Introduction to your tz655 with HP Anyware's Trust Center

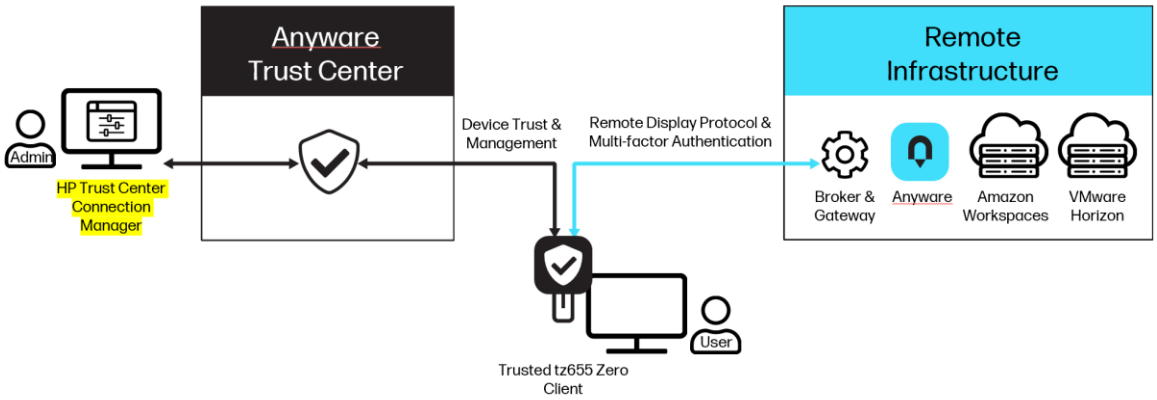
What is this whitepaper about?

This whitepaper provides you with the necessary steps to set up your tz655 device for the first time. This device pairs with HP Anyware's Trust Center, a management and security plane for a Trusted Zero Client deployment.

By following this guide, you will be able to:

- Connect your tz655 device and register it with HP Anyware's Trust Center
- Access the HP Anyware dashboard and monitor your device status and activity
- Apply security policies and updates to your device and applications

What is HP Anyware's Trust Center?



HP Anyware's Trust Center is a cloud-based security platform that serves as a secure hub for managing trusted endpoints within the Anywhere platform. The Anyware Trust Center establishes trust between a remote Trusted Client device in several key ways:

- Birth Certificates: Each factory-provisioned PCoIP Trusted Client provides a certificate, assigned when provisioned by the vendor, which is used to establish a trust relationship with your Anyware Trust Center. If a device has an unknown birth certificate, or if its certificate is not signed as expected, it cannot connect.
- Digital Twins: The Anyware Trust Center maintains a copy of the expected state and the current (actual) state of each Trusted Zero Client it manages. Each time a Trusted Zero Client connects, the Anyware Trust Center reads the endpoint's current state and compares it with the expected state. If the Trusted Zero Client has been tampered with, the two states will not match, and your Endpoint Management Software (EMS) can revoke its trusted status. When administrators modify a Trusted Zero Client's settings, the Anyware Trust Center updates its local copy (the expected state), and pushes the changes to the physical Trusted Zero Client the next time it connects.

- Direct Secure Boot: Users cannot access the firmware, BIOS, or operating system of the Trusted Zero Clients. Each device securely boots directly into the PCoIP client application.
- OTA Updates: Firmware updates for Trusted Zero Clients are delivered Over the Air (OTA), so bug fixes and security updates can be provided immediately when available. OTA updates are delivered using TUF and Uptane frameworks, providing an update mechanism capable of resisting even nation-state level actors.

From establishing trust relationships to implementing robust security measures, the Trust Center plays a vital role in ensuring the integrity and confidentiality of data transmissions across diverse networks. With detailed instructions and best practices provided in the guide, administrators can navigate the Trust Center's functionalities with confidence, safeguarding critical assets and upholding the highest standards of security within their organization's digital infrastructure.

What do you need to get started?

