BYPASSING CCX OOBE SETUP WIZARD USING POLY LENS

FORWARD

When referring to the related Poly KB articles, in order to bypass the Setup Wizard, the settings to the right need to be made in order to successfully bypass the OOBE wizard.

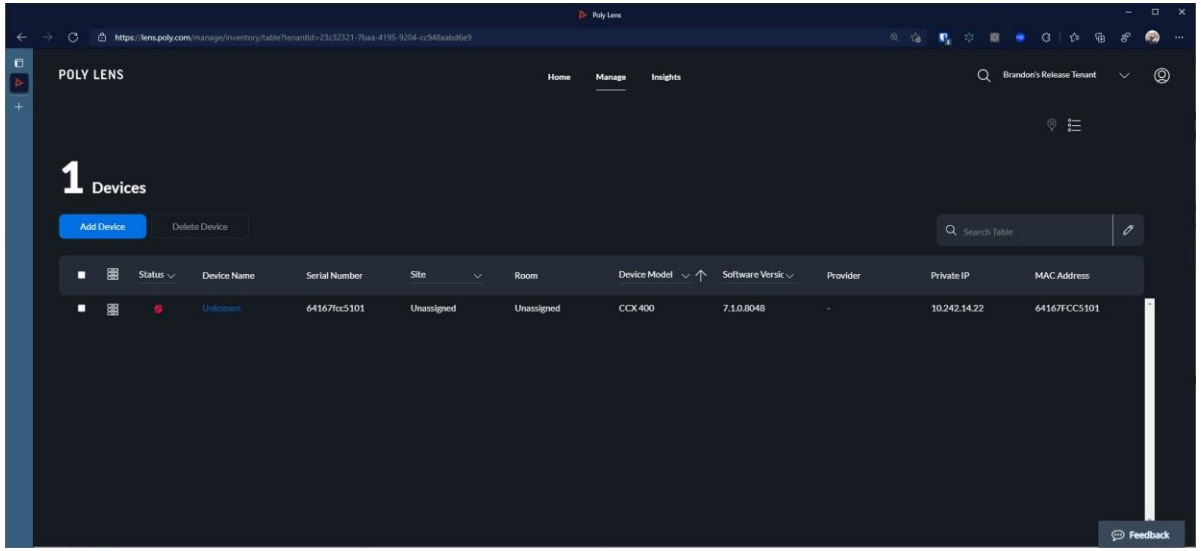
NOTE: The values presented they are set to are just examples and can be adjusted based on your deployment needs

This guide will walk through configuring a new Poly Lens Account for performing these steps for a customer.
IMPORTANT: Access to the DHCP Server to specify the DHCP Option 66 is mandatory for completing this task

```
device.auth.localAdminPassword=“789”
device.auth.localAdminPassword.set=“1”
device.baseProfile=“Lync”(“MSTeams”/“Generic”)
device.baseProfile.set=“1”
device.eulaAccepted=“1”
device.eulaAccepted.set=“1” device.set=“1”
feature.webSignIn.enabled=“1”
lcl.ml.lang=“English_United_States”
prov.eula.accepted=“1”
tcpIpApp.sntp.olsonTimezoneID=“America/Denver”
```

SETTING UP THE ENVIRONMENT

Before you plug in any devices

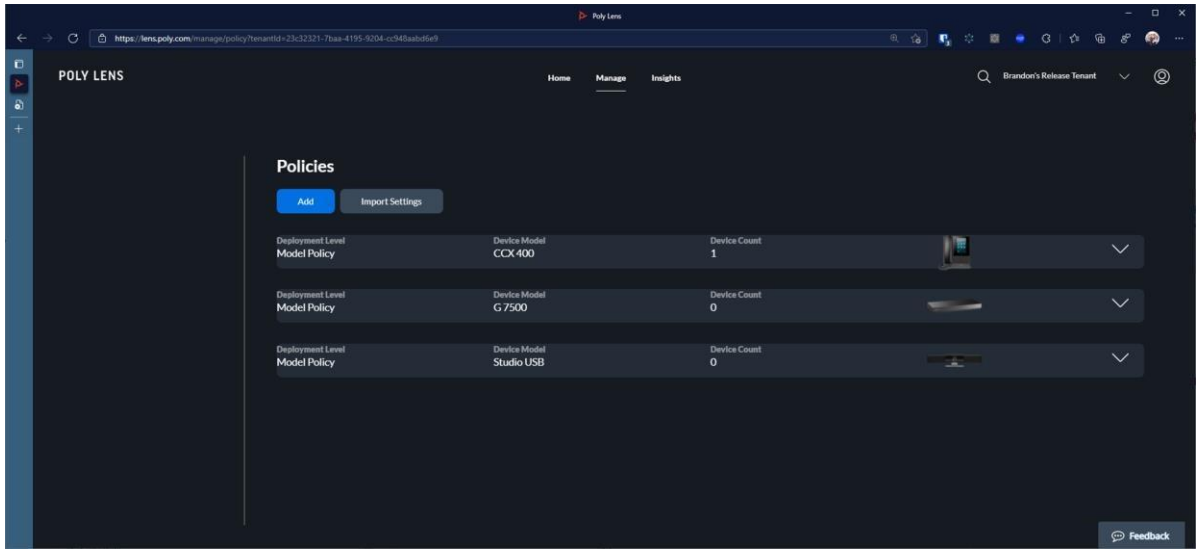


Staring from a new account and a scenario example of deploying new CCX 600s, we have an account that only has a single CCX 400 deployed.

NOTE: These steps were performed with a CCX 600, but would apply to any CCX Model (400/500/600/700)

