

# Certificate Troubleshoot using AirWatch

TEIS Digital Workplace

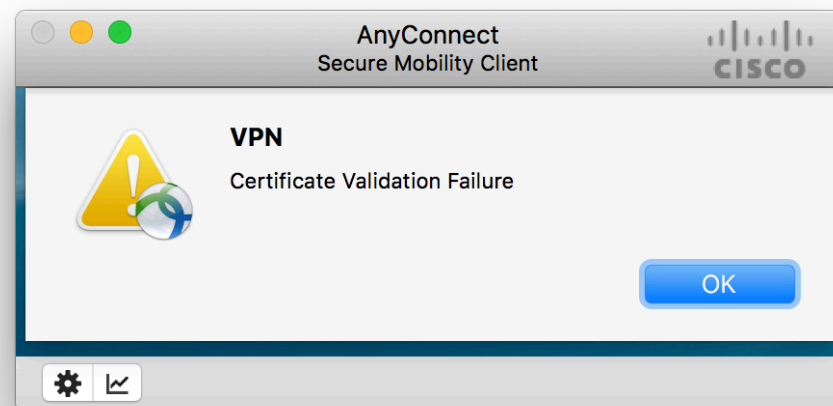


EVERY CONNECTION COUNTS



# Issue Verification

AnyConnect refuses to establish a VPN connection, reporting a “Certificate Validation Error”.



# OS Version

This troubleshooting is only valid on macOS Sierra devices, that are enrolled in AirWatch.

Begin by verifying the OS using the “About this Mac” option from the Apple menu. You are looking for a version number of 10.12.0 or higher.

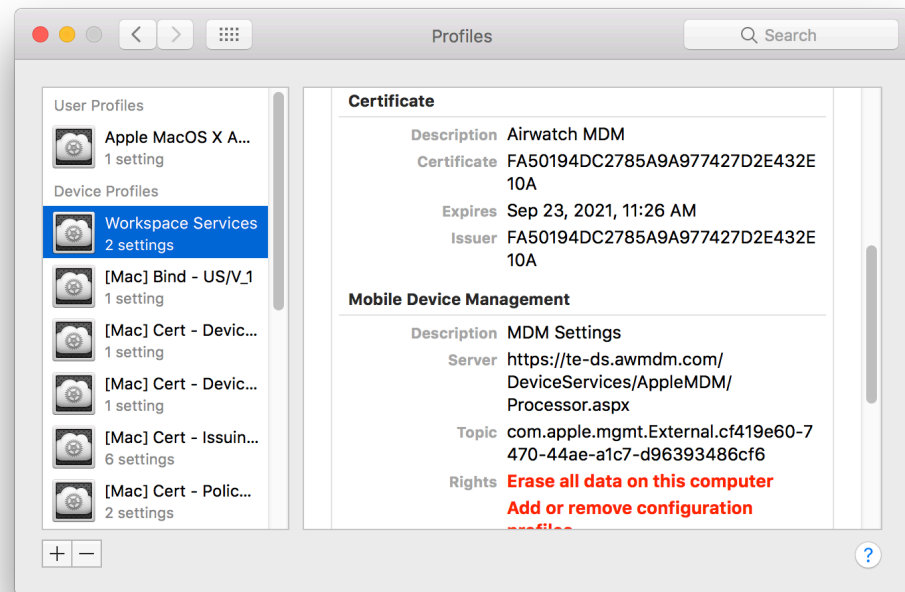


# Management Profiles

This troubleshooting is only valid on macOS Sierra devices, that are enrolled in AirWatch.

Verify that the device is enrolled by checking the Profiles pane of System Preferences for the “Workspace Services” profile. Scroll down and verify that the “Server” field is set to some variation of:

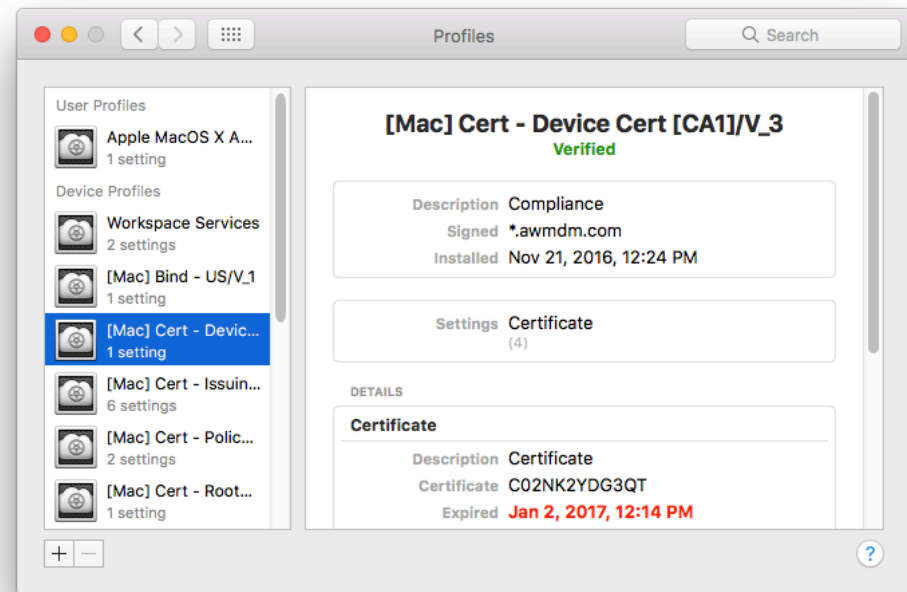
<https://te-ds.awmdm.com>



# Check for Cert Profile

While in the Profiles pane of System Preferences, also verify that the “Device Cert” profile is present.

