OEM Build 7 Release - SQAP

Introduction

This test plan will serve as a quality gate for the OEM Build-7 Release sign-off.

The result can be one of the following:

PASSED ✅

PASSED CONDITIONALLY ✅

FAILED ❌

Cannot Test ⛔

Acronyms

Acronym	Description
TC	Trust Center
TA	Trust Agent
EKS	Elastic Kubernetes Service
ESX/ESXi	Elastic Sky X Integrated
EPS	Endpoint Simulator is an example of implementing a client of Trust Center API
OTA	Over-The-Air update - a set of tools providing the functionality of updating the firmware of endpoints

Trust Center

Automated Test Suites:

	Test Suite/	Description	CloudCity Builds	Comments	Assignee/Test Result
1	E2E Tests (GCP)	Happy Path Tests to validate the endpoints, management API, endpoint simulator, Health, OTA, registration, management routes, etc.	E2E and Schemathesis Tests (GCP)		PASSED ✅

2	TA/TC Integration Tests	Deploys a virtualized instance of the endpoints with the Trust Agent and runs the tests. These verify the TA and API Compatibility.	TA/TC Integration Tests (GCP)		PASSED

3	Schemathesis Tests	Using the Trust Center OpenAPI specification to run a set of tests that validate the APIs conform to the schema as defined.	E2E and Schemathesis Tests (GCP)	Currently disabled in the pipeline.*
				• Run these automated tests locally for now.
					PASSED
					Test result (rc3)
					`./run.sh`
					`========== test session starts ==========`
					`platform linux -- Python 3.10.8, pytest-6.2.5, py-1.10.0, pluggy-0.13.1 -- /home/vshurygin/src/prod/trust-center/schemathesis/venv/bin/python`
					`cachedir: .pytest_cache`
					`hypothesis profile 'default' -> database=DirectoryBasedExampleDatabase('/home/vshurygin/src/prod/trust-center/schemathesis/.hypothesis/examples')`
					`rootdir: /home/vshurygin/src/prod/trust-center/schemathesis`
					`plugins: subtests-0.4.0, schemathesis-3.1.1, hypothesis-5.49.0`
					`collected 12 items`
					
					`tests/test_api.py::test_api[GET:/api/v1/endpoints][P] PASSED`
					`tests/test_api.py::test_api[GET:/api/v1/endpoints/{endpointId}][P] PASSED`
					`tests/test_api.py::test_api[PUT:/api/v1/endpoints/{endpointId}][P] PASSED`
					`tests/test_api.py::test_api[POST:/api/v1/endpoints/{endpointId}/commands][P] PASSED`
					`tests/test_api.py::test_api[GET:/api/v1/endpoints/{endpointId}/commands][P] PASSED`
					`tests/test_api.py::test_api[GET:/api/v1/endpoints/{endpointId}/commands/{commandId}][P] PASSED`
					`tests/test_api.py::test_api[PUT:/api/v1/endpoints/{endpointId}/default][P] PASSED`
					`tests/test_api.py::test_api[DELETE:/api/v1/endpoints/{endpointId}/default][P] PASSED`
					`tests/test_api.py::test_api[PUT:/api/v1/endpoints/{endpointId}/desired][P] PASSED`
					`tests/test_api.py::test_api[DELETE:/api/v1/endpoints/{endpointId}/desired][P] PASSED`
					`tests/test_api.py::test_api[GET:/api/v1/endpoints/{endpointId}/updates][P] PASSED`
					`tests/test_api.py::test_api[GET:/api/v1/endpoints/{endpointId}/updates/status][P] PASSED`
					
					`==========`

4	Docs Integration Tests (Examples)	Tests to make sure the example cases work fine and are compatible with the new API Changes.	Docs Tests	Currently disabled in the pipeline.*
				• Run these automated tests locally for now.
					PASSED
					test result (rc5)
					`python3 -m unittest discover`
					`2022-12-08 11:19:45,135 - INFO - create_service_account - creating service account asset`

```
2022-12-08 11:19:48,379 - INFO -
create_service_account - service account
"asset" created
2022-12-08 11:19:48,572 - INFO - create_asset
- creating new asset
.2022-12-08 11:19:48,785 - INFO -
create_service_account - creating service
account asset
2022-12-08 11:19:52,549 - INFO -
create_service_account - service account
"asset" created
2022-12-08 11:19:52,744 - INFO - create_asset
- creating new asset
2022-12-08 11:19:52,930 - INFO - delete_asset
- remove asset id=639238d863e10702a98fa708
.2022-12-08 11:19:53,120 - INFO -
create_service_account - creating service
account asset
2022-12-08 11:19:56,316 - INFO -
create_service_account - service account
"asset" created
2022-12-08 11:19:56,495 - INFO -
get_all_assets_internal - retrieving list of
assets metadata
.2022-12-08 11:19:56,673 - INFO -
create_service_account - creating service
account asset
2022-12-08 11:19:59,017 - INFO -
create_service_account - service account
"asset" created
2022-12-08 11:19:59,331 - INFO - create_asset
- creating new asset
2022-12-08 11:19:59,521 - INFO - get_asset -
retrieving asset metadata for
id=639238df63e10702a98fa709
.2022-12-08 11:19:59,693 - INFO -
create_service_account - creating service
account asset
2022-12-08 11:20:02,715 - INFO -
create_service_account - service account
"asset" created
2022-12-08 11:20:02,915 - INFO - create_asset
- creating new asset
2022-12-08 11:20:03,093 - INFO -
get_asset_content - retrieving asset content
for id=639238e363e10702a98fa70a
.....2022-12-08 11:20:19,379 - INFO -
create_service_account - creating service
account endpoint-config
2022-12-08 11:20:22,337 - INFO -
create_service_account - service account
"endpoint-config" created
.2022-12-08 11:20:22,943 - INFO -
create_service_account - creating service
account endpoint-config
2022-12-08 11:20:24,948 - INFO -
create_service_account - service account
"endpoint-config" created
.2022-12-08 11:20:25,715 - INFO -
create_service_account - creating service
account endpoint-config
2022-12-08 11:20:27,068 - INFO -
create_service_account - service account
"endpoint-config" created
.2022-12-08 11:20:27,839 - INFO -
create_service_account - creating service
account endpoint-config
2022-12-08 11:20:29,063 - INFO -
create_service_account - service account
"endpoint-config" created
.2022-12-08 11:20:29,814 - INFO -
```

```
create_service_account - creating service
account endpoint-config
2022-12-08 11:20:31,950 - INFO -
create_service_account - service account
"endpoint-config" created
.2022-12-08 11:20:32,715 - INFO -
create_service_account - creating service
account endpoint-metadata
2022-12-08 11:20:37,017 - INFO -
create_service_account - service account
"endpoint-metadata" created
.2022-12-08 11:20:37,212 - INFO -
create_service_account - creating service
account endpoint-metadata
2022-12-08 11:20:39,799 - INFO -
create_service_account - service account
"endpoint-metadata" created
.2022-12-08 11:20:40,535 - INFO -
create_service_account - creating service
account logs
2022-12-08 11:20:42,567 - INFO -
create_service_account - service account
"logs" created
.
----------------------------------------------
-----------------------
Ran 17 tests in 57.635s

OK
```

