PCoIP License Server 22.01 Offline Administrators' Guide

This guide is intended for PCoIP system administrators who are deploying an offline PCoIP License Server as part of their Cloud Access Software solution.

The License Server can be used with or without a connection to the public internet. Since usage is different in each case, we've documented each environment separately.

> ⚡ **These instructions are for users with offline (dark) environments only**
>
> The instructions and specifications included are specifically written for deployments where the PCoIP License Server *does not* have a connection to the public internet.
>
> Users with a connection to the public internet should use the Online Administrators' Guide instead.

> ⚠️ **Warning: Only internal network usage is supported**
>
> The PCoIP License Server only supports company internal network usage. It is not designed to receive connections from the public internet.

The Teradici PCoIP License Server is a standalone service that handles both PCoIP session license registrations and PCoIP session request authorization.

This documentation assumes that you have a thorough understanding of virtual machines and networking concepts, including firewall configuration. Knowledge of Linux systems in general and RHEL or CentOS in particular will also be helpful, although all required Linux commands are included here.

> 🔥 **Important: The License server is only required for local license management**
>
> This software is not required for organizations using Teradici Cloud Licensing.

Important: Access to teradici.flexnetoperations.com required

Before you can activate licenses with an offline license server, you must be given access to https://teradici.flexnetoperations.com. To request access, create a ticket with Teradici support. Be prepared to provide a valid activation key, and the name and email address of a contact person who should have access.

About the Teradici PCoIP License Server

Most PCoIP deployments use Teradici automatic Cloud Licensing Service, and do not need a local license server. If your deployment cannot use cloud licensing, either because the site is not connected to the public internet or you need to retain control of your own session licenses, the Teradici PCoIP License Server is required.

> ✏ **Note: Session license types**
>
> Teradici cloud licensing uses *registration codes*, which are different than the *activation keys* used by the license server. The type of license is specified at purchase.

The Teradici PCoIP License Server is a standalone software service that and handles both PCoIP session license registrations and PCoIP session request authorization. The PCoIP License Server maintains its license activation and checkout states in a local trusted storage database.

When a PCoIP agent attempts to establish a new PCoIP session, it will first request authorization from its assigned PCoIP License Server. The PCoIP License Server checks to see if an activated PCoIP session license is available in its trusted storage, and authorizes the session if one is. Each PCoIP session activation consumes one PCoIP session license.

The PCoIP License Server can run as an online service with a connection to the outside internet, or in an offline environment without internet access. The installation and operation procedures are different in each use case. This document explains how to use the PCoIP License Server as an **offline** service.

About Offline Environments

A PCoIP License Server that has no connection to the outside internet is considered to be in an *offline environment* (this scenario is also often referred to as a *dark site*). Since the PCoIP License Server cannot reach the internet, both software installation and license management must be done indirectly, via a separate internet-connected machine.

> 🔥 **Important: Offline deployments can be in the cloud**
>
> The term *offline environment* does not imply a dependency on physical hardware or datacenter deployments. The PCoIP License Server can be deployed securely as an offline service on AWS EC2 cloud-based infrastructure with appropriate firewall configuration.

About PCoIP Session Licensing

PCoIP session licenses are managed in pools, which are created at the time of purchase. Each new purchase of licenses is assigned an activation code, which will be used to activate, view, or return all the licenses in that purchase. You can use licenses from multiple activation codes simultaneously.

For example, when you purchase 30 licenses, you will receive an activation code that allows you to activate, view, or return those 30 licenses. If you subsequently purchased additional licenses, you would receive an additional activation code for each new bundle.

In this example, you own 60 licenses, managed by three different activation codes:

An example of three license pools. All of these licenses can be activated on the same license server, or spread across multiple servers.

> ✏️ **Cloud Licensing FAQ**
>
> For more information, including answers to frequently asked licensing questions, see FAQ - Licensing Cloud Access Software.

