Contents

Version Details

Version Number	Changes	Reviewer/Contributor
1.0	Initial release of guide.	Andrew Price

Authors and Contributors

Andrew Price – Senior Systems Engineer, End-User Computing

andrewprice@vmware.com

Purpose

The Purpose of this document is to provide documented steps on successful troubleshooting measures when supporting Chrome OS managed devices within your environment. The document covers useful resources on Chrome OS integration into Workspace One UEM, differences between profile options and how to do some device side troubleshooting techniques that may help investigating challenges within an environment.

Chrome OS Troubleshooting Guide

How do I configure Chrome OS Management within Workspace One UEM?

To configure Chrome Management within your environment, there is an end-to-end guide available on TechZone at the following link. As a part of this guide, we will not walk through the entire setup process, we will however be confirming your integration has been setup successfully.

https://techzone.vmware.com/managing-chrome-os-devices-vmware-workspace-one-operational-tutorial#286225

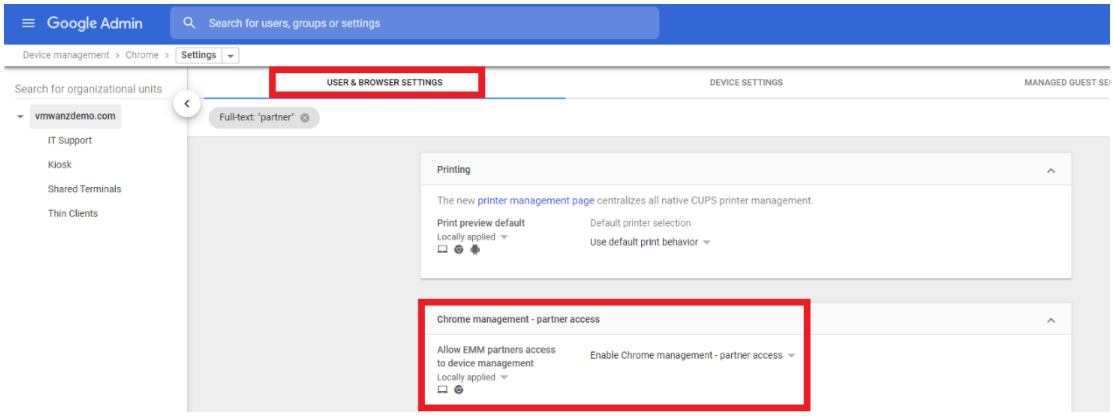
Confirming your Integration

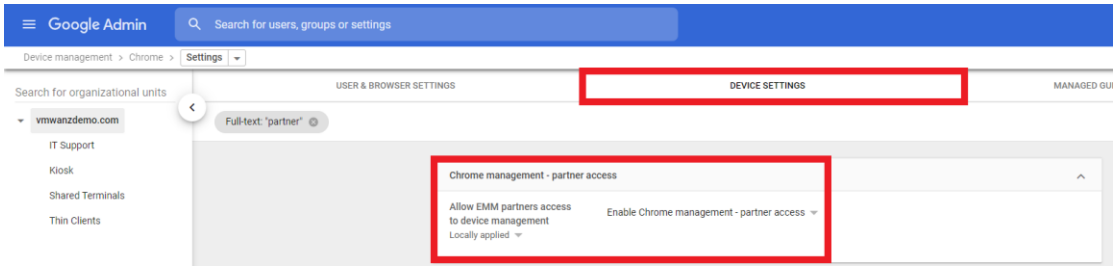
To confirm the environment has been configured correctly, there are several things to double check on both the Google Admin Console and inside Workspace One UEM.

First, check your Google Admin Console to confirm both Device and User policies have been enabled for 'Partner Access'. This is required to configure and deploy User and Device Profiles from Workspace One UEM.

