Pharos OEM Beta - Quick Start Guide

Getting Started

Pharos OEM Beta is a release for selected partners and customers of the Trust Center and Trusted Zero Client.

This guide covers the basics of setting up a Trust Center and connecting a Trusted Zero Client. It assumes you already have a device that is factory provisioned and pre-loaded with Trusted Zero Client software. (ODM partners, please refer to the Factory Provisioning Guide - sent separately). It also assumes that you have an HP Anyware desktop to connect to.

To get started, a Trust Center is required to operate your Trusted Zero Client. The Trust Center is the root of the Trusted Zero Client's security posture and provides a Zero Trust Architecture on the device and through the network it is connected on to provide a world-class security experience.

Setting up a Trust Center requires:

- requesting a certificate,
- setting up DNS records (FQDNs) to point to the Trust Center,
- customizing the Trust Center config file,
- then running the Trust Center installer.

From there you will connect your Trusted Zero Client by entering the FQDN you defined for the Trust Center. Once your Trusted Zero Client is up and running you may start connecting to your remote desktops!

Trust Center Installation

This section describes the procedure to run the stand-alone installer on a single machine. To jump straight into installing your Trust Center into a new or existing Kubernetes cluster refer to the Pharos OEM Beta - Advanced Trust Center Install Guide.

Prerequisites

Request a Registration Certificate

The Trust Center needs an FQDN to operate. This is the root of our security model as it is used to create a Trust Center certificate that creates a chain of trust with Trusted Zero Clients.

Requesting a certificate requires generating a private key and a corresponding Certificate Signing Request (CSR) with your desired FQDN.

> ⚠ The FQDN you choose must be under a domain you control, as you will have to create DNS A records for it in a later step.

At minimum the CSR **MUST** contain:

- **CN** field matching the FQDN of the Trust Center
- **SubjectAltName** with the FQDN of the Trust Center
- **DNS** entries matching the FQDN of the Trust Center and the default FQDN pcoiptrustcenter

A tool such as openssl can accomplish this. Below is the bare minimum set of commands to generate a private key and a CSR. Copy paste these into a shell to execute them:

Issue Certificate

```
export DOMAIN="<enter your desired domain here>"

cat > registration.cfg << EOF
[req]
default_bits = 4096
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn
[ dn ]
C=CA
O=MyOrg
OU=MyOrgUnit
emailAddress=me@working.me
CN = register.${DOMAIN}
[ req_ext ]
subjectAltName = @alt_names
[ alt_names ]
DNS.1 = register.${DOMAIN}
DNS.2 = pcoiptrustcenter
EOF

openssl req -nodes -new -keyout registration.key -out registration.csr -config registration.cfg
```

⚠ Make sure to securely save the private key (registration.key in the above script) as this is required later on to deploy the Trust Center. This key should never be shared.

Once the CSR is generated, it must be sent to your HP contact in PEM format (do NOT send the private key with the CSR). You will get back a certificate chain in PEM format for the provided CSR .

Obtain Registration Certificate and Credentials

Your HP contact will send you the signed registration certificate as well as download links and credentials.

Please be sure to copy the values and save them in a secure location as they are required for installation of the Trust Center:

- `partner-entitlement-token`: the token for downloading Trust Center and endpoint updates, also used in `config.yaml`

Deploy a VM

The Trust Center requires:

- RHEL 8 or CentOS 8
- 8 vCPUs
- 32GB RAM
- 80GB free disk space
- IP network accessible by your endpoints, with DNS configured as described below
    - **NOTE**: *the Trust Center no longer supports connections via raw IP addresses.*

Create DNS Records

You must create the following DNS A records to point to your Trust Center VM:

- `trust-center.<domain>`
- `endpoint-connector.<domain>`
- `ota.<domain>`
- `register.<domain>`

Where <domain> is the same as the domain specified in the CSR you provided to us.