SETTING UP THE ENVIRONMENT

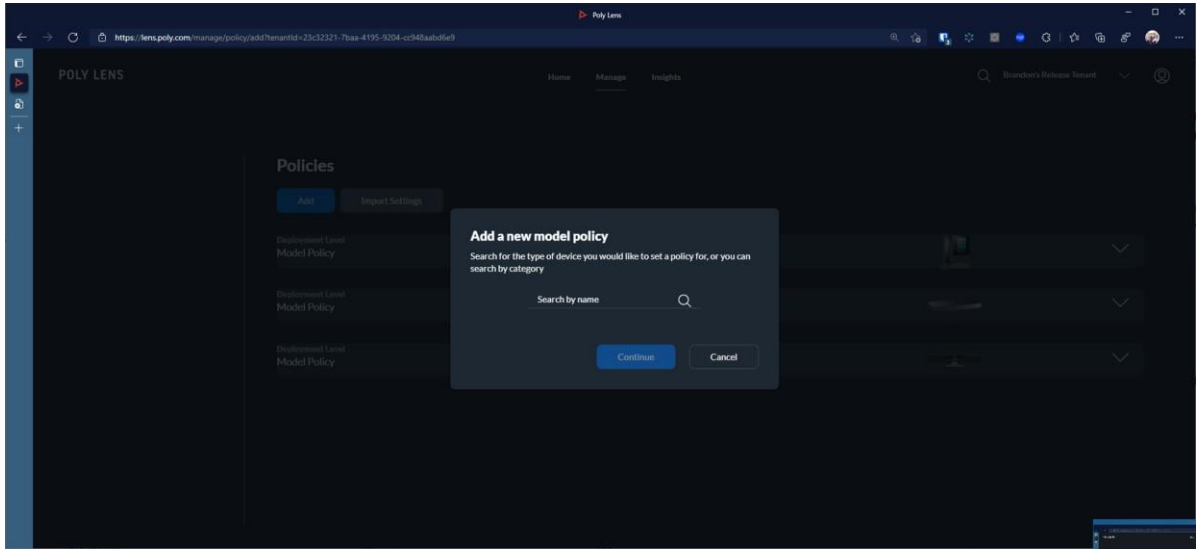
Before you plug in any devices

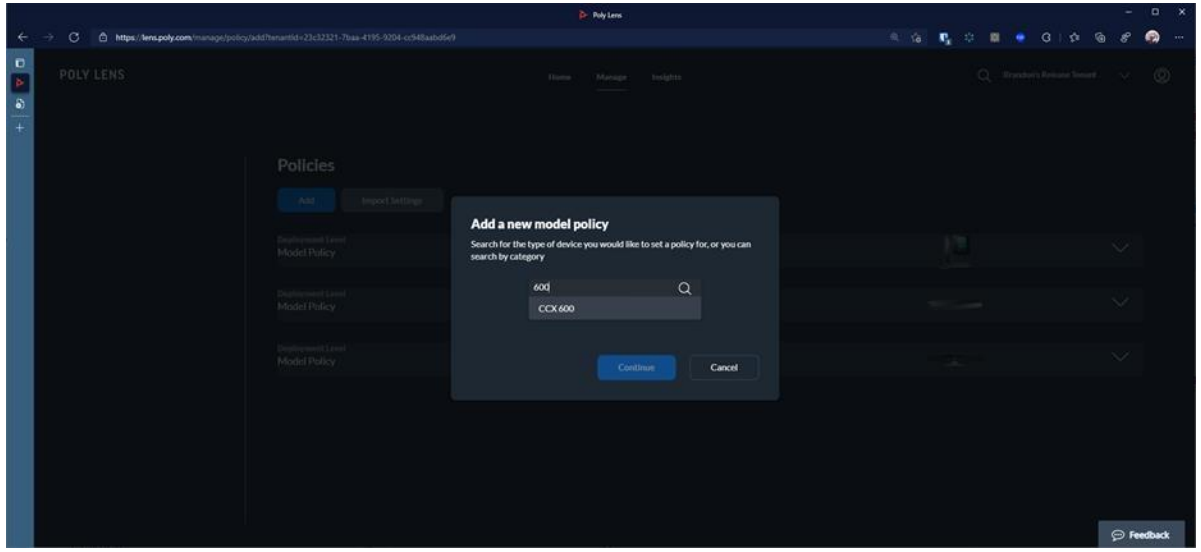


First step is to define the model policy

Manage > Policies

SETTING UP THE ENVIRONMENT





SETTING UP THE ENVIRONMENT

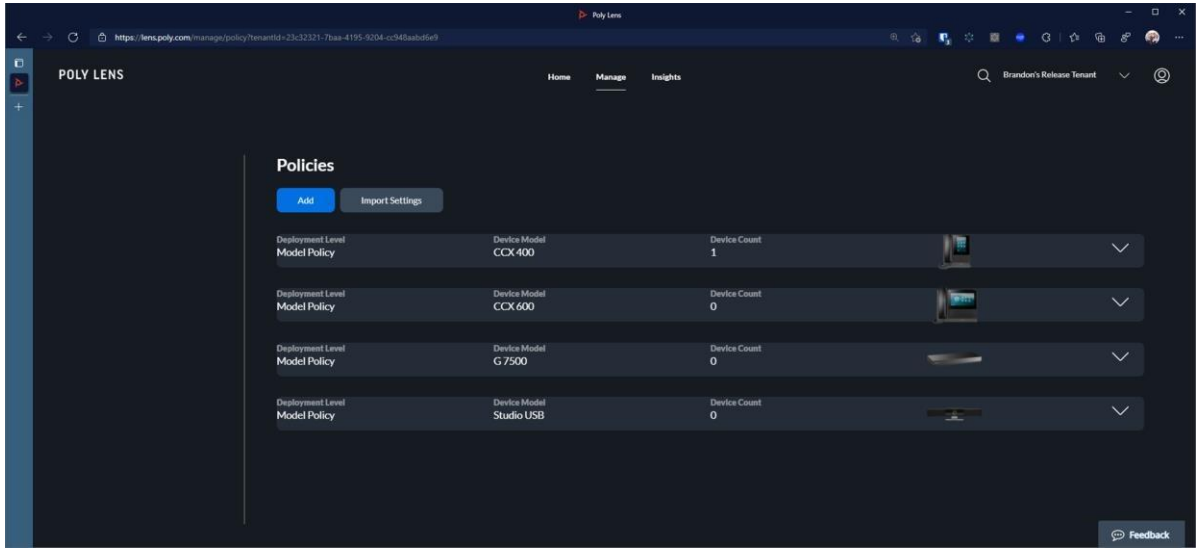
As This account did not have any CCX600s, we need to add that model to this account.

Click *Add*

Specify the Model, in this case, it's a CCX 600

SETTING UP THE ENVIRONMENT

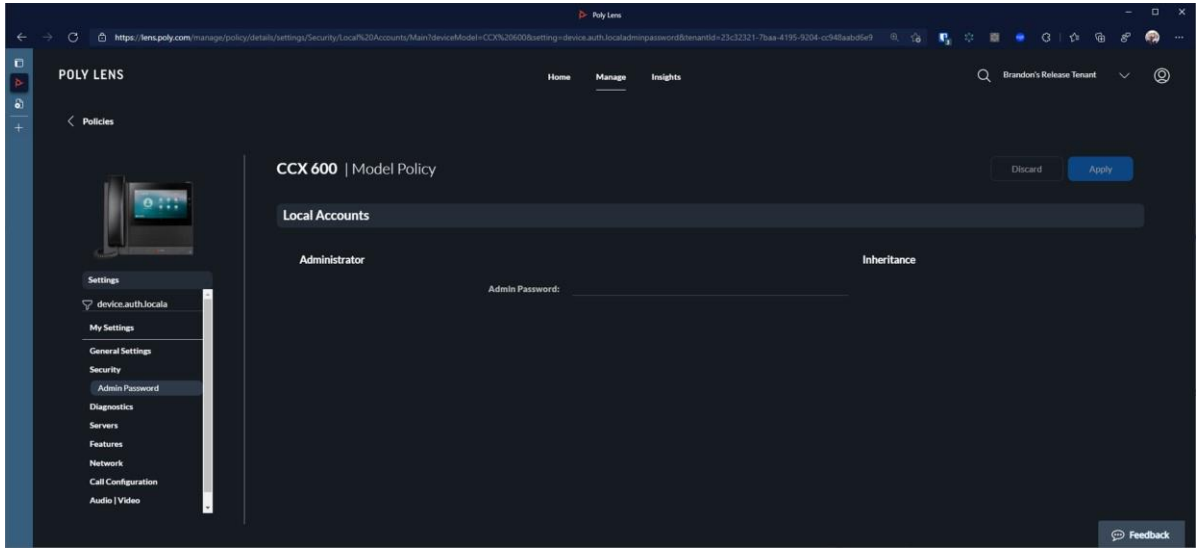
Before you plug in any devices



Now that it's added, we can click in and select the model to start specifying the policy