To set up your tz655 device with HP Anyware's Trust Center and HP Trust Center Connection Manager, you will need the following:

- A tz655 device
- A copy of your zero client receipt
- HP Anyware's Admin Guide
- HP Trust Center Connection Manager Admin Guide
- HP Trust Center Connection Manager OVF disk files
    - Alternative installation: Deb installation package on Ubuntu 20.04

Once you have these ready, you can proceed to the next section of the whitepaper, where you will learn how to connect your tz655 device to the internet and register it with HP Anyware's Trust Center.

Accessing your Trust Center for the first time

HP is excited to announce that each Trusted Zero Client shipped after July 27, 2023 includes a one-year subscription to HP Anyware Trust Center.

To register your subscription and access it for the first time, follow these steps:

-Go to this URL

-Enter your information including your name, email address, and invoice information

-Upload a copy of your proof of purchase and select the file that contains your receipt or invoice for the tz655 zero client device

-Once your purchase is verified, you will receive an email directing you to access your Trust Center and confirming that your subscription is active.

Setting up your Trust Center for the first time

Trust Center Connection Manager is available for setup and deployment in two ways. One is to install the OVF file (Open Virtulization Format, OVF), which contains the major components of DMS, including: application server, database server, web server, file server, FTP server, TFTP server and UPnP server. The other is to install the .deb installation package on a specified version of Linux operating system.

Red Hat Linux Deployment

- Set up a new Red Hat Enterprise Linux 9.3 Installation
- Choose to manually partition the installation

  Note: If you choose to automatically partition the image, the setup will give you 70GiB of VAR and not the 80GiB of VAR required
- Add a new mount point
  - Mount point: /var
    - Desired capacity: 80 GiB
  - Mount point: /home
    - Desired capacity: 145.54 GiB
  - Mount point: /boot/efi
    - Desired capacity: 600 MiB
  - Mount point: /boot
    - Desired capacity: 1024 MiB
  - Mount point: swap
    - Desired capacity: 7.87 GiB
  - Mount point: /
    - Desired capacity: [leave blank]

    Note: This will give the remaining capacity to the main root

Image taken of a 225 GiB disk example

- Accept changes and move to installation summary
- Click “Network & Host Name”
- Name your Host Name/Trust Center
    - It is recommended to use a “-“ between trust and center for example: “trust-center.thincloud.local”
- Apply and partition your image
    - *Note: If you do not name your Host Name what you expect your Trust Center to be called, your install may fail to work after reboot and trust center may need to be reinstalled*

Accessing HP Trust Center Connection Manager

Please switch to the HP Trust Center Connection Manager Admin Guide for step by step instructions on installing the Connection Manager with your 3 OVF template files.

Alternatively, if you wish to use the deb installation please follow the instructions below.

DEB Installation

For the Deb installation it is recommended to use Ubuntu 20.04.

Please use an account that can execute sudo commands on the terminal and ensure connecting to the Internet. The installation steps are as follows (YY.MM.XX is the DMS release version):

Step 1: Unzip the DMS installation file on the host

Command: tar -zxvf <DMS file name, e.g. dmsc00-vYY.MM.XX-inst.tgz>

Step 2: Move to the directory with the unzipped file

Command: cd <DMS file name, e.g. dmsc00-vYY.MM.XX-inst>

Step 3: Install the DMS

Command: ./DMS_Installer

After Installation

It is important to note that once you have installed the Connection Manager and point it to your Trust Center, the administrator password is automatically generated. For more information please refer to the “After Installation” portion in the HP Anyware Admin Guide for more details but for your convenience the yaml data is provided below:

Note: yaml file domain should be edited to “api.[your domain]”

Note: The administrator password is automatically generated

The administrator password is automatically generated by the Anyware Trust Center installer, and has the ability to create service account keys. The generated password is placed in the `config.yaml` file in your installation directory.

`<installation_folder>/config.yaml`:

```
global:
images:
    registry: "docker.cloudsmith.io/teradici/trust-center"
    username: "teradici/trust-center"
    password: <repository password>
tc:
    domain: api.<your domain>
    password: <this is the auto-generated password>
    endpointUpdate:
      accessKey: <repository password>
      repository: "teradici/trusted-zero-client"
```