5	Load Tests	K6 load tests	Load Tests	I was not able to run Load test on release branch, however TC, manual deployment with trust-center-tgz/23.01.0-rc2.tar successfully passed	PASSED CONDITIONALLY
					Test result (rc5)
					`? _config_success_rate..........: 100.00% ? 400 ? 0`
					`? _endpoint_success_rate.....: 100.00% ? 400 ? 0`
					`data_received.....: 3.5 MB 30 kB/s`
					`data_sent.....: 188 kB 1.6 kB/s`
					`http_req_blocked.....: avg=1.17ms min=0.00ms med=0.00ms max=186.90ms p(90)=0.00ms p(95)=0.00ms`
					`http_req_connecting.....: avg=0.54ms min=0.00ms med=0.00ms max=54.27ms p(90)=0.00ms p(95)=0.00ms`
					`http_req_duration.....: avg=79.13ms min=68.68ms med=74.30ms max=3421.87ms p(90)=82.75ms p(95)=87.01ms`
					`{ expected_response:true }...: avg=79.13ms min=68.68ms med=74.30ms max=3421.87ms p(90)=82.75ms p(95)=87.01ms`
					`http_req_failed.....: 0.00% ? 0 ? 1204`
					`http_req_receiving.....: avg=0.10ms min=0.06ms med=0.09ms max=7.60ms p(90)=0.11ms p(95)=0.12ms`
					`http_req_sending.....: avg=0.12ms min=0.06ms med=0.10ms max=0.31ms p(90)=0.16ms p(95)=0.17ms`
					`http_req_tls_handshaking.....: avg=0.56ms min=0.00ms med=0.00ms max=59.34ms p(90)=0.00ms p(95)=0.00ms`
					`http_req_waiting.....: avg=78.92ms min=68.53ms med=74.08ms max=3421.66ms p(90)=82.51ms p(95)=86.82ms`
					`http_reqs.....: 1204 10.263563/s`
					`iteration_duration.....: avg=58652.51ms min=3905.19ms med=58652.51ms max=113399.82ms p(90)=102450.36ms p(95)=107925.09ms`
					`iterations.....: 1 0.008525/s`
					`vus.....: 1 min=0 max=1`
					`vus_max.....: 1 min=1 max=1`

7	Run through the quick start guide for TC.	Pharos OEM Beta - Quick Start Guide			PASSED
8	Run through the Factory provisioning guide for TC	Pharos OEM Beta - Factory Provisioning Guide			PASSED

Manual Tests:

TC Deployment Tests:

	Test Name	Description	Steps to Test	Result	Comments

1	Deploy the Trust Center	Tests the ability to deploy the Trust Center by using the installer archive package	1. Download the Trust Center Installation package from Cloudsmith. 2. Extract the tarball. 3. Follow the instructions found in INSTALL.md. a. Note that Ingress controllers will take 10-15 minutes to spin up on a fresh VM. During this time docker images are being downloaded and containers are being started, etc. 4. Verify that you can view the API reference docs at: `https://<fqdn-of-trust-center-machine>:32443/api/v1/docs`. Note that the Trust Center currently uses self-signed keys.	PASSED	
2		Upgrade (OEM 6 to 7)		FAILED	**Known Issue.** Do a fresh install instead of upgrading.
3		Uninstall	sudo ./uninstall.sh	PASSED	

Trust Center Administration and Management:

Prerequisite:

- Trust Center deployed.
- Download the examples tarball from Cloudsmith
  - The Prerequisites in the README.md in the link above have been met
- Ability to run Python scripts

	Test Name	Description	Steps to Test	Result
1	Assets	Tests the ability of TC Asset Management API. This test covers: • Creating(uploading) a new asset • Downloading assets • Retrieving a list of available assets • Deleting assets	1. Run the following script from the examples repo `./assets.py` 2. Verify that the script ran successfully	PASSED
2	Authentication	Tests the ability to authenticate as an admin, manage service accounts, and authenticate as a service account. This test covers: • Signing in as an admin user • Creating a service account key • Deleting a service account key • Signing in as a service account	1. Run the following script from the examples repo `./tc.py config add tc-release -a FQDN -p PASSWORD` 2. Verify that the script ran successfully	PASSED

3	Reset Admin password	changing tcAdmin user password	1. Run the following script from the examples repo.
			`# update tcAdmin user password`
			`./tc.py set admin -p new_password`
			2. Verify that you can connect to TC with new password
			`# connect with new password`
			`./tc.py config add tc-test -a trust-center.example-corp.com -p=new_password`
				PASSED

<table>
<tr>
<td>4</td>
<td>TC diagnose command (k3s)</td>
<td>ability to create TC diagnostic bundle</td>
<td>Prerequisite: trust center ctl tool uploaded to the Trust Center

1. Uploaded trust-center-ctl to Trust Center

<pre>scp -i path_to_private_key trust-center-ctl tcAdmin@tc-fqdn:/home/tcAdmin/trust-center-ctl</pre>
2. ssh to Trust Center VM

<pre>ssh -i path_to_private_key tcAdmin@tc-fqdn</pre>
3. Run the following script from the examples repo.