Using PCoIP Session Licenses

PCoIP session licenses must be activated on a PCoIP License Server before they can be used. You can activate licenses on one license server, or split them among multiple PCoIP License Servers depending on your deployment requirements.

Once installed and running, the PCoIP License Server will authorize new PCoIP sessions until it runs out of available active licenses.

About the Licensing Grace Period

PCoIP agents request validation from their PCoIP License Server each time a connection is established. Once a PCoIP agent has successfully established a licensed PCoIP session, it will continue to work even if the PCoIP License Server is subsequently unavailable or offline. This grace period extends 7 days from the first unsuccessful validation attempt. This enables you to perform system maintenance or upgrades without disrupting your existing PCoIP users.

Once a connection is re-established with the PCoIP License Server, the grace period is reset. The next failed connection will initiate another 7-day grace period.

There is no user-facing indication that a PCoIP agent is in a grace period. Administrators can check the status of individual PCoIP agents by referring to the PCoIP agent logs, or by using the `pcoip-validate-license` command on the PCoIP Agent machine.

For specific command information, refer to the appropriate PCoIP Agent guides:

- Graphics Agent for Windows Administrators' Guide

- Graphics Agent for Linux Administrators' Guide

- Standard Agent for Windows Administrators' Guide

- Standard Agent for Linux Administrators' Guide

What's New in This Release

Release 22.01 of the PCoIP License Server includes the following changes:

- Adds support for Rocky Linux 8

- When installed on RHEL 8 or Rocky Linux 8, connections can now use TLS 1.3 (in addition to TLS 1.2). RHEL/CentOS 7 are limited to TLS 1.2.

- Downgrading the PCoIP License Server is not supported. Attempting a downgrade can result in corrupted data or an inoperable server.

System Requirements

The PCoIP License Server requires an environment with the following minimum specifications:

	Requirement
Available disk space	500 MB
Available RAM	4 GB minimum available RAM
CPU	2GHz (2 cores)
Supported virtual environments	Amazon EC2 VMware ESXi 6.5 QEMU-KVM 2.7 Google Compute Cloud instances Microsoft Azure (tech preview) [1]
Operating System	CentOS 7 RHEL 7, 8 Rocky Linux 8
Compatible PCoIP agents	2.11+ (any agent type)

> ⚠️ **Caution: Systems with less than 4GB of available RAM may fail**
>
> You should have at least 4GB of available RAM on the License Server machine. Instances with insufficent memory may not work.

> ⚠️ **Caution: Don't install more than one type of license server on the same machine**
>
> The PCoIP License Server version 22.01 cannot be installed on the same machine as the PCoIP License Server 1.x *or* an NVIDIA GRID License Server.

> 🔥 **Important: PCoIP agent compatibility requirement**
>
> The PCoIP License Server 22.01 is compatible with all PCoIP agents version 2.11 or newer.

> 🔥 **Important: Network visibility**
>
> The PCoIP License Server must be visible on the network to any PCoIP agents that use it for license validation.

> ⚡ **Danger: Migrating from RHEL 7 to RHEL 8**
>
> If you have currently deployed a PCoIP License Server on RHEL 7 and wish to upgrade to RHEL 8, **do not upgrade the operating system in place**. Updating the operating system could invalidate your PCoIP licenses. See Migrating from RHEL 7 to RHEL 8 for a supported migration path.

> 🔥 **Important: Offline license activation requirement**
>
> Offline license activation requires the ability to transfer files from the PCoIP License Server to an internet-connected machine. If you are not able to transfer files in this manner, Teradici Global Support Services will facilitate license activation for you. See Activating Licenses in an Offline Environment for more information.

1. The PCoIP License Server 22.01 is currently supported as a technology preview on Microsoft Azure machines. It is intended for early adopters and may not work as expected in all situations. It is not appropriate for production systems.

Frequently Asked Questions

Which password does the `pcoip-set-password` command set?

`pcoip-set-password` sets the PCoIP License Server Administrator's password, which controls access to the license server's trusted storage. Trusted Storage is a secured database where license keys and license server settings are stored. The password is required for administrators to add, remove, or view license information.

