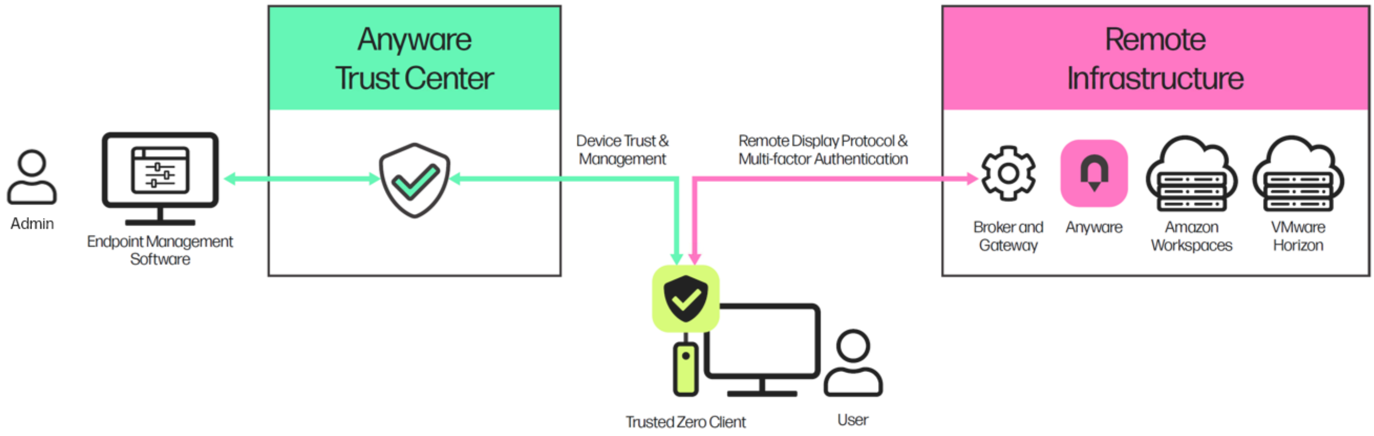
Anyware Trust Center Administrators' Guide

24.03

Table of Contents

Anyware Trust Center Administrators' Guide

The Anyware Trust Center provides a management and security plane for a Trusted Zero Client deployment. Using the Anyware Trust Center, administrators can register Trusted Zero Clients, manage their capabilities and features, enable and disable connections, and monitor access behavior.



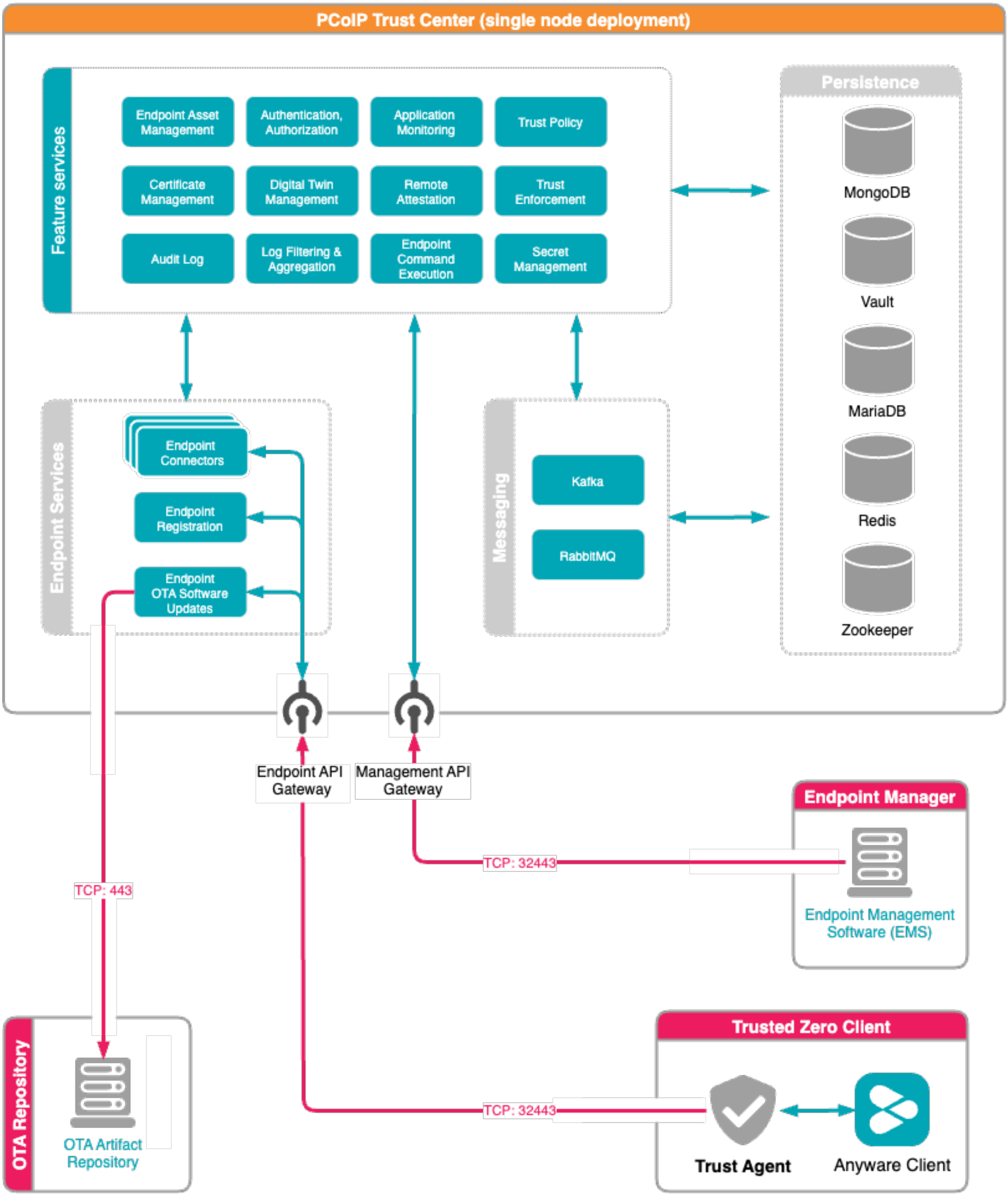
The Anyware Trust Center is an application composed of multiple services on a single VM. It connects to Trusted Zero Client endpoints and your Endpoint Manager.

Important: About Endpoint Managers

The Anyware Trust Center is an API service, and has no user interface. All user interaction and interfaces are provided by an *Endpoint Manager*, also called *Endpoint Management Software (EMS)*. Endpoint Management Software is available from the hardware manufacturer of your Trusted Zero Client.

Anyware Trust Center Architecture

The Anyware Trust Center is composed of multiple feature services which communicate internally within the cluster, and also securely communicate with the distributed Trusted Zero Clients and the Endpoint Manager.


PCoIP Trust Center (single node deployment)
Feature services
Endpoint Asset Management
Authentication, Authorization
Application Monitoring
Trust Policy
Certificate Management
Digital Twin Management
Remote Attestation
Trust Enforcement
Audit Log
Log Filtering & Aggregation
Endpoint Command Execution
Secret Management
Persistence
MongoDB
Vault
MariaDB
Redis
Zookeeper
Endpoint Services
Endpoint Connectors
Endpoint Registration
Endpoint OTA Software Updates
Messaging
Kafka
RabbitMQ
Endpoint API Gateway
Management API Gateway
TCP: 443
TCP: 32443
TCP: 32443
Endpoint Manager
Endpoint Management Software (EMS)
Trusted Zero Client
Trust Agent
Anyware Client
OTA Repository
OTA Artifact Repository

About Anyware Trust Center Persistence

The Anyware Trust Center uses multiple services for data persistence. The following table lists these services and briefly describes how each is used.

Service	Description
MongoDB	MongoDB maintains management data, including endpoint configuration, digital twins, and system configuration.
MariaDB	Provides OTA update data and metadata.
Vault	Holds auth secrets, Anyware Trust Center user credentials, and endpoint operational PKI.
Redis	Audit logging and general system caching.