SETTING UP THE ENVIRONMENT

Define the necessary Policy



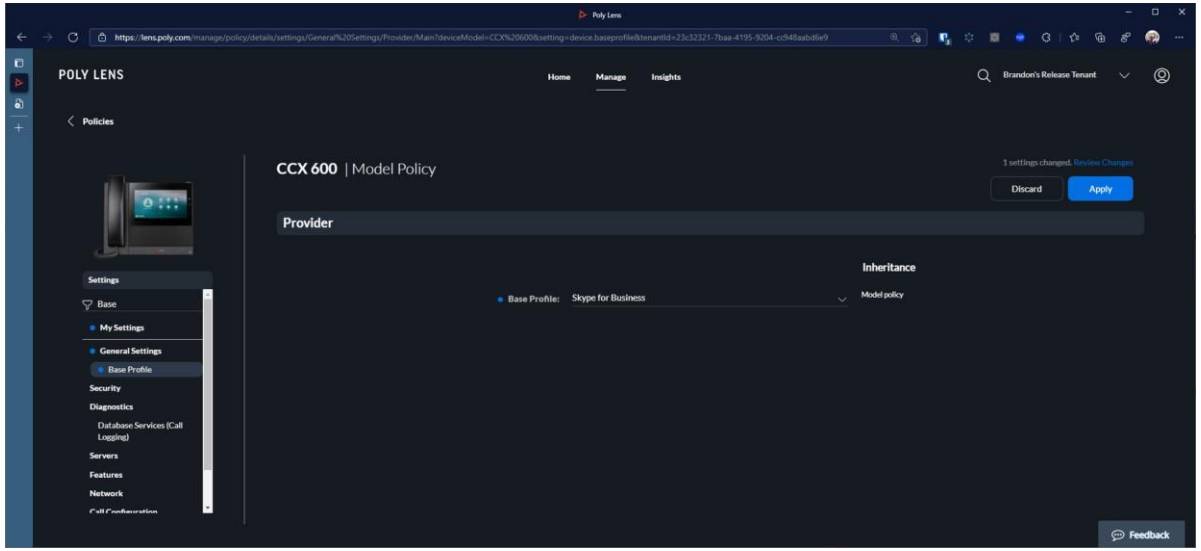
`device.auth.localAdminPassword`

Security > Local Accounts > Administrator

Admin Password

SETTING UP THE ENVIRONMENT

Before you plug in any devices



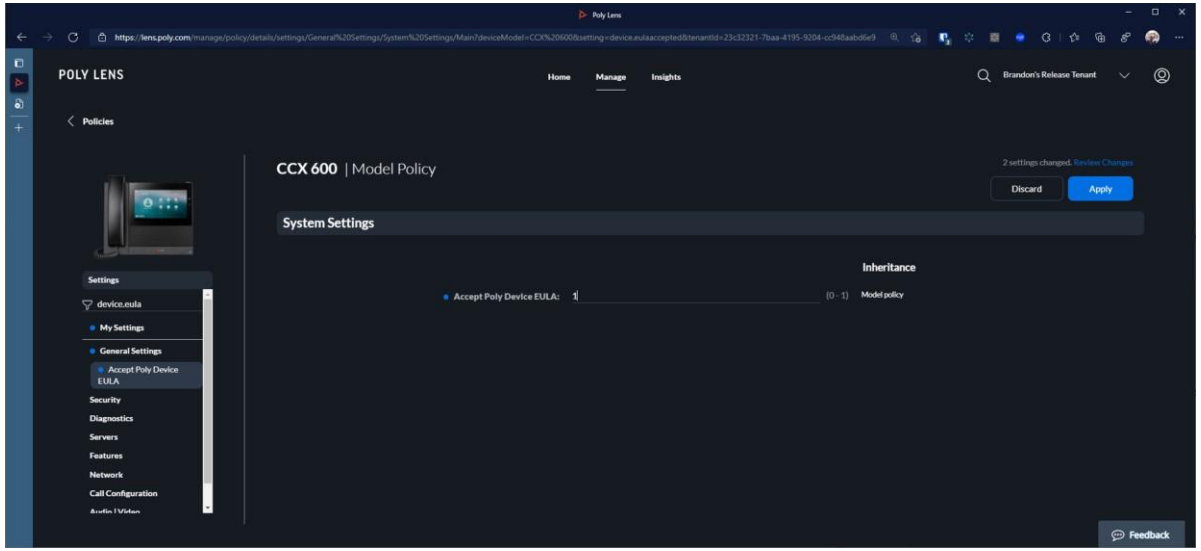
`device.baseProfile`

General Settings > Provider

Base Profile

SETTING UP THE ENVIRONMENT

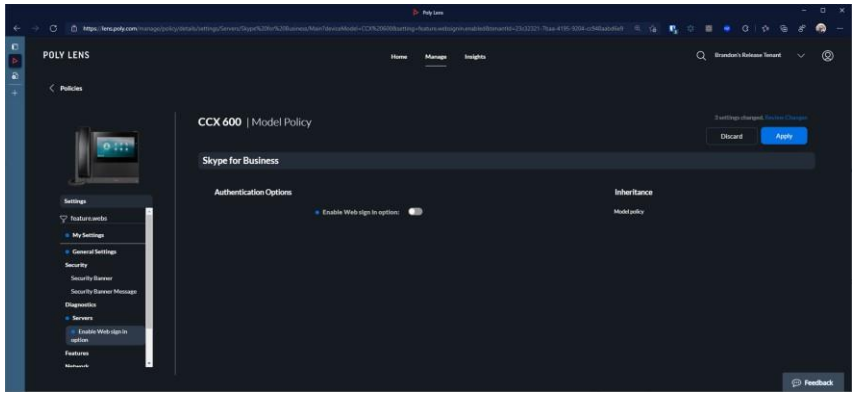
Before you plug in any devices

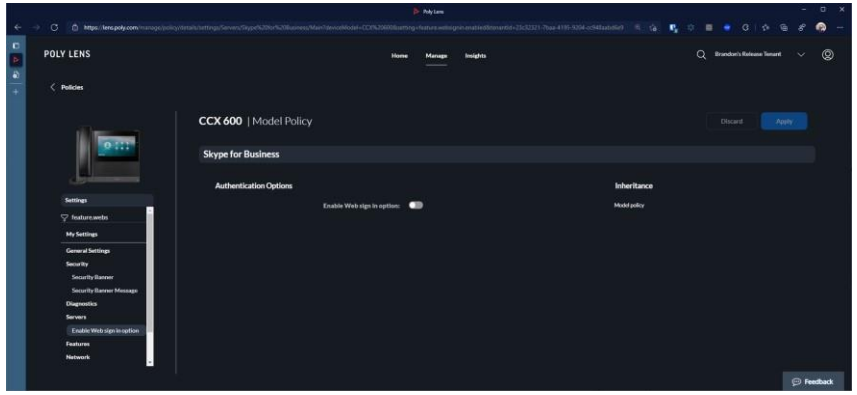


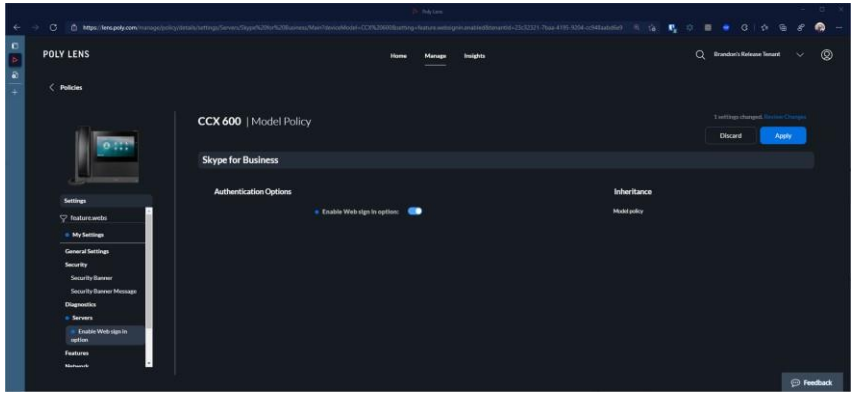
`device.eulaAccepted`

General Settings > System Settings Accept

Poly Device EULA







SETTING UP THE ENVIRONMENT

Before you plug in any devices

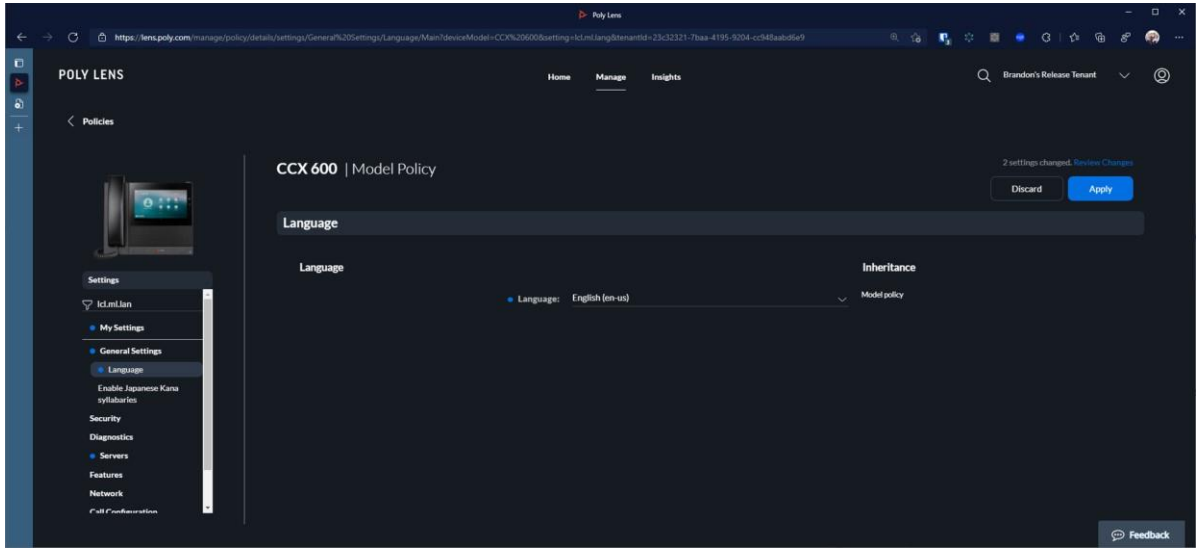
`feature.webSignIn.enabled`

Servers > Skype for Business > Authentication Options

Enable Web Sign in option

SETTING UP THE ENVIRONMENT

Before you plug in any devices



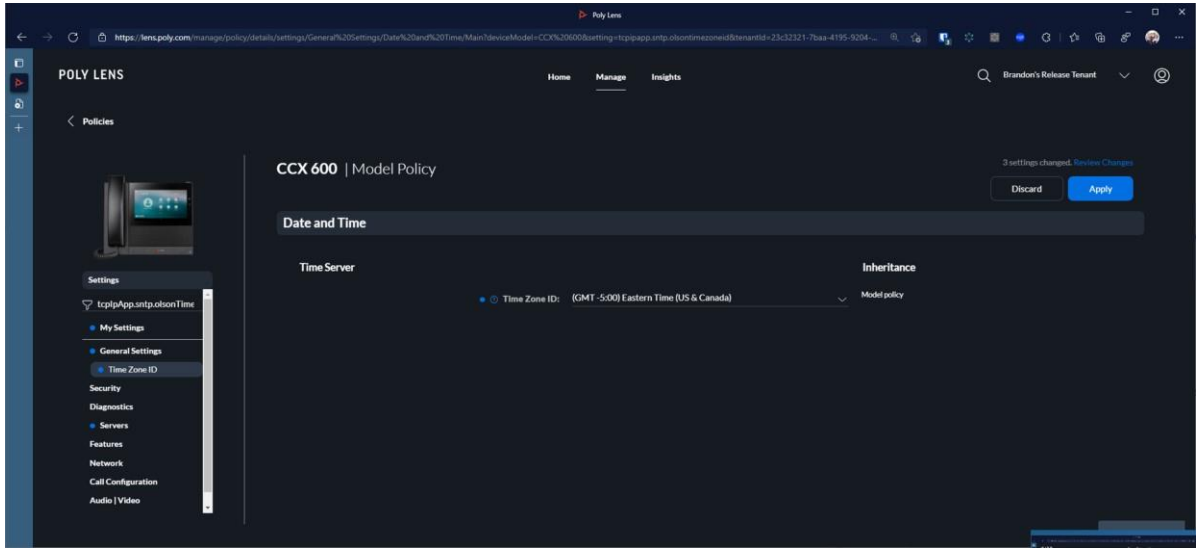
`lcl.ml.lang`

General Settings > Language

Language

SETTING UP THE ENVIRONMENT

Before you plug in any devices