<pre>sudo ./trust-center-ctl diagnose --support-bundle --out %tc.support_bundle_path%; sudo chown tcAdmin %tc.support_bundle_path%</pre>
4. The command should be run without issues</td>
<td>PASSED

Sample output:

<pre>[tcAdmin@dogfood-ibeta-vm-trust-center temp_winnie]$ sudo ./trust-center-ctl diagnose --support-bundle --out /home/tcAdmin/temp_winnie/bundle
[2022-12-07T20:05:50Z] INFO Diagnosing Trust Center version=
Version: 23.01.0-rc2
Build date: 2022-12-02

[2022-12-07T20:05:50Z] INFO Creating support bundle...
[2022-12-07T20:05:50Z] INFO support-bundle: Copying log files...
[2022-12-07T20:05:50Z] INFO support-bundle: Checking SELinux configuration...
[2022-12-07T20:05:50Z] INFO support-bundle: Checking firewall configuration...
[2022-12-07T20:05:50Z] INFO support-bundle: Checking network configuration...
[2022-12-07T20:05:50Z] INFO support-bundle: Getting OS information...
[2022-12-07T20:05:53Z] INFO support-bundle: Collecting Kubernetes information; this may take a while...
[2022-12-07T20:06:39Z] INFO support-bundle: Creating archive...
[2022-12-07T20:06:40Z] INFO ***** Support bundle was created successfully *****
[2022-12-07T20:06:40Z] INFO Support bundle path: /home/tcAdmin/temp_winnie/bundle
[2022-12-07T20:06:40Z] INFO Please deliver this file to Teradici support personnel for analysis.
[tcAdmin@dogfood-ibeta-vm-trust-center temp_winnie]$ ls -l
total 45872
-rw-r-----. 1 root   root   4782959 Dec 7 20:06 bundle
-rwxr-xr-x. 1 tcAdmin tcAdmin 42188800 Dec 7 20:02 trust-center-ctl
[tcAdmin@dogfood-ibeta-vm-trust-center temp_winnie]$ sudo chown tcAdmin . /bundle
[tcAdmin@dogfood-ibeta-vm-trust-center temp_winnie]$ ls -l
total 45872
-rw-r-----. 1 tcAdmin root   4782959 Dec 7 20:06 bundle
-rwxr-xr-x. 1 tcAdmin tcAdmin 42188800 Dec 7 20:02 trust-center-ctl</pre></td>
</tr>
<tr>
<td>5</td>
<td>Run through Python examples</td>
<td>Only those not covered by "Endpoint Management via the Trust Center" below</td>
<td>Follow https://git.teradici.com/projects/TC/repos/docs/browse/examples/README.md and run all tests.</td>
<td>PASSED</td>
</tr>
</table>

Environment-Specific Deployment Tests

As we have customer-varied deployment environments with customized VM s, we need to test the TC deployment with various configurations and environments.

Simulate the customer's environment to validate the single node TC deployment.

	Platform	Assignee/ Test Result	Comments
1	ESXi single node	**Cannot Test**	Need more details on the customer using this platform.

TeamCity: https://cloudcity.teradici.com/project/Staging_Products_TrustCenter_2_Tests?mode=builds

Client (UI)

Automated E2E Tests (PlayWright)

Client (UI) automated tests are written in Playwright, and cover the major functionality in terms of end-to-end tests.

	Test Suite	CloudCity Builds/Confluence	Test Result
1	PlayWright E2E and Integration Tests	E2E and Integration Tests	PASSED
2	Run through the Quick-Start guide (TC and UI on a physical device)		PASSED
3	Run Tests in the Pharos device manually	*Refer to the section 'Manual Tests'*	PASSED

For more details on Client UI Playwright tests, click here.

Manual Tests:

Endpoint Provisioning

Prerequisite:

- Trust Center is deployed as in A1
- Endpoint hardware (Leadtek or AHK board)
- A Provisioner (downloaded from Cloudsmith) written to a USB drive using either dd or Win32DiskImager

	Test Name	Description	Steps to Test	Result
1	Provision the board	Tests that the board can be provisioned with the latest provisioner, which contains • Wind River Linux • Teradici Client UI • Trust Agent • Services to make the above apps work together	1. Plug provisioner USB into Leadtek or AHK board (if the latter make sure you have a provisioner with a V1000 image). 2. Press ESC (on Leadtek board) or Delete (on AHK board) during boot to get into the boot menu. ⚠ If you get "Linpus lite has been blocked by the current security policy", try disabling secure boot: • Open the "Administer Secure Boot" menu ◦ Might need a reboot • Disable "Enforce Secure Boot" 3. Choose the provisioner USB in the "Boot Manager" menu. 4. Wait for provisioning to be complete. a. In the case of a Leadtek board, the board should automatically reboot and the Teradici UI should come up. b. In the case of an AHK board, an error may appear. Simply remove the USB stick and reboot manually. 5. Remove provisioner USB. 6. Let the device boot into a desktop, 7. Verify that the Teradici Client application eventually pops up	PASSED
		Tests that the UI can connect to the Trust Center correctly	1. If your Trust Center is at pcoiptrustcenter a. Verify that the landing page shows the list of trusted brokers (which may be blank) 2. If your Trust Center is elsewhere a. Put in your trust center's FQDN, and proceed b. Verify that the page now shows the list of trusted brokers (which may be blank)	PASSED

Endpoint Management via the Trust Center

Prerequisite:

- Same as suite A2. See the TroubleShooting section in the README.md if the example script fails to run.
- Additionally, the endpoint has been provisioned as in Test Suite B1
- You have a Linux machine which is able to access the Trust Center via IP (this is where you'll be performing the steps below)
- The endpoint ID of the endpoint you're managing is known (usually in the form of *endpoint-<machine id>,* such as *endpoint-58339fccf46546e386207f2e8cdf416b*)
    - Please see Obtaining Endpoint ID for how to obtain your endpoint ID

	Test Name	Description	Steps to Test	Result
1	Verify Registration	Assuming B1 is complete, test that the first boot successfully registered this endpoint with the Trust Center	1. Run the following script from the examples repo. `./tc.py get endpoints -id <your endpoint Id>` 2. Verify that your endpoint ID is found.	PASSED
2	PowerOff command test	Tests the ability to process **power-off** commands from the Trust Center to the endpoint	1. Run the following script from the examples repo. NOTE: your endpoint will power off in 10 seconds, so make sure this does not disrupt your work. `./tc.py set endpoint power-off -id <your endpoint Id> -d 10` 2. Verify that the script ran successfully 3. Verify that the endpoint is powered off after 10 seconds	PASSED
3	Reboot command test	Tests the ability to process **reboot** commands from the Trust Center to the endpoint	1. Run the following script from the examples repo. NOTE: your endpoint will reboot in 10 seconds, so make sure this does not disrupt your work. `./tc.py set endpoint reboot -id <your endpoint Id> -d 10` 2. Verify that the script ran successfully 3. Verify that the endpoint is rebooted after 10 seconds	PASSED
4	Factory reset command	Tests the ability to process **factory-reset** commands from the Trust Center to the endpoint	1. On the endpoint, use the command prompt or SSH to go to a. /home/pharos and make note of the last modified times of appendonly.aof and cache folder. b. /var/sota/import and make note of the last modified times of client.pem, gateway.url, pkey.pem, root.crt 2. Run the following script from the examples repo. NOTE: your endpoint will be factory-reset `./tc.py set endpoint factory-reset -id <your endpoint Id>` 3. Verify that the script ran successfully 4. Verify that the endpoint is rebooted 5. On the endpoint, use the command prompt or SSH to go to /home/pharos and verify that the following file and folder have been newly created. a. cache b. appendonly.aof 6. On the endpoint, use the command prompt or SSH to go to /var/sota/import and verify that the following file and folder have been newly created. a. client.pem b. gateway.url c. pkey.pem d. root.crt	PASSED