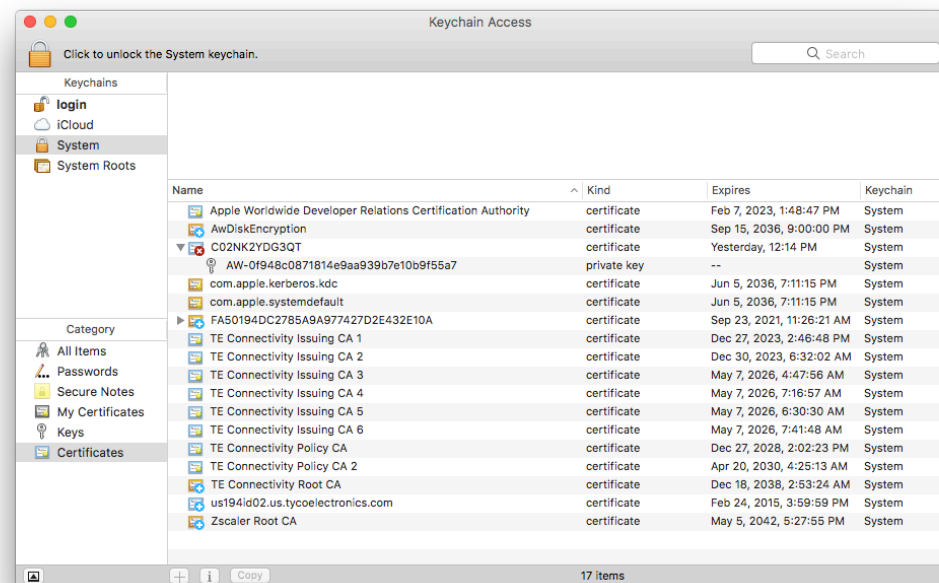
In cases of an expired certificate, the expiration date will be listed in the profile.



# Keychain Verification

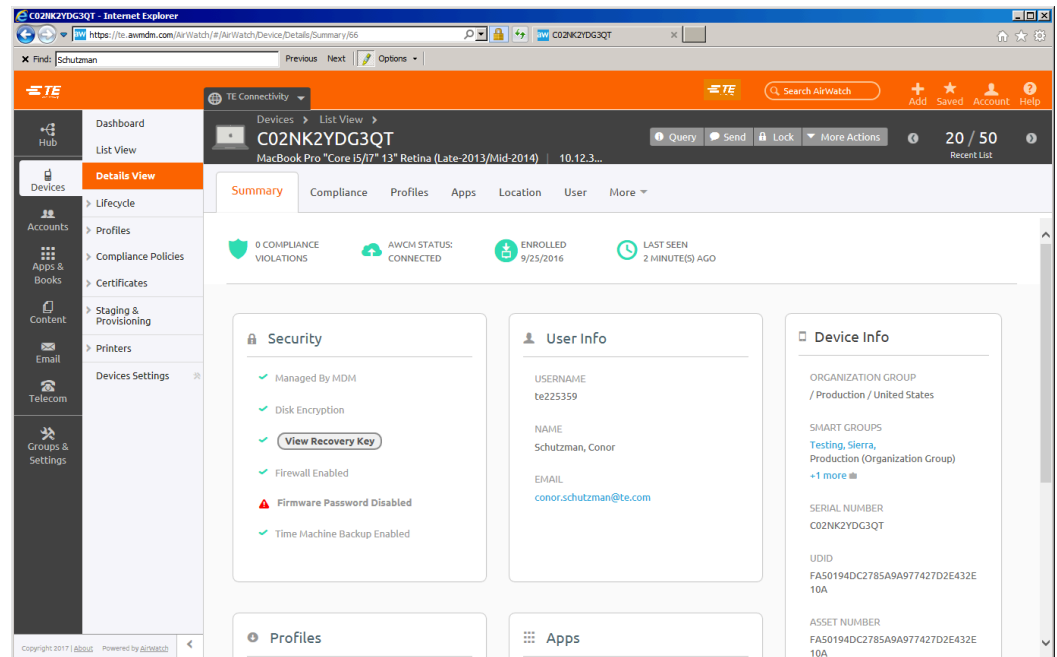
Additionally, in cases of expired certificates, the previous certificate should be visible in Keychain Access.

Launch Keychain Access from the Utilities folder, then select “System” from the “Keychains” section, and “Certificates” from the “Category” section. The list on the right should then include a certificate named for the serial number of the device. Clicking the disclosure triangle should reveal a private key named “AW-” followed by a long hexadecimal string.