Google Admin Console

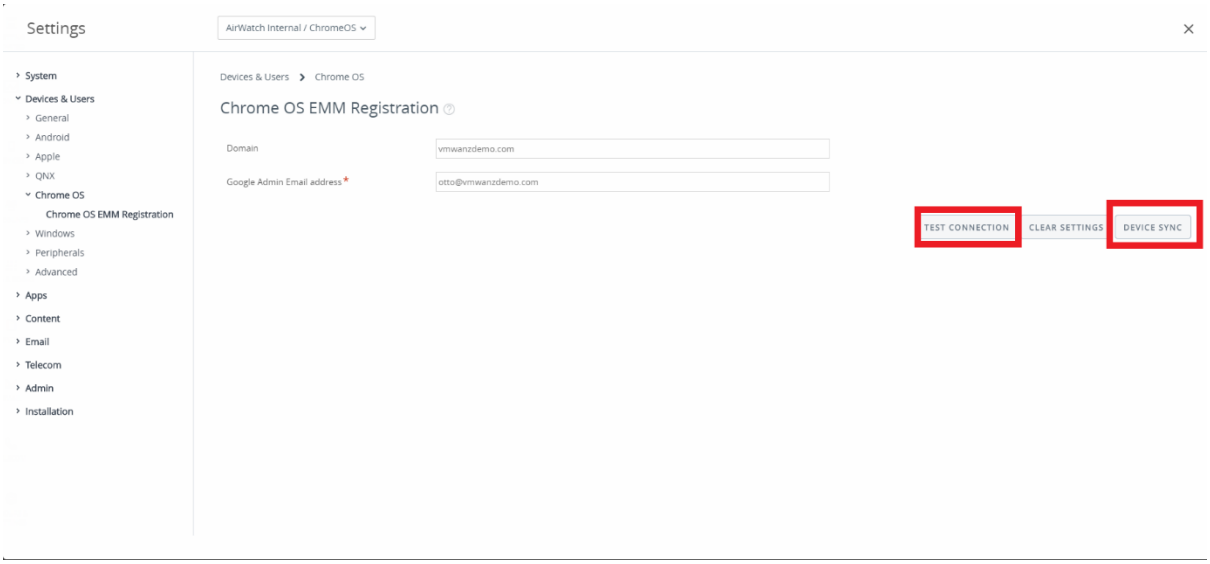
1. Navigate to admin.google.com and login with your admin credentials.
2. Navigate to Devices > Chrome Management > User & Browser Settings
3. Search for 'Partner Access' under both User and Device tabs and confirm they are 'Enabled'.



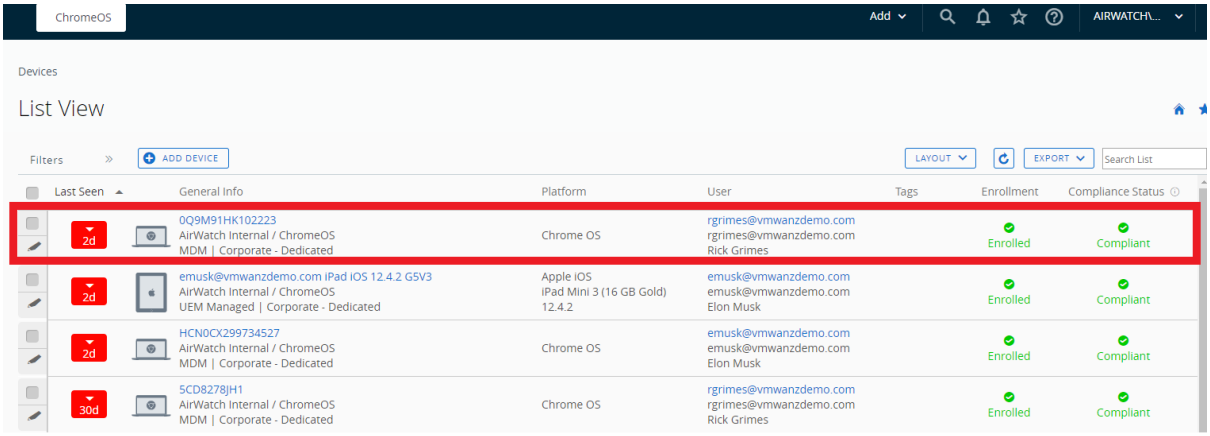


Workspace One UEM Console:

1. Navigate to your UEM Console and login.
2. Navigate to Device > Device Settings > Chrome OS > Chrome OS EMM Integration
3. Use the 'Test Connection' and the 'Device Sync' buttons to confirm the Integration is communicating correctly.



4. When you hit the Device Sync button, the devices within your environment should update with the last time they communicated with the Google Admin Console (UEM does not talk directly to the device).



How do Profiles work on Chrome OS deployments?

Within Workspace One UEM, you have the option of configuring either Device or User Profiles.

Device Profiles effect the entire system irrelevant of the logged-on user.

Example Device Profiles

- Enable/Disable Guest Mode on the OS.
- Enabling/Disabling System Updates and the conditions on how they install.
- Configuring Sign on Settings to use an Identity Provider.

User Profiles are configurations that are deployed to individual users irrelevant of which device that user logs into.

Example User Profiles

- The configuration of Chrome Bookmarks
- Enabling/Disabling the user from accessing Chrome Browser Incognito Mode.
- The deployment of Extensions (AKA Chrome Apps) from the Chrome Web Store. If the device supports it, Android apps can also be installed.

