

JANUARY
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

\ 'präk-sē \

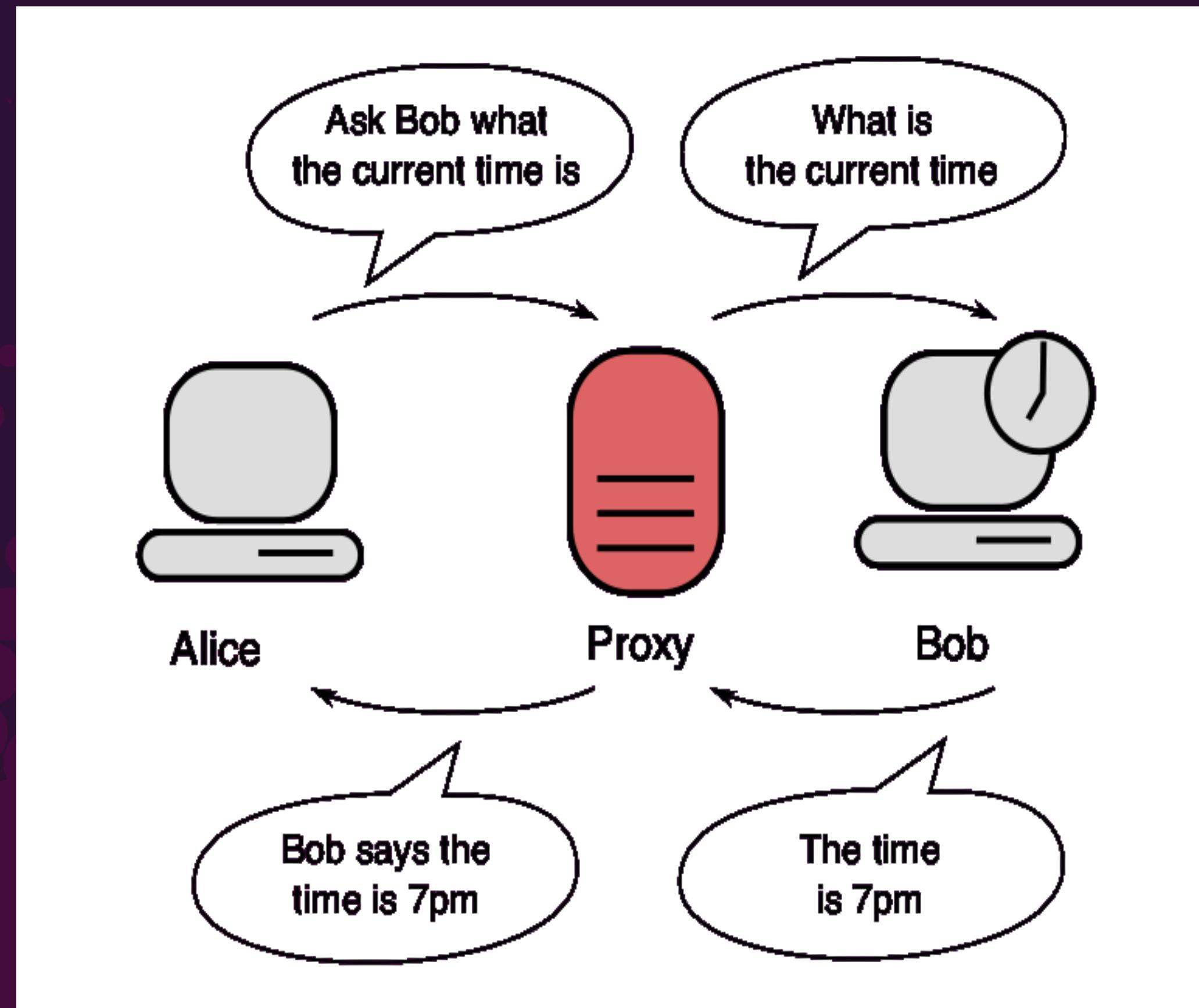
plural **proxies**

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

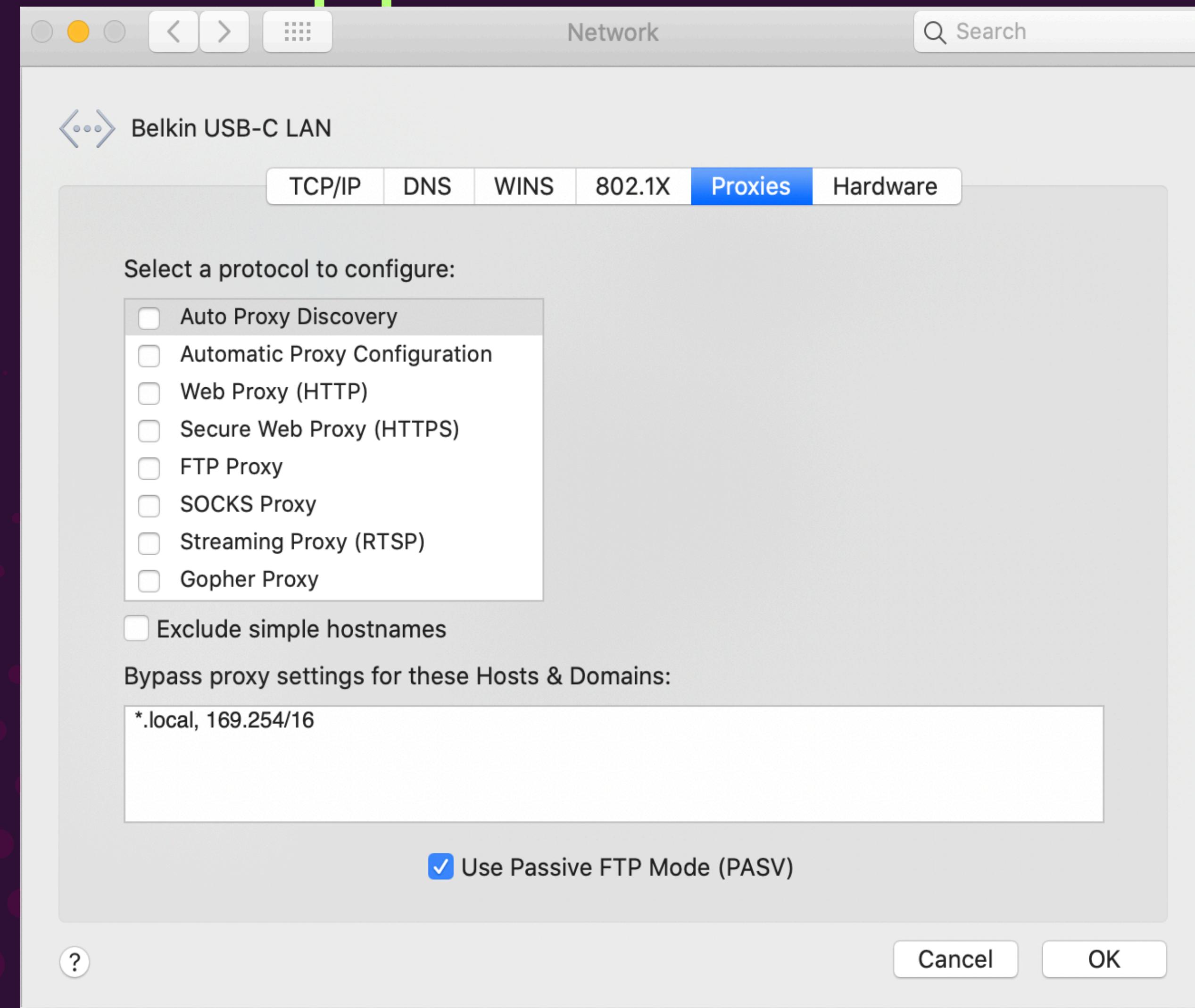


Proxy in a Tech Sense

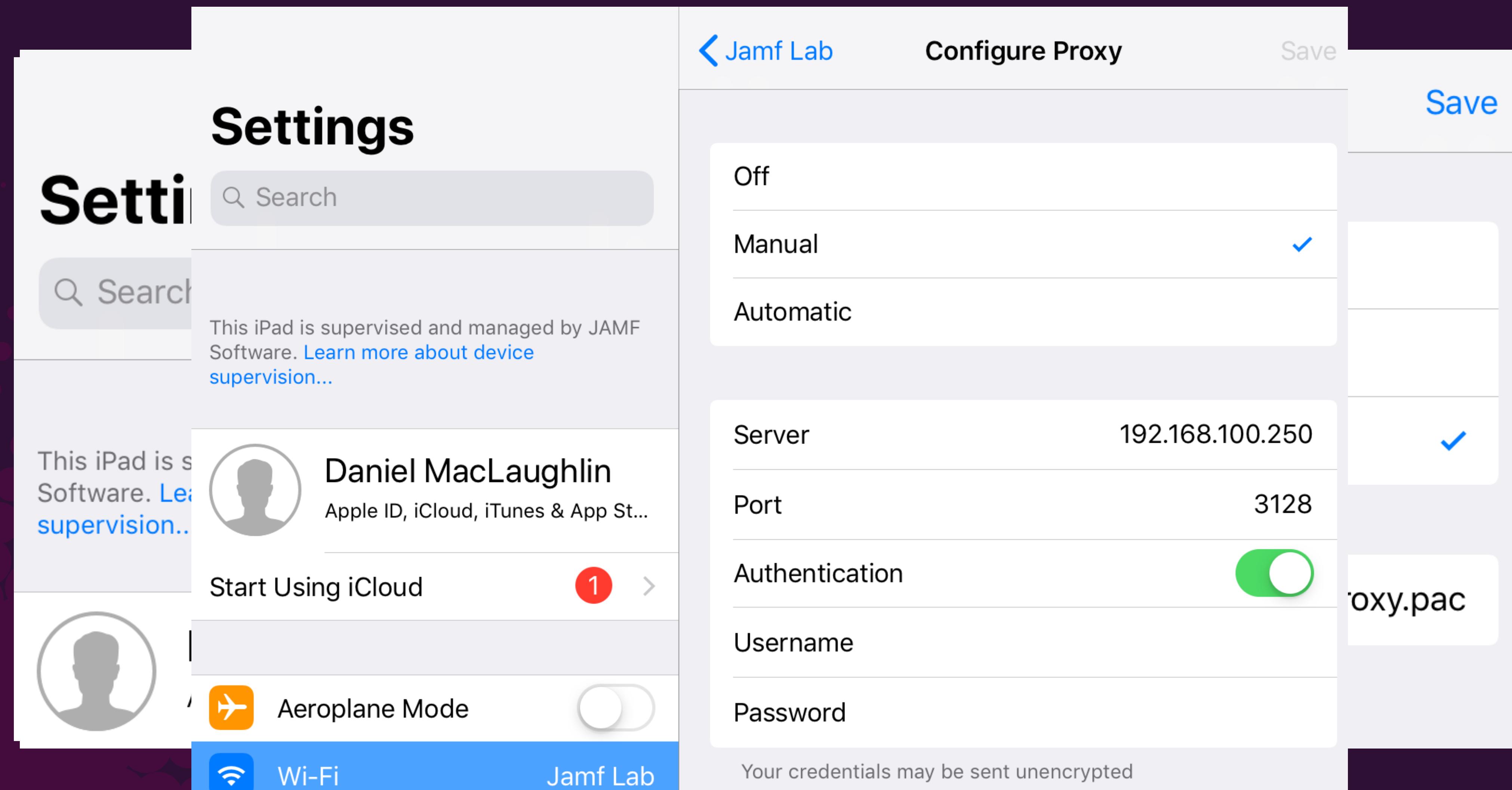


Alice isn't talking to Bob directly.
Bob doesn't see a request from Alice.
The Proxy is acting like a relay.

Proxies and Apple



Proxies and Apple



The image displays two screenshots illustrating proxy configuration on an iPad.

Left Screenshot: iOS Settings

- This iPad is supervised and managed by JAMF Software. [Learn more about device supervision...](#)
- User: Daniel MacLaughlin (Apple ID, iCloud, iTunes & App Store)
- Start Using iCloud (with a red notification badge showing 1)
- Aeroplane Mode (switch off)
- Wi-Fi (selected)
- Jamf Lab

Right Screenshot: Configure Proxy

Configure Proxy

- Proxy Type: Manual (selected)
- Server: 192.168.100.250
- Port: 3128
- Authentication: On
- Username: oxy.pac
- Password: (Field)

Your credentials may be sent unencrypted

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?