5	Support-bundle (triggered from TC)	Test ability to create support bundle, triggering by Trust Center command	Prerequisites: device connected to TC 1. Run the following script from the examples repo. ``` # send command to endpoint to create support-bundle ./tc.py set ep support-bundle -id <your endpoint Id> ``` 2. Verify that the script ran successfully 3. Verify that the support-bundle is created ``` # get list of support-bundles for device ./tc.py get bundles -eid <your endpoint Id> ``` 4. Verify that the script ran successfully and has support-bundle metadata 5. Verify that the support-bundle content can be downloaded and unpacked ``` # get support-bundle content ./tc.py get support-bundles contents -id assetID -f /path/to /save/support_bundle ``` 6. Verify that support-bundle can be removed ``` # delete support-bundle from TC ./tc.py del support-bundles -id assetID ```	PASSED
6	Support-bundle (triggered from device)	Test ability to create support bundle, triggering by User From Client UI	Prerequisites: device connected to TC 1. Run ????????????? 2. Verify that the script ran successfully 3. Verify that the support-bundle is created ``` # get list of support-bundles for device ./tc.py get bundles -eid <your endpoint Id> ``` 4. Verify that the script ran successfully and has support-bundle metadata 5. Verify that the support-bundle content can be downloaded and unpacked ``` # get support-bundle content ./tc.py get support-bundles contents -id assetID -f /path/to /save/support_bundle ``` 6. Verify that support-bundle can be removed ``` # delete support-bundle from TC ./tc.py del support-bundles -id assetID ```	PASSED

7	NTP	Tests the ability to change endpoint's NTP configurations, including
		• Set the desired NTP setting, and verify via the endpoint
		• Check the reported NTP setting
		• (maybe more)
			1. Run
			`./tc.py set ep prop -id <your endpoint Id> --path="/time/ntp/enabled" --value=true`
			2. On the endpoint, via the command line or ssh, run
			`systemctl status systemd-timesyncd`
			3. Confirm that the service is "active (running)"
			4. Run
			`./tc.py set ep prop -id <your endpoint Id> --path="/time/ntp/enabled" --value=false`
			5. Confirm that the service is "inactive"
				PASSED

8	Trusted Brokers test	Tests the ability to:
		• Add a trusted brokers
		• Remove a trusted broker
		• Verify the list of trusted brokers
			1. Run
			`./tc.py set ep prop -id  <your endpoint Id> --path="/brokering/trustedBrokers" --value="[{\"address\": \"desktop.teradici.com\", \"connectionType\": \"pcoipConnectionBroker\"}]"`
			2. On the endpoint, verify that the landing page has been updated with the corresponding broker
			3. Run
			`./tc.py set ep prop -id  <your endpoint Id> --path="/brokering/trustedBrokers" --value="[]"`
			4. On the endpoint, verify that the landing page now shows a message telling you to add a trusted broker
				PASSED

9	Log Level	Tests the ability to:
		• Update endpoint log level
		• Verify new log level is respected
		• Update endpoint log level back to default
			1. On the endpoint, open a terminal and tail the trust agent log under /var/anyware
			2. Plug/unplug a USB device, and verify that debug log of the USB device changes can be seen.
			3. Run
			`./tc.py set ep prop -id  <your endpoint Id> --path="/logging/logLevel" --value="info"`
			4. Plug/unplug a USB device, verify that debug log is no longer visible
			5. Run
			`./tc.py set ep prop -id  <your endpoint Id> --path="/logging/logLevel" --value="debug"`
			6. Plug/unplug a USB device, and verify that debug log of the USB device changes can be seen again.
				PASSED

10	Timezone	Tests the ability to:
		• Update endpoint timezone
		• Verify timezone has been updated
		• Update endpoint timezone back to default
			1. Run
			`./tc.py set ep prop -id  <your endpoint Id> --path="/time /timeZone" --value="Asia/Bangkok"`
			2. On the endpoint, verify the current timezone using 'timedatectl'. Ensure it matches the timezone above.
			3. Run
			`./tc.py set ep prop -id  <your endpoint Id> --path="/time /timeZone" --value="UTC"`
			4. On the endpoint, verify the current timezone using 'timedatectl'. Ensure it matches the timezone above.
				PASSED

Endpoint Operation via the Teradici Client UI

Prerequisite

- A Trust Center is deployed
- The endpoint has been provisioned as in B1, and the landing page has been verified
- A list of your preferred trusted brokers has been pushed to the device as in B2.5
    - The list is visible on the UI

	Test Name	Description	Steps to Test
1	About button	Tests that the about page is functional and shows the correct information	1. On the top right of the UI, click "About" 2. Ensure that an About page pops up, and the content of the About dialogue is sensible
2	Shutdown button	Tests that one can shut down the device via the UI's Power button	1. On the top left of the UI, click "Power" 2. Then click "Shutdown" 3. Ensure that the device shuts down correctly
3	Reboot button	Tests that one can reboot the device via the UI's Reboot button	1. On the top left of the UI, click "Power" 2. Then click "Reboot" 3. Ensure that the device reboots correctly
4	Connect to a Desktop without MFA	Tests that one can connect to a desktop using one of the trusted brokers	1. Ensure "Connect" dialog is visible 2. Select an internal broker (such as desktop) from within the same network 3. Enter Credentials 4. Choose the VM/Machine to connect 5. Ensure that the connection is successful and keyboard/mouse works 6. Move the cursor to the top of the screen to display the dropdown menu 7. Select Connection | Disconnect to disconnect 8. Ensure disconnection was successful and Trusted Zero Client landing page is visible
5	Connect to a Desktop with MFA	Tests that one can connect to a desktop using one of the trusted brokers, with MFA	Same as above except select a broker that requires MFA (such as desktop-external)
6	In-session dropdown menu	Tests the options avaiable in in-session dropdown menu	1. Repeat steps as mentioned in previous tests to connect to a desktop. 2. Ensure in-session is **fullscreen**. 3. Move the cursor to the top of the screen to display the dropdown menu and try each option. If the option triggers disconnection, go back in-session and continue. 4. Check Anyware PcoIP Client About, verify an About page comes up 5. Check Anyware PcoIP Client Quit, verify disconnection happens 6. Check Connection Send CTRL-ALT-DEL, verify it works 7. Check ConnectionDisconnect, verify disconnection happens 8. Check ConnectionUSB Devices, verify USB device window comes up 9. Check ViewLeave Fullscreen, verify in-session stays fullscreen 10. Check ViewMinimize Client, verify in-session stays fullscreen 11. Check HealthConnection Health, verify Connection Health box comes up
7	Remote Audio	Tests that remote audio in and out are both functional	Prerequisite • You have an analog output and an analog input device (if your hardware has separate headphone and microphone jacks) or an analog conference headphone (if your hardw • The devices are plugged in before the session is established • You have completed C1.3 and are now in a remote desktop 1. Within your remote desktop, access something that has audio output, such as music or a Youtube video 2. Play the medium 3. Ensure that the sound from the medium can be heard via your audio output device 4. Procure a sound recording software such as Audacity or Window's Voice Recorder 5. Start recording audio using the application, and speak into your microphone 6. Stop recording 7. Playback the recording 8. Ensure that your recording can be heard