Chrome Devices that Support Android Apps - https://www.chromium.org/chromium-os/chrome-os-systems-supporting-android-apps

Why Are Device and User Policies Important?

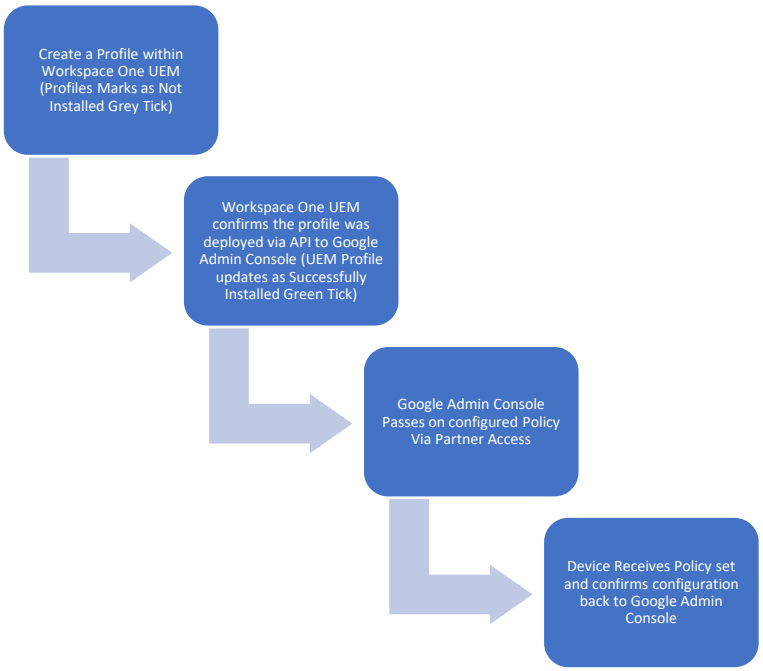
There are a couple of reasons both Device and User profiles important. The first reason being is that both will be utilised across an environment to meet the overall objectives of a Chrome deployment. Secondly, these profiles deploy to different scopes within Workspace One UEM.

Device Profiles can be deployed to an Organisation Group within the console or to an Assignment Group. User Profiles only deploy to User Groups so the way the deployment is managed is not necessarily the same as the other OS deployment scenarios within a customer's environment.

When considering deploying Chrome Devices within Workspace One UEM, it is essential that the customer understands this and can create required groups so that Profiles can be deployed.

How do Profiles get Delivered to a Device?

Because Workspace One UEM does not communicate directly to the device, Policies/Profiles are delivered via the Google Admin Console. The way this will happen will look like the following



How can I Confirm if my Profiles have been Configured on the Device?

On the device side you can complete the following.

- Login to the Chrome device
- Open a new Web Browser and navigate to Chrome://Policy
- Search this list for the setting you enabled/disabled (See example below of my setting to block Guest Mode).
- Alternatively, confirm whether the setting you have configured (EG: Bookmarks) have installed, configured or been enabled/disabled.

What else Does the Policy section tell me?

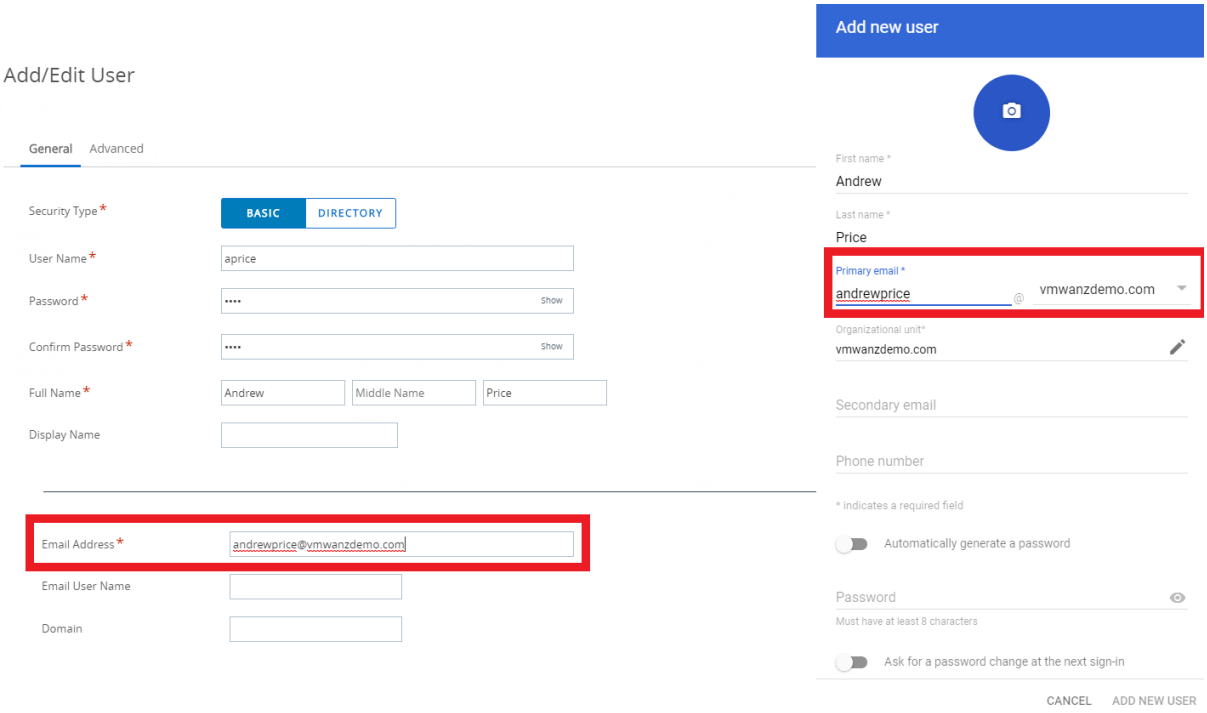
There are a bunch of additional resources that appear when you navigate to Chrome://policy on a Chrome Device. These details can also be exported to JSON in case you need to reference further Some of these include the following.