# AirWatch Admin Console

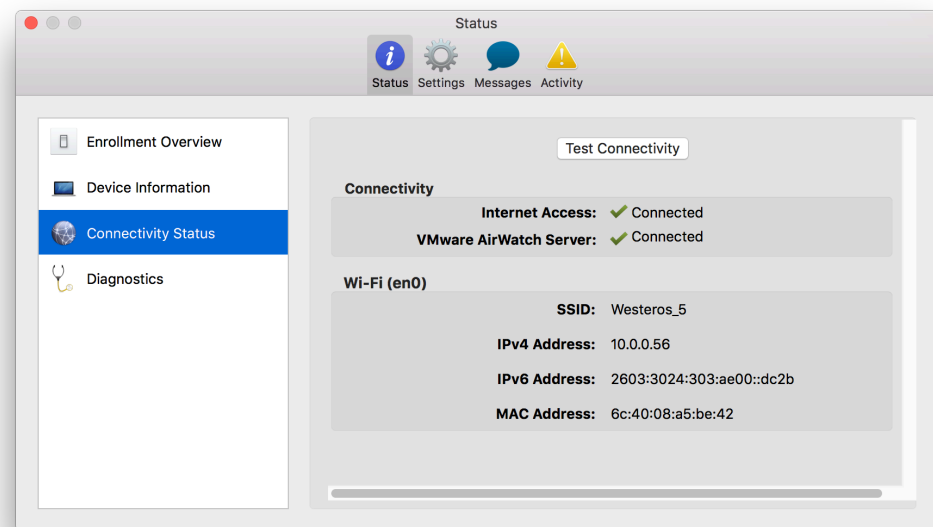
The device should be visible in the AirWatch Admin Console. Navigate to go/AirWatch and login using your network credentials (NOT your ADM account). From the list on the left, select “Devices”, then select “List View” from the sub menu. In the list that appears, search for the serial number of the device (you can also search by the network ID of the primary user of the device). Clicking on the entry in the list will bring up a detailed view.



# Connection Verification

At the top of the details view, take note of the “AWCM Status” and “Last Seen” fields, as they will provide information about how well the device is communicating with the server.

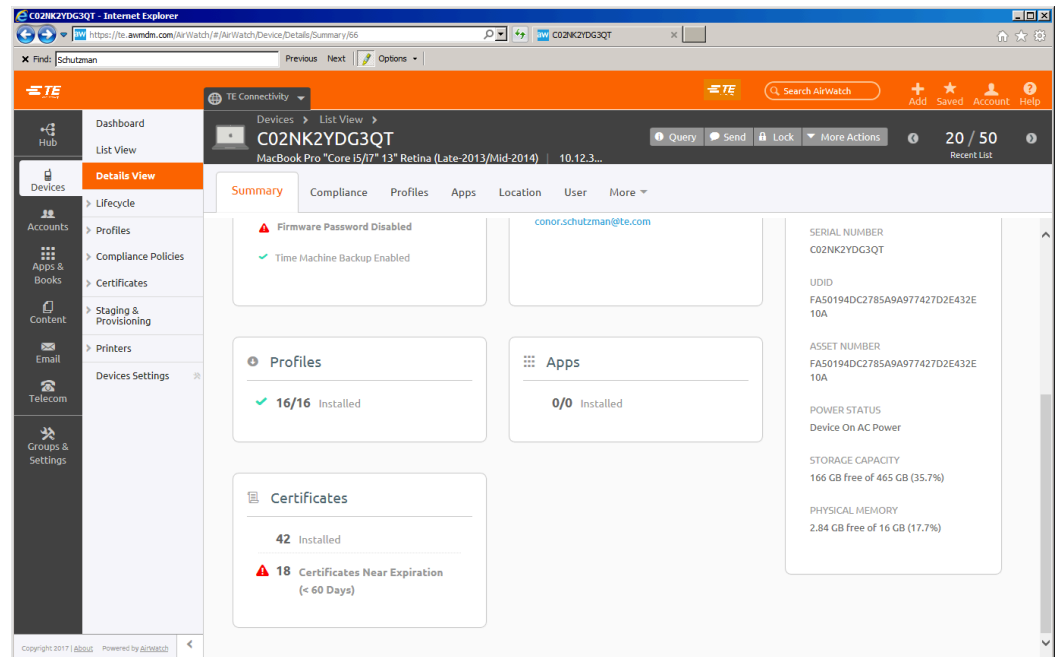
On the client side, you can use the “Preferences” entry of the AirWatch menu item to verify connectivity.





# Details View

Further down the initial details screen on the Admin Console, note the “Profiles” and “Certificates” listing. Clicking on either of these category headings will show you detailed information on those specific facets of the device.



# Certificate Details

Clicking on the Certificates heading will display the current certificates on the device.

In the case of an expired certificate, there will be an entry in this list, named with just the device serial number, that lists as "Expired" with a status of either "Installed" or "Revoked"