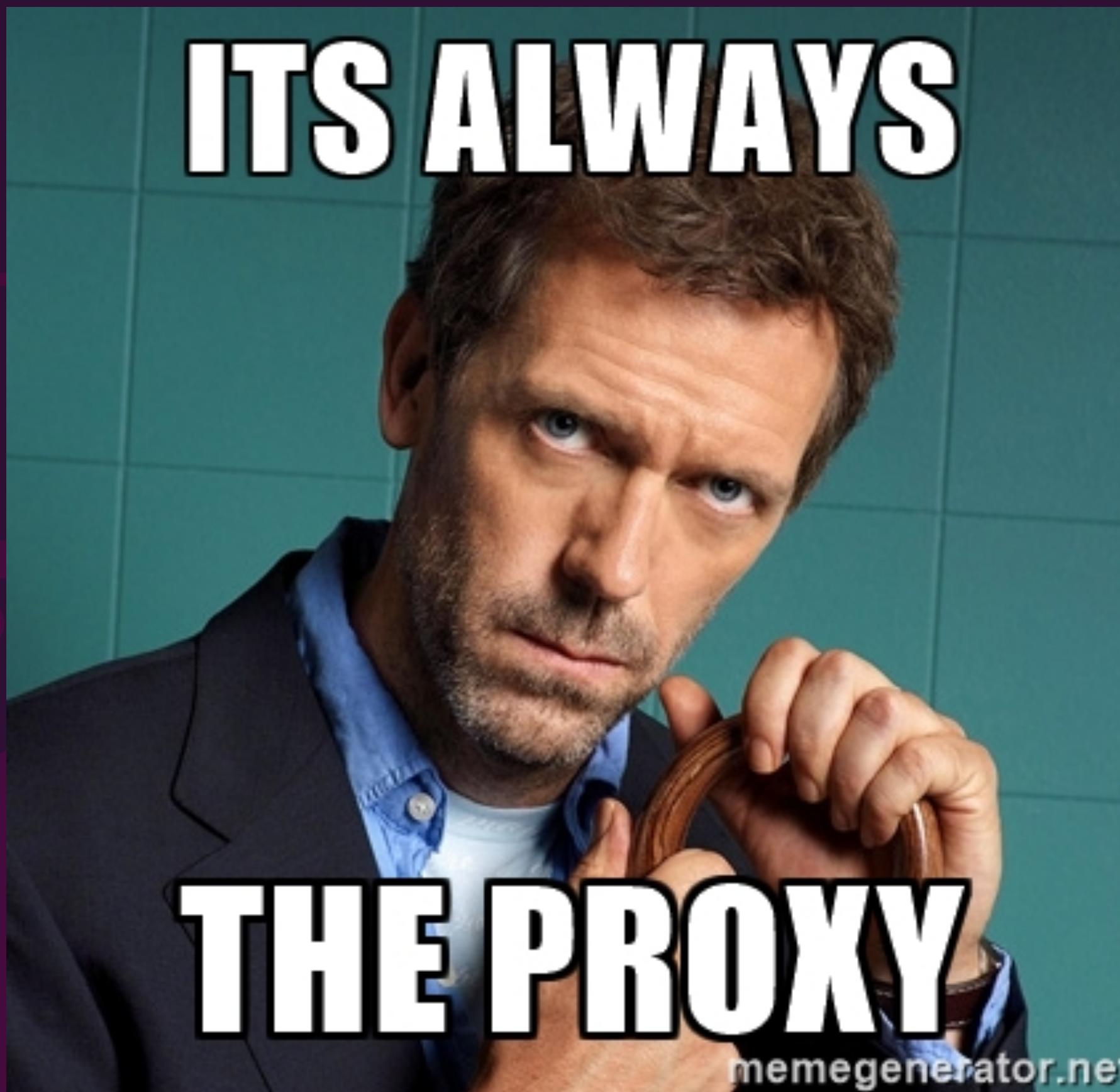


Did we miss something?

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

SSL Man In the Middle Filtering

HTTPS/SSL Interception Enable SSL filtering.

SSL/MITM Mode Splice Whitelist, Bump Otherwise ▼
The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled.
Default: Splice Whitelist, Bump Otherwise. [Click Info for details.](#) i

SSL Intercept Interface(s) LAN
WAN

The interface(s) the proxy server will intercept SSL requests on. [Use CTRL + click to select multiple interfaces.](#)

SSL Proxy Port 3129

This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

SSL Proxy Compatibility Mode Modern ▼
The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. [Click Info for details.](#) i

DHParams Key Size 2048 (default) ▼
DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

CA PFSense CA ▼
Select Certificate Authority to use when SSL interception is enabled. [Click Info for details.](#) i

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.

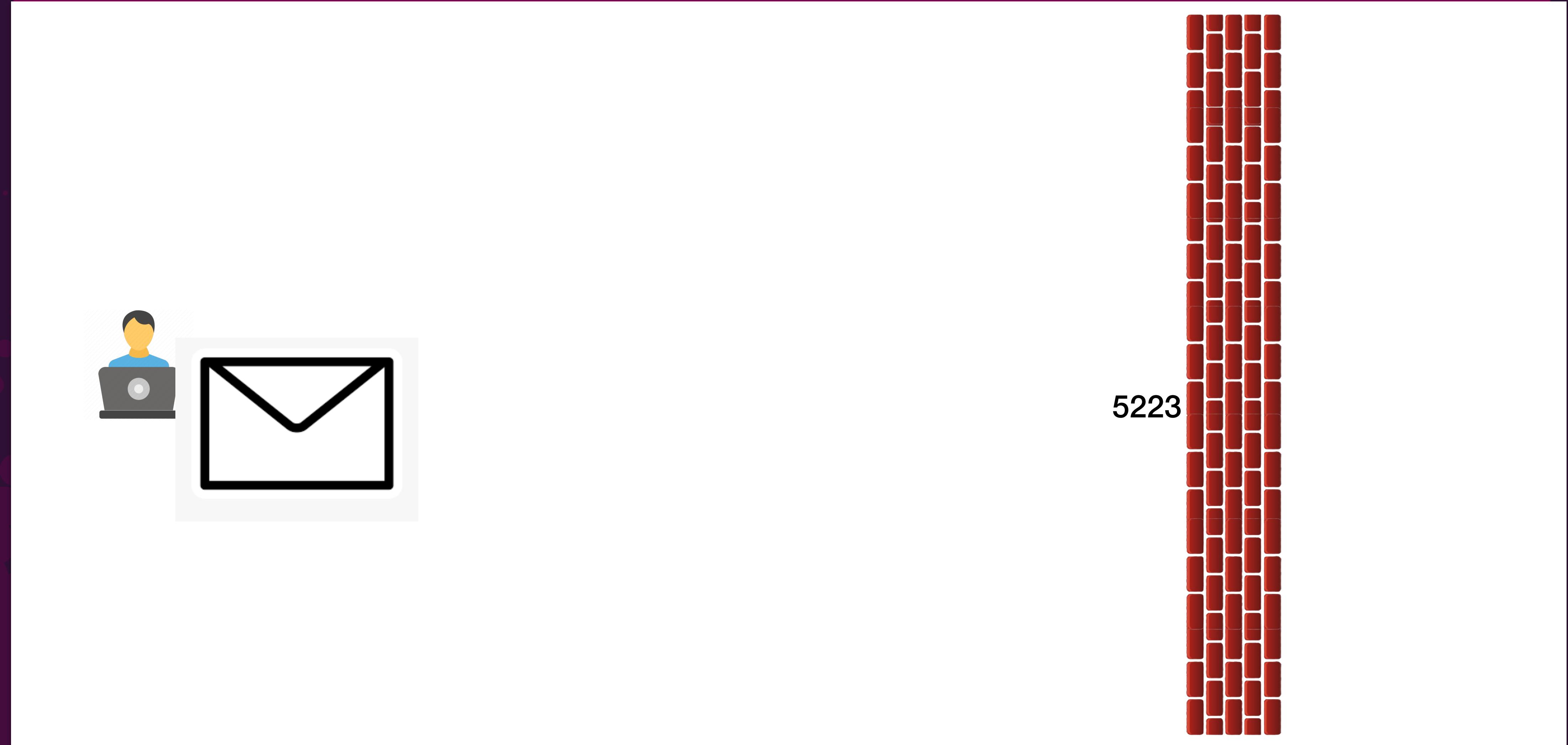
The APNs servers use load balancing, so your devices don't always connect to the same public IP address for notifications. It's best to let your device access these ports on the entire 17.0.0.0/8 address block, which is assigned to Apple.

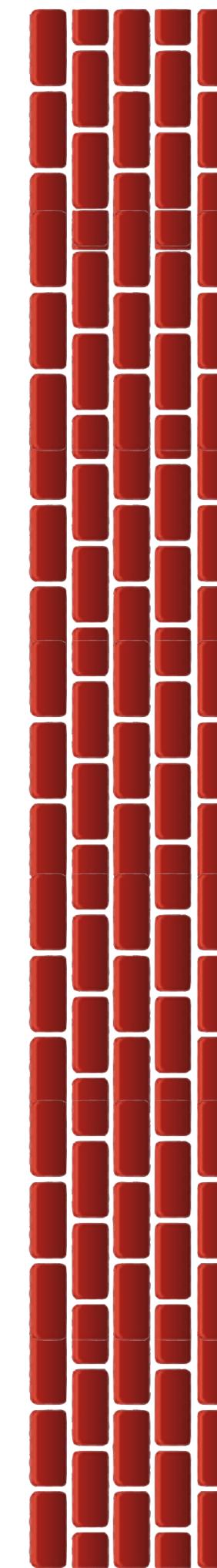
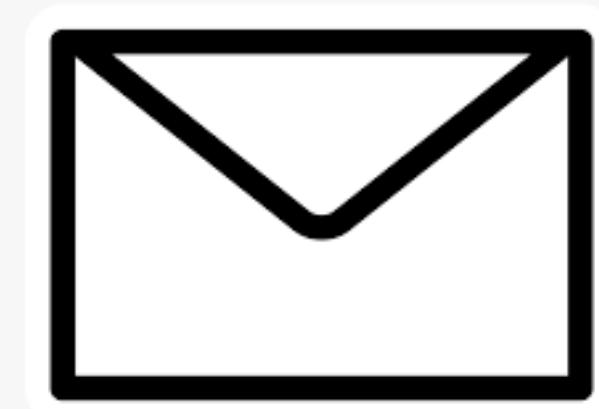
Windows clients **do not** support all proxies, the connection to WNS must be a direct connection.