- Enrolment Domain: Shows the domain I have enrolled the device into.
- Fetch Interval: Shows when the device should 'Check In' to the Google Admin Console.
- Last Fetched: This field highlights when the device last talked back to the Google Admin Console for Policy Update.
- Further down the list you will also see configurations of Extension and their Extension ID from the Chrome Web Store. We'll cover this in more detail later.

How are Users Synced From Workspace One UEM into the Google Admin Console and Vice Versa?

In short, they are not between Workspace One and Google. Workspace One UEM would integrated into directory services via the VMware Enterprise Systems Connector and Google Users would sync to the Google Administrator Console via the Google Cloud Directory Sync Tool.
https://support.google.com/a/answer/106368?hl=en

What you should be cognizant of when utilising Chrome OS Management within Workspace One UEM is that your user account does exist in both environments AND the unique identifier for this user is their email address (Google Users do not have the concept of username). See below example.



The benefit of this scenario though is that AD synchronisation is not necessarily required for either Google or Workspace One because you have the ability to create a 'Google Account' natively from the Google Admin Console and you can create a Basic User within Workspace One UEM.

Workspace One UEM Extension for Chrome OS – What is it and why do we have it?

In Workspace One UEM version 1910 we introduced a new component in the form of an Extension to allow Administrators to manage at scale, the distribution of client certificates to devices and users. This is the recommended approach from Google to achieve this.

https://support.google.com/chrome/a/answer/6080885?hl=en

https://developer.chrome.com/extensions/enterprise_platformKeys

The UEM Extension supports both Device and User certificates deployed via profiles and is deployed via the Network Profile in either Device or User context. The reason for this as you may have scenarios within Chrome OS which apply to either context.

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1912/Chrome_-OS_Platform/GUID-E663EB1C-A262-467B-998E-0A61547CC9CB.html

User Context:

- User Authentication on to a corporate network specific to one user account. When a new user logs into the device, they authenticate using their own certificate.

Device Context:

- Network Authentication using a certificate for a device in Kiosk Mode.

One thing to consider in either scenario is that Extensions are only delivered in a User context so even if you are deploying certificates in a device Context, you will still need to authenticate onto the device prior to using Kiosk Mode.

Uploaded Certificates

Certificates can additionally be uploaded and manually deployed out via the Profile without using a CA template at all. This is common in a scenario such as the Root CA certificate which may not be included in the client certificate chain.

What Type of Certificates are Support and How does a Certificate Land on the Device?

Currently, Microsoft Active Directory Certificate Services (ADCS) are supported within the UEM Extension.

Where do I find the Extension?