> ✏️ **Note: The PCoIP License Server administrator's password is not the system user's password**
>
> The PCoIP License Server administrator's password controls access to privileged PCoIP License Server commands. It is not the same as your system user password.

Can I install multiple license servers?

Yes. Teradici recommends using multiple license servers if you are deploying services in remote global regions, and want to optimize performance by having a license server located near your PCoIP host machines. Each license server must be activated separately with a pool of licenses.

How do I move licenses from one PCoIP License Server to another?

To move licenses between servers, you must first return all the licenses controlled by the origin server, then activate them on the destination server:

- Return the licenses as described in *Returning Licenses in Offline Environments*.
- Activate the licenses as described in *Activating Licenses in an Offline Environment*.

How can I activate all the licenses available under an activation code?

You must explicitly state the number of licenses to activate for each activation code when invoking `pcoip-activate-offline-license`. If you do not know the number of licenses available, consult the verification email you received when purchasing the bundle of licenses.

What happens when PCoIP session licenses expire?

PCoIP agents relying on expired licenses will no longer establish PCoIP connections. This does not affect the remote host machine; only the ability to connect to it using PCoIP.

Can I upgrade my PCoIP License Server without impacting my users?

Yes. When an active PCoIP agent—an agent which has established at least one successful PCoIP session—cannot validate its license for any reason, it will enter a 7-day grace period. During the grace period, PCoIP agents will continue to work normally.

You can safely take the PCoIP License Server offline and update the software without affecting users during this 7-day grace period. Once the PCoIP License Server is back online, the PCoIP agents exit the grace period.

How do I know if a PCoIP agent has entered a grace period?

PCoIP agents that have entered grace periods will indicate their status in their logs. You can also use the `pcoip-validate-host` command on the PCoIP Agent machine to check the status of an individual PCoIP agent.

What is the Unique Identifier Associated with my License Server's VM?

In some debugging or support scenarios, you may need to find the unique identifier of your License Server's machine. To get the ID number, use the `pcoip-get-license-server-id` command.

This command requires the License Server password. You can include it with the command using the `-p` option. If you omit the password, you will be prompted for it.

How can I tell if my license server is up and running remotely?

If you can access the license server from a remote location, run the following curl command:

```
curl https://<license-server-address>:7071/api/1.0/health
```

The response should look something like:

```
{
    "GLS" :
        {
            "version" : "2018.02",
            "buildDate" : "2018-02-27T17:03:40Z",
            "buildVersion" : "225119",
            "branch" : "mainline",
            "patch" : "0",
            "fneBuildVersion" : "220112",
            "database" :
                {
                    "connectionCheck" : "success"
                }
        }
}
```

A `connectionCheck` value of `success` indicates that the License Server is running. Any other `connectionCheck` response means that the License Server is not running, or is not reachable.

Are there tools available to help use the PCoIP License Server?

Teradici maintains a public Github repo with open-source scripts that you can use in conjunction with the PCoIP License Server. For more information, see Additional Tools.

Installing the PCoIP License Server

The method you will use to install the PCoIP License Server depends on whether you can open a temporary internet connection to the License Server machine.

- **If you can open a temporary connection to the internet**, you can install the software and dependencies directly and then remove the internet connection.

- **If you cannot connect to the internet**, you must obtain dependencies and License Server software via a temporary internet-connected machine and transfer the files yourself.

> 🔥 **Important: Migrating from RHEL 7 to RHEL 8**
>
> If you have currently deployed a PCoIP License Server on RHEL 7 and wish to upgrade to RHEL 8, **do not upgrade the operating system in place**. Updating the operating system could invalidate your PCoIP licenses. See Migrating from RHEL 7 to RHEL 8 for a supported migration path.

> ⚠️ **Caution: Don't install more than one type of license server on the same machine**
>
> The PCoIP License Server version 22.01 cannot be installed on the same machine as the PCoIP License Server 1.x *or* an NVIDIA GRID License Server.