Note: About external services

The Anyware Trust Center does not currently support external instances of these services.

We recommend backing up the Anyware Trust Center and all persistent storage volumes.

About the Zero Trust Ecosystem

The PCoIP Zero Trust Ecosystem is a robust architecture for PCoIP deployments, founded on zero-trust principles and providing extremely secure PCoIP deployments. There are two primary components in the Zero Trust ecosystem: **Trusted Zero Clients**, which allow end users to connect to their remote desktops, and the **Anyware Trust Center**, which manages the Trusted Zero Clients and enforces policies and integrity.

Throughout this document, the Trusted Zero Clients may be referred to as *endpoints*. Currently, the Trusted Zero Client is the only endpoint managed by the Anyware Trust Center.

Security Provisions

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 Anyware 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.

Important Terminology

- **Provisioning**: Provisioning is performed at the factory, when the Trusted Zero Client is prepared for delivery. This process includes creating the device's birth certificate and signing it with an HP certificate authority.
- **Registration**: The initial connection between a Trusted Zero Client and the Anyware Trust Center, when the Trusted Zero Client is added to the Anyware Trust Center's list of managed devices. After registration, the Trust Center can manage the Trusted Zero Client, and users can connect to their authorized desktops.
- **PKI**: PKI stands for *Public Key Infrastructure*, which is a method of distributing and managing security certificates. The Anyware Trust Center supports either an external PKI, which you provide, or an internal service for smaller or less-complex deployments. External PKIs must provide an externally-issued signing CA that the Anyware Trust Center uses to generate operational certificates.
- **Endpoint Management Software (EMS)**: Also called an *Endpoint Manager*, the Endpoint Management Software is a third-party application that provides a user interface for the Anyware Trust Center. The Endpoint Management Software is available from your Trusted Zero Client manufacturer.

What's New in This Release

Release 24.03 of the Anyware Trust Center includes the following:

Static IP Support

You can now configure a Trusted Zero Client's IPv4 and IPv6 settings via the Trusted Zero Client's interface, or by pushing from the Anyware Trust Center.

New Device Timeout Policy

You can now set a policy for the length of time that a Trusted Zero Client can remain disconnected from a Anyware Trust Center before it becomes untrusted.

Support for 802.1x EAP-TLS

With this release, you can now manually provision Trusted Zero Client devices with certificates for networks which require 802.1x authentication. The method used to do this depends on your Endpoint Management System (EMS); refer to your manufacturer's documentation for more information.

Client Firmware Version Enforcement

A new Trusted Zero Client policy has been added that allows administrators to set a desired firmware version number, and then block new sessions for any Trusted Zero Client devices that are out of date.

Setting desired/trust/policies/version to the desired version number will enforce this policy.

Support for Darksite Installations

The Anyware Trust Center can now be installed in dark sites, which do not have a connection to the public internet. Installing in a dark site requires a temporary internet-connected machine, which downloads required packages and creates an installation bundle. The installation bundle is then transferred to the dark site machine and installed. For system requirements, see Dark Site System Requirements. For installation instructions, see Dark Site Installation.

Note: OTA updates to Trusted Zero Client devices in dark sites is not supported in this release.

System Requirements

The Anyware Trust Center is installed on a machine that meets the following minimum requirements:

Requirement	
Operating System	• RHEL 9 • Rocky Linux 9
CPUs	4 vCPUs
Memory	16GB RAM
Disk	120GB+, including 80GB+ disk space on `/var` for persistent volumes
Network	• IP network accessible by your endpoints, with configured DNS. The Anyware Trust Center does not support connections via raw IP addresses. • TCP 32443 (Communication with Trusted Zero Clients) • TCP 443 (Communication with OTA update CDN)
Python	The post-installation and initialization scripts require Python 3.8.2+.
Other software	The OS must have cURL available.

Note that the specifications listed here are minimums. Large or complex deployments should expect to use machines with higher specifications.

Important: A management tool is required

The Anyware Trust Center is an API service and has no user interface. The Anyware Trust Center must be able to connect to a compatible Endpoint Management Tool from a supported manufacturer.

Dark Site System Requirements

The Anyware Trust Center can be installed in dark sites (sites without a connection to the public internet). Installing in a dark site requires two machines: a temporary internet-connected machine to assemble the installer bundle, and the unconnected machine that will host the Anyware Trust Center. For installation instructions, see Dark Site Installation.

Bundler System Requirements:

Note: The bundler system is temporary

The bundler machine can be temporary, and is required when doing any of the following:

- Creating an installation bundle to install a new Anyware Trust Center
- Creating an update bundle to update an existing Anyware Trust Center
- Downloading and installing firmware updates on Trusted Zero Clients.

You can stop or delete the machine when finished with each task. If you delete the machine, you will need to re-create when you are ready to proceed with the others.

Requirement	
Operating System	• RHEL 9 • Rocky Linux 9
CPUs	4 vCPUs
Memory	16GB RAM
Disk	At least 20GB free space available for the generated dark site bundle.
Network	The machine used to create the bundle must be connected to the public internet.
Software	Docker v25.01+, cURL, DNF

Dark Site Machine Requirements

Note: The dark site machine is permanent

This machine hosts the Anyware Trust Center in the darksite location and is permanent.

Requirement	
Operating System	• RHEL 9 • Rocky Linux 9
CPUs	4 vCPUs
Memory	16GB RAM
Disk	120GB+, including 80GB+ disk space on `/var` for persistent volumes
Network	A default gateway is required, even without an internet connection. If the machine does not have one, a dummy route is required for installation. See Checking for a Default Gateway for instructions.
Software	DNF

Anyware Trust Center Features

The Anyware Trust Center supports a number of endpoint management settings and capabilities, some of which are constrained by your subscription level. The available features and support level are described next.

About Licensing and Subscription Tiers

Most Anyware Trust Center functionality requires a subscription. Basic functionality is available for free for users who have small deployments, or who are testing proof-of-concept scenarios.

New Trusted Zero Client devices ship with a 12-month free subscription.

Endpoint Management

Feature	Free tier	Subscriber
Endpoints under management	up to 50	up to 5,000[1]
Endpoint monitoring	Yes	Yes
Device Logging	Yes	Yes
Endpoint power management	Yes	Yes
Endpoint factory reset	Yes	Yes
Over-the-Air (OTA) updates	—	Yes
Set USB usage policies	—	Yes

Endpoint Under Management

The Anyware Trust Center can manage a large number of endpoint devices. The specific number of supported endpoints supported depends on your subscription tier, as noted above. The free tier, which does not require a subscription, is limited to 50 devices.

Endpoint Auto-Discovery and Configuration

When a new Trusted Zero Client connects to the Anyware Trust Center, it will automatically register and configure it according to policies established in your EMS software.

Endpoint Monitoring

The Anyware Trust Center supports status monitoring of all devices in your deployment, which can be used to display dashboards and other relevant management information in your Endpoint Manager.

Device Logging

The Anyware Trust Center can access logs for all of its managed Trusted Zero Clients, allowing administrators to troubleshoot deployment problems and monitor unusual activity.

Endpoint Power Management

The Anyware Trust Center can shut down or restart the endpoint devices it manages.

Endpoint Factory Reset

The Anyware Trust Center can reset any endpoint to factory defaults.

After a factory reset, the endpoint must re-register with the Trust Center. If it is on the same network as the Trust Center, and if the discovery DNS record is created, this will happen automatically when the device boots up. Otherwise, you will be prompted for the FQDN of the Trust Center.

Over-the-Air (OTA) Updates

The Anyware Trust Center can retrieve device software updates and deploy them to its endpoints automatically. Updates can be configured to install immediately, on a schedule, or by prompting the end user.

Set USB Usage Policies

USB policies can be set for each Trusted Zero Client that the Anyware Trust Center manages. Note that USB policies can also be set on remote PCoIP agents; USB devices must be allowed by *both* the Anyware Trust Center and the PCoIP agent. PCoIP agents, by default, permit all supported USB access.