8	Add New Connection	Tests that new connection can be added	1. On the Connect page, click "Add New Connection" 2. Enter invalid host address or registration code 3. Click "Add Connection", ensure an error message appears 4. Enter valid host address or registration code 5. Click "Add Connection" and ensure new entry shows up on Connect page 6. Try adding another valid host address or registration code 7. This time also enter a Connection Name 8. Click "Add Connection" and ensure the Connection Name appears on Connect page. When you mouse over the Connection Name, it should show the associated host addr
9	Settings->General	Tests the settings under Settings->General	1. On the top left, click Settings 2. Select the General tab, ensure all settings on this page are populated. 3. Change TimeZone and ensure the date & time at the top is updated correctly 4. Likewise, change Date Format and check 5. Likewise, change Time Format and check 6. Change Language. At the moment, it does not actually update the display language. 7. Change Log Level. Try plugging/unplugging a usb device to generate some logging and go to Settings->LogView Log Files, scroll to the end of trust-agent.log to see the diff 8. Click Client Information to display device info and ensure the information is correct.
10	Settings->Network	Tests that SettingsNetwork displays correct information	1. On the top left, click Settings 2. Select the Network tab, ensure ETH0 is under active networks. 3. With ethernet cable connected, ensure ETH0 is indicated as "Connected", expand to view the additional information 4. Unplug and plug back ethernet cable several times, ensure ETH0 status is updated correctly.
11	Settings->ConnectionsUSB Devices	Tests that connected usb devices are detected	1. On the top left, click Settings 2. Select ConnectionsUSB Devices, and ensure all connected USB devices are correctly detected. 3. Try unplugging/plugging usb device and ensure the page is updated correctly. 4. Test the Copy Info button and ensure selected usb device info is copied 5. Verify the KMP device checkbox is disabled.
12	Settings->Advanced->Reset	Tests that factory reset works	1. Go to weston terminal and make note of the files (e.g. timestamp) under /home/pharos/ 2. On the top left, click Settings 3. Select Advanced->Reset, click Reset and Confirm, device shall be rebooted right away. 4. Once device is up again, go to weston terminal and confirm that files under /home/pharos have been recreated.
13	Settings->Advanced->Security Modes	Tests that Secuity mode setting works	1. On the top left, click Settings 2. Select AdvancedSecurity Modes, ensure all existing connections are under the dropdown. 3. Try updating the security mode for one or all connections and ensure the update works.
14	Network Health	Tests that Network Health displays correct status	1. On the top right, click Network Health 2. Assuming device is configured properly to connect to Trust center, check that all dots are green and connection is indicated as Healthy. 3. Unplug ethernet cable, check that all dots are red. Click on properties should show ETH0 as disconnected. 4. Plug cable back, check that all connection status are back to healthy state.
15	USB autoforward (Windows VM only)	Tests that usb device autoforward works	1. Setup connection to a Windows VM and go in-session 2. Plug in a mass storage USB device and ensure auto forward works 3. Try connecting USB device both before and after in-session and verify autoforward works.
16	Startup Splash Screen		1. Go to PowerReboot to reboot device 2. When it comes back up, verify the Anyware Startup Splash Screen appears before the landing page.
17	Log Viewer		1. Repeat steps as mentioned in previous tests to connect to a desktop. 2. Select Connection | Disconnect to disconnect to go back to Trusted Zero Client landing page 3. Go to Settings->LogView Log Files, check the files below: a. teradici/factoryProvisioningAssets/endpoint*.crt b. teradici/factoryProvisioningAssets/registration-ca.crt c. teradici/factoryProvisioningAssets/log/factory_provisioner.log d. tmp/anyware/client/anyware-client.log e. tmp/teradici-client*.txt f. /var/anyware/trust-agent.log g. /var/anyware/trust-agent-stdout.log h. /var/anyware/anyware-client.log i. /var/anyware/actualizr.log j. /home/pharos files
18	Log Viewer searching		1. Go to Settings->LogsView Log Files, select anyware/trust-agent.log 2. Enter text in the search box and verify the log filter works. Verify by toggling the "Show lines with matches only" button and check the number of matches. 3. With the same search string, move on to another logfile and check again. 4. Try replace the search string, repeat the steps.
19	Log file rotation		1. Leave the device running for a couple days. 2. Go to Settings->LogsView Log Files, and check the files under anyware 3. Verrify that log rotation is happening for each type of log files.

20	Help Icon		1. Click the **Help** icon on the right upper corner next to the **About** icon
			2. A Help window comes up. Enter a brief description, make a note of it, then click **Send**.
			3. Help window shall close as soon as **Send** is clicked.
			4. Go to Settings->LogsView Log Files, search for keyword from the description entered and confirm matches are found.
			5. Select /var/anyware/trust-agent.log from the left file explorer and scroll to the end of the file to where the search highlights start. Look for
			a. "Support bundle request received from UI"
			b. "Generating support bundle"
			c. "Proceed to send support bundle"
			d. "Sending <filename>"
			e. Return status 201 from the bundle transmission with info similar to below:
			`2022-12-01T14:10:23.618657Z TA:endpoint-4995ef7810ca40fdb10054279b8cfa02[16504]: LOC`
			`"code" : 201,`
			`"data" : {`
			`"assetId" : "6389264fee6cd14879559e4f",`
			`"contentType" : "application/octet-stream",`
			`"createdBy" : "638645d8e973a6dffa653a90",`
			`"createdOn" : "2022-12-01T22:10:22Z",`
			`"fileName" : "support-bundle-endpoint-4995ef7810ca40fdb10054279b8cfa02-1669932`
			`"hash" : "71c513b3cdde87a807186d99e9fbb2a9a689e6b17011133abde5aeb540f94917cedc`
			`"size" : 24831293,`
			`"upn" : "endpoint-4995ef7810ca40fdb10054279b8cfa02"`
			`},`
			`"status" : "success"`
			`}`
			6. On another where you can access the tc.py script in the examples repo, enter the following and verify bundle info identical to previous step can be found.
			`./tc.py get bundles -eid <endpoint-id>`
			7. Enter the command below to extract the support bundle file
			`./tc.py get b c -id <assetId> --file bundle.tar.gz`
			8. Look for bundle.tar.gz in the current folder and use tar to extract the content.
			`tar -xvzf bundle.tar.gz`
			9. Verify the expected files are successfully extracted.