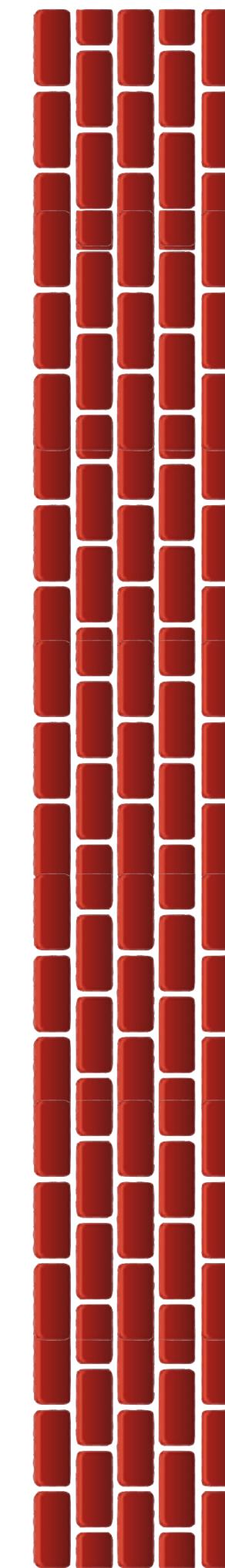


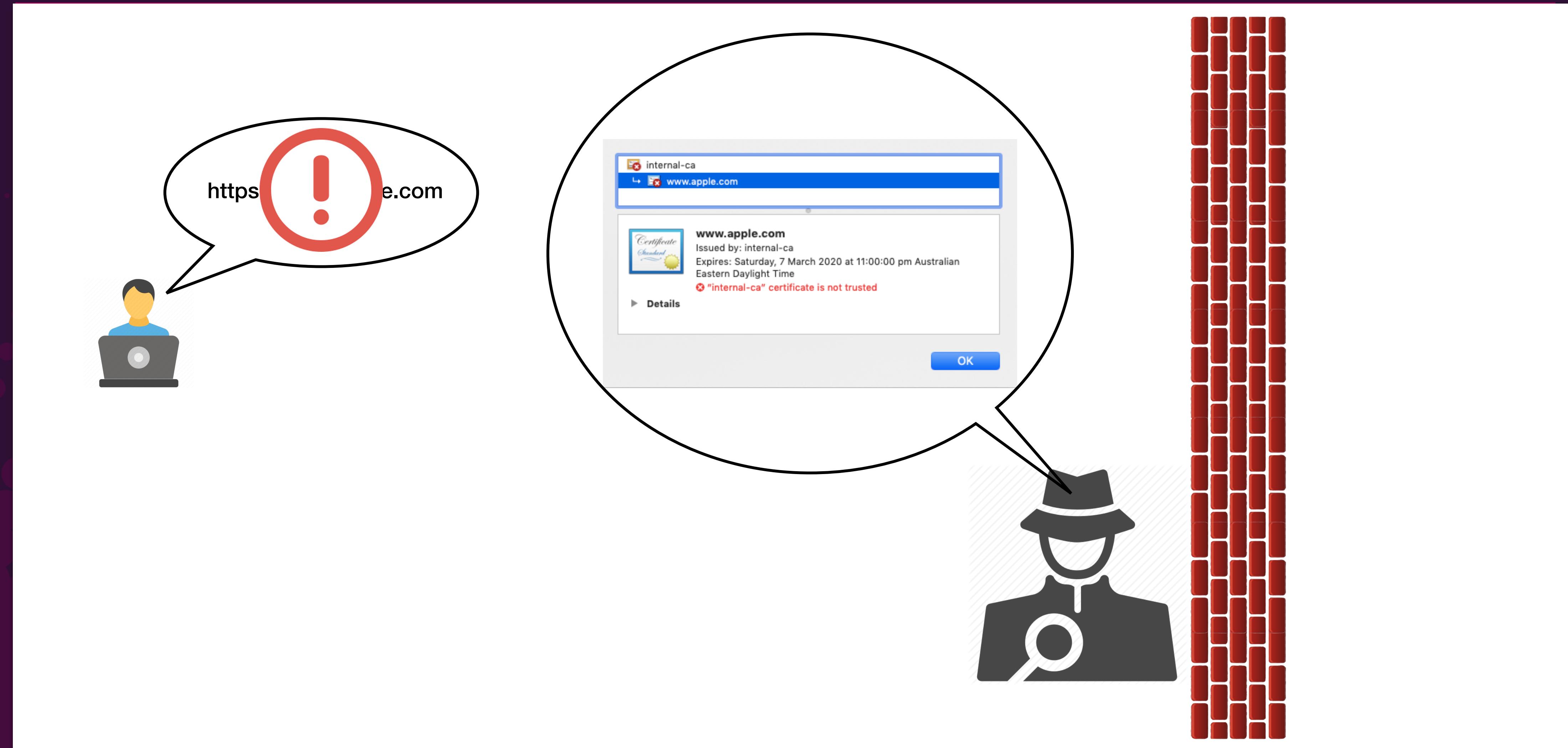
NETWORK SAYS TRAFFIC ISN'T BLOCKED

IS IT THOUGH

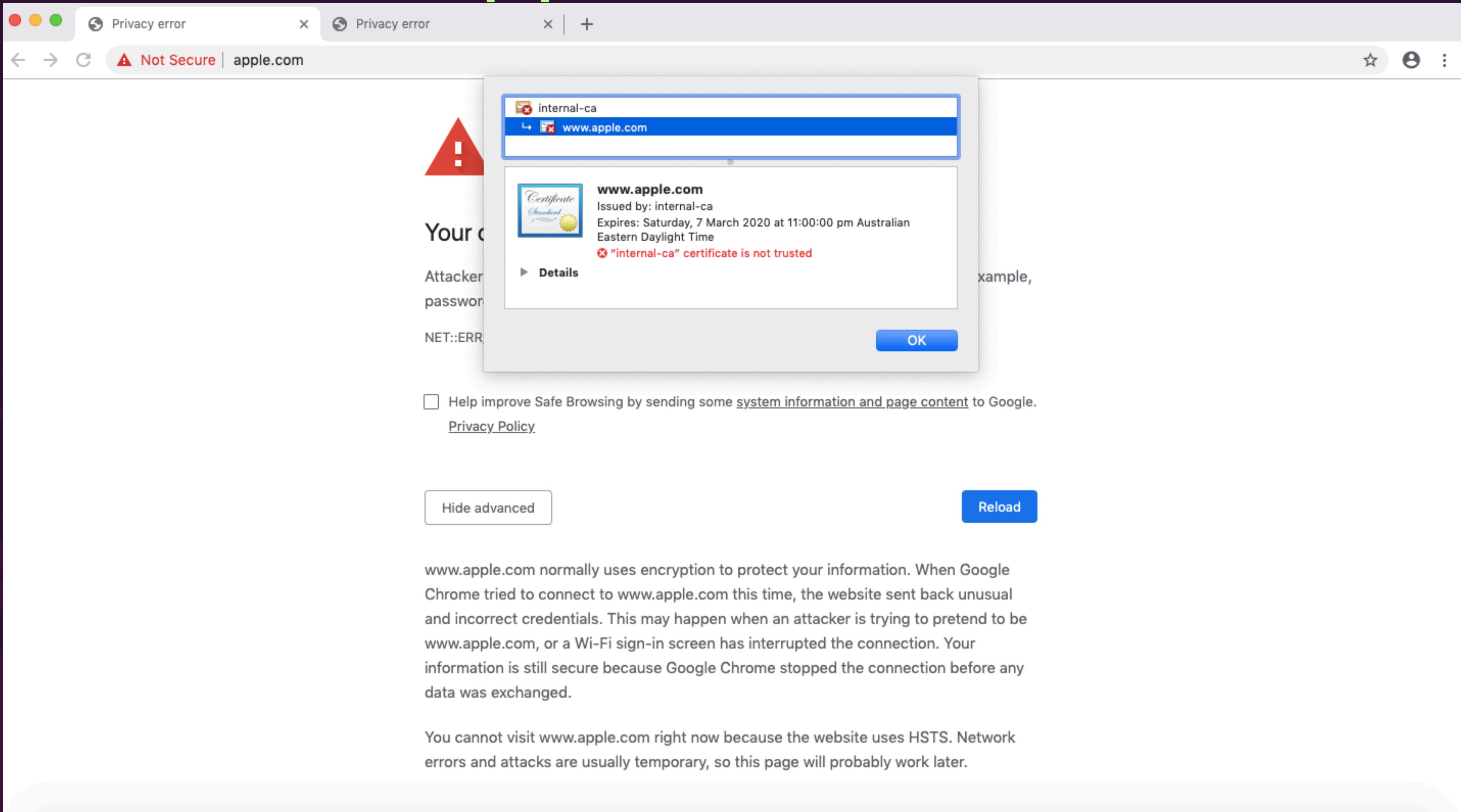








Proxies and Apple



The screenshot shows a web browser window with two tabs, both titled "Privacy error". The address bar indicates "Not Secure | apple.com". A prominent red warning icon with an exclamation mark is displayed. The main content area contains the following text:

Your connection is not private
Attackers may be trying to steal your information from www.apple.com or to fake the site. NET::ERR_CERT_AUTHORITY_INVALID

internal-ca
www.apple.com
Issued by: internal-ca
Expires: Saturday, 7 March 2020 at 11:00:00 pm Australian Eastern Daylight Time
✗ "internal-ca" certificate is not trusted

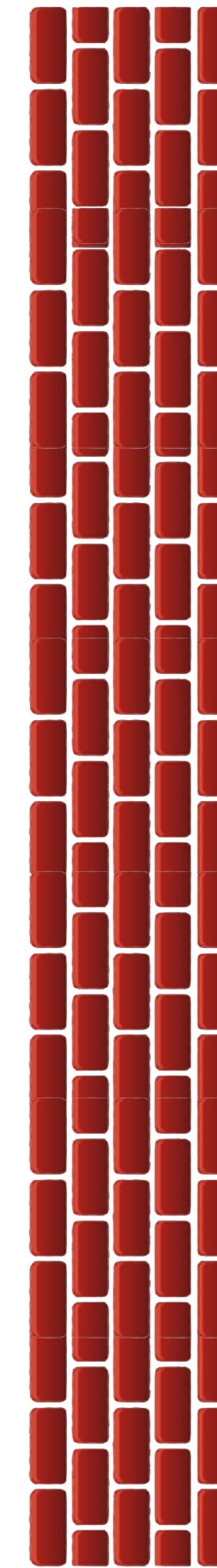