Anyware Trust Center Management

Feature	Free tier	Subscriber
Concurrent Anyware Trust Center user access	—	Yes
PKI Support	—	Yes
Configure trusted connections	—	Yes

Concurrent User Access

Any number of users can access the Anyware Trust Center via your EMS software at once.

PKI Support

The primary PKI is an internal Hashicorp Vault instance in the Anyware Trust Center. You can provide an issuing CA cert and key to the internal Vault, which allows the root of Trust to come from your existing PKI.

Configure Trusted Connections

Trusted connections can be configured on the Anyware Trust Center. When configured this way, the Trusted Zero Client devices registered with the Anyware Trust Center will not be able to set their own connections, and must use the connections configured.

1. The initial release of Anyware Trust Center supports up to 500 devices connected with a paid subscription. This limit will be increased to 10,000 in a future release. ↩

Installing

Trust Center Installation Overview

Deployment Modes

The current release of the Anyware Trust Center uses a **single-node** installation into a K3S cluster using a provided script. The installation script creates and configures the node for you, and does not require manual setup.

Future releases of the Anyware Trust Center will support multi-node environments, installed into a Kubernetes cluster which you create and manage yourself.

When to Use Single-Node Deployments

The single-node instance of the Anyware Trust Center is appropriate for the following use cases:

- You do not require high availability or redundancy; your security policies permit delayed policy enforcement in the event your Anyware Trust Center is down or unavailable for any reason.
- You are deploying a proof-of-concept system for testing purposes.
- You do not have in-house Kubernetes expertise, and are not retaining our Professional Services team.
- You do not expect to grow beyond the initial node.

Note: Migrating from single-node to multi-node deployments

When multi-node deployments are available, a migration procedure will be published to support moving from one model to the other.

FAILURE RAMIFICATIONS IN SINGLE-NODE DEPLOYMENTS

The single-node deployment of the Anyware Trust Center is not a high-availability configuration. If the Anyware Trust Center is unavailable for any reason, including network connectivity issues, the following will occur until service is restored:

- Endpoints cannot be managed and policies cannot be enforced.
- New endpoints cannot be added.
- Monitoring and logging of endpoints will be paused.
- **Users can still connect to remote sessions while the Anyware Trust Center is down**.

Trusted Zero Clients continue to accumulate logging data even if the Anyware Trust Center is offline. When the Anyware Trust Center is reachable again, logging data will catch up automatically, without loss in continuity.

Planning for Future Multi-Node Deployments

Important: This method is not currently available

Multi-node deployments are not supported in this release of the Anyware Trust Center. This information is included here to help you plan for future deployments.

If any of the following describe your use case, you should plan to use the Multi-Node Installation method when it is available:

- You require high-availability SLAs and real-time monitoring of endpoints (in a single-node deployment, if the Anyware Trust Center is unreachable, monitoring is unavailable until the connection is restored).
- You have enterprise requirements such as multiple Trust Centers deployed in different regions, or a mix of cloud and on-premesis deployments.
- You will create or extend your own self-managed Kubernetes cluster, either by yourself or in consultation with our Professional Services team.

Single-Node Anyware Trust Center Installation

For small deployments, or as a proof-of-concept test, you can deploy the Anyware Trust Center using the included `trust-center-ctl` script. This script will create a single-node Kubernetes cluster and install the Anyware Trust Center and its dependencies.

Deploying the Anyware Trust Center involves the following steps:

1. Create a new VM to host the Anyware Trust Center.
2. Choose a domain name for connections to the Anyware Trust Center.
3. Configure DNS for the new machine.
4. Get the installation script from our website.
5. Run the installation script on the Anyware Trust Center machine.

1. Create a New VM

Deploy a dedicated server to host the Anyware Trust Center. The method used to do this will depend on your environment; if you are unsure how to proceed, ask your system administrators.

The Anyware Trust Center requires a dedicated server with the following specifications:

Requirement	
Operating System	• RHEL 9 • Rocky Linux 9
CPUs	4 vCPUs
Memory	16GB RAM
Disk	120GB+, including 80GB+ disk space on `/var` for persistent volumes
Network	• IP network accessible by your endpoints, with configured DNS. The Anyware Trust Center does not support connections via raw IP addresses. • TCP 32443 (Communication with Trusted Zero Clients) • TCP 443 (Communication with OTA update CDN)
Python	The post-installation and initialization scripts require Python 3.8.2+.
Other software	The OS must have cURL available.

2. Choose a Domain Name

The Anyware Trust Center requires 5 domain names added to your DNS records. In this step, you're creating the *base* domain for the Anyware Trust Center, which will be used to construct the other 4 subdomains. You'll use this value in multiple locations during setup, so record the value and be ready to copy it.

In this procedure, we will use `trust-center.example.com` to demonstrate the domain name, and how it is leveraged to create the other required values.

3. Create DNS Records

Once your new dedicated server has been created, you must set up the following DNS A records that point to it. For each of the following items, replace `<domain-name>` with the domain name you recorded in the previous step.

- `<domain-name>`
- `api.<domain-name>`
- `endpoint-connector.<domain-name>`

- `ota.<domain-name>`
- `register.<domain-name>`

Important: Supporting automatic Anyware Trust Center discovery

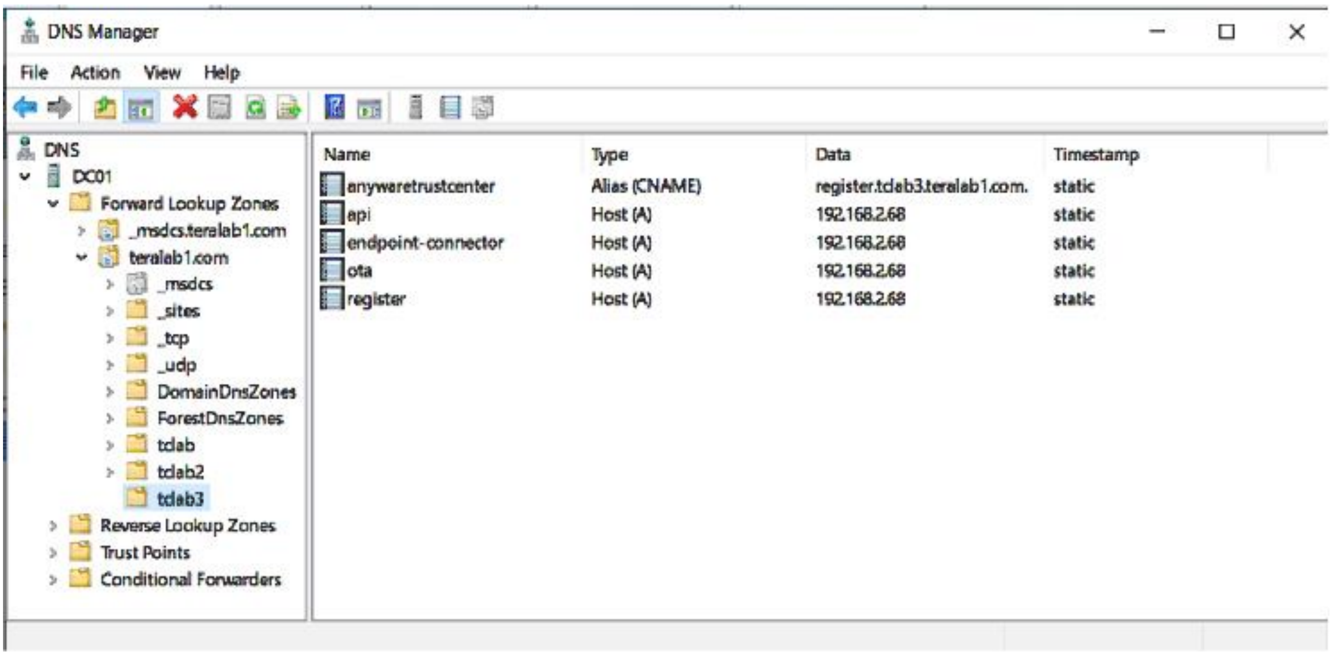
If you plan to support automatic Anyware Trust Center discovery by endpoints, you must also create a CNAME record that redirects `anywaretrustcenter` to `register.<domain-name>`.