21	Support bundle content validation		1. Follow **Help Icon** test above to send support bundle to Trust Center, then retrieve bundle file from Trust Center. 2. Extract the bundle content and carefully examine to ensure no sensitive data is included. 3. Include the extracted list of files here for record/reference later. **Extracted Files** | **Extracted Files**

```
wpoon@TERVDIU18AZR085:~/temp$ tar -
xvzf rc4.tar.gz
var/teradici/log/factory_provisioner.
log
var/teradici
/factoryProvisioningAssets/default-
properties.json
var/teradici
/factoryProvisioningAssets
/registration-ca.crt
var/teradici
/factoryProvisioningAssets/endpoint-
b449563f86bd414fbe74ba270b3dbe05-TPM.
crt
home/pharos/appendonly.aof
home/pharos/etc/ssl/registration
/certs/TeraRootTCCA.pem
home/pharos/etc/ssl/registration
/certificate.pem
home/pharos/etc/ssl/operational/certs
/TCRootCA.pem
home/pharos/etc/ssl/operational
/certificate.pem
home/pharos/cache/Registration.json
var/anyware/
var/anyware/trust-agent.log-20221210
var/anyware/trust-agent.log
var/anyware/aktualizr.log
var/anyware/anyware-client.log-
20221210
var/anyware/aktualizr.log-20221210
var/anyware/trust-agent-stdout.log
var/anyware/trust-agent-stdout.log-
20221210
var/anyware/syslog_state_files/
var/anyware/anyware-client.log
tmp/teradici-
client_2022_12_09T21_48_38Z_00000406-
BYfk9F.txt
tmp/teradici-
client_2022_12_09T21_50_54Z_00000406-
TrTuwO.txt
tmp/teradici-
client_2022_12_09T22_59_58Z_00000406-
YyZgb2.txt
tmp/teradici-
client_2022_12_09T23_00_02Z_00000406-
XfbAeV.txt
tmp/teradici-
client_2022_12_09T23_03_43Z_0000e298-
l2aZm0.txt
tmp/teradici-
client_2022_12_09T23_05_05Z_0000e298-
r2OtP0.txt
tmp/teradici-
client_2022_12_10T00_02_29Z_0000e298-
WtvYs7.txt
tmp/teradici-
client_2022_12_10T00_02_34Z_0000e298-
PhtS72.txt
tmp/anyware/client/
tmp/anyware/client/client_id
tmp/anyware/client/settings.dat
tmp/anyware/client/attachments/
tmp/anyware/client/completed/
tmp/anyware/client/pending/
tmp/anyware/client/new/
tmp/anyware/client/anyware-client.log
```

```
var/teradici/log/factory_provisioner.
log
var/teradici/factoryProvisioningAssets/defau
json
var/teradici/factoryProvisioningAssets/regis
crt
var/teradici/factoryProvisioningAssets/endpo
crt
home/pharos/appendonly.
aof
home/pharos/etc/ssl/registration/certs/TeraR
pem
home/pharos/etc/ssl/registration/certificat
pem
home/pharos/etc/ssl/operational/certs/TCRoot
pem
home/pharos/etc/ssl/operational/certificate
pem
home/pharos/cache/Registration.
json
var
/anyware/
var/anyware
/syslog_state_files/
var/anyware/trust-agent.
log
var/anyware/aktualizr.
log
var/anyware/anyware-client.
log
var/anyware/trust-agent-stdout.
log
tmp/teradici-client_2022_12_12T17_48_03Z_000
txt
tmp/teradici-client_2022_12_12T17_48_06Z_000
txt
tmp/anyware
/client/
tmp/anyware/client
/client_id
tmp/anyware/client/settings.
dat
tmp/anyware/client
/attachments/
tmp/anyware/client
/completed/
tmp/anyware/client
/pending/
tmp/anyware/client
/new/
tmp/anyware/client/anyware-client.log
```

22	In-Session timezone and locale		1. On the top left, click Settings 2. Select the General tab, change TimeZone to a different one, make note of it. 3. Repeat steps as mentioned in previous tests to connect to a desktop. 4. Verify the in-session timezone is identicial to what was set in Step 2. 5. Select Connection | Disconnect to disconnect 6. Go to SettingsGeneral, change lanuage to French 7. Repeat steps as mentioned in previous tests to connect to a desktop. 8. Verify the in-session language is identicial to what was set in Step 7.
23	Desktop Bookmarking /Renaming /Info		1. Repeat steps as mentioned in previous tests to connect to a desktop. 2. Follow the UI until you get passed the Multifactor authentication page and land on the Desktop selection page. 3. Click on the 3 dots beside the Desktop name, select **Rename** to change the desktop name. Verify the renaming works. 4. Click on the 3 dots beside the Desktop name, select **Info** to view the desktop info. 5. Click on the bookmark next to the desktop name, and observe that it goes under the favorites list.
24	Utility menu options (Edit /Delete /Info) for the Brokers list.		1. On the connection page, click on the 3 dots next to a saved connection, edit the connection and verify it works. 2. Similiary, click on the 3 dots next to a saved connection, delete the connection and verify connection is deleted. 3. Lastly, click on the 3 dots next to a saved connection, select the info and verify the information is correct.
25	Restart Desktop		1. Repeat steps as mentioned in previous tests to connect to a desktop. 2. Follow the UI until you get passed the Multifactor authentication page and land on the Desktop selection page. 3. Click on the 3 dots beside the Desktop name, select **Restart** to restart the selected desktop. Verify the restart happens.
26	Cancel an in-progress session.		1. Repeat steps as mentioned in previous tests to connect to a desktop. 2. Follow the UI until you get passed the Multifactor authentication page and land on the Desktop selection page. 3. Select a desktop to connect and while it's launching, select **Cancel**. Verify the cancellation works.
27	Visibility icon on password field		1. Repeat steps as mentioned in previous tests to connect to a desktop. 2. While on the Username/Password page, verify the visibility icon appears as soon as you start typing in the Password field. Toggle the icon and verify it works as expected.
28	Settings->AdvancedTrust Center		1. Go to Settings->AdvancedTrust Center and verify the Trust Center Address is correct.
29	Memory and CPU usage monitor		1. ssh to the pharos device and run top to monitor CPU and memory usage 2. Repeat steps as mentioned in previous tests to connect to a desktop, observe CPU and memory usage while in-session 3. Select Connection | Disconnect to disconnect, observe CPU and memory usage aftering exiting session 4. Repeat Step 2 & 3 many times to note down any abnormality in CPU and memory usage. 5. If no abnormality observed, this test passes.