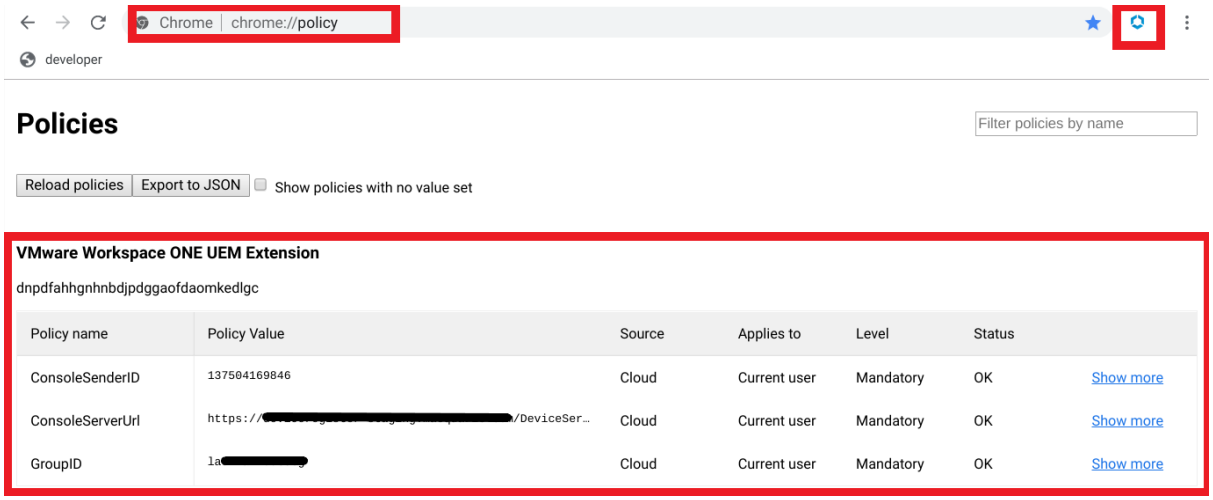
The Extension is available at the following URL. If you search the Chrome Webstore from a device though, you will not find it as it is hidden.

https://chrome.google.com/webstore/detail/vmware-workspace-one-uem/dnpdfahhgnhnbdjpdggaofdaomkedlgc

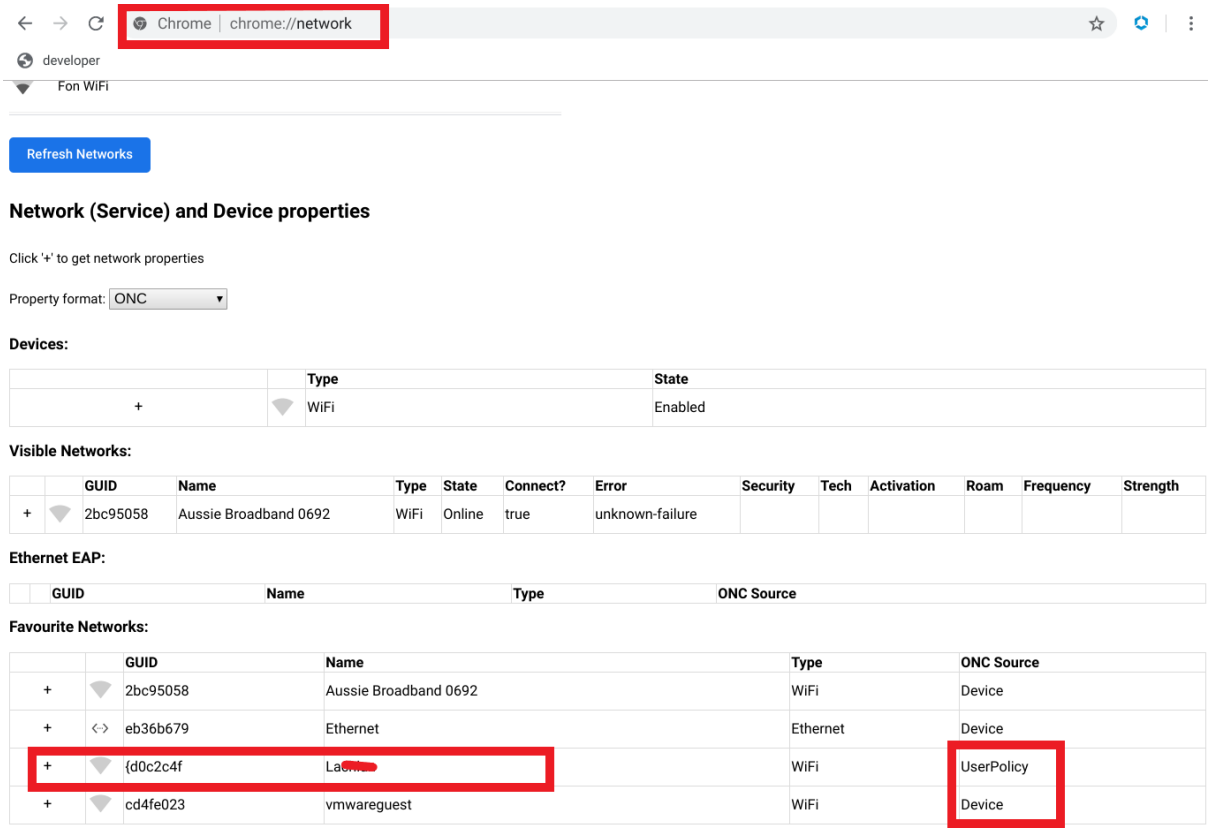
What are some of things I can look out for when Troubleshooting Certificate Issues?