Example: using `trust-center.example.com`

Using `trust-center.example.com` as the base domain, you would create DNS records for the following:

- `trust-center.example.com`
- `api.trust-center.example.com`
- `endpoint-connector.trust-center.example.com`
- `ota.trust-center.example.com`
- `register.trust-center.example.com`

This example shows a different DNS configuration using Windows DNS Manager:



Name	Type	Data	Timestamp
anywaretrustcenter	Alias (CNAME)	register.tclab3.teralab1.com.	static
api	Host (A)	192.168.2.68	static
endpoint-connector	Host (A)	192.168.2.68	static
ota	Host (A)	192.168.2.68	static
register	Host (A)	192.168.2.68	static

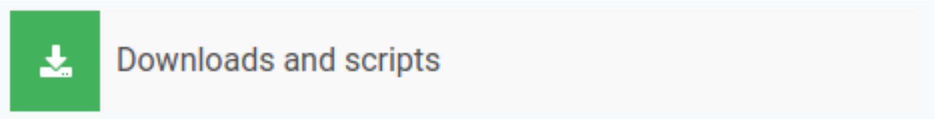
4. Get the Installation Script

Note: Support account is required

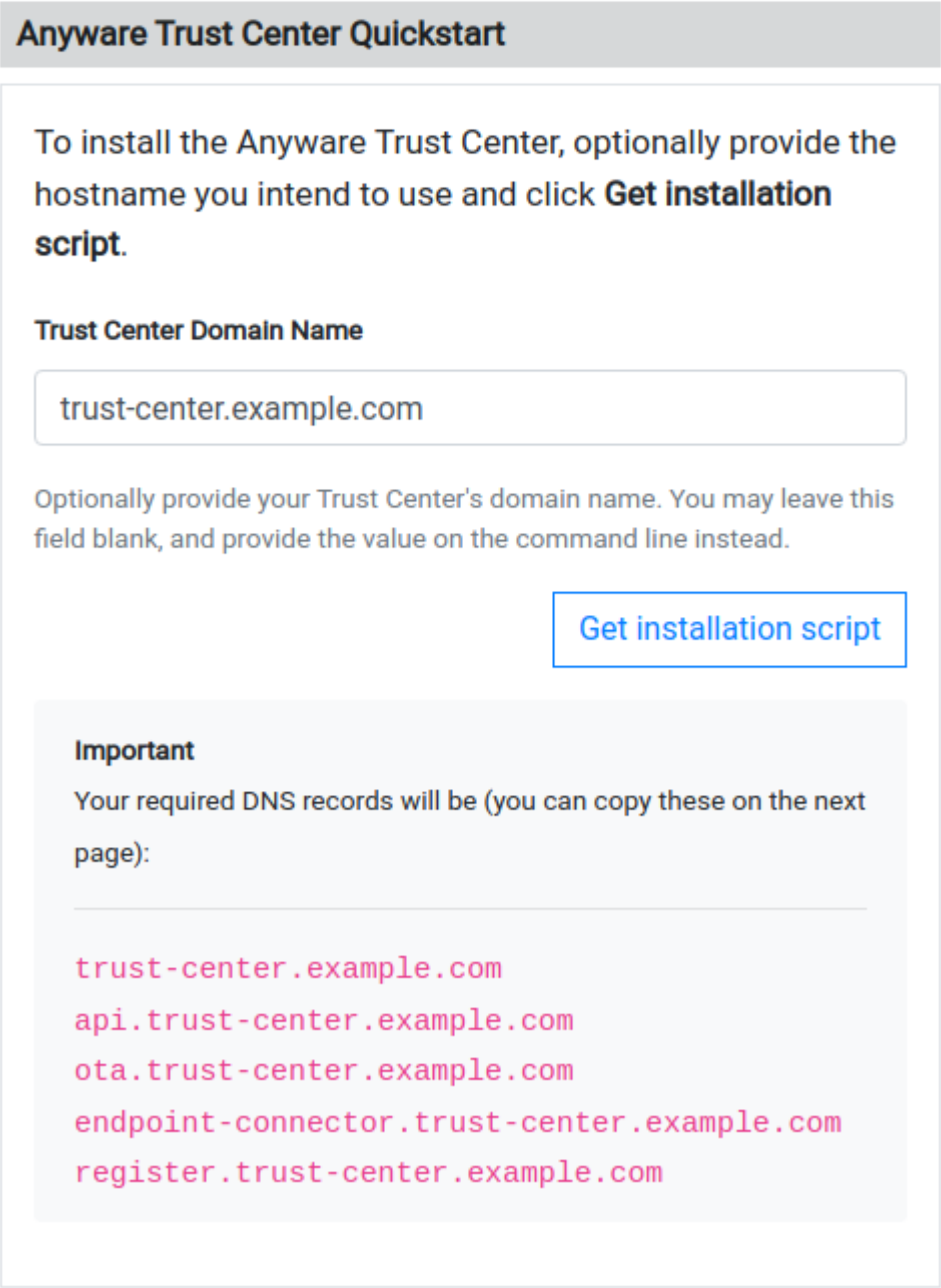
To download the Anyware Trust Center installer, you must have an account on our support site (https://help.teradici.com). You can create one from the login screen if you don't already have one.

To download the installer:

1. Go to https://anyware.hp.com/find/product/anyware-trusted-endpoints/2024.03/anyware-trust-center.
2. If you are not already logged in, click **Log in to download** and authenticate your session.
3. Click **Downloads and scripts**:



4. Read and accept the *End User License Agreement*. Once the agreement has been accepted, the download form is shown:



Anyware Trust Center Quickstart

To install the Anyware Trust Center, optionally provide the hostname you intend to use and click **Get installation script**.

Trust Center Domain Name

trust-center.example.com

Optionally provide your Trust Center's domain name. You may leave this field blank, and provide the value on the command line instead.