Details OK

Help improve Safe Browsing by sending some [system information and page content](#) to Google.
[Privacy Policy](#)

Hide advanced Reload

www.apple.com normally uses encryption to protect your information. When Google Chrome tried to connect to www.apple.com this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be www.apple.com, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Google Chrome stopped the connection before any data was exchanged.

You cannot visit www.apple.com right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.



Proxies and Apple

[!\[\]\(0a023d01ac3b7c728c29528b0758e35e_img.jpg\) Back](#)[Next !\[\]\(230490b09f1763ff4241372da7cf5f63_img.jpg\)](#)

Remote Management

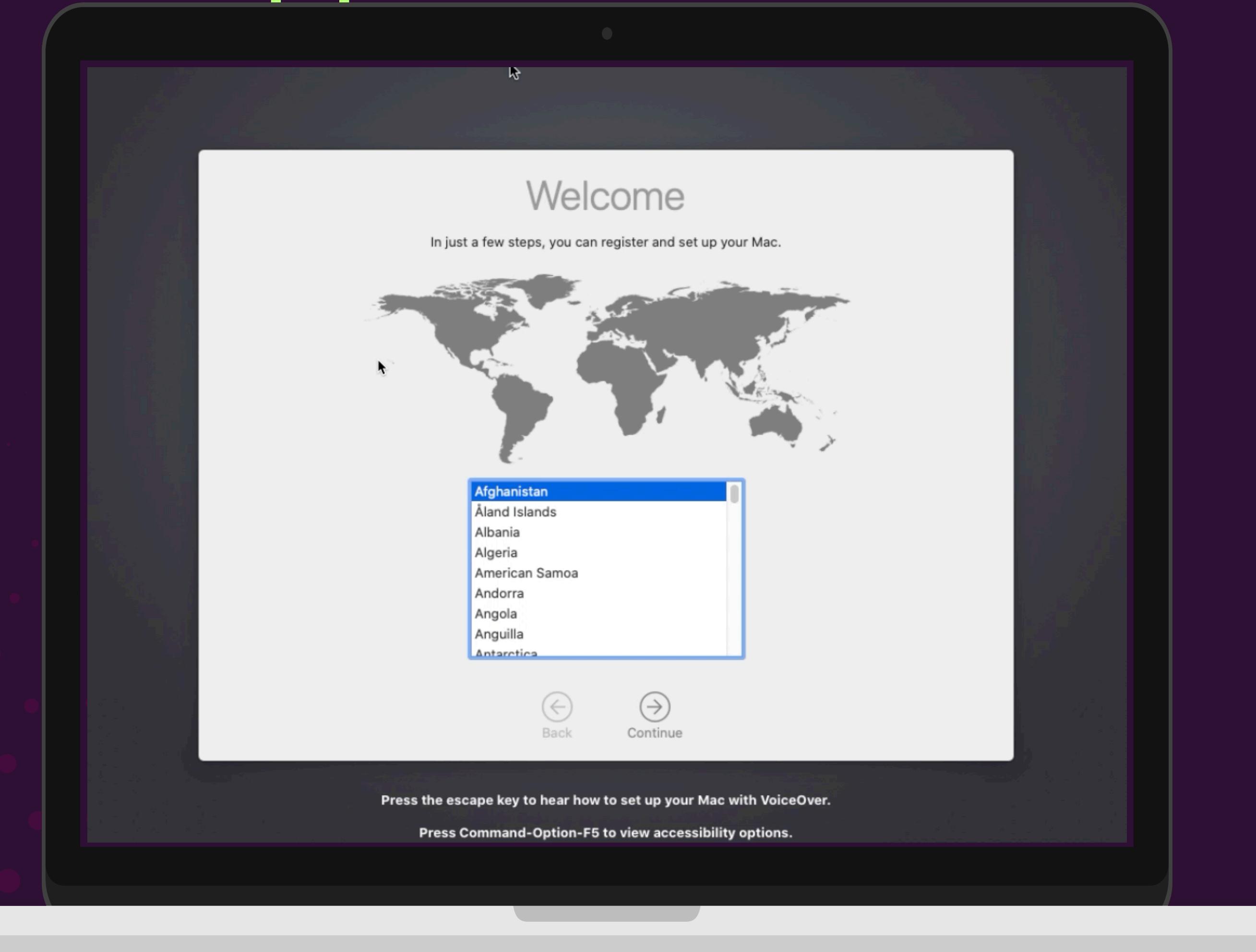
The configuration for your iPad could not be downloaded from
JAMF Software.