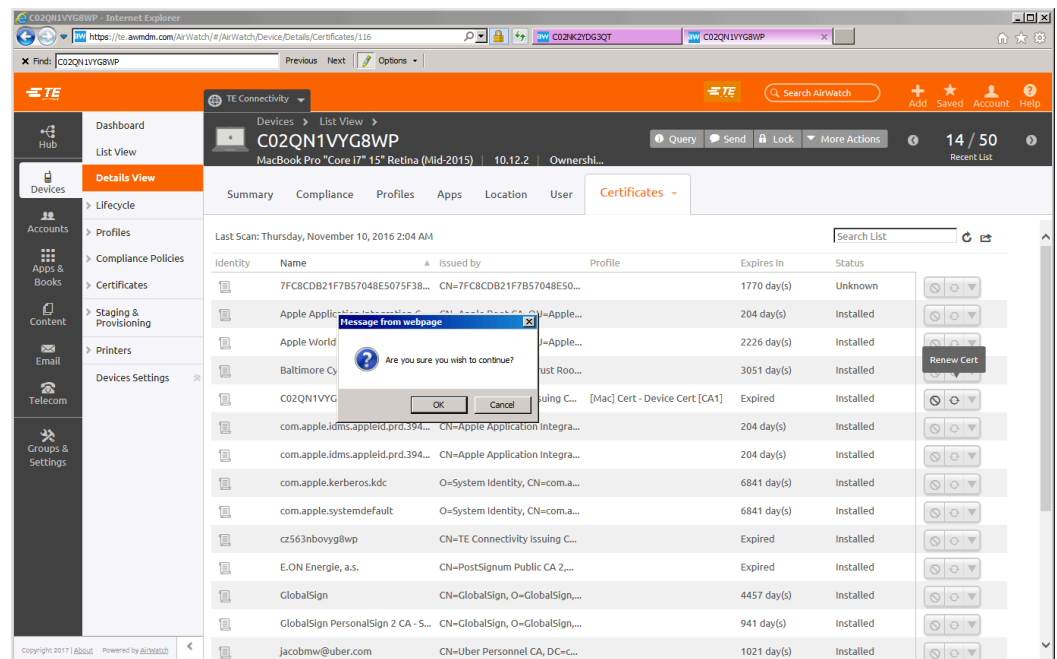
Identity	Name	Issued by	Profile	Expires In	Status
		CN=COMODO Client Authent...		Expired	Installed
		OU=VeriSign Trust Network,...		4228 day(s)	Installed
	Apple Application Integration C...	CN=Apple Root CA, OU=Apple...		204 day(s)	Installed
	Apple Worldwide Developer Rel...	CN=Apple Root CA, OU=Apple...		2226 day(s)	Installed
	AwDiskEncryption	O=TEConnectivity, CN=AwDis...		7196 day(s)	Unknown
	C02NK2YDG3QT	CN=TE Connectivity Issuing C...	[Mac] Cert - Device Cert [CA1]	Expired	Revoked
	C02NK2YDG3QT	CN=TE Connectivity Issuing C...	[Mac] Cert - Device Cert [CA1]	Expired	Revoked
	C02NK2YDG3QT	CN=TE Connectivity Issuing C...		Expired	Installed
	C02NK2YDG3QT	CN=TE Connectivity Issuing C...		Expired	Installed
	Collaboration Certification Auth...	OU=VeriSign Trust Network,...		Expired	Installed
	com.apple.idms.appleid.prd.636...	CN=Apple Application Integra...		204 day(s)	Installed
	com.apple.idms.appleid.prd.636...	CN=Apple Application Integra...		204 day(s)	Installed
	com.apple.kerberos.kdc	O=System Identity, CN=com.a...		7093 day(s)	Installed
	com.apple.systemdefault	O=System Identity, CN=com.a...		7093 day(s)	Installed

# Manual Renewal

In some cases, there will be a circular arrow icon that will allow you to manually request a renewal of the expired certificate.

You will be prompted to confirm this action.

After issuing the renewal, the “Query” button at the top of the panel (or having the client use “Sync Now” from the AirWatch menu icon), followed by refreshing the page, should show a new certificate with a 42 day expiration.



# Failed Renewals

If, after querying and refreshing, perhaps waiting and retrying, a new certificate is not being issued, you may need to confirm if there was an issue with the renewal.

From the right most tab (defaults to “More”) of the details view, select “Troubleshooting” from the drop down. You are looking for any “Error” events that reference a certificate server in the event details. The timestamps will help you confirm that these are in response to the request you just made. Please note any errors in the case notes.

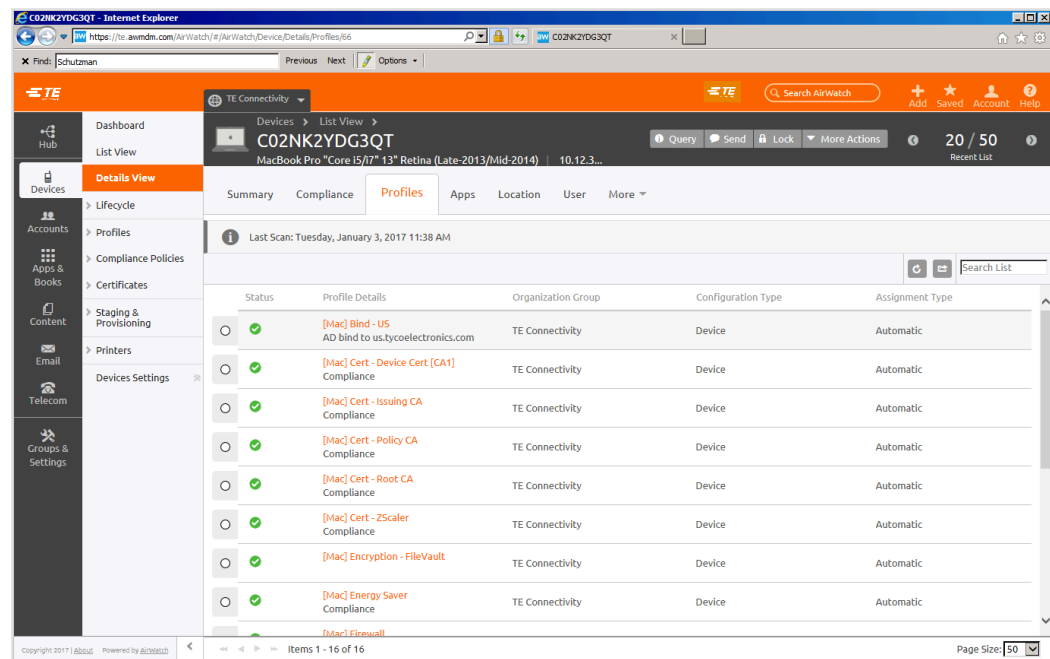
The screenshot shows the TE Connectivity AirWatch interface for device C02QN1VYG8WP. The 'Troubleshooting' tab is selected, displaying an 'Event Log' with the following data:

Severity	Time	Device	User	Source	Module	Category	Event	Admin	Event t
Error	1/2/2017 3:25 AM	C02QN1VYG8WP	EV000901	Device	Certificate Management	Certificates	Certificate Request Failed	sysadmin	Certific
Notice	1/2/2017 3:25 AM	C02QN1VYG8WP	EV000901	Server	Dashboard	Command	Install Profile Requested	te116666	Profile :
Notice	1/2/2017 3:25 AM	C02QN1VYG8WP	EV000901	Server	Dashboard	Command	Install Profile Requested	te116666	Profile :
Error	1/2/2017 3:22 AM	C02QN1VYG8WP	EV000901	Device	Certificate Management	Certificates	Certificate Request Failed	sysadmin	Certific
Notice	1/2/2017 3:22 AM	C02QN1VYG8WP	EV000901	Server	Dashboard	Command	Install Profile Requested	te116666	Profile :
Notice	1/2/2017 3:22 AM	C02QN1VYG8WP	EV000901	Server	Dashboard	Command	Install Profile Requested	te116666	Profile :
Error	1/2/2017 3:22 AM	C02QN1VYG8WP	EV000901	Device	Certificate Management	Certificates	Certificate Request Failed	sysadmin	Certific
Notice	1/2/2017 3:22 AM	C02QN1VYG8WP	EV000901	Server	Dashboard	Command	Install Profile Requested	te116666	Profile :
Notice	1/2/2017 3:02 AM	C02QN1VYG8WP	EV000901	Device	Catalog	Device	App Catalog Launch	sysadmin	
Notice	1/2/2017 2:53 AM	C02QN1VYG8WP	EV000901	Device	Catalog	Device	App Catalog Launch	sysadmin	
Notice	1/2/2017 2:50 AM	C02QN1VYG8WP	EV000901	Device	Catalog	Device	App Catalog Launch	sysadmin	
Notice	1/2/2017 2:49 AM	C02QN1VYG8WP	EV000901	Device	Catalog	Device	App Catalog Launch	sysadmin	

# Profile Details

As the certificates are governed by the installation of profiles, it is important to verify that the relevant profile is also installed. You can either select “Profiles” from the drop down on the right most tab in the details view, or click on the “Profiles” category heading towards the bottom of the summary tab.

Note any profiles that do not have a green checkmark. It may be worth attempting to re-push any missing profiles.



Status	Profile Details	Organization Group	Configuration Type	Assignment Type
○ ✓	[Mac] Bind - US AD bind to us.tycoelectronics.com	TE Connectivity	Device	Automatic
○ ✓	[Mac] Cert - Device Cert [CA1] Compliance	TE Connectivity	Device	Automatic
○ ✓	[Mac] Cert - Issuing CA Compliance	TE Connectivity	Device	Automatic
○ ✓	[Mac] Cert - Policy CA Compliance	TE Connectivity	Device	Automatic
○ ✓	[Mac] Cert - Root CA Compliance	TE Connectivity	Device	Automatic
○ ✓	[Mac] Cert - ZScaler Compliance	TE Connectivity	Device	Automatic
○ ✓	[Mac] Encryption - FileVault	TE Connectivity	Device	Automatic
○ ✓	[Mac] Energy Saver Compliance	TE Connectivity	Device	Automatic
○ ✓	[Mac] Firewall	TE Connectivity	Device	Automatic

# Alternative Certificates

If the default Certificate Authority (CA 1) is not issuing a valid certificate to the device, our one remaining troubleshooting step is to assign the device to get it's device certificate from our secondary server (CA 2). The following steps will outline this process.