In addition, if you with to support automatic Trust Center discovery by endpoints, you will need to create a CNAME record redirecting "pcoiptrustcenter" to "register.<domain>"

Installation

Choose an existing or create a new directory to perform the installation from on the VM you created. The following steps take place within that directory.

Download and extract installer

Download the Trust Center Stand-alone Installer from the provided link.

Extract the tarball:

Download and extract installer

```
curl -o trust-center-installer.tar.gz https://dl.teradici.com/<partner-entitlement-token>/trust-center-beta/raw
/names/trust-center-tgz/versions/22.07.0-rc10.tar/trust-center_22.07.0-rc10.tar.gz
tar -xvf trust-center-installer.tar.gz
```

Create and populate config file

Below is the bare minimum config template to deploy the Trust Center. You must populate following variables with the values provided in your credentials package:

- <container-registry-username>
- <container-registry-password>
- <partner-entitlement-token>

Populate <domain> with the domain used for the CSR and <admin-password> with a password of your choice (this is required later on to initialize the Trust Center so you must save the password).

config.yaml

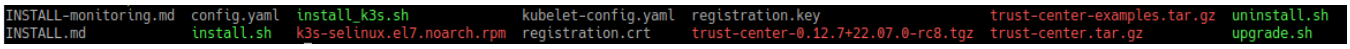
```
global:
  images:
        registry: "docker.cloudsmith.io/teradici/trust-center-beta"
    username: "teradici/trust-center-beta"
    password: "<partner-entitlement-token>"
  tc:
    domain: "<domain>"
    username: tcAdmin
    password: "<admin-password>"
    endpointUpdate:
      accessKey: "<partner-entitlement-token>"
      repository: "teradici/trusted-zero-client-beta"
```

Edit the file called config.yaml and populate it with the contents of the above template; replacing the placeholders with the credentials you were provided.

Copy Registration Certificate and Key

You must provide your issued Trust Center Registration certificate chain and key at install time by providing PEM files for the cert and key. The installation script defaults to looking in the current directory for files named `registration.crt` and `registration.key`.

Create and populate the file `registration.crt` by copying and pasting the contents of the issued certificate chain that is sent to you. The `registration.key` file containing private key that was generated in the prerequisite steps must also be present.



Run the installer

- `Run sudo ./install.sh`

- Running this script will use the provided configuration to deploy the Trust Center, installing all required dependencies
- The installation process takes around 10 to 15 minutes to complete
- See the Troubleshooting section below if any issues arise during installation

Post Install

Once installation is complete, you can set up your Management Console to interact and manage Trusted Zero Clients through your Trust Center.

Troubleshooting

See the troubleshooting section of `INSTALL.md` that is packaged with the Trust Center Installer if you experience any issues not listed below while deploying.

Support Bundle

Download and execute the Trust Center Diagnostic Tool to create a support bundle. This captures the state of the Trust Center. Send the generated archive back to us so we can help resolve your issue.

To Generate Support Bundle

```
curl -o trust-center-ctl.tar.gz https://dl.teradici.com/<partner-entitlement-token>/trust-center-beta/raw/names
/trust-center-ctl-amd64-tgz/versions/22.07.0-rc10/trust-center-ctl_22.07.0-rc10_linux_amd64.tar.gz
tar -xvf trust-center-ctl.tar.gz
sudo ./trust-center-ctl diagnose --support-bundle --cluster-type k3s
```