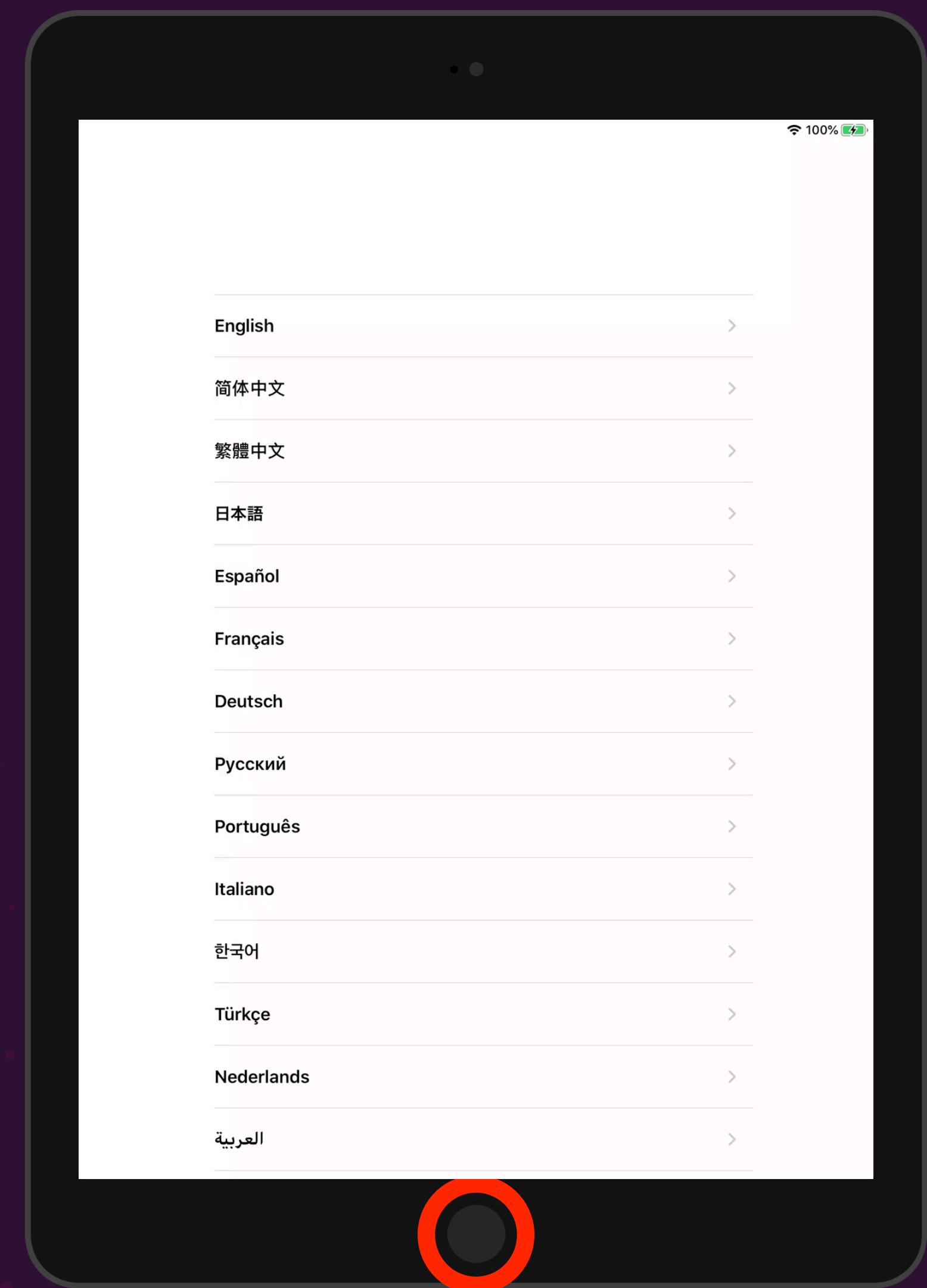
cancelled

Proxies and Apple



Proxies and Apple





Proxies and Apple

```
Daniel-Demos-MacBook-Air:~ daniel-demo$ sudo jamf policy  
2019-09-26 14:08:56.538 jamf[7179:129195] NSURLSession/NSURLConnection HTTP load failed (kCFStreamErrorDomainSSL, -9813)  
Error getting version information from the JSS. Attempting to gather the information from a policy request...  
2019-09-26 14:08:58.365 jamf[7179:129195] NSURLSession/NSURLConnection HTTP load failed (kCFStreamErrorDomainSSL, -9813)  
  
There was an error.  
  
The jamf binary could not connect to the JSS because the web certificate is not trusted.
```