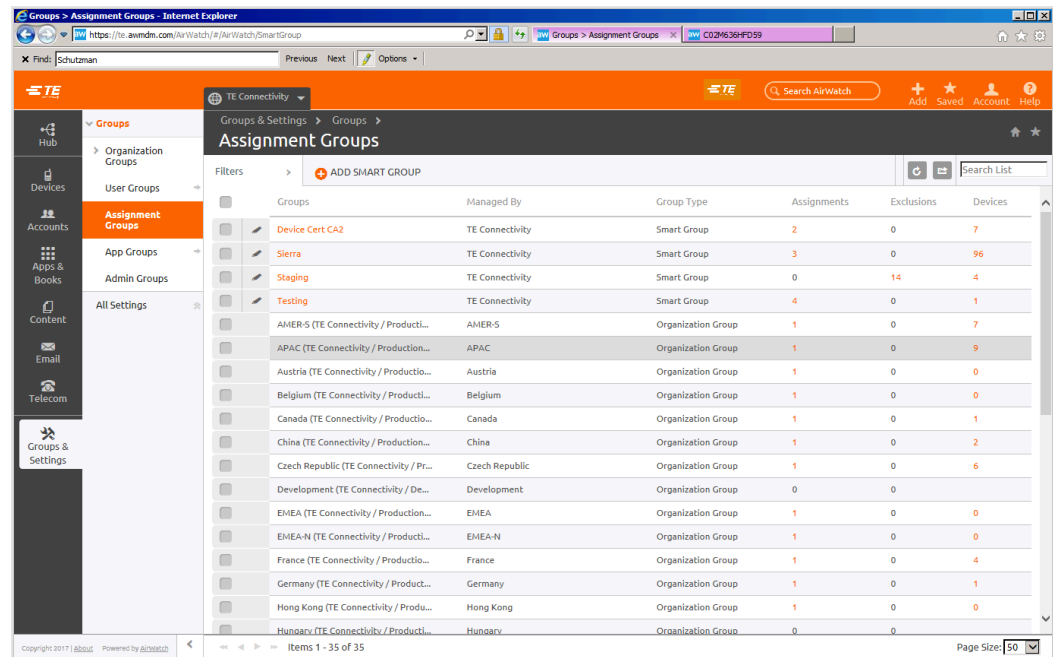
All profiles, and their current assignments can be viewed by selecting the “List View” from the “Profiles” section of the Devices menu in the AirWatch console.

Profile Details	Managed By	Assignment Type	Assigned Groups	Installed Status	Status
[Mac] Bind - US Apple macOS - Device Directory	TE Connectivity	Auto	United States	54 1 55	✓
[Mac] Cert - Device Cert [CA1] Apple macOS - Device Credentials	TE Connectivity	Auto	Sierra	92 2 94	✓
[Mac] Cert - Device Cert [CA2] Apple macOS - Device Credentials	TE Connectivity	Auto	Device Cert CA2	6 1 7	✓
[Mac] Cert - Issuing CA Apple macOS - Device Credentials	TE Connectivity	Auto	Production	103 0 103	✓
[Mac] Cert - Policy CA Apple macOS - Device Credentials	TE Connectivity	Auto	Production	103 0 103	✓
[Mac] Cert - Root CA Apple macOS - Device Credentials	TE Connectivity	Auto	Production	103 0 103	✓
[Mac] Cert - ZScaler Apple macOS - Device Credentials	TE Connectivity	Auto	Production	103 0 103	✓
[Mac] Encryption - FileVault				1	✓

# Assignment Groups

To assign the device to get a certificate from the secondary server, you will need to manually add it to a custom group within AirWatch.

Select the “Groups and Settings” icon from the bottom of the far left menu, then “Assignment Groups” from the sub menu.



The screenshot shows the AirWatch web interface for managing Assignment Groups. The left sidebar contains navigation options: Hub, Devices, Accounts, Apps & Books, Content, Email, Telecom, and Groups & Settings. The 'Groups & Settings' menu is expanded, showing 'Organization Groups', 'User Groups', 'Assignment Groups' (selected), 'App Groups', 'Admin Groups', and 'All Settings'. The main content area displays a table of Assignment Groups with the following columns: Groups, Managed By, Group Type, Assignments, Exclusions, and Devices. The table lists various groups, including 'Device Cert CA2', 'Sierra', 'Staging', 'Testing', and several regional/departmental groups like 'AMER-S', 'APAC', 'Austria', 'Belgium', 'Canada', 'China', 'Czech Republic', 'Development', 'EMEA', 'EMEA-N', 'France', 'Germany', 'Hong Kong', and 'Hungary'.