`tcpIpApp.sntp.olsonTimezoneID`

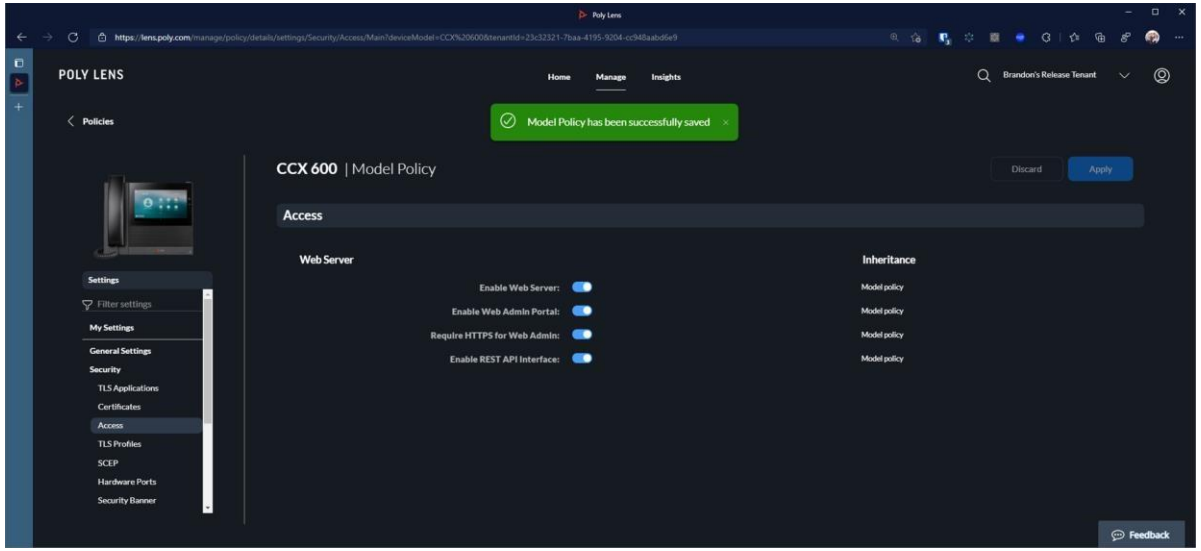
General Settings > Date and Time > Time Server

Time Zone ID

SETTING UP THE ENVIRONMENT

Before you plug in any devices

Enabling Web Server (Optional for Validation)



Security > Access > Web Server

Enable Web Server

Enable Web Admin Portal

Require HTTPS for Web Admin

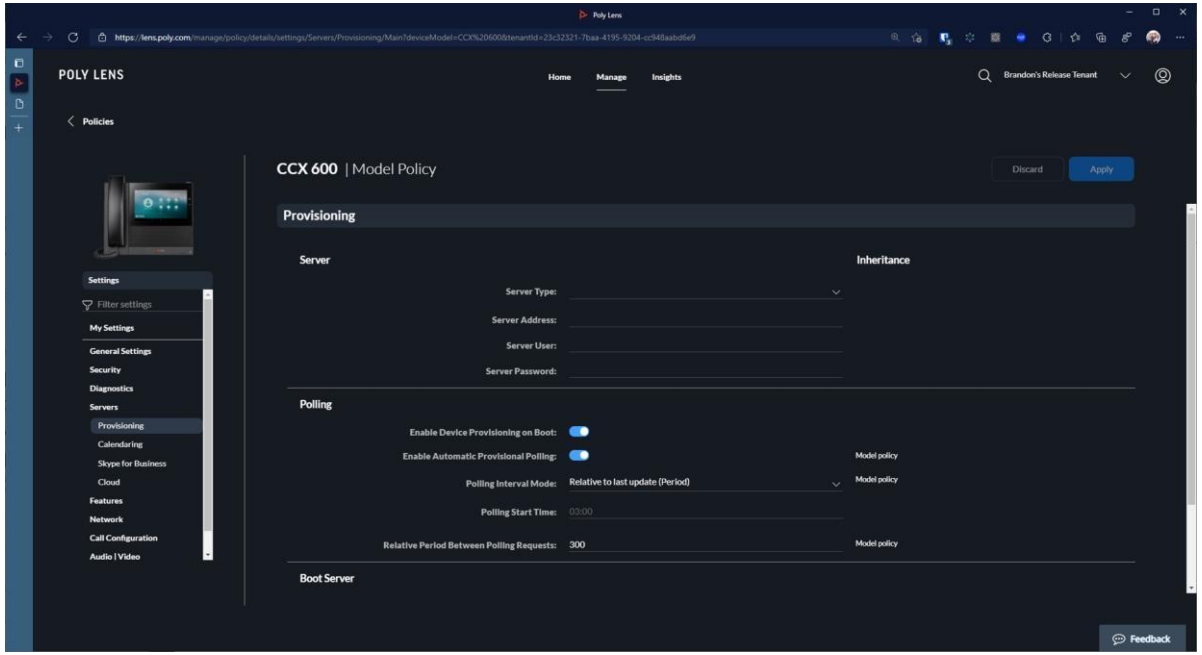
Enable REST API Interface

Before you plug in any devices

Shorten Polling Period for quicker config sync's

SETTING UP THE ENVIRONMENT

(optional)



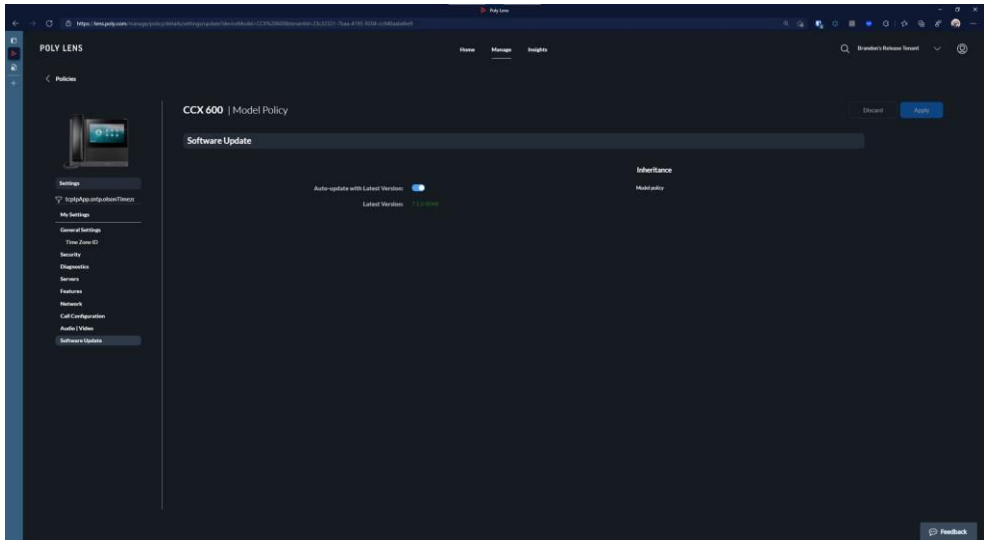
Servers > Provisioning > Polling

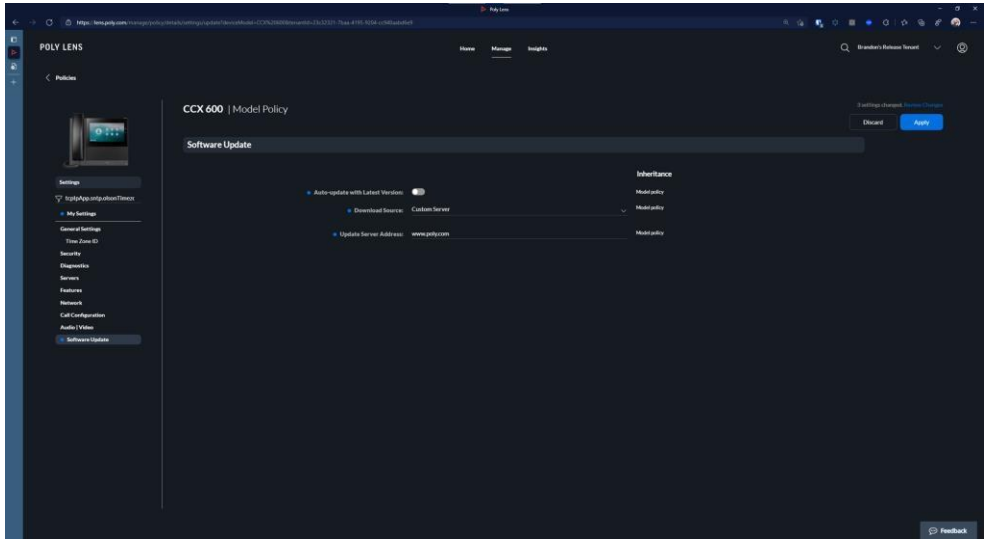
Enable Automatic Provisional Polling

Polling Interval Mode

Relative Period Between Polling Requests

NOTE: This step is optional as the device will get a generic Lens Policy having the device check every 24 hours, this just allows for a shorter interval. Although 300 was defined here, for early releases of CCX, 3600 seconds, or every hour, is the minimum polling period. Setting 300 will default on the device to 3600.