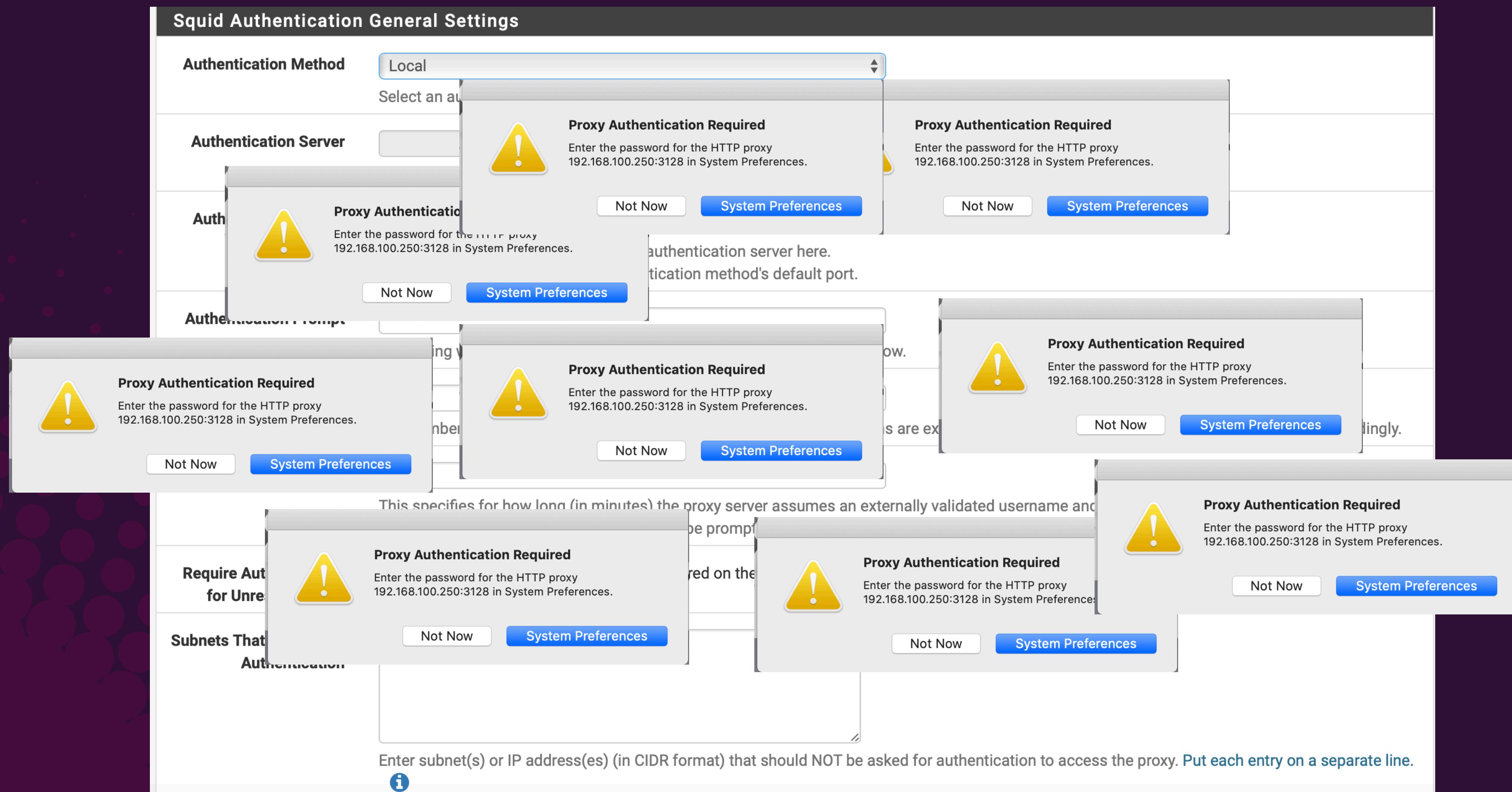
Proxies and Apple

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

HTTP Proxy Settings

Proxy Host:port

Proxy Username

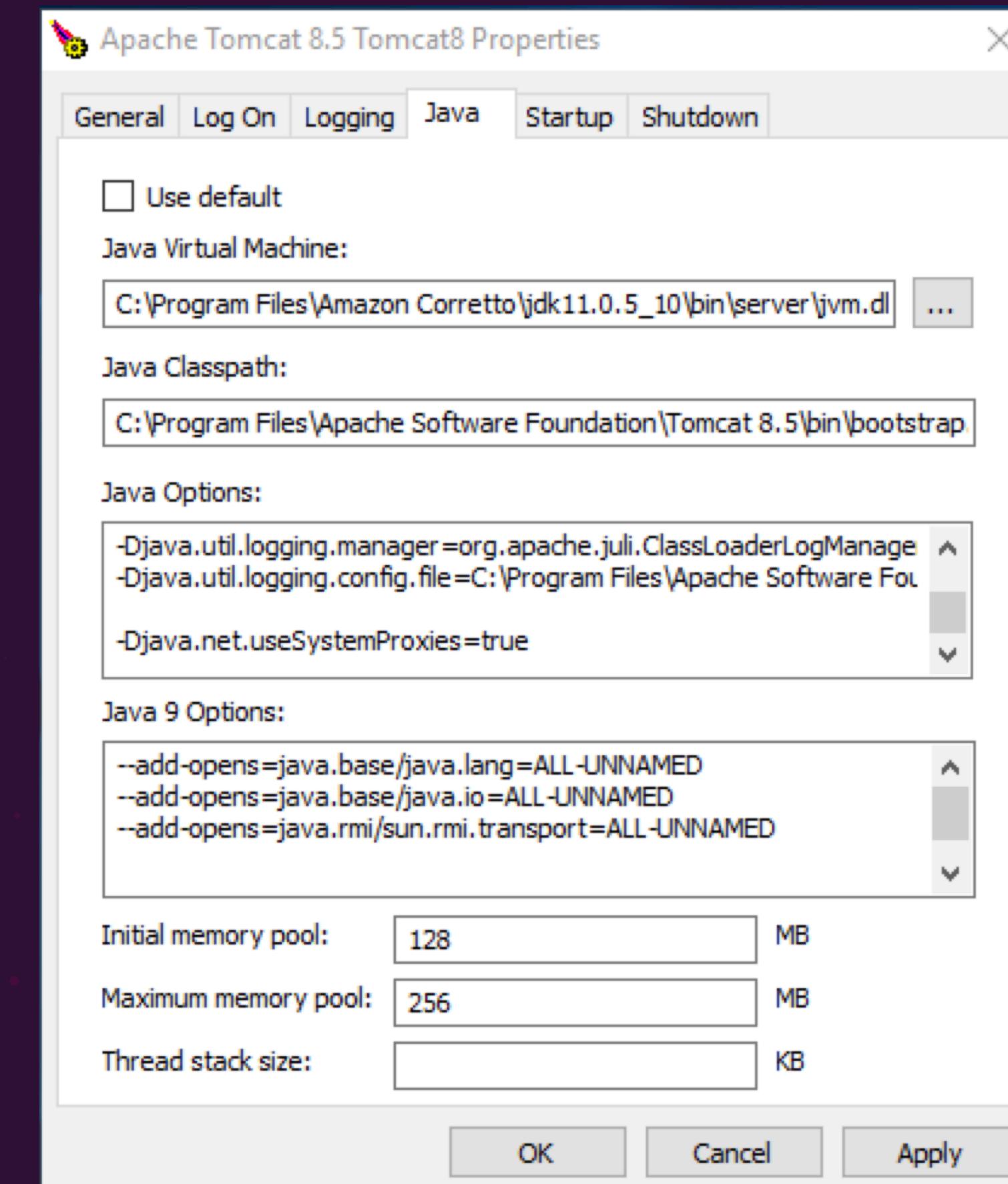
Proxy Password

Confirm Password

Save



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

▼ Transport Layer Security

 ▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello

 Content Type: Handshake (22)

 Version: TLS 1.0 (0x0301)

 Length: 512

 ▼ Handshake Protocol: Client Hello

 ▼ Extension: encrypted_server_name (len=366)

 Type: encrypted_server_name (65486)

 Length: 366

 Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

 ▼ Key Share Entry: Group: x25519, Key Exchange length: 32

 Group: x25519 (29)

 Key Exchange Length: 32

 Key Exchange: c3ec5aaeb1ddc2ce04e85277c014e2ab1e42bb59e52e0866...

 Record Digest Length: 32

 Record Digest: c6ce4a88f23b89ec33a5defea1f234b68cc6b32b9cbf7191...

 Encrypted SNI Length: 292

Encrypted SNI: a99de6255f4ce1dbe001b5e1bec65ea956c6c484528380e7...

► Extension: Unknown type 28 (len=2)

01d0	0d 69 a2 2e 9b 7d 01 24 a9 9d e6 25 5f 4c e1 db	.i...}.\$...%_L..
01e0	e0 01 b5 e1 be c6 5e a9 56 c6 c4 84 52 83 80 e7^ V...R..

► Extension: extended_master_secret (len=0)

00b0	00 11 00 00 0e 63 6c 6f 75 64 66 6c 61 72 65 2eclo uflare.
00c0	63 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 0e	com.....