Important

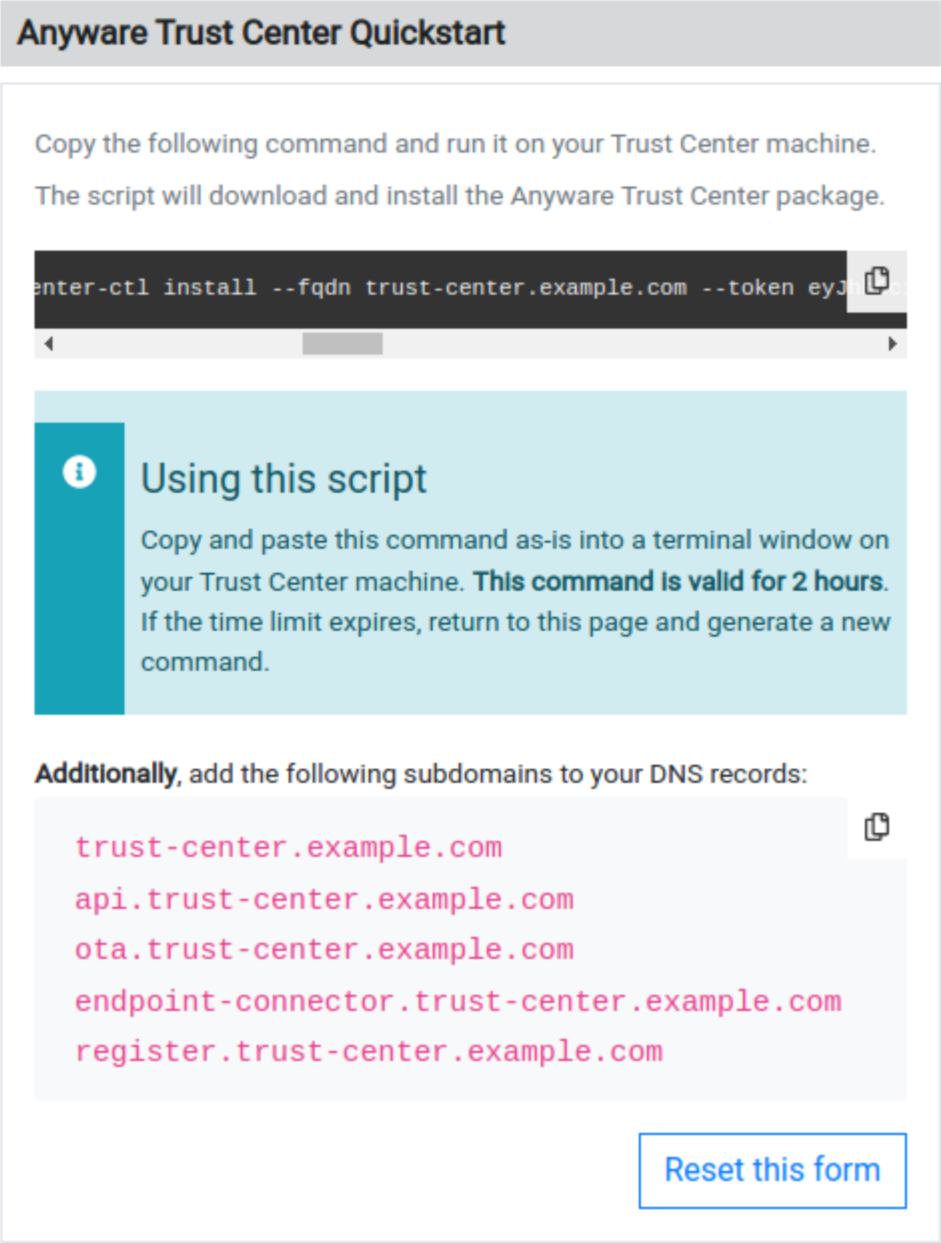
Your required DNS records will be (you can copy these on the next page):

```
trust-center.example.com
api.trust-center.example.com
ota.trust-center.example.com
endpoint-connector.trust-center.example.com
register.trust-center.example.com
```

5. Provide your chosen FQDN—recorded earlier—in the **Trust Center Hostname (FQDN)** field, and click **Get installation script**.

> **Note: FQDN field is optional**
>
> The FQDN value is required to run the installer, but you do not have to supply it here. If you leave this field blank, you must manually add the actual FQDN to the script command before executing it.

6. The website will generate a download command and display it:



Anyware Trust Center Quickstart

Copy the following command and run it on your Trust Center machine.

The script will download and install the Anyware Trust Center package.

```
enter-ctl install --fqdn trust-center.example.com --token eyJ
```

Using this script

Copy and paste this command as-is into a terminal window on your Trust Center machine. **This command is valid for 2 hours.** If the time limit expires, return to this page and generate a new command.

Additionally, add the following subdomains to your DNS records:

```
trust-center.example.com
api.trust-center.example.com
ota.trust-center.example.com
endpoint-connector.trust-center.example.com
register.trust-center.example.com
```

Copy the *entire* command displayed. There are two parts, and both are required: a curl command that downloads the installation script, and second command that executes the script.

The installation script command looks like this:

```
curl -sSL https://dl.anyware.hp.com/{token}/trust-center/raw/names/trust-center-tgz/versions/{version}/trust-center_{version}.tar.gz | tar -xz && sudo ./trust-center-ctl install --fqdn {trust-center-FQDN} --token {jwt token}
```

> **Important: This script is time-limited**
>
> The generated command is valid for 1 hour

, after which installation will fail. If that occurs, return to the download page and generate a new command.

The rest of the steps below take place on the Anyware Trust Center VM. If you acquired the script command on a different machine, transfer it to the Anyware Trust Center VM using any acceptable method.

5. Run the Installation Script

1. Create or choose a directory on your newly-created VM, and enter it. The following example will create and enter a new `tc-installation` directory:

```
mkdir tc-installation
cd tc-installation
```

2. In a terminal window, paste the installation script command you copied earlier.

   The installation script will download all required packages and install them on the machine. **The installer takes approximately 15 minutes to complete**. There will be periods of time where the process stops printing messages to the terminal and may appear to hang; this is normal.

> **Note: Troubleshooting problems**
>
> If you encounter breaking issues during installation, see troubleshooting for help.

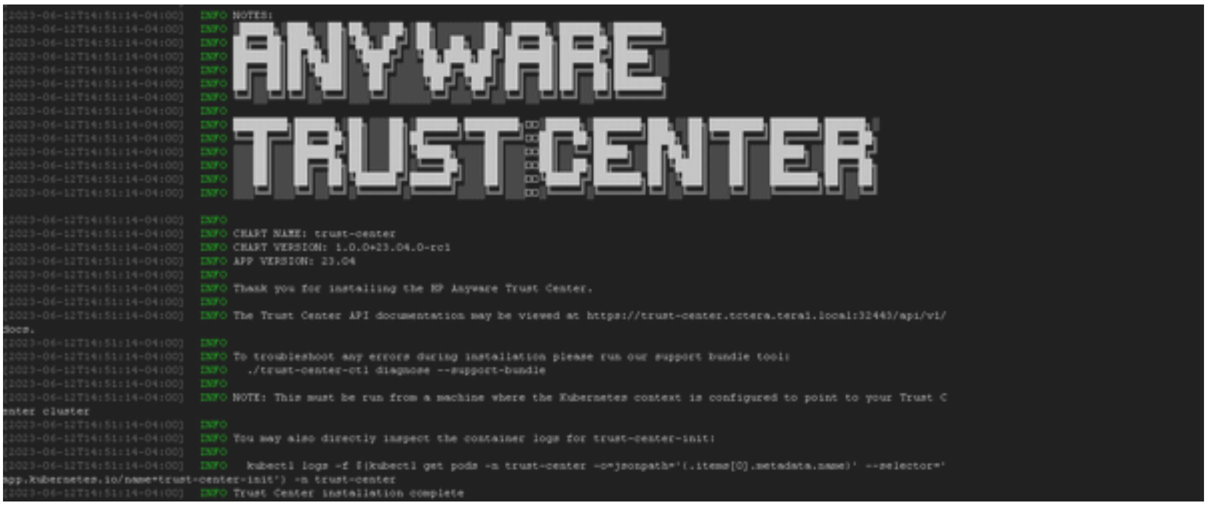
When executed, the installation command does the following:

- Downloads the archive for the installer executable
- Unzips the installer
- Run the installer as root, passing in two required flags:
- `fqdn`: The value must be a valid fully-qualified domain name *using only lowercase letters, numbers, and periods*, and should point to the location where the Anyware Trust Center is installed.

- `token`: the JWT token provided by the support site. This value should not be modified, and is valid for one hour after creation.

> **Note: Installation certification errors**
>
> You may see certification errors during installation, which are related to a plugin for Anyware Manager. These errors can be disregarded.

After installation completes, you will see a message similar to this:



```
[2023-06-12T14:51:14-04:00]   INFO NOTES:
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO      ANYWARE
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO      TRUST CENTER
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO

[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO CHART NAME: trust-center
[2023-06-12T14:51:14-04:00]   INFO CHART VERSION: 1.0.0+23.04.0-rc1
[2023-06-12T14:51:14-04:00]   INFO APP VERSION: 23.04
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO Thank you for installing the HP Anyware Trust Center.
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO The Trust Center API documentation may be viewed at https://trust-center.tctera.teral.local:32443/api/v1/
docs.
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO To troubleshoot any errors during installation please run our support bundle tool:
[2023-06-12T14:51:14-04:00]   INFO   ./trust-center-ctl diagnose --support-bundle
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO NOTE: This must be run from a machine where the Kubernetes context is configured to point to your Trust C
enter cluster
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO You may also directly inspect the container logs for trust-center-init:
[2023-06-12T14:51:14-04:00]   INFO
[2023-06-12T14:51:14-04:00]   INFO   kubectl logs -f $(kubectl get pods -n trust-center -o=jsonpath='{.items[0].metadata.name}' --selector='
app.kubernetes.io/name=trust-center-init') -n trust-center
[2023-06-12T14:51:14-04:00]   INFO Trust Center installation complete
```

3. To validate the installation, run the following command:

```
sudo ./trust-center-ctl diagnose
```

All services should report healthy.