SETTING UP THE ENVIRONMENT

Before you plug in any devices

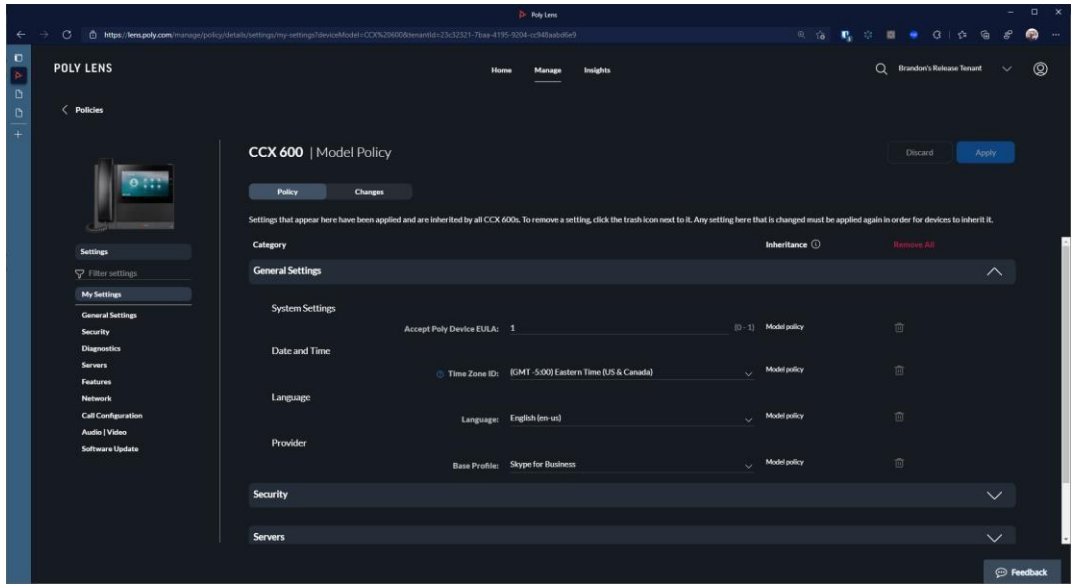
Define a policy to provide no software

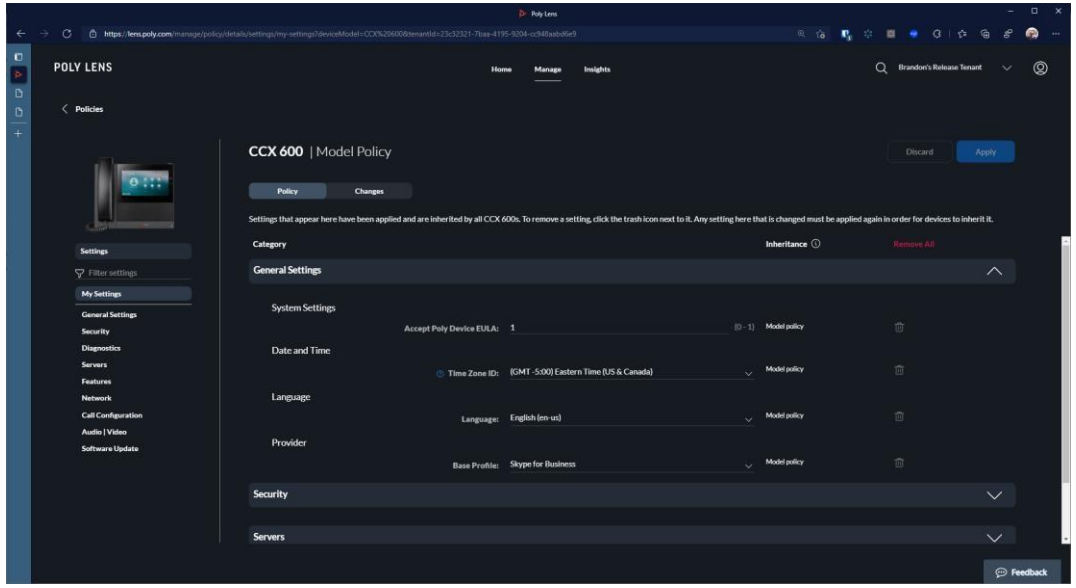
Software Update

Disable Auto-update with Latest Version

Set the download server to Custom Server

Provide a generic fake address (in this case pointing to just www.poly.com is enough as there are no valid files there, but you can also just put something like. www.file.loc) as a value here is necessary to save the Policy.





SETTING UP THE ENVIRONMENT

Verify your Configuration Policy is defined

Now that all settings are defined, go through ‘My Settings’ to verify that the policy is defined.

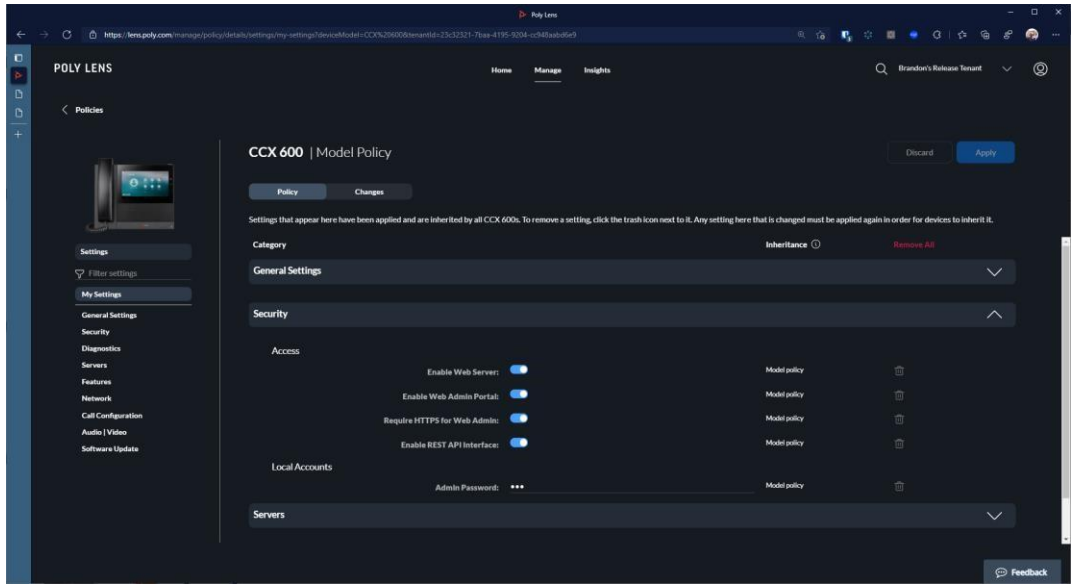
Make sure they match what’s expected, additional settings can be defined here, but validate that the mandatory settings are showing here.