OTA

OTA Operation:

Prerequisite:

- A Trust Center
- A Linux machine that is able to access the Trust Center via IP with Python 3.6.9+
  - D1.2
    - scripts are cloned
    - credentials are cached
- A registered endpoint
  - The endpoint ID of the endpoint you're managing is known (usually in the form of *endpoint-<machine id>*, such as *endpoint-58339fccf46546e386207f2e8cdf416b*)
    - Please see Obtaining Endpoint ID for how to obtain your endpoint ID

	Test Name	Description	Steps to Test	Result

<table>
<tr>
<td>1</td>
<td>Aktualizr (OTA Client) is running</td>
<td>Ensure Aktualizr service is running on endpoint</td>
<td>
1. Access endpoint via the terminal or ssh
2. Elevate privileges because aktualizr-info requires root
<pre>
su
<enter password>
</pre>
3. Run aktualizr-info
<pre>
aktualizr-info

sample output
amdx86-64:~$ su
Password:
amdx86-64:/home/pharos# aktualizr-info
Device ID: 8884cfb2-51fb-51a5-b7a8-3d91d010e04a
Primary ECU serial ID:
13971302a7a25f19f5b4993f94b6df6affbee02fc471f4cf48fe310f47b2cfb0
Primary ECU hardware ID: amdx86-64
Provisioned on server: yes
Fetched metadata: yes
Current Primary ECU running version:
5936e90391cb67e189a52d3a0e7e726ff1ed4b399950119343ad5b61852db9da
</pre>
</td>
<td>PASSED</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Query OTA server for available firmware versions</td>
<td>
1. From Linux
<pre>
list all firmware versions (sorted by version)
$ ./tc.py get repo --target amdx86-64 | jq
{
    "createdAt": "2022-06-30T01:50:18Z",
    "hash":
"7bea0bc82d08e33bb220acd8fbd596827f6f44c0e5fbe544c14823c2648b9a0f"
,
    "name": "trusted-zero-client-amdx86-64",
    "targets": [
        "amdx86-64"
    ],
    "updatedAt": "2022-06-30T01:50:18Z",
    "version": "22.07.0-rc4"
},
 ...

list newest version sorted by updatedAt key
$ ./available_firmware_versions.py | jq '.[0]'

list 2nd newest version sorted by updatedAt key
$ ./available_firmware_versions.py | jq '.[1]'
</pre>
2. Note the "version" and "hash" property to be used in the update. Also note expected changes.
</td>
<td>PASSED</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Update a device to a newer firmware</td>
<td>
1. Log aktualizr service
    a. Access endpoint via the terminal or ssh
    b. journalctl -fu aktualizr.service
    c. look for a successful connection "response http code: 200"
2. Choose
    a. target
        i. amdx86-64 (e.g. Leadtek board)
3. <code>Make sure connected to dogfood TC</code>
    a. <code>./tc.py config del dogfood</code>
    b. <code>./tc.py config add dogfood -a trust-center.dogfood-ibeta.hydra.teradici.com -p <password-from-lastpass></code>
4. Start the update using endpoint_ota_updates.py
</td>
<td>PASSED</td>
</tr>
</table>

5.
```
# update endpoint-a12170845ac34e22a8910498a28866bf with an amdx86-64 image with version 22.07.0-rc4
$ ./tc.py set endpoint firmware -t amdx86-64 -v 22.07.0-rc4 -id endpoint-a12170845ac34e22a8910498a28866bf

2022-02-04 02:37:59,484 - INFO - <module> - Running example: retrieving all the firmware versions available for download
2022-02-04 02:37:59,610 - INFO - <module> - Running example: retrieves the current software update status
2022-02-04 02:38:00,077 - INFO - <module> - firmware update for endpoint "endpoint-a12170845ac34e22a8910498a28866bf" was triggered
```

6. Check on the update status

```
./tc.py get endpoint -id endpoint-a12170845ac34e22a8910498a28866bf history
[
    {
        "OTADeviceStatus": "Outdated",
        "endpointId": "endpoint-a12170845ac34e22a8910498a28866bf",
        "os": {
            "currentVersion": {
                "hash": "5936e90391cb67e189a52d3a0e7e726ff1ed4b399950119343ad5b61852db9da"
            }
        },
        "status": {
            "lastSeen": "2022-02-04T02:38:49Z",
            "online": true
        }
    }
]
```

OTADeviceStatusis status of aktualizr client: it has values:

1. UpToDate - all required changes applied
2. Outdated - device in the process of applying changes
3. Error - last operation completed with an error
4. NotSeen - device hasn't connected to OTA

7. (workaround) Check that ostree-pull succeeds. If not, run endpoint_ota_updates.py again

```
Feb 04 03:14:35 amdx86-64 aktualizr[13788]: ostree-pull:
Receiving objects: 1%
Feb 04 03:14:36 amdx86-64 aktualizr[13788]: ostree-pull:
Receiving objects: 2%
...
...
Feb 04 03:15:30 amdx86-64 aktualizr[13788]: ostree-pull:
Receiving objects: 98%
Feb 04 03:15:34 amdx86-64 aktualizr[13788]: libostree pull from
'aktualizr-remote' for 0 refs complete
                                            security: GPG: disabled
http: CA-pinned
                                            non-delta: meta: 2
content: 809
                                            transfer: secs: 60 size:
183.1 MB
Feb 04 03:15:34 amdx86-64 aktualizr[13788]: ostree-pull: 2
metadata, 809 content objects fetched; 178845 KiB transferred in
60 seconds
Feb 04 03:15:34 amdx86-64 aktualizr[13788]: got
DownloadTargetComplete event
Feb 04 03:15:34 amdx86-64 aktualizr[13788]: got
AllDownloadsComplete event with status: "Success"
```

Look for successful status lines including

a. got AllDownloadsComplete event with status: "Success"
b. Pending update for Primary ECU was not applied because reboot was not detected, continuing with initialization
c.