After Installing

After installation completes, you can set up your management tool to interact and manage Trusted Zero Clients via the Anyware Trust Center.

Refer to the API documentation installed with the Anyware Trust Center for complete details.

> **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: <your domain>
>     password: <this is the auto-generated password>
>     endpointUpdate:
>       accessKey: <repository password>
>       repository: "teradici/trusted-zero-client"
> ```

Troubleshooting

Installation failures

Installation can fail on some distributions or environments unless additional configuration is done. Check the additional configuration requirements listed above. If any steps were missed:

1. Uninstall the Anyware Trust Center
2. Perform the relevant configuration steps
3. Install the Anyware Trust Center again. You will likely need to return to the download site and generate a new download command.

Creating a Support Bundle

Support bundles are archives that capture the current state of the Anyware Trust Center, and are used by our support team to diagnose and troubleshoot issues you may experience.

If you need to contact support, generate a support bundle using the procedure detailed in Creating a Support Bundle.

Dark Site Installation

The Anyware Trust Center can be installed in dark sites, without a connection to the public internet. Dark site installation involves these general steps:

1. Create a new VM to host the Anyware Trust Center.
2. Choose a domain name for connections to the Anyware Trust Center.
3. Configure DNS for the new machine.
4. Create dummy gateway, if the machine does not already have a default gateway.
5. Create a temporary VM that will download the required files.
6. Get the installation script from our website.
7. Transfer the files to the production VM.
8. Run the installation script on the Anyware Trust Center machine.

1. Create the Dark Site Machine

Deploy a dedicated server to host the Anyware Trust Center. You must be able to transfer files to this machine, using USB drives, SSH, or another acceptable method.

The Anyware Trust Center requires a dedicated server with the following specifications (note that the *network* and *software* requirements are different from standard installations):

Requirement	
Operating System	• RHEL 9 • Rocky Linux 9
CPUs	4 vCPUs
Memory	16GB RAM
Disk	120GB+, including 80GB+ disk space on `/var` for persistent volumes
Network	A default gateway is required, even without an internet connection. If the machine does not have one, a dummy route is required for installation. See Checking for a Default Gateway for instructions.
Software	DNF

2. Choose a Domain Name

The Anyware Trust Center requires 5 domain names added to your DNS records. In this step, you're creating the *base* domain for the Anyware Trust Center, which will be used to construct the other 4 subdomains. You'll use this value in multiple locations during setup, so record the value and be ready to copy it.

In this procedure, we will use `trust-center.example.com` to demonstrate the domain name, and how it is leveraged to create the other required values.

3. Create DNS Records

Once your new dedicated server has been created, you must set up the following DNS A records that point to it. For each of the following items, replace `<domain-name>` with the domain name you recorded in the previous step.

- `<domain-name>`
- `api.<domain-name>`
- `endpoint-connector.<domain-name>`
- `ota.<domain-name>`
- `register.<domain-name>`

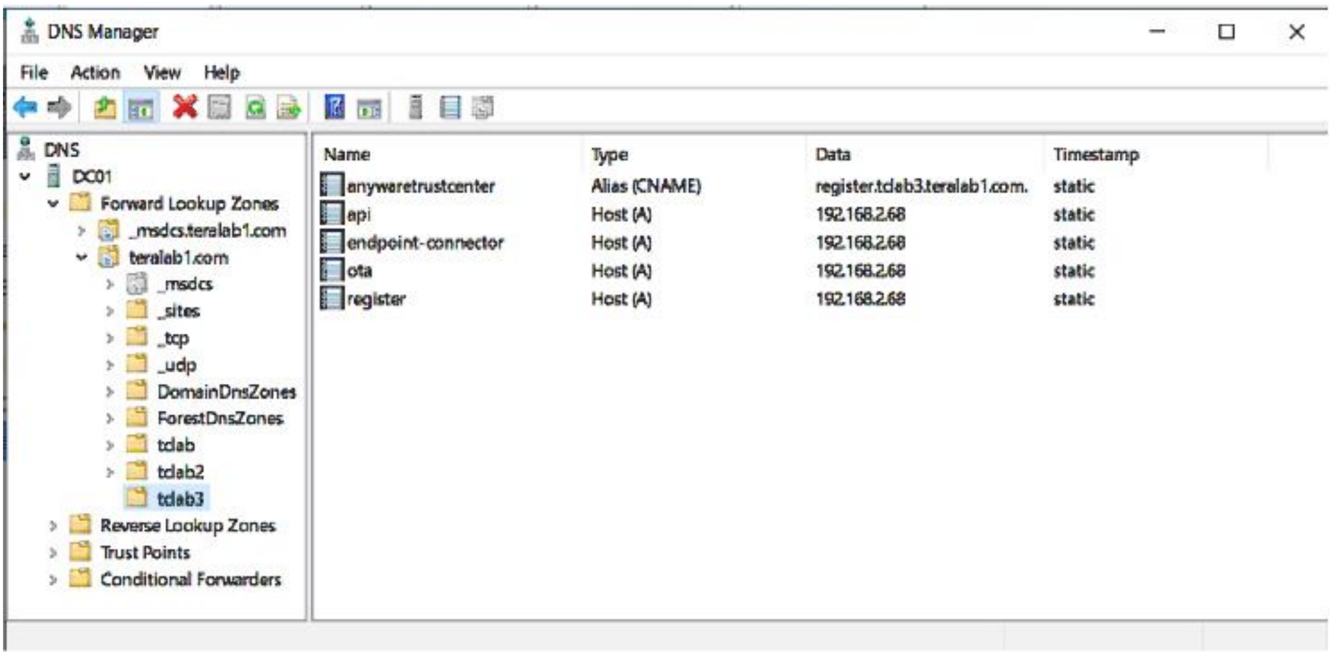
> **Important: Supporting automatic Anyware Trust Center discovery**
>
> If you plan to support automatic Anyware Trust Center discovery by endpoints, you must also create a CNAME record that redirects `anywaretrustcenter` to `register.<domain-name>`.

Example: using `trust-center.example.com`

Using `trust-center.example.com` as the base domain, you would create DNS records for the following:

- `trust-center.example.com`
- `api.trust-center.example.com`
- `endpoint-connector.trust-center.example.com`
- `ota.trust-center.example.com`
- `register.trust-center.example.com`

This example shows a different DNS configuration using Windows DNS Manager:



Name	Type	Data	Timestamp
anywaretrustcenter	Alias (CNAME)	register.tclab3.teralab1.com.	static
api	Host (A)	192.168.2.68	static
endpoint-connector	Host (A)	192.168.2.68	static
ota	Host (A)	192.168.2.68	static
register	Host (A)	192.168.2.68	static

4. Verify or create a default gateway on the darksite machine

The Anyware Trust Center requires a default gateway even when an internet connection is not present. If you are not sure whether your machine already has one, see Checking For a Default Gateway. below, for steps to check and to create one if necessary.

If the machine already has a default gateway, this step is not required.

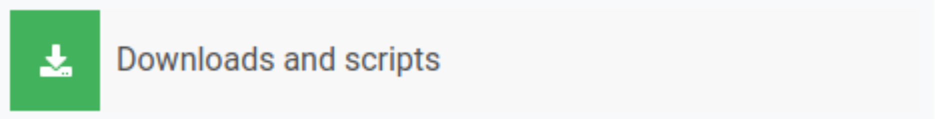
5. Create a temporary internet-connected machine

This machine will be used to download files and create an installer. The bundler machine must meet minimum requirements.