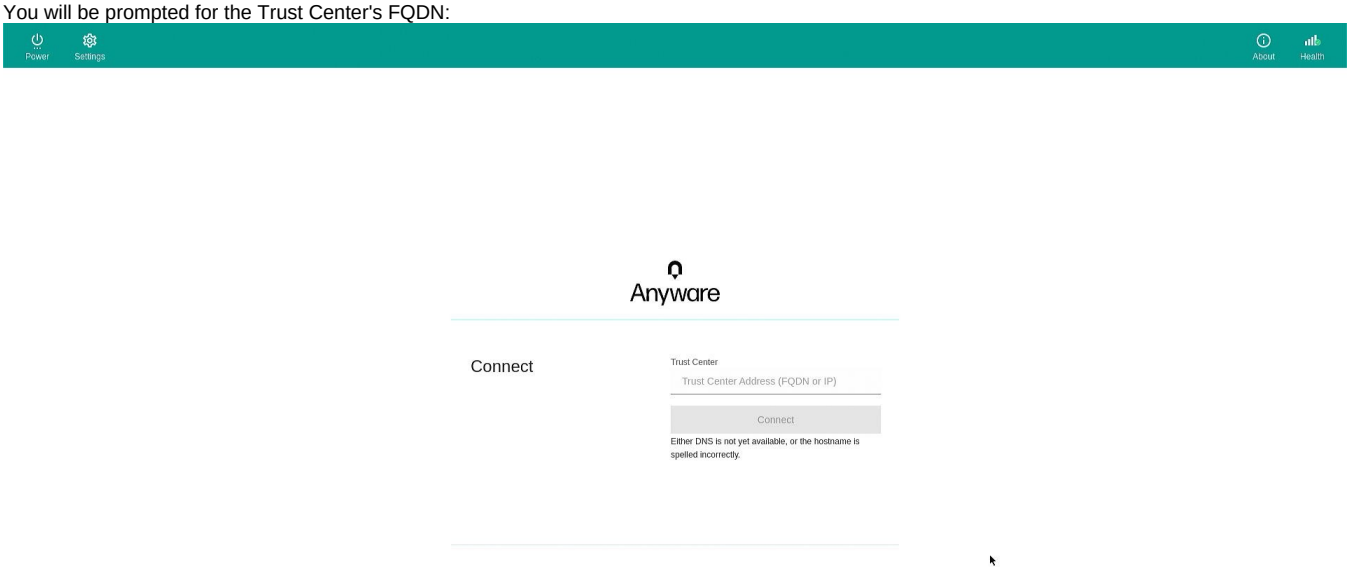
Trusted Zero Client Configuration

Connect to a Trust Center

Establish a connection with your Trust Center

Ensure that your network is configured such that your Trust Center is reachable by the Trusted Zero Client on port 32443.

You will be prompted for the Trust Center's FQDN:



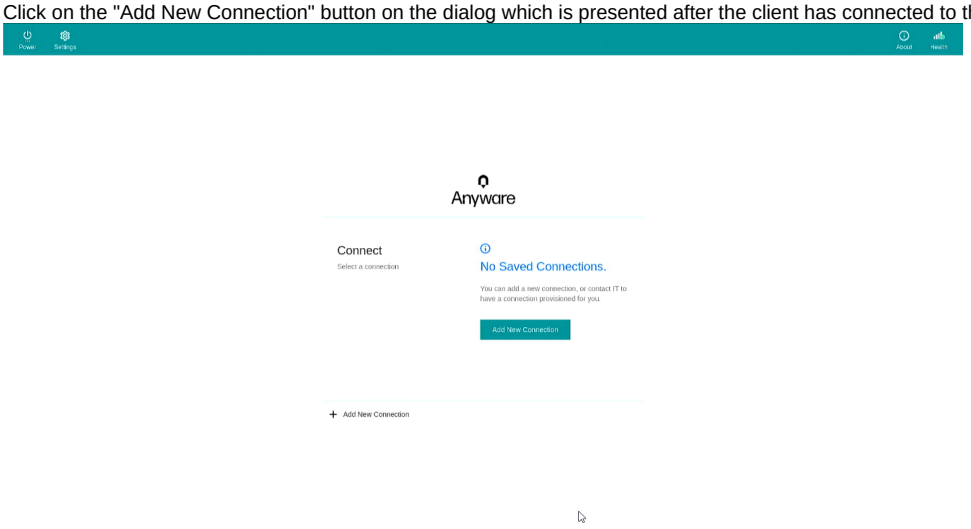
Provide the correct FQDN and click **connect**. If the address is valid and reachable, the Trusted Zero Client will register itself with the Trust Center and show the connection page.