Keeping Passwords Secure

Some commands documented in this guide allow the use of the `-p` flag to provide password values inline, rather than stopping for a user input prompt. Although the PCoIP License Server does not log or distribute passwords provided this way, it can be difficult to tell whether other system loggers (like `/var/log/secure` and bash history) are capturing them, leading to inadvertent disclosures. For this reason, Teradici strongly discourages the use of the `-p` flag (or the related `-n` flag used by `pcoip-set-password`).

The PCoIP license server supports the use of system environment variables to securely store and recall the license server password. To register the password as an environment variable, open a console window and run the following commands, substituting your password for `your_license_server_password`:

```
export HISTIGNORE="export*"
export TERADICI_LICENSE_SERVER_PASSWORD=<your_license_server_password>
```

If the PCoIP License Server password is registered in this way, the PCoIP License Server can use it automatically without needing the `-p` flag.

> ⚡ **If you must use the `-p` flag**
>
> If you prefer to use these flags, or have no alternative, you should run `sudo -i` first. This changes to the Linux root user, and may avoid logging your password into `/var/log/secure`. You may also run `export HISTIGNORE="sudo pcoip-*"` to avoid logging password into bash history.

Installing With a Temporary Internet Connection

To install the software with a temporary internet connection:

1. Open the internet connection on the License Server machine.

2. SSH into your License Server machine.

3. For RHEL/CentOS 7, install wget and yum-utils *(skip this step for RHEL/Rocky Linux 8)*:

   ```
   sudo yum install wget
   sudo yum install yum-utils
   ```

4. Install the Teradici `pcoip-license-server` repository, using the shell script available here. The script will discover your operating system and configure the repo appropriately.

5. Install the license server:

   • **For RHEL/CentOS 7**:

     ```
     sudo yum install -y pcoip-license-server
     ```

   • **For RHEL/Rocky Linux 8**:

     ```
     sudo dnf install -y pcoip-license-server
     ```

6. Set your PCoIP License Server administrative password with `pcoip-set-password`.

> ⚠️ **Change the default password immediately**
>
> Until the default password is changed, commands can be issued to the license server without your knowledge.

> ℹ️ **Info: Password Rules**
>
> Passwords should be surrounded with single quotation marks like 'password', and must conform to the following rules:
>
> - Must be between 8 and 30 characters long
> - Must contain at least one lowercase letter
> - Must contain at least one uppercase letter
> - Must contain at least one digit
> - Must contain at least one symbol, excluding ' (single quote), " (double quote), \ (backslash), and spaces.

> ✏️ **Note: Default password**
>
> The default password in new installations is `1P@ssw0rd!`, where the leading `1` is a numeral one and `0` is a zero. When setting the password on a clean installation, use this as your curent password.

- To set the new password:

```
sudo pcoip-set-password
```

You will be prompted for the old and new passwords.

> 🔥 **Register your password as an environment variable**
>
> Teradici recommends that you register your password as a system environment variable, which will allow you to run commands without providing the password inline via the `-p` flag. **Providing the passwords inline can have security implications** and Teradici recommends against it. See Keeping Passwords Secure at the top of this page for more information and methods for mitigating the security concerns.
>
> To register the PCoIP password as an environment variable, run the following commands, replacing `<your_license_server_password>` with your license server password:
>
> ```
> export HISTIGNORE="export*"
> export TERADICI_LICENSE_SERVER_PASSWORD=<your_license_server_password>
> ```

You can specify the old and new passwords inline, by including the `-p` and `-n` flags; to do this, you would enter `sudo pcoip-set-password -p <old_password> -n <new_password>`. This method may expose your password via system loggers, and Teradici strongly discourages it.

7. Remove the internet connection.

8. If you need to change the PCoIP License Server's listening port, see *Configuring the License Server's Listening Port*.

The PCoIP License Server starts automatically when it is installed.