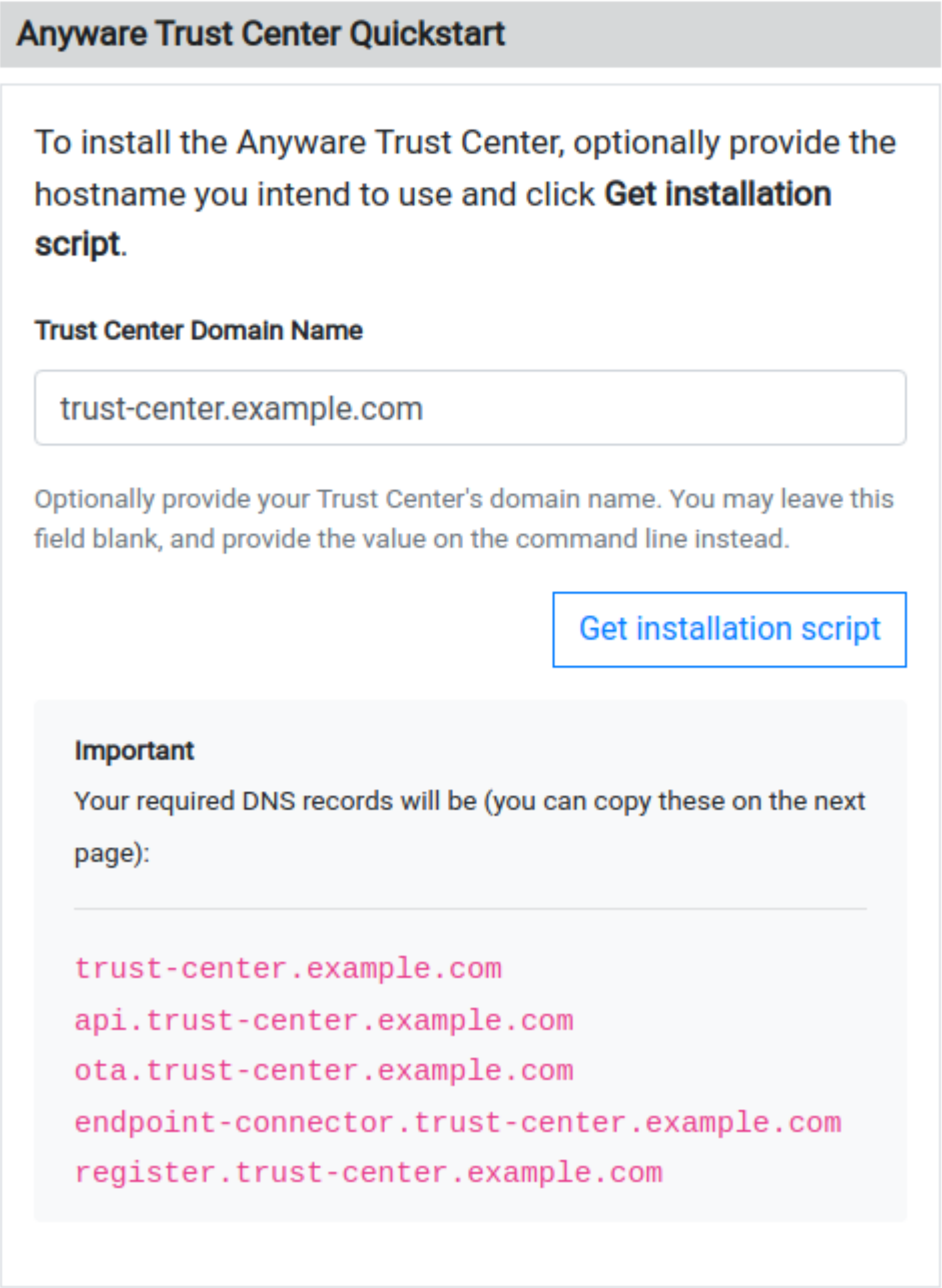
6. Download the site package and scripts

This section is done from the temporary internet-connected machine:

1. Go to https://anyware.hp.com/find/product/anyware-trusted-endpoints/2024.03/anyware-trust-center.
2. If you are not already logged in, click **Log in to download** and authenticate your session.
3. Click **Downloads and scripts**:

4. Read and accept the *End User License Agreement*. Once the agreement has been accepted, the download form is shown:



Anyware Trust Center Quickstart

To install the Anyware Trust Center, optionally provide the hostname you intend to use and click **Get installation script**.

Trust Center Domain Name

trust-center.example.com

Optionally provide your Trust Center's domain name. You may leave this field blank, and provide the value on the command line instead.

Important

Your required DNS records will be (you can copy these on the next page):

```
trust-center.example.com
api.trust-center.example.com
ota.trust-center.example.com
endpoint-connector.trust-center.example.com
register.trust-center.example.com
```

5. Provide your chosen FQDN—recorded earlier—in the **Trust Center Hostname (FQDN)** field, and click **Get installation script**.

> **Note: FQDN field is optional**
>
> The FQDN value is required to run the installer, but you do not have to supply it here. If you leave this field blank, you must manually add the actual FQDN to the script command before executing it.

6. Find the **Dark Site Installation** field, and copy it.

Download darksite

Copy the *entire* command displayed. There are two parts, and both are required: a curl command that downloads the installation script, and second command that executes the script.

The preparation script command looks like this:

```
curl -sSL https://dl.anyware.hp.com/{token}/trust-center/raw/names/trust-center-tgz/versions/{version}/trust-center_{version}.tar.gz | tar -xz && sudo ./trust-center-ctl install dark-site prepare --fqdn {trust-center-FQDN} --token {jwt token}
```

Important: This script is time-limited

The generated command is valid for 1 hour. If the token expires before you run it, return to the download page and generate a new command. **The time limit applies to running the *prepare* command, not installing the package**. Once you have successfully generated the installation bundle, you can install the package at any time.

7. Copy downloaded files to the dark site machine

The following files are created by the preparation script. Transfer all three files to the isolated machine that will host the Anyware Trust Center using any acceptable method, such as USB drive or SSH:

- `trust-center-ctl`
- `anyware-trust-center-bundle.tar`
- `anyware-trust-center-bundle.sha`

Place these files in a clearly identified location on the new machine; this will become your installation directory, and subsequent commands will be run there.

Once these files are transferred, the temporary machine is no longer needed (note that you will need it, or a new instance of it, to upgrade the Anyware Trust Center or to push firmware updates to your Trusted Zero Clients).

8. On the dark site machine, run the installation command

Open a terminal window and navigate to your installation directory (the location you used when you copied the installation files). Run the following command:

```
sudo ./trust-center-ctl install --darksite
```

To validate the installation after it completes, run the following command:

```
sudo ./trust-center-ctl diagnose
```

All services should report healthy.

After Installing

After installation completes, you can set up your management tool to interact and manage Trusted Zero Clients via the Anyware Trust Center.

Refer to the API documentation installed with the Anyware Trust Center for complete details.