1. The first thing to check is whether the UEM Extension is installed on the device. There are a few ways to confirm this.
    a. First, within the Chrome Browser itself, you should be able to see that the UEM Extension is appearing in the top bar, on the right-hand side. See example below.

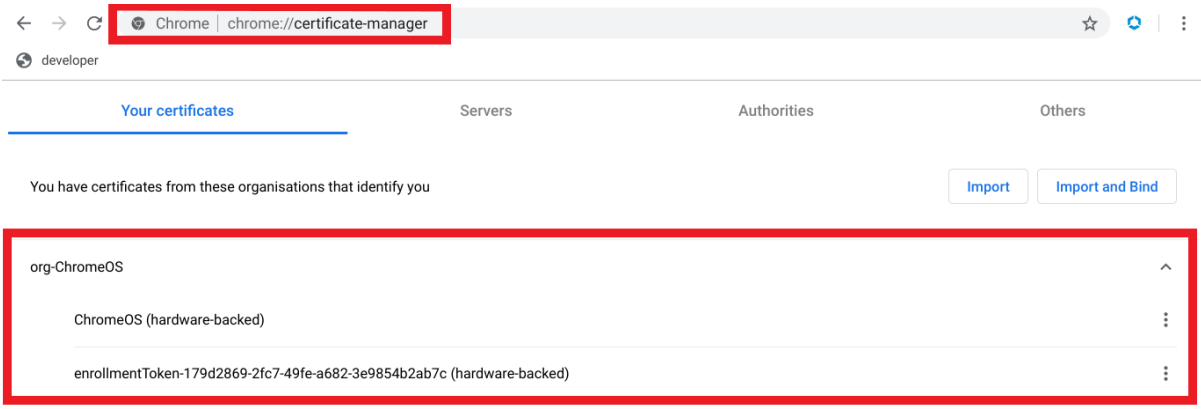
    b. Secondly, within the Chrome Browser, navigate to Chrome://Policy and confirm whether you can view the UEM environment details (DS Server, GroupID) in the Extension information.