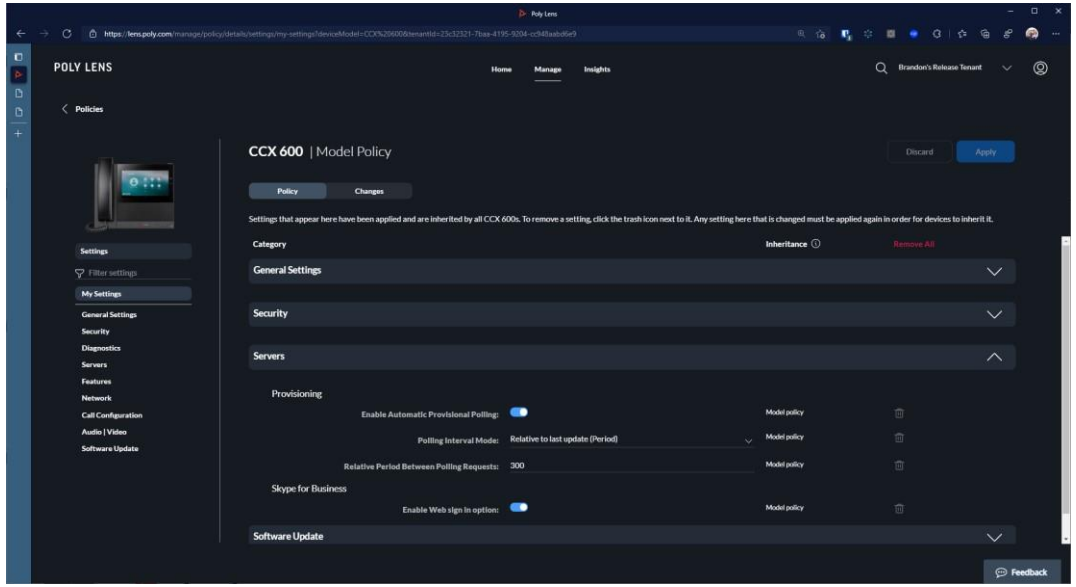
This model policy will be applied to the devices of that model. Since these devices are being added automatically by DHCP option, they will have no Device Policy.

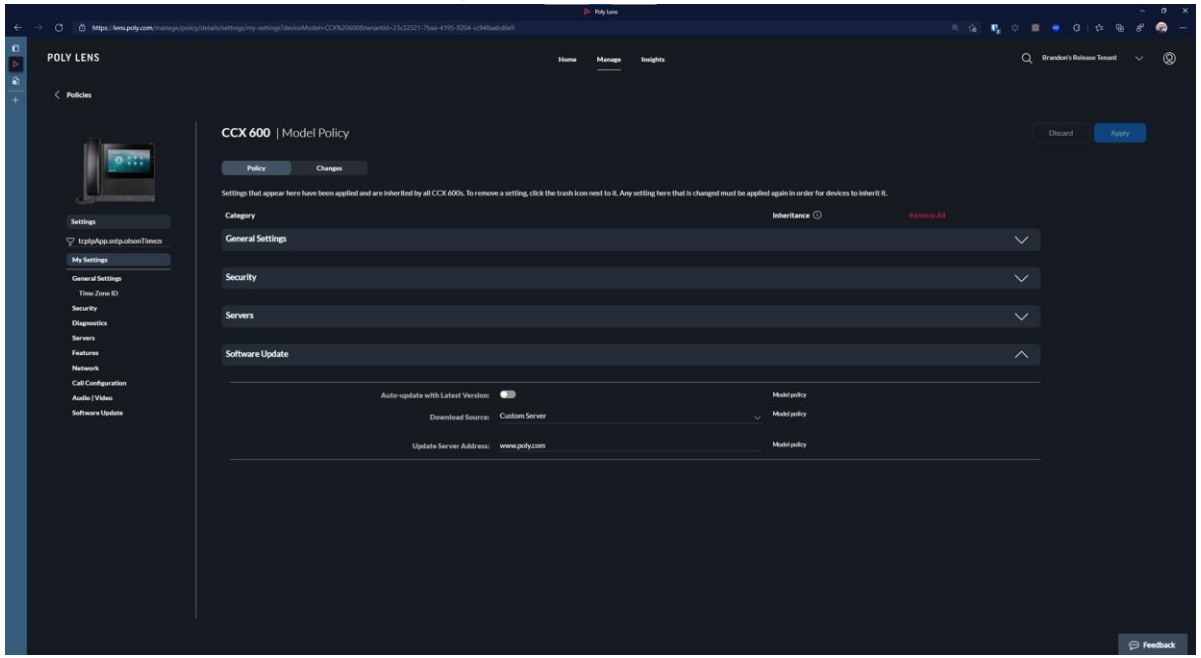
If you are currently using automatic site association by IP subnet with site policy, make sure that none of these policies are overlapping or conflicting (i.e. with software by Site)

SETTING UP THE ENVIRONMENT

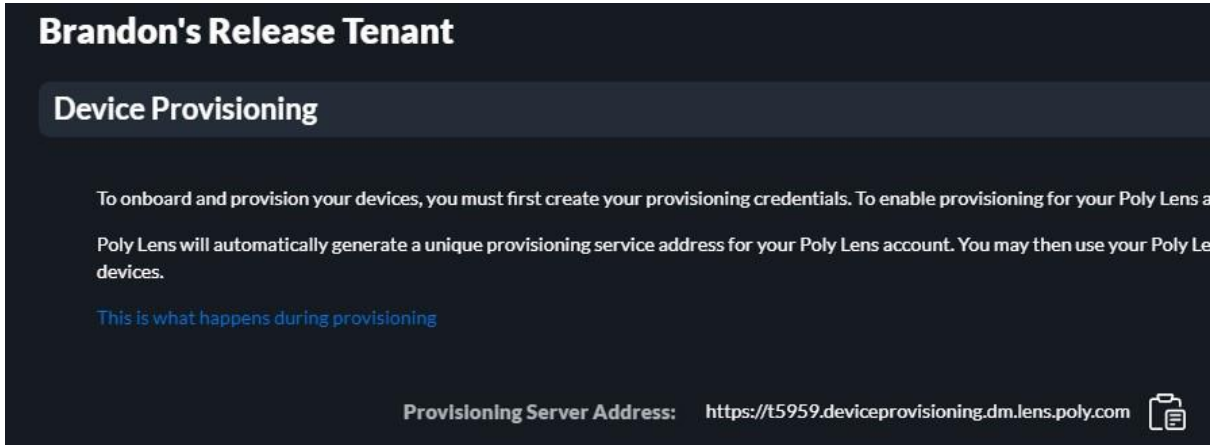
Verify your Configuration Policy is defined

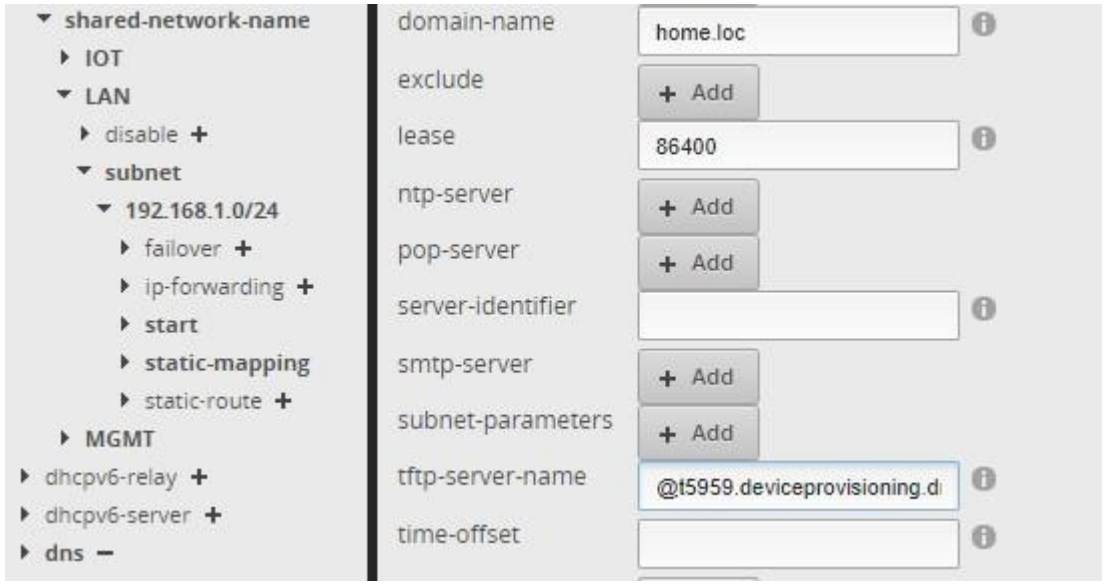






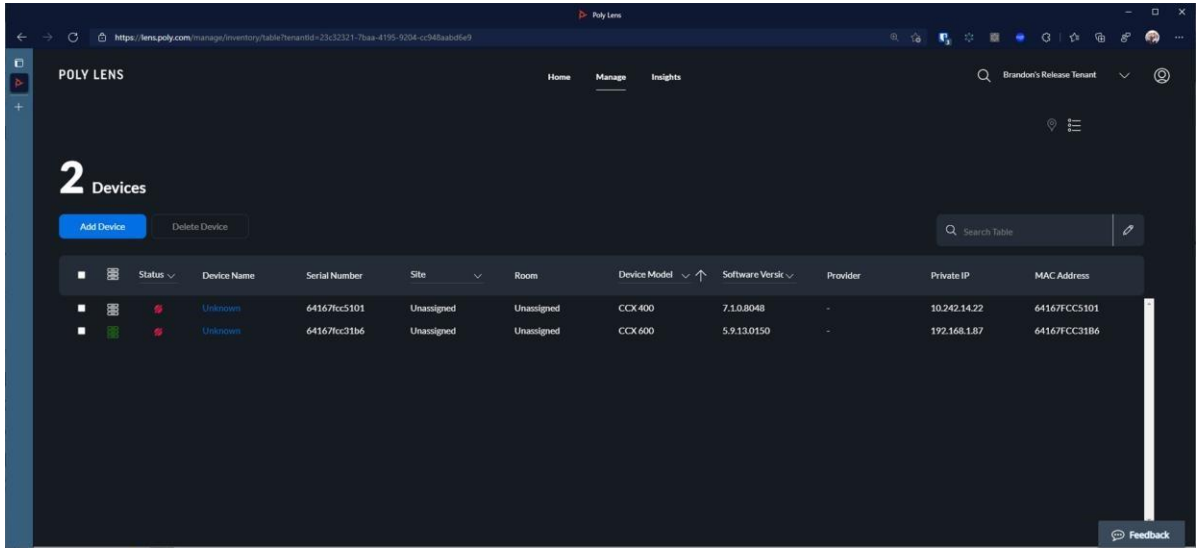
CONFIGURING YOUR DHCP SERVER





From your account settings, gather your account provisioning address and define as option 66 within your DHCP Server.