On subsequent power-ups, the Trusted Zero Client will automatically connect to the Trust Center.

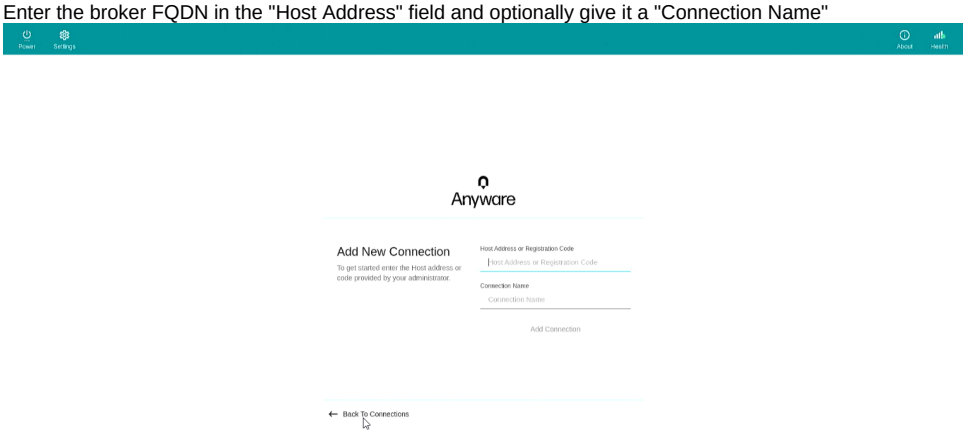
Connect to a PCoIP Broker and Enter a PCoIP Session

Creating a "Connection" via the Trusted Zero Client UI

- Click on the "Add New Connection" button on the dialog which is presented after the client has connected to the Trust Center.

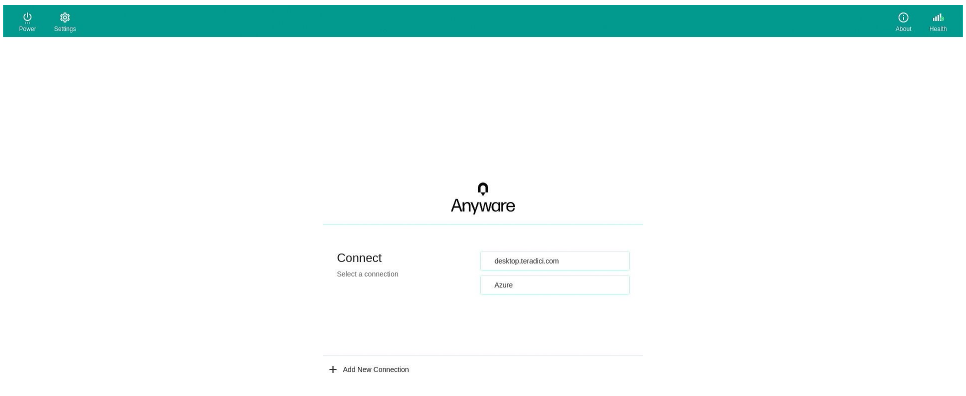


- Enter the broker FQDN in the "Host Address" field and optionally give it a "Connection Name"



Establish a PCoIP Session

- Once you have added one or more Trusted Brokers, they will appear as connections in the UI:



- Begin by selecting a Connection.

- Authenticate with the broker and select a remote desktop (if there is more than one).
- A PCoIP session will be established with the remote desktop.
- To exit the session and return to the connection selection dialog, type <CTRL><ALT><F12>

Next Steps

You've now setup a basic installation of your Trust Center, Management Console, and Trusted Zero Client. Explore more features of your Trust Center in the Advanced Guide!