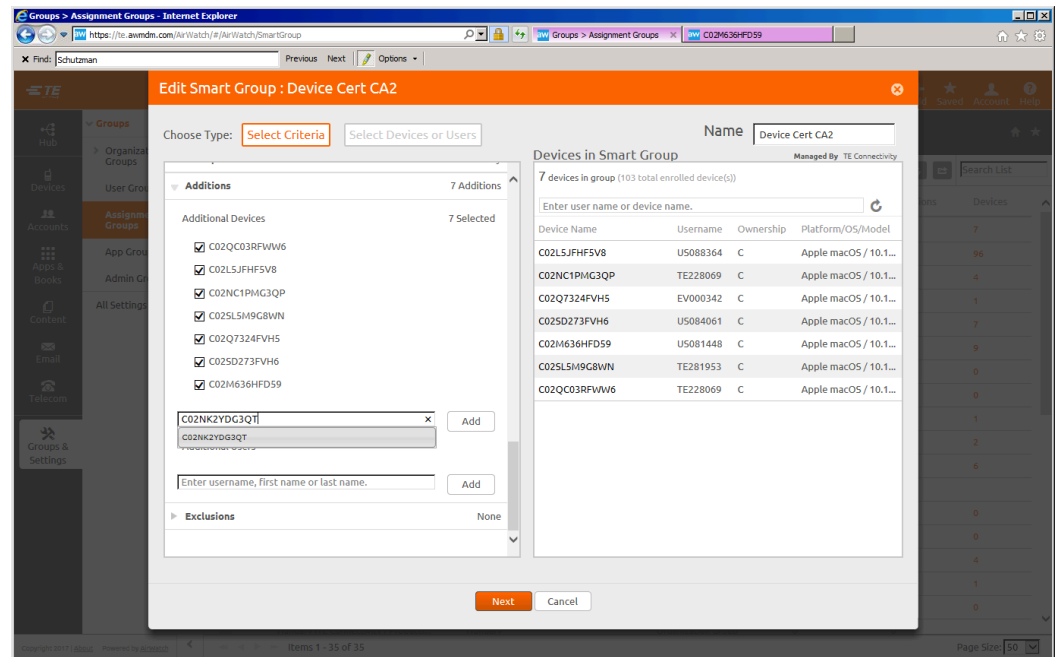
Groups	Managed By	Group Type	Assignments	Exclusions	Devices
Device Cert CA2	TE Connectivity	Smart Group	2	0	7
Sierra	TE Connectivity	Smart Group	3	0	96
Staging	TE Connectivity	Smart Group	0	14	4
Testing	TE Connectivity	Smart Group	4	0	1
AMER-S (TE Connectivity / Producti...	AMER-S	Organization Group	1	0	7
APAC (TE Connectivity / Production...	APAC	Organization Group	1	0	9
Austria (TE Connectivity / Producti...	Austria	Organization Group	1	0	0
Belgium (TE Connectivity / Producti...	Belgium	Organization Group	1	0	0
Canada (TE Connectivity / Producti...	Canada	Organization Group	1	0	1
China (TE Connectivity / Production...	China	Organization Group	1	0	2
Czech Republic (TE Connectivity / Pr...	Czech Republic	Organization Group	1	0	6
Development (TE Connectivity / De...	Development	Organization Group	0	0	0
EMEA (TE Connectivity / Production...	EMEA	Organization Group	1	0	0
EMEA-N (TE Connectivity / Producti...	EMEA-N	Organization Group	1	0	0
France (TE Connectivity / Productio...	France	Organization Group	1	0	4
Germany (TE Connectivity / Product...	Germany	Organization Group	1	0	1
Hong Kong (TE Connectivity / Proda...	Hong Kong	Organization Group	1	0	0
Hungary (TE Connectivity / Producti...	Hungary	Organization Group	0	0	0

# Editing the CA 2 Group

From the Assignment Groups screen, click in little pencil icon next to “Device Cert CA 2”. A list of criteria for group membership will appear. Scroll down to the bottom and expand the “Additions” section. Enter the serial number of the affected device in the field provided, it should return a list of search results (likely a single entry), select that result, and click the Add button.

The device should be added to the list on the right that shows the current members of that group.

Click Next.

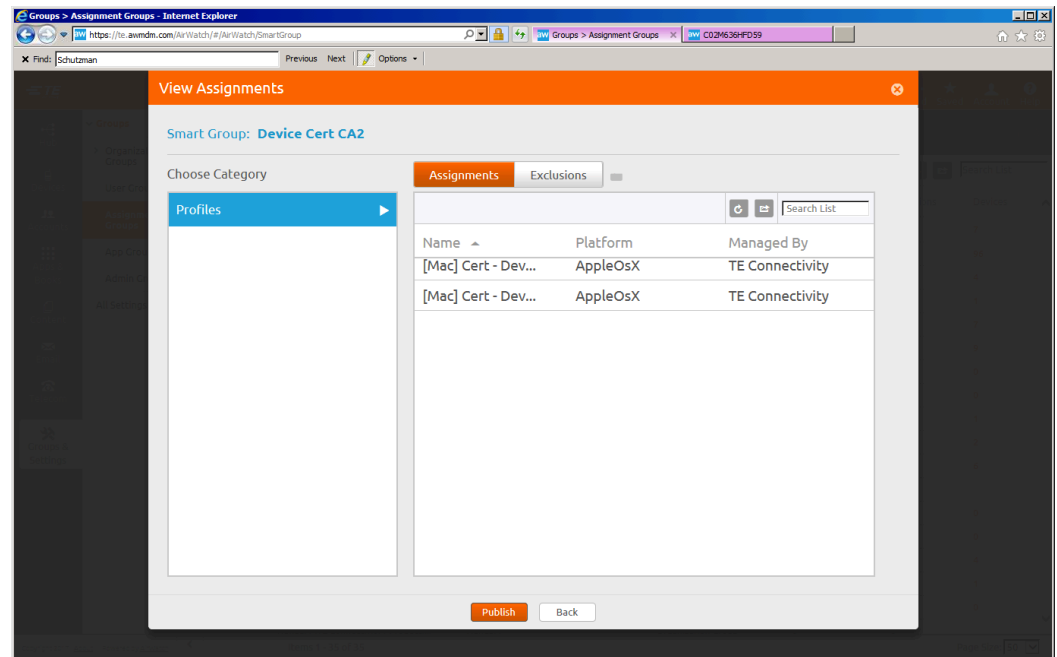




# Confirmation Screen

You will then be presented with a screen that shows two profiles that have been modified by this change in group membership, and will be sent to the device you added.