Copying /etc changes: 7 modified, 2 removed, 17 added
Bootloader updated; bootconfig swap: yes; deployment count change: 0

Freed objects: 243.3?MB

8. aktualizr-info to check that the new version (hash) is "Pending"
   a. Access endpoint via the terminal or ssh
   b. su
   c. aktualizr-info

```
amdx86-64:~$ su
Password:
amdx86-64:/home/pharos# aktualizr-info
Device ID: 8884cfb2-51fb-51a5-b7a8-3d91d010e04a
Primary ECU serial ID:
13971302a7a25f19f5b4993f94b6df6affbee02fc471f4cf48fe310f47b2cfb
0
Primary ECU hardware ID: amdx86-64
Provisioned on server: yes
Fetched metadata: yes
Current Primary ECU running version:
5936e90391cb67e189a52d3a0e7e726ff1ed4b399950119343ad5b61852db9d
a
Pending Primary ECU version:
7bea0bc82d08e33bb220acd8fbd596827f6f44c0e5fbe544c14823c2648b9a0f
```

9. Graceful reboot
   a. short power button press
   b. terminal | reboot
   c. Rebooting may take some time to complete as updates are applied.
      i. If the tty is still available, you should see
         1. A stop job is running for Aktualizr update service
10. After boot, check status with either:

    a. ./endpoint_ota_update_status.py .

       i. Outdated => still updating
       ii. UpToDate => done
    b. aktualizr-info
       i. "Pending Primary ECU version" present => still updating
       ii. No "Pending Primary ECU version" => done
    c. ./endpoint_metadata.py <endpointID> | jq '.properties.reported.os'
       i. hash
11. Verify changes are present in the updated version.

4		Update a device to an older firmware	Repeat upgrade steps, but update to an older version.	PASSED

5	OTA Update Notification from UI	Update device to a different version and verify Teradici Client picks it up	1. Go to Network Health and ensure the device is connected to Trust Center 2. Go to the About page and note down the firmware version number 3. Repeat Test 3 above to upgrade the device to a different firmware 4. Verify that a notification appears on the UI with a new version pending 5. Click Reboot from the notification message or go to top left Power icon to reboot the device. 6. After reboot, ensure the notification message no longer appears. 7. Go to the About page and ensure the version number is correct.	PASSED

Network Related Tests

Manual Tests:

Split Network (Bootstrap on one network, Connect to a PCoIP session on another network)

<not yet supported in OEM Build 4; teradici-client will block until the TC is available>

Cases 2 & 4: Some customers plan to bootstrap/register/stage devices on one network then ship/move the devices to another network before connecting to a broker.

Case 2 connects to an endpoint connector; Case 4 does not.

Prerequisite:

- A Trust Center
- A Linux machine that is able to access the Trust Center via IP with Python 3.6.9+
- A network that can NOT see the Trust Center via IP
- A registered endpoint
    - The endpointID of the endpoint you're managing is known (usually in the form of *endpoint-<machine id>,* such as *endpoint-58339fccf46546e386207f2e8cdf416b*)
        - Please see Obtaining Endpoint ID for how to obtain your endpoint ID

	Test Name	Description	Steps	Result
1	Verify Registration	Bootstrap endpoint to a new TC	1. Metadata appears for endpoint in Trust Center a. ./endpoint_metadata.py <endpointID> i. Follow example script from **OTA Setup Test 2** b. Postman | Query Specific Endpoint 2. Configure a trusted broker (**Endpoint Management via the Trust Center Test 6 - Trusted Brokers Configuration**)	PASSED
2	Connect to broker	Connect to broker	1. Disconnect ethernet from bootstrap network a. terminal | ip addr b. note the current eth0 subnet 2. Power off client 3. Connect ethernet to a network that can NOT see the Trust Center via IP 4. Power on client 5. Ensure subnet has changed a. terminal | ip addr b. note the current eth0 subnet; should differ from 1.b 6. Connect to broker and start a PCoIP session.	PASSED

Troubleshooting

Obtaining Endpoint ID

Once you have access to the terminal, you can obtain the endpoint ID by doing

```
ENDPOINT_ID="endpoint-`cat /etc/machine-id`"
echo $ENDPOINT_ID
```

This endpoint ID will be needed to manage this endpoint from the Trust Center. In the future, there will be a more user-friendly way to identify your endpoint via the UI.

Issues observed during testing

Component	Issue description	Type	Jira ID
UI	Log Viewer's **Show Search Lines only** and **# matches** do not get properly refreshed when you click on a new log	Functional	TSW-173465 - Getting issue details... STATUS
UI	Pharos endpoint is able to connect to PCoIP Agents without a Trust Center	Functional	TSW-173135 - Getting issue details... STATUS
UI	**Desktop restart** is shown even for "unknown" desktop.	Functional	TSW-173500 - Getting issue details... STATUS
UI	**Desktop restart** no happening.	Functional	TSW-173173 - Getting issue details... STATUS
UI	Clicking "Reload" flashes the screen and the message "Something went wrong" repeats.	Functional	TSW-173175 - Getting issue details... STATUS
UI	**In-session dropdown menu** options causing undesired outcome	Functional	TSW-173474 - Getting issue details... STATUS
UI	**Logviewer** not showing /home/pharos	Functional	TSW-173501 - Getting issue details... STATUS
UI	A link missing in About page when in French	Cosmetic	TSW-173488 - Getting issue details... STATUS
UI	Not using alias on desktop page?	Cosmetic	TSW-173489 - Getting issue details... STATUS
UI	Possible memory leak when going in/out session	Functional	TSW-173490 - Getting issue details... STATUS
UI	Deleted connections magically re-appear	Functional	TSW-173282 - Getting issue details... STATUS
UI	Clicking on any of the links in **AboutTerms & Conditions** will open up the link in fullscreen with no way to exit **The only way out is Reboot**	Functional	TSW-173496 - Getting issue details... STATUS
UI	LogViewer not showing rotated files	Functional	TSW-173497 - Getting issue details... STATUS
TA	**Log rotation** not happening	Functional	TSW-170838 - Getting issue details... STATUS
TA	Factory reset not cleaning up log files	Functional	TSW-173498 - Getting issue details... STATUS
TA	Support bundle filtering seems to be picking up files from excluded list	Functional	TSW-170838 - Getting issue details... STATUS
TA	Log rotation fix doesn't seem to be setting /var/anyware permission correctly	Functional	TSW-170838 - Getting issue details... STATUS
TC	Upgrade OEM6 to OEM7 TC is failing	Functional	TSW-173467 - Getting issue details... STATUS

OTA	Endpoint shows "No currently running version" after factory reset.	Functional	TSW-173365 - Getting issue details... STATUS
Client SDK	**In-session locale** doesn't seem to work. Changed language to French, went in session, but client menu at the top was not in French.	Functional	TSW-94648 - Getting issue details... STATUS