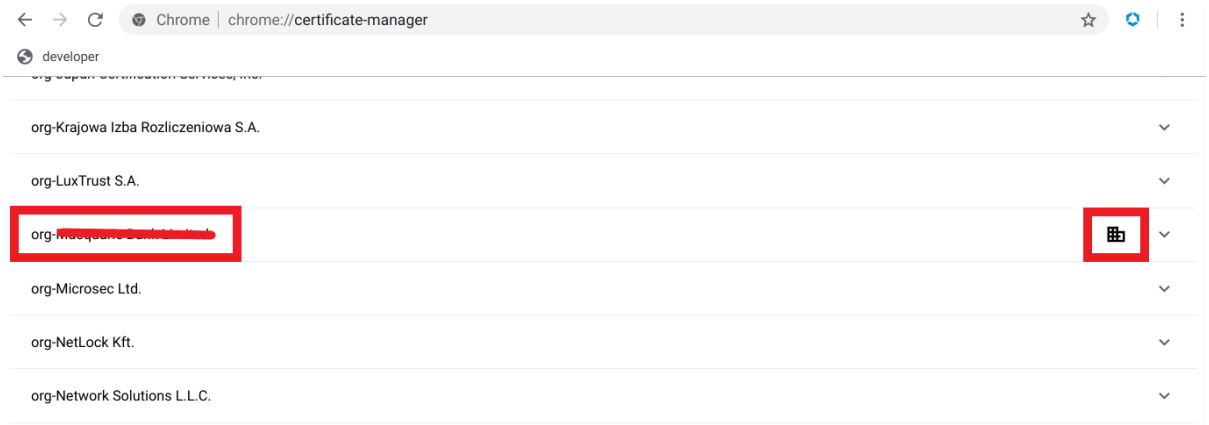


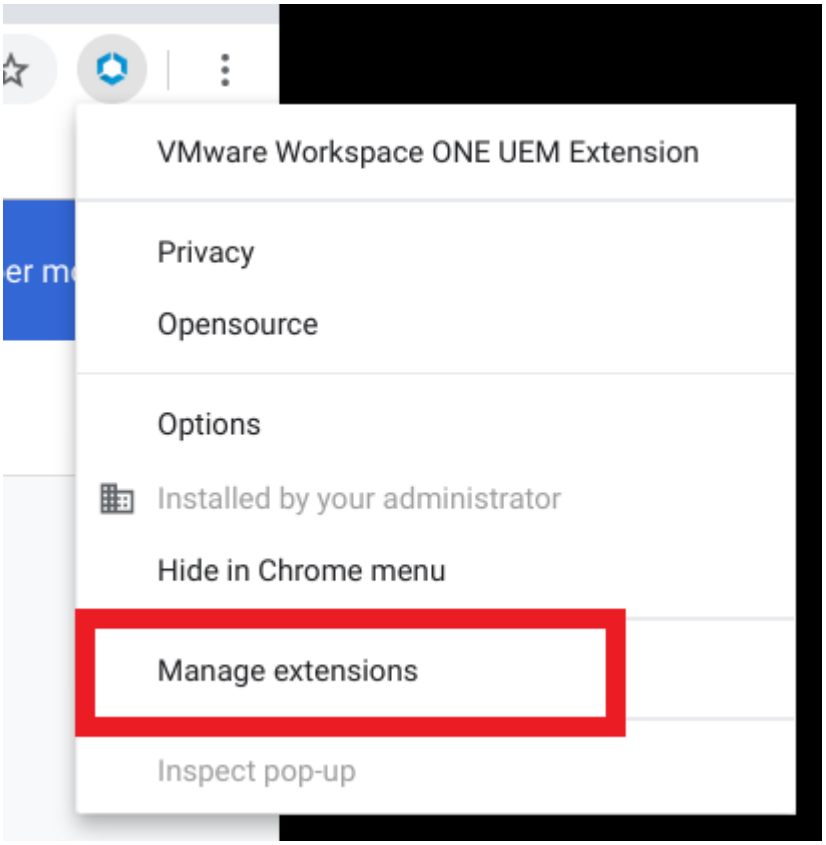
2. Confirm whether the SSID details you have deployed within your profile have landed on the device. To this, you can navigate to Chrome://network on the device and confirm the SSID appears in the list. On the far-right hand side, you can also confirm the context on which you have deployed in by viewing the Device or User.



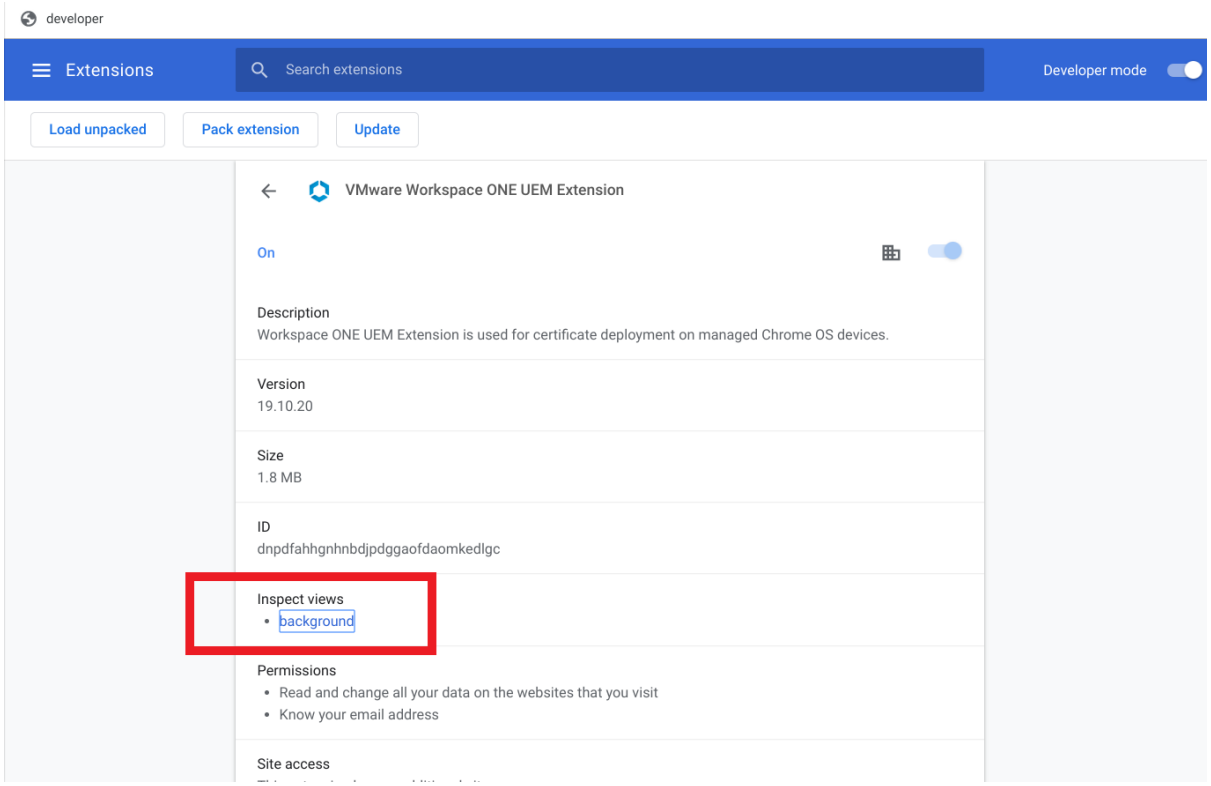
3. Confirm whether a certificate has landed on the device. To do this, navigate to Chrome://certificate-manager. Under the 'Your Certificates' field, you should see a certificate included with the details you have included in your Certificate Authority Template. Additionally, if you navigate to the 'Authorities' tab, you should find your CA details with a building icon depicting that the configuration is managed by your Organisation.