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:

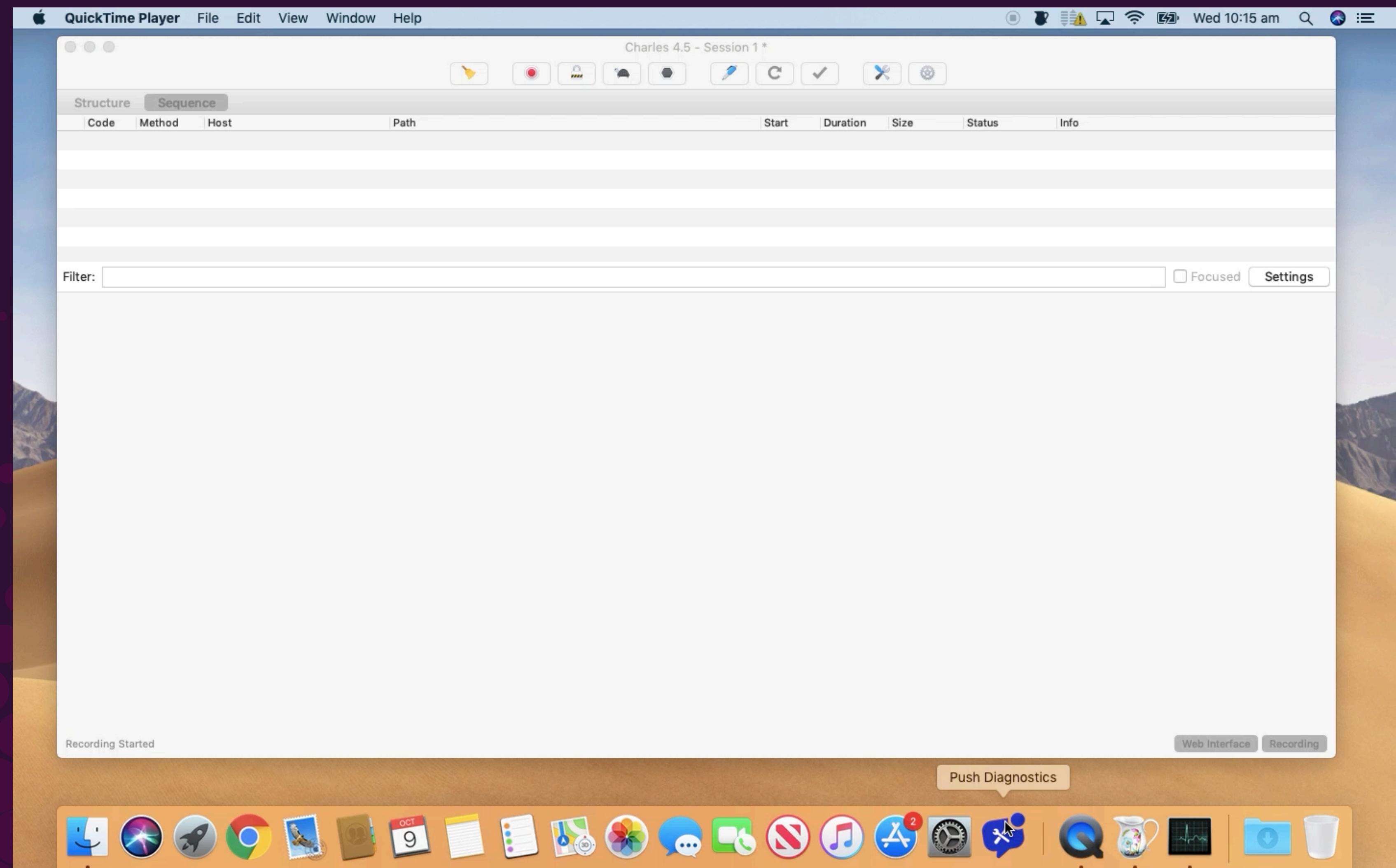
Apple Configurator 2

Wireshark using rvictl

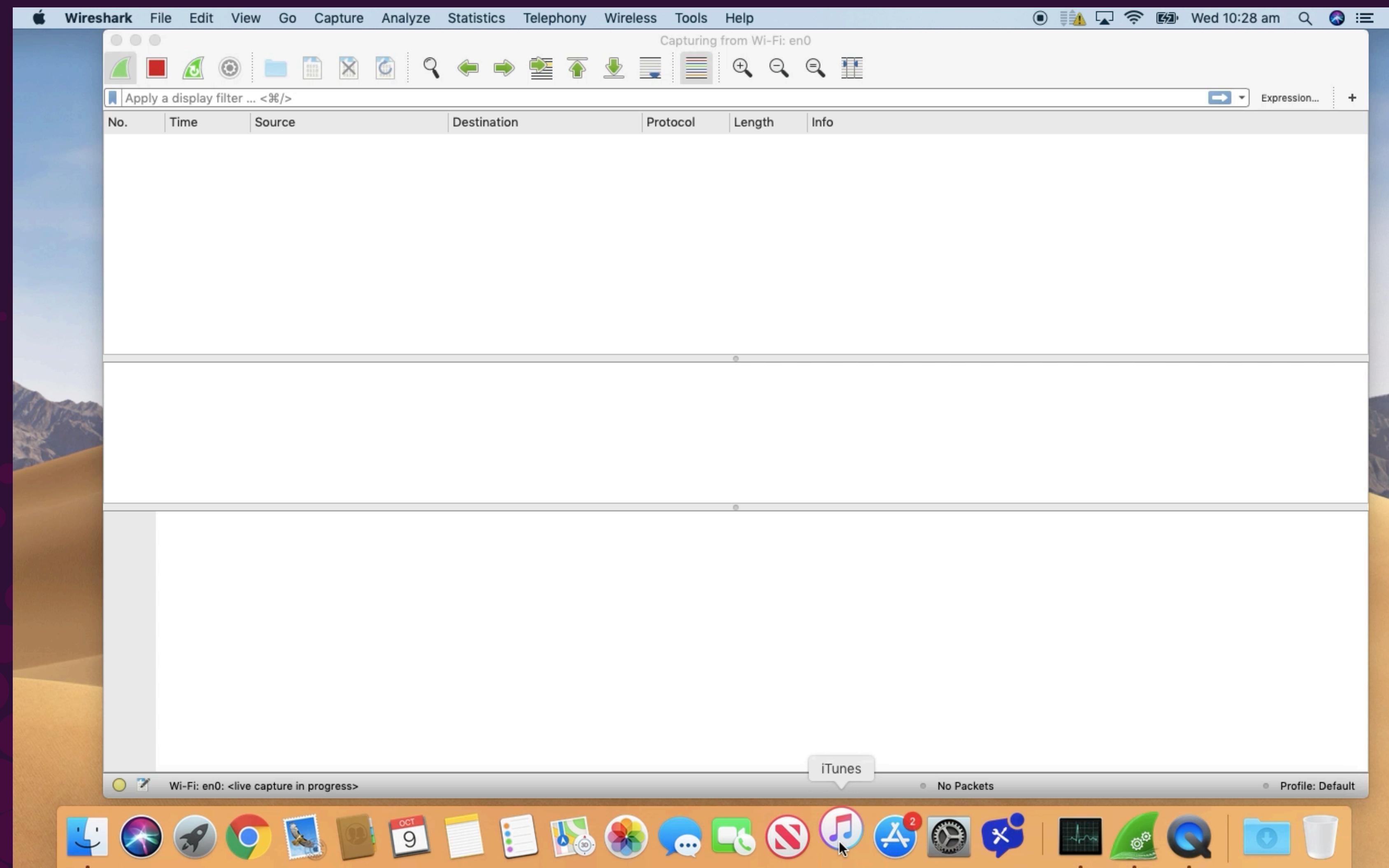
tcpdump using rvictl



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)