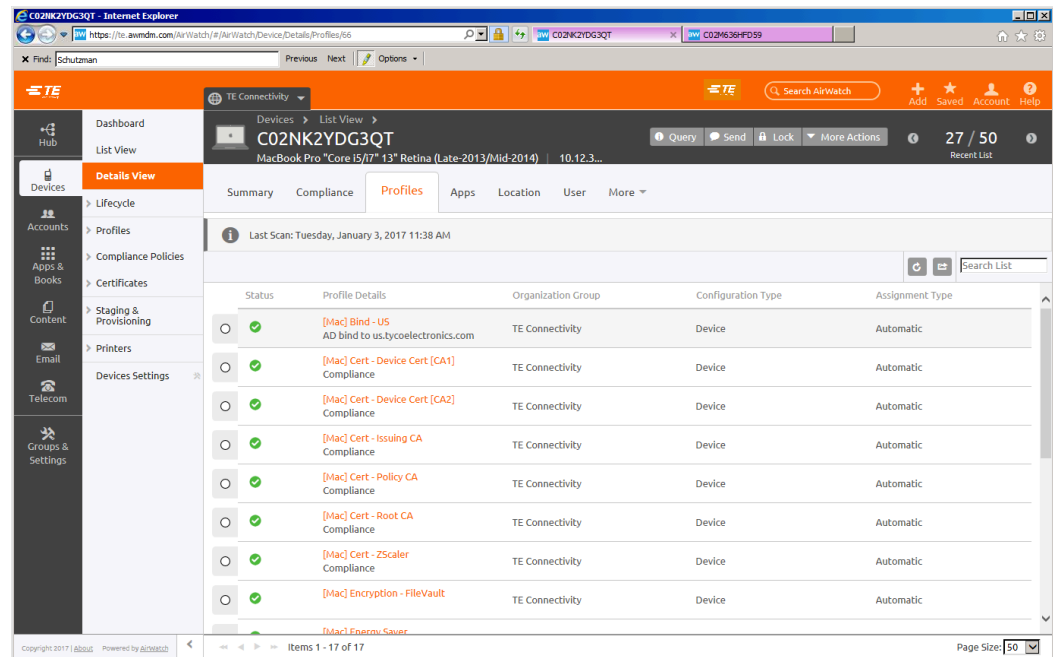
Click “Publish” to confirm this change and push the profiles to the affected device.



# Profile Installation

You can verify that the new profile has been successfully installed on the device by changing back to the profiles section of that device record.

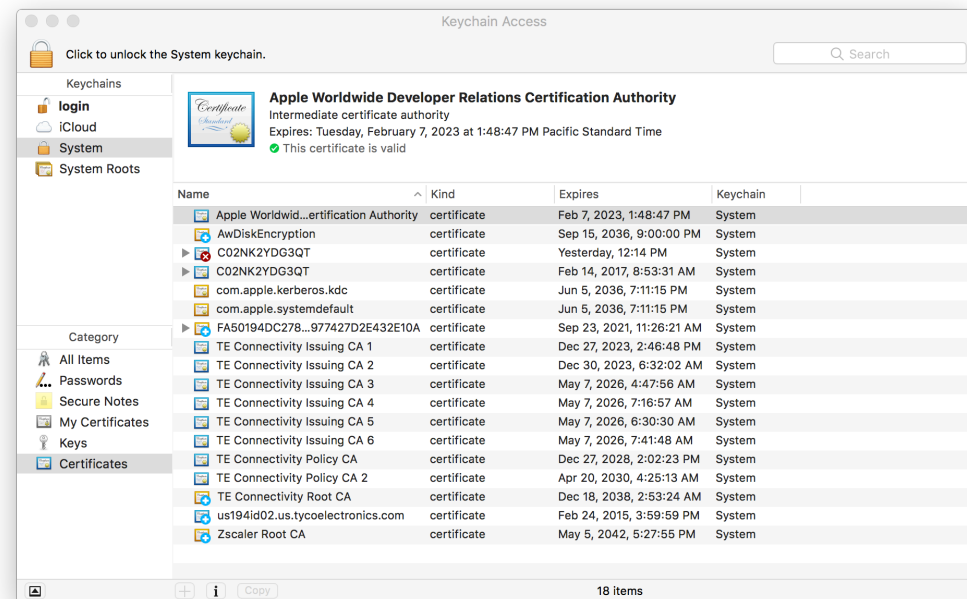
It may take several minutes for the device to receive the new profile. During this time, the checkmark will be grey instead of green, just keep querying and refreshing this screen until the check turns green. If it instead displays a red X or yellow exclamation mark, the profile has not installed and more targeted troubleshooting will be needed.





# Final Confirmation

A new certificate, with the same name as the device's serial number, should also be visible in Keychain Access.



---

# Conclusion

- Please be sure to include screenshots or exact text of any errors, either on the client or the AirWatch Admin Console, in the case notes.
- If the above process does not result in a new certificate being issued, please contact me separately, as interactive troubleshooting will likely be required.
- This process is only applicable to macOS Sierra devices that have been enrolled in AirWatch through running TEMPO. Devices that do not meet these requirements may be experiencing other issues outside of what this process outlines.