OBSERVING THE DEVICE



Before you plug in any devices

At this point the configuration provided by Lens is sufficient for bypassing the OOBE Setup Wizard for CCX device.

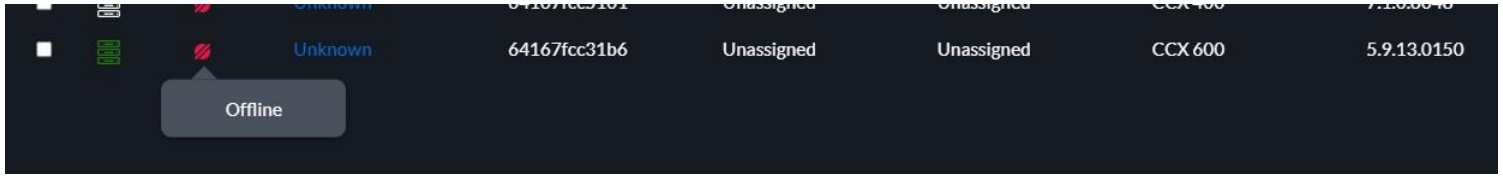
Once you plug in your device, the configuration will be retrieved, and the device will reboot multiple times.

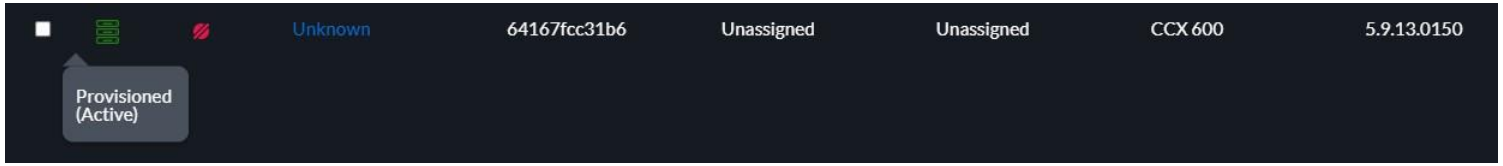
Once the device has connected to Lens to retrieve it's config, it'll be listed within the Inventory.

NOTE: Lens inventory is not dynamically updated, you must manually refresh the page within the browser to re-query the Inventory

OBSERVING THE DEVICE

As the early versions of CCX do not support the Lens agent, they will not fully reflect status within Lens. They will show as offline, but the provisioning status will show as connected.