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: <your domain>
    password: <this is the auto-generated password>
    endpointUpdate:
      accessKey: <repository password>
      repository: "teradici/trusted-zero-client"
```

Troubleshooting

Installation failures

Installation can fail on some distributions or environments unless additional configuration is done. Check the additional configuration requirements listed above. If any steps were missed:

1. Uninstall the Anyware Trust Center
2. Perform the relevant configuration steps
3. Install the Anyware Trust Center again. You will likely need to return to the download site and generate a new download command.

Creating a Support Bundle

Support bundles are archives that capture the current state of the Anyware Trust Center, and are used by our support team to diagnose and troubleshoot issues you may experience.

If you need to contact support, generate a support bundle using the procedure detailed in Creating a Support Bundle.

Checking for a Default Gateway

The Anyware Trust Center requires a default gateway to be set on the dark site machine, even without an internet connection.

To check whether a default gateway exists:

1. Open a console window, and run:

   ```
   ip route | grep default
   ```

   If the response looks similar to this example, then a default route already exists, and you can continue with installation:

   ```
   default via 10.X.X.X dev ens5 proto dhcp src 10.X.X.X metric 100
   ```

2. If the response indicates that no default gateway is present, run the following commands to create a dummy route:

```
ip link add dummy0 type dummy
ip link set dummy0 up
ip addr add 203.0.113.254/31 dev dummy0
ip route add default via 203.0.113.255 dev dummy0 metric 1000
```

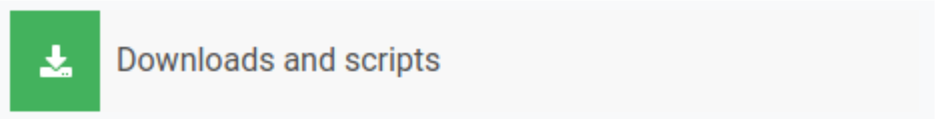
Upgrading the Anyware Trust Center

You can upgrade your Anyware Trust Center by running an upgrade script that we provide. The script will download the new package and automatically upgrade your installation.

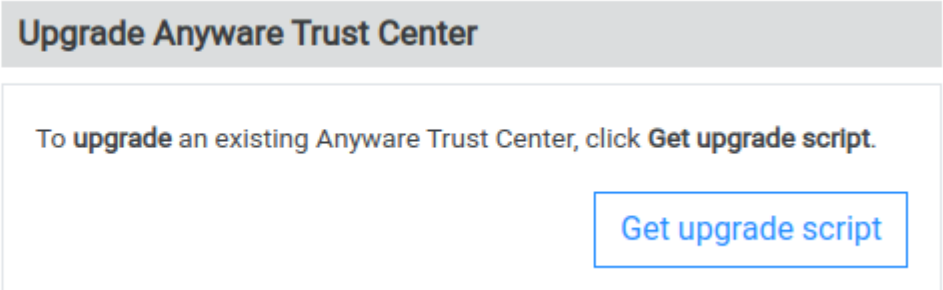
> **Note: Support account is required**
>
> To download the new Anyware Trust Center package, you must have an account on our support site (https://help.teradici.com). You can create one from the login screen if you don't already have one.

To upgrade your Anyware Trust Center:

1. Go to https://anyware.hp.com/find/product/anyware-trusted-endpoints/2024.03/anyware-trust-center.
2. If you are not already logged in, click **Log in to download** and authenticate your session.
3. Click **Downloads and scripts**:



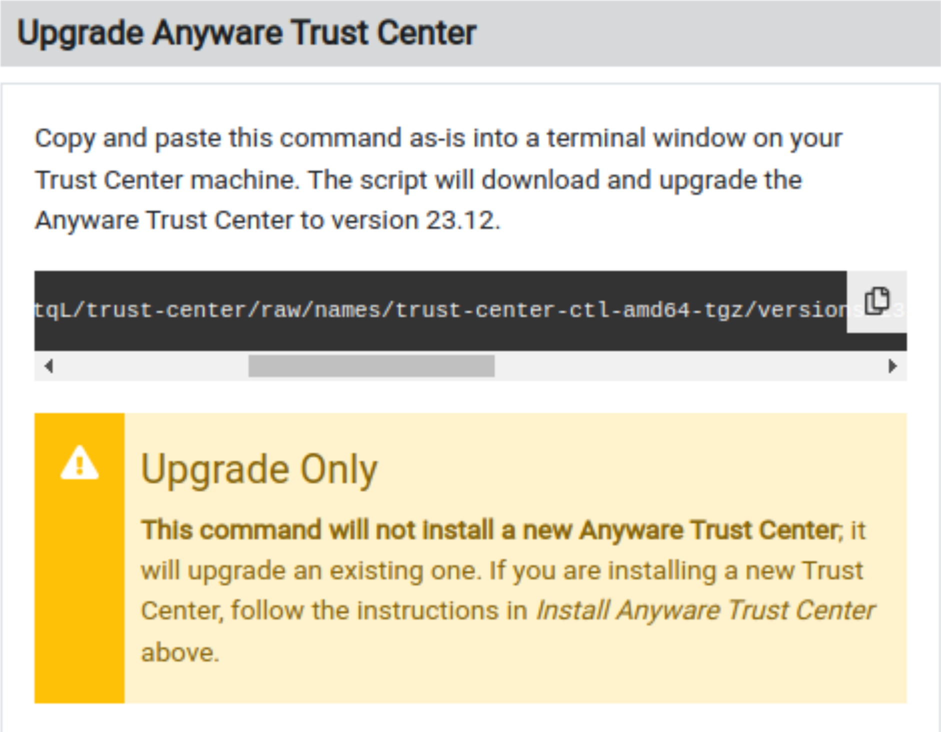
4. Read and accept the *End User License Agreement*. On the next screen, find the *Upgrade Anyware Trust Center* section, and click the **Get upgrade script** button.:



Upgrade Anyware Trust Center

To **upgrade** an existing Anyware Trust Center, click **Get upgrade script**.

5. The website will generate an upgrade command and display it:



Upgrade Anyware Trust Center

Copy and paste this command as-is into a terminal window on your Trust Center machine. The script will download and upgrade the Anyware Trust Center to version 23.12.

```
tqL/trust-center/raw/names/trust-center-ctl-amd64-tgz/versior
```

Upgrade Only

This command will not install a new Anyware Trust Center; it will upgrade an existing one. If you are installing a new Trust Center, follow the instructions in *Install Anyware Trust Center* above.

Copy the *entire* command displayed. There are two parts, and both are required: a curl command that downloads the new package, and second command that executes the script.

The upgrade script command looks like this:

```
curl -sSL https://dl.anyware.hp.com/{token}/trust-center/raw/names/trust-
center-tgz/versions/{version}/trust-center_{version}.tar.gz | tar -xz &&
sudo ./trust-center-ctl upgrade
```

6. On the Anyware Trust Center VM, open a terminal window and navigate to the same directory used to install the original Anyware Trust Center.
7. Paste the command you copied in step 5 and press **Enter**.

> **Important: Upgrade must run in the Installation directory**
>
> The upgrade script must be run in the same directory used to install the Anyware Trust Center. If you run the script in a different location, the package will be downloaded but the upgrade script will fail.

The command will download the new package and execute an upgrade script.

Uninstall the Anyware Trust Center

You can uninstall the Anyware Trust Center completely from your system.

Danger: Data will be removed

Running this uninstall script will also remove all locally-stored data. Be sure to back up your system data if you are not using an external data store.

To uninstall the Anyware Trust Center and remove its data:

1. Open a console window and navigate to the installer directory.
2. In the console window, run the uninstall command:

```
sudo ./trust-center-ctl uninstall
```

Troubleshooting

Creating a Support Bundle

Support bundles are archives that capture the current state of the Anyware Trust Center, and are used by our support team to diagnose and troubleshoot issues you may experience.

> **Note: Support bundle includes a README file**
>
> The generated support bundle includes a README file at the root of the archive, containing information about viewing the files and folders in it.

To create a support bundle:

1. Open a console window and navigate to the working directory.
2. In the console window, run the following command:

```
sudo ./trust-center-ctl diagnose --support-bundle --cluster-type k3s
```

Support

If you encounter a problem setting up or using the Anyware Trust Center, there are a number of troubleshooting and support resources you can access.

- We maintain an extensive **knowledge base** which answers many questions and documents solutions to common problems. The knowledge base is part of the Knowledge Center; click on the *Articles* tab to access it, or enter a search query in the search field at the top of the page.
- We host a **community forum**, allowing you to ask questions and get answers from other IT professionals and our support team, which monitors this channel. The forum is part of the Knowledge Center; click on the *Discussions* tab to access it.
- If you need more help, open a support ticket and our support team will engage with you directly.