Installing With No Internet Connection

If you cannot open an internet connection on the License Server machine, you must create a temporary machine to download the License Server software and its dependencies and then manually transfer and install them.

To install the software without an internet connection:

1. Create a disposable internet-connected RHEL (or CentOS) machine for downloading and inspecting packages. This machine should be identical to the license server machine.

2. SSH into the new temporary machine.

3. Install the Teradici repository by running the shell script available here. The script will discover your operating system and configure the repo appropriately.

4. Create a new directory to hold the downloaded package manager files. In the following examples, we are creating folders in your user home directory (`~/`). You can create them anywhere; just keep track of them and modify subsequent commands as necessary:

   ```
   cd ~/
   ```

   ```
   mkdir ./rpms/
   mkdir ./updates/
   ```

5. Download required updates to the new `/updates/` folder:
   - RHEL/CentOS 7

```
sudo yum update -y --downloadonly --downloaddir=./updates
```

- RHEL/Rocky Linux 8

```
sudo dnf update -y --downloadonly --downloaddir=./updates
```

6. Download the RPM packages to the new `/rpms/` folder:

   - RHEL/CentOS 7

```
sudo yum install --downloadonly --downloaddir=./rpms pcoip-license-server -y
```

   - RHEL/Rocky Linux 8

```
sudo dnf install --downloadonly --downloaddir=./rpms pcoip-license-server -y
```

7. Transfer the RPMs directory containing the packages to your license server machine using any acceptable method, such as a USB flash drive.

   > ✏️ **The temporary machine is no longer needed**
   >
   > We are now done with the temporary machine, and it can be safely destroyed.

8. Connect to the license server machine using a console.

9. Install the updates from the **updates/** directory you transferred earlier. The following example assumes the **updates/** directory is in the user home directory; if you put it somewhere else, modify these instructions accordingly:

   - RHEL/CentOS 7

```
cd ~/updates/
sudo yum install --disablerepo="*" -y *
```

   - RHEL/Rocky Linux 8

```
cd ~/updates/
sudo dnf install --disablerepo="*" -y *
```

10. Install the PCoIP License Server from the `rpms/` directory you transferred earlier. The following example assumes the `rpms/` directory is in the user home directory; if you put it somewhere else, modify these instructions accordingly:

- RHEL/CentOS 7

```
cd ~/rpms/
sudo yum install --disablerepo="*" -y *
```

- RHEL/Rocky Linux 8

```
cd ~/rpms/
sudo dnf install --disablerepo="*" -y *
```

> 🔥 **Important: Long installation times are possible**
>
> When installing the PCoIP License Server offline, installation times of up to 10 minutes are possible. This is expected behavior.

11. Set your PCoIP License Server administrative password with `pcoip-set-password`.

> ⚠️ **Change the default password immediately**
>
> Until the default password is changed, commands can be issued to the license server without your knowledge.

> ℹ️ **Info: Password Rules**
>
> Passwords should be surrounded with single quotation marks like 'password', and must conform to the following rules:
>
> - Must be between 8 and 30 characters long
> - Must contain at least one lowercase letter
> - Must contain at least one uppercase letter
> - Must contain at least one digit
> - Must contain at least one symbol, excluding ' (single quote), " (double quote), \ (backslash), and spaces.

> ✏️ **Note: Default password**
>
> The default password in new installations is `1P@ssw0rd!`, where the leading `1` is a numeral one and `0` is a zero. When setting the password on a clean installation, use this as your curent password.

To set the new password:

```
sudo pcoip-set-password
```

You will be prompted for the old and new passwords.