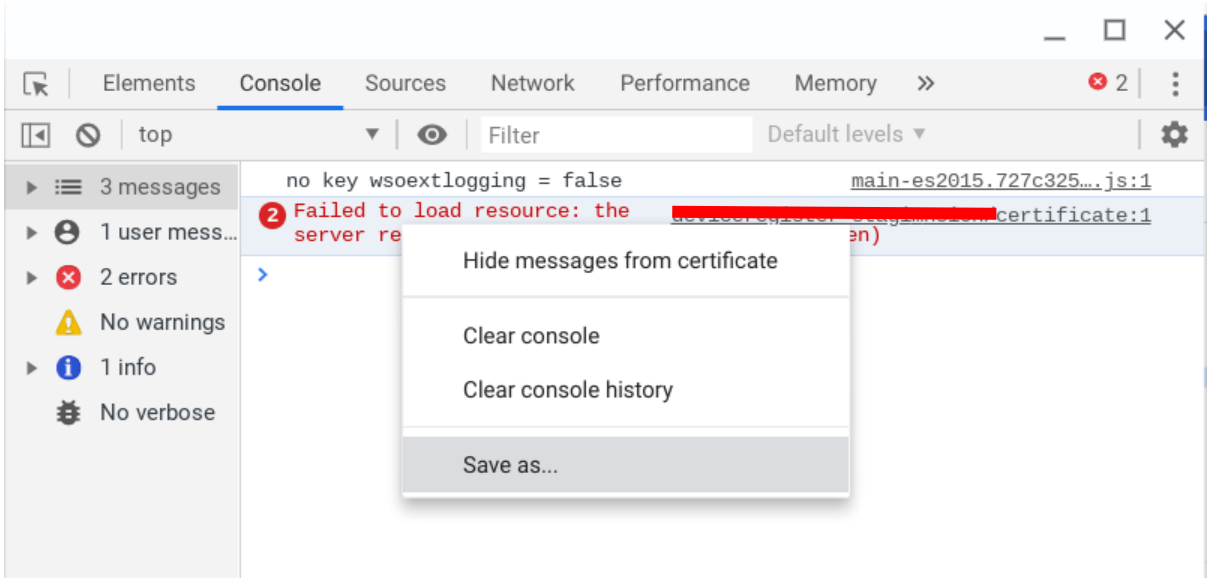


4. You can view the Extension logs by right-clicking on the extension and clicking on ‘Manage Extensions’.
   a. 

   b. From here, you should be able to see the extension details and a field to inspect ‘Views’.



c. From here, click the 'Background' option and confirm whether there are any errors appearing in the log files. If needed, right click and export the logs to a file for further troubleshooting.



Additional useful resources that may help with Troubleshooting

1. Navigating to Chrome://device-log may be helpful in determining whether there are any communication or overall issues. This should highlight all different components from

Network, User, Device, Policy and errors which may help if you are looking for specific issues within an environment.

2. Chrome OS Operational Tutorial on Techzone - https://techzone.vmware.com/managing-chrome-os-devices-vmware-workspace-one-operational-tutorial#286225
3. VMware Docs Chrome OS Extension List - https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1912/Chrome_-OS_Platform/GUID-E663EB1C-A262-467B-998E-0A61547CC9CB.html
4. Chrome Device Management by Google - https://support.google.com/chrome/a/answer/1289314?hl=en