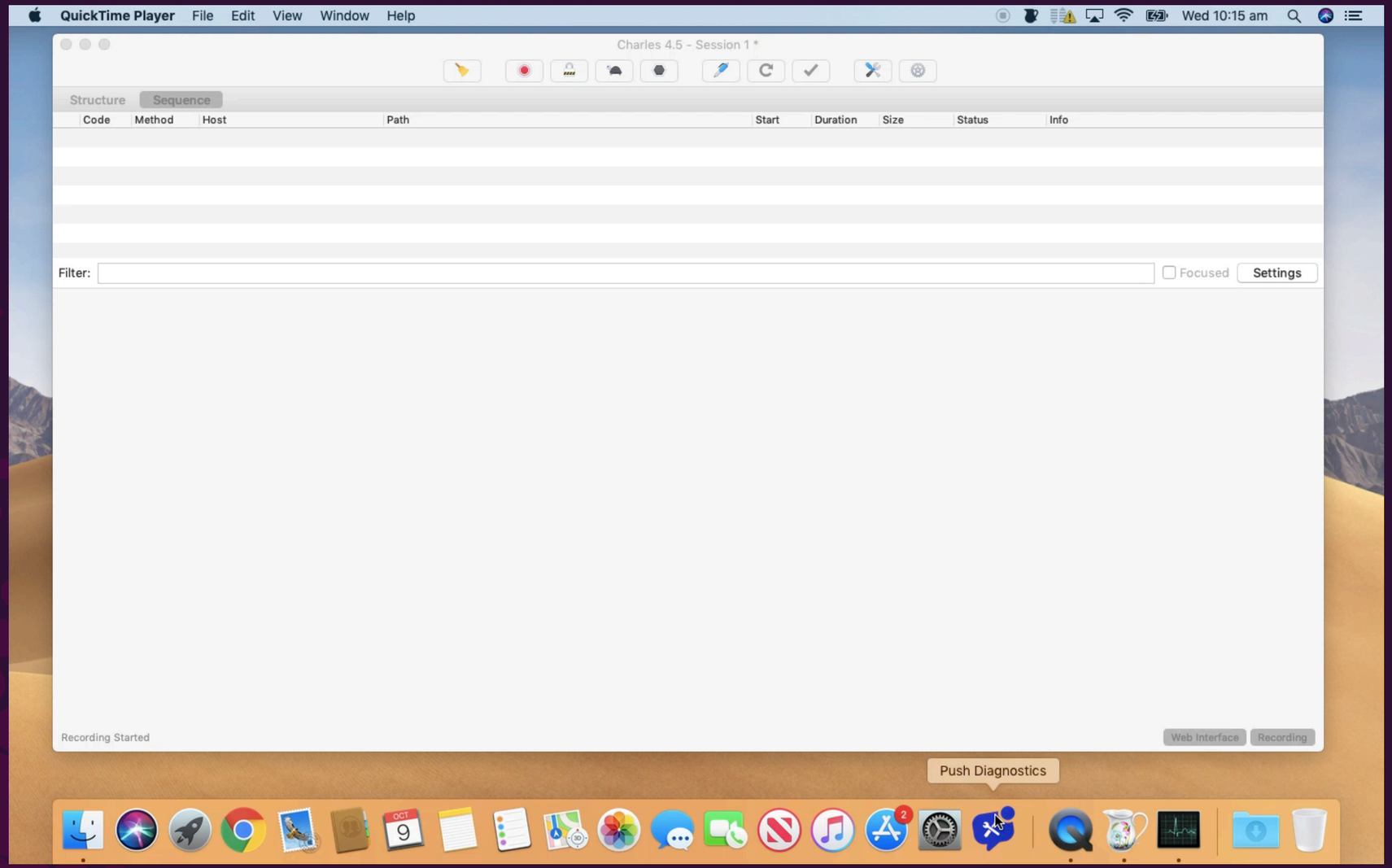
For iOS:

Apple Configurator 2

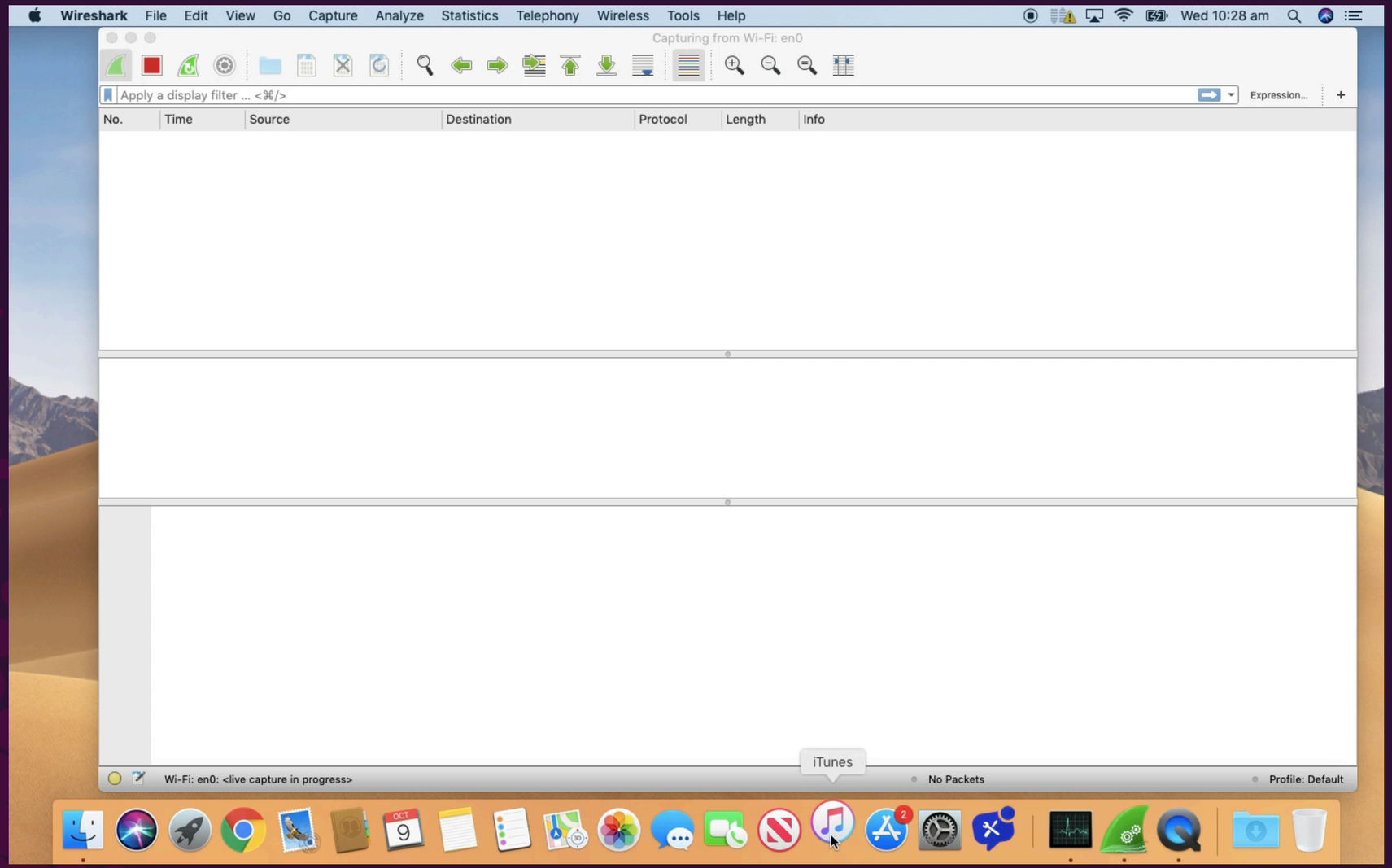
WireShark using rvictl

tcpdump using rvictl

What are we looking for



What are we looking for



Takeaways

- Don’t use manual settings
- Do use explicit over transparent
- Some URLS just gotta be un-authed
- Don’t inspect SSL

Links

Not Getting Push:

https://support.apple.com/en-us/HT203609

Use Apple on Enterprise Networks:

https://support.apple.com/en-us/HT210060

Getting Started with ABM or ASM with MDM

https://support.apple.com/en-us/HT207516

Enterprise Firewall for WNS:

https://docs.microsoft.com/en-au/windows/uwp/design/shell/tiles-and-notifications/firewall-allowlist-config

Network Ports used by Jamf Pro

https://www.jamf.com/jamf-nation/articles/34

Links

Configuring the JSS to use an HTTP Proxy Server

https://jamf.com/jamf-nation/articles/379

Recording a Packet Trace

https://developer.apple.com/documentation/network/recording_a_packet_trace

Third Party Network Tools

https://developer.apple.com/documentation/network/taking_advantage_of_third-party_network_debugging_tools

CloudFlare ESNI

https://blog.cloudflare.com/encrypted-sni

Q & A

Thank you

Thank you for listening!

Give us feedback by completing the 2-question session survey in the JNUC 2019 app.

UP NEXT

Session title *(JNUC team will add this)*

Session time (JNUC team will add this)