> 🔥 **Register your password as an environment variable**
>
> Teradici recommends that you register your password as a system environment variable, which will allow you to run commands without providing the password inline via the `-p` flag. **Providing the passwords inline can have security implications** and Teradici recommends against it. See Keeping Passwords Secure at the top of this page for more information and methods for mitigating the security concerns.
>
> To register the PCoIP password as an environment variable, run the following commands, replacing `<your_license_server_password>` with your license server password:
>
> ```
> export HISTIGNORE="export*"
> export TERADICI_LICENSE_SERVER_PASSWORD=<your_license_server_password>
> ```

You can specify the old and new passwords inline, by including the `-p` and `-n` flags; to do this, you would enter `sudo pcoip-set-password -p <old_password> -n <new_password>`. This method may expose your password via system loggers, and Teradici strongly discourages it.

12. If you need to change the PCoIP License Server's listening port, see *Configuring the License Server's Listening Port*.

The PCoIP License Server starts automatically when it is installed.

> ⚠️ **Do not modify the trusted storage database**
>
> The PCoIP License Server installs a trusted storage database in `/var/opt/flexnetls/TERADICI.`
>
> If the contents of this directory are moved or modified, the license server will consider the trusted storage corrupted. The server will log an error and refuse to start.

Migrating from RHEL 7 to RHEL 8

If you have an exisitng PCoIP License Server on RHEL 7 and wish to upgrade to RHEL 8, you must create a new machine and transfer the license activations to it. You cannot upgrade the operating system in place.

To migrate licenses from a RHEL 7 to a RHEL 8 PCoIP License Server:

1. On the existing RHEL 7 machine, record the number of activated licenses using the `pcoip-list-licenses` command, replacing `<password>` with your PCoIP License Server password:

   ```
   sudo pcoip-list-license
   ```

   Note the number of licenses returned by this command; we will use it to verify the migration in the last step.

2. Create a new offline RHEL 8 machine.

3. Follow the instructions above to install the PCoIP License Server on the new machine.

4. Return the licenses on the RHEL 7 machine, using the instructions here.

   The command will provide the number of licenses returned; note this value. We'll use it in the next step.

5. On the new RHEL 8 machine, activate the same number of licenses that were returned in the previous step, using the instructions here. When following these instructions, use the number returned in the previous step for `<license count>`.

6. Repeat steps 4 and 5 for each of your activation codes, until all licenses have been returned from the old machine and re-activated on the new one.

7. On the new machine, verify that all the licenses have been successfully activated with the `pcoip-list-licenses` command, replacing `<password>` with your PCoIP License Server password:

   ```
   sudo pcoip-list-license
   ```

   The value returned by this command should match the total number of licenses returned on the old license server.

Updating the PCoIP License Server

> ✏️ **Check the location of .jks file before upgrade license server**
>
> If you enable HTTPS, please ensure .jks file is not placed under `/opt/flexnetls/TERADICI/` folder, which may be overwritten by future upgrades, as described here. You may reset the .jks file to another location before upgrade.

To update PCoIP License Server software on an offline machine, obtain a new installer and run it in place. You do not need to uninstall first. Follow the instructions for *Installing PCoIP License Server in an Offline Environment*.

While an upgrade is in progress, the License Server will be offline. Current PCoIP sessions will not be affected, and existing users will still be able to establish PCoIP connections. New users and connections that do not already have validated licenses will be unable to connect until the upgrade is complete.

After the upgrade finishes, check the following items:

- Run the following commands, the reported version number should match the expected installer version.

    - **For RHEL/CentOS 7**:

    ```
    yum info pcoip-license-server
    ```

    - **For RHEL/Rocky Linux 8**:

    ```
    dnf info pcoip-license-server
    ```

- Run pcoip-list-licenses to verify that current licenses were not impacted by the upgrade procedure.

> ⚠️ **Warning: Downgrading is not supported**
>
> Downgrading the PCoIP License Server to a previous version may result in application failure or corrupted data, and is not supported.

Configuring the PCoIP License Server

The PCoIP License Server requires minimal configuration. This section describes the configuration settings and options available.

> 🔥 **Important: Configure PCoIP Agents and Connection Managers**
>
> The PCoIP License Server URL must be provided to the *Connection Manager* managing your PCoIP agents, or to each of your *PCoIP Agents* if you are not using a Connection Manager. The License Server URL format is:
>
> ```
> https://<license-server-address>:<port>/request
> ```
>
> If you have not configured your PCoIP License Server to use HTTPS/TLS, use http:// instead of https://.