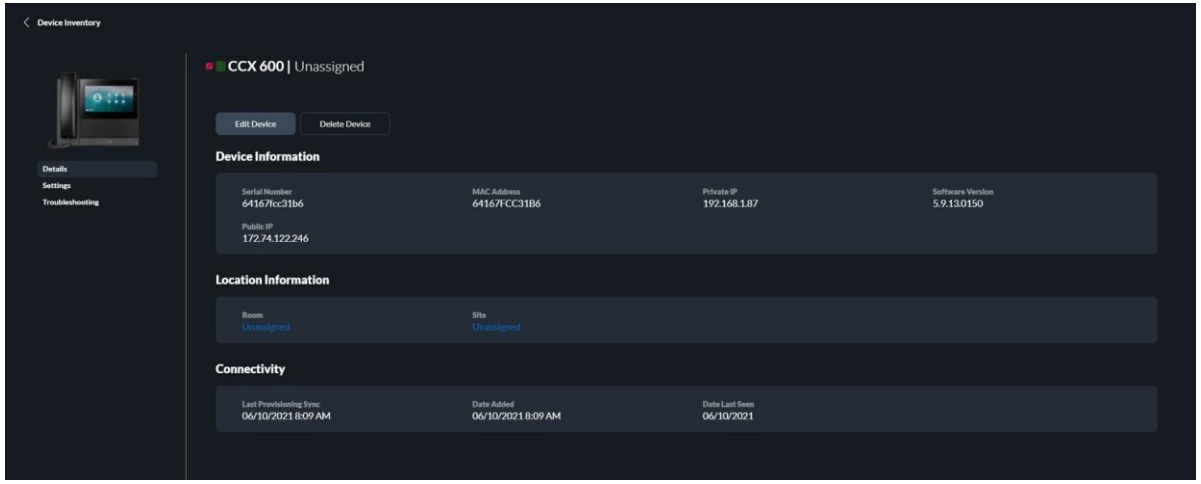


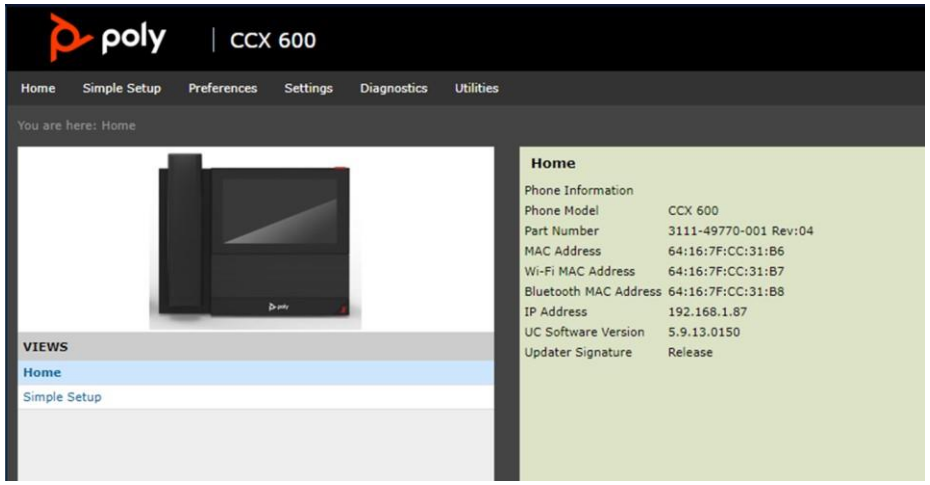


OBSERVING THE DEVICE

Before you plug in any devices

This is also seen in the Connectivity Tab of the Lens Device Information Page





VERIFYING THE CONFIGURATION

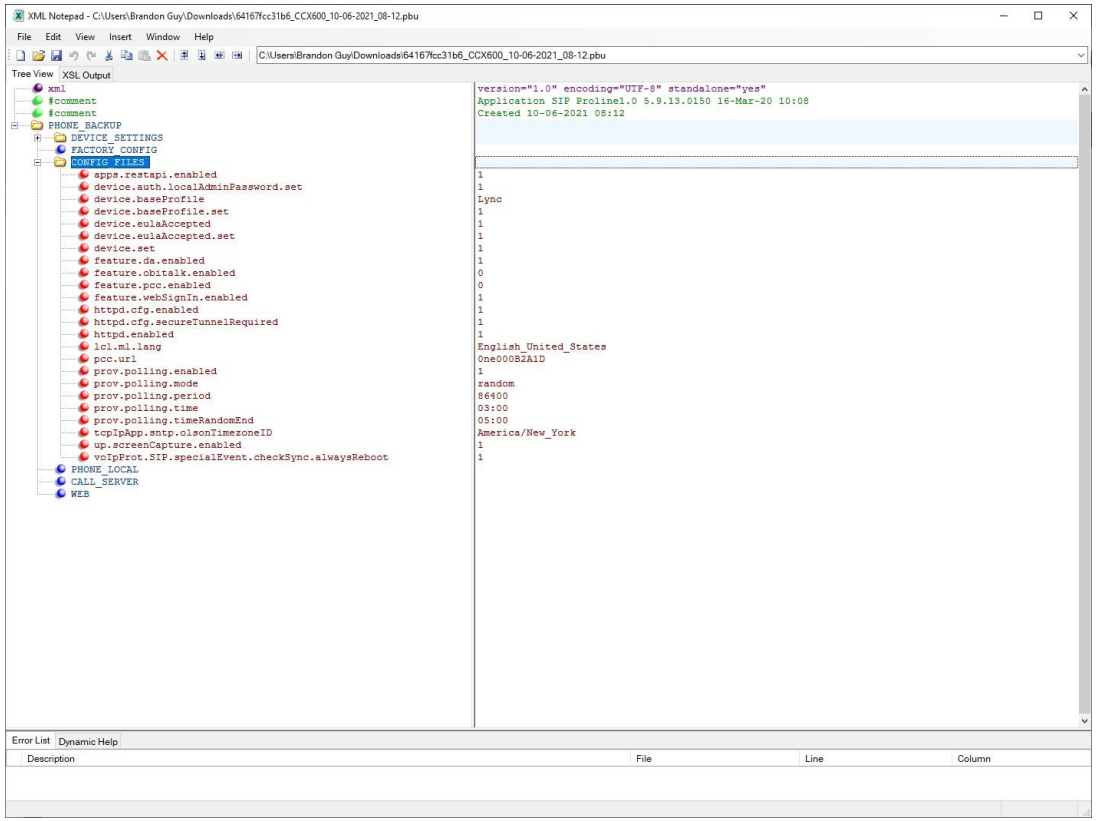
Before you plug in any devices

We can also verify what is provided by Lens by exporting the config on the Device (access available as the Web Server was enabled)

Utilities > Phone Backup & Restore

Export the Phone Backup

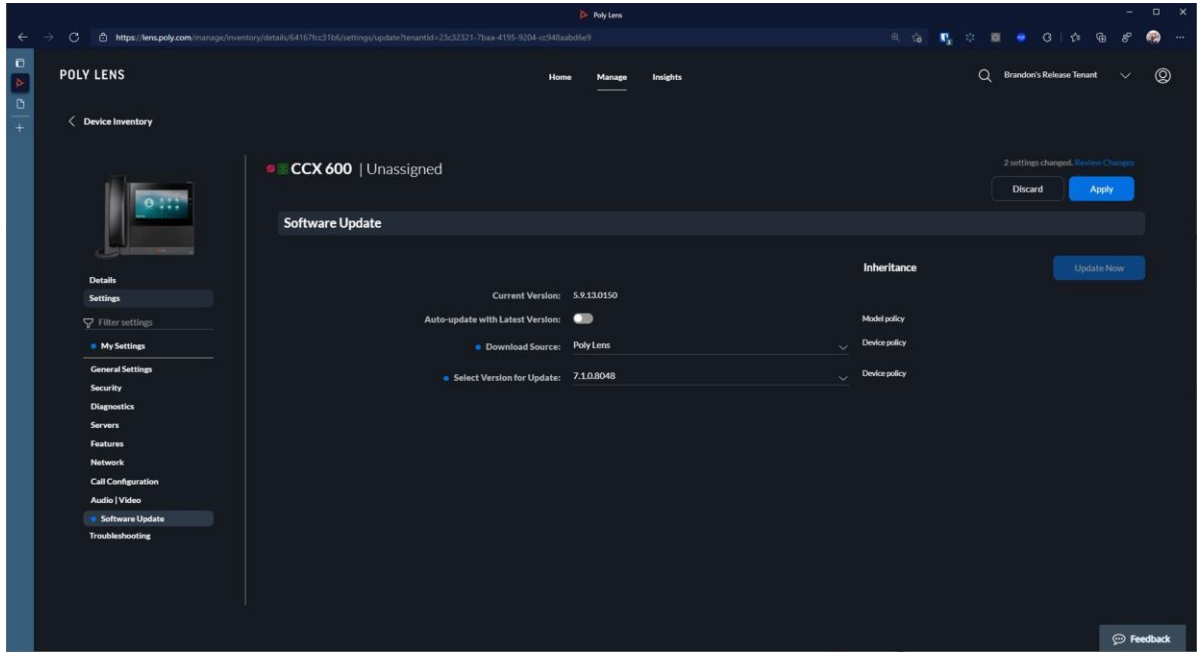
VERIFYING THE CONFIGURATION



Open the exported file in an XML editor or Notepad to see the configuration was provided as expected.

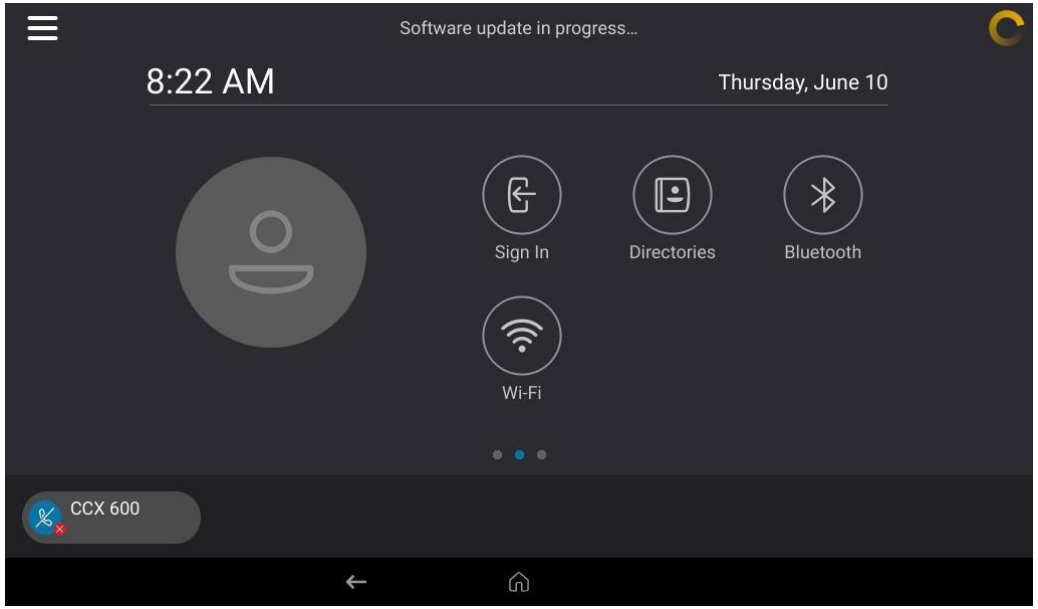
UPGRADING THE DEVICE SOFTWARE

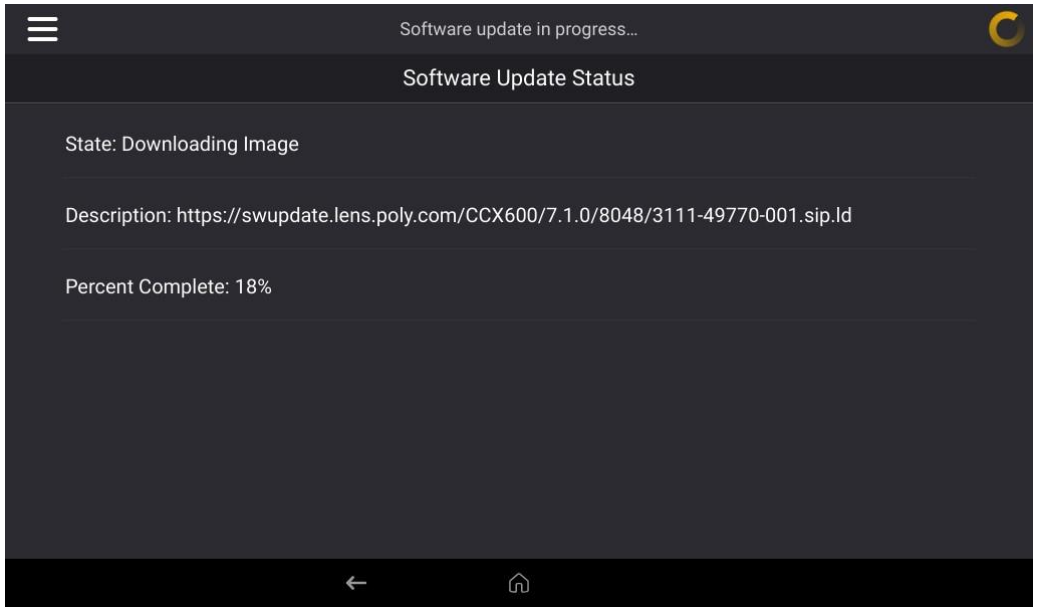
Step 2 of the deployment



Now that the device is online and, in the inventory, we know that it has completed the OOBE.

The device can now have a Device Policy created which will upgrade to the latest version.





Site Policy may also be used by manually attaching the device to a site whereby the site policy assigns a software version.

UPDATE THE DEVICE SOFTWARE

Step 2 of the deployment

Since we specified a shorter period of polling, the device is checking in regularly looking for new policy updates.

At the next check-in/Poll, the device will start the software update.