Setting the License Server's Administrator Password

The License Server administrator's password is set using the `pcoip-set-password` command. You must have superuser (sudo) permissions to use `pcoip-set-password`.

> ℹ️ **Info: Password Rules**
>
> Passwords should be surrounded with single quotation marks like 'password', and must conform to the following rules:
>
> - Must be between 8 and 30 characters long
> - Must contain at least one lowercase letter
> - Must contain at least one uppercase letter
> - Must contain at least one digit
> - Must contain at least one symbol, excluding ' (single quote), " (double quote), \ (backslash), and spaces.

To set the PCoIP License Server Password:

1. Invoke `pcoip-set-password` to set your new password.

> ✏️ **Note: Default password**
>
> The default password in new installations is `1P@ssw0rd!`, where the leading `1` is a numeral one and `0` is a zero. When setting the password on a clean installation, use this as your curent password.

- If you do not supply any flags, you will be prompted for your current and new passwords:

```
sudo pcoip-set-password
```

- You can also supply the current and new password inline, by using `-p` and `-n` flags:

```
sudo pcoip-set-password -p <current password> -n <new password>
```

Configuring the License Server's Listening Port

The PCoIP License Server listens for communication from PCoIP agents in your deployment on a defined listening port. By default, this listening port is set to 7070, but can be changed by specifying the PORT setting in the `/opt/flexnetls/TERADICI/local-configuration.yaml` configuration file.

> ⚠️ **Enable HTTPS/TLS**
>
> Teradici strongly recommends enabling HTTPS/TLS for secure communications with the PCoIP License Server. For instructions, see Enabling TLS.

> 🔥 **Important: PCoIP agents and License Server must use the same port**
>
> PCoIP agents are configured to use port 7070 by default. If you change the license server port, you must also change the configuration of all PCoIP agents that use it.

To change the license server listening port:

1. Open `/opt/flexnetls/TERADICI/local-configuration.yaml` in a text editor.

2. Locate the port assignment line:

```
# HTTP listening port. Default is 7070. You can bind to an interface with
this syntax: '[127.0.0.1].7070'.

port: 7070
```

3. Change the value of port to the new value. The port number must be an integer between 1 and 65535.

> ✏️ **Note: Reserved port numbers**
>
> Port numbers below 1024 are reserved for processes running as root unless you are using port forwarding, or tools like *setcap*, *setuid*, or *authbind*.

4. Save the file and exit the editor.

5. Restart the license server for the new value to take effect:

```
sudo systemctl restart flexnetls-TERADICI
```

6. Update the configuration of any PCoIP agents that communicate with this PCoIP License Server. For instructions, see one of the following guides:

   - Teradici PCoIP® Graphics Agent for Windows Administrators' Guide
   - Teradici PCoIP® Graphics Agent for Linux Administrators' Guide
   - Teradici PCoIP® Standard Agent for Windows Administrators' Guide
   - Teradici PCoIP® Standard Agent for Linux Administrators' Guide

Enable HTTPS/TLS for PCoIP License Server

> 🔥 **Important: Always use HTTPS**
>
> The following instructions document the use of HTTPS with TLS. The default communication protocol is HTTP, which is less secure than HTTPS. Teradici strongly recommends using HTTPS when communicating with the local PCoIP license server.

> ⚠️ **Warning: Only internal network usage is supported**
>
> The PCoIP License Server only supports company internal network usage. It is not designed to receive connections from the public internet.

> ✏️ **TLS 1.1 on RHEL/Rocky Linux 8**
>
> TLS 1.1 is disabled by default in RHEL/Rocky Linux 8. Attempts to use it in those operating systems may result in errors.
>
> **TLS 1.1 is insecure and Teradici strongly recommends that you do not enable it.** If you *must* enable TLS 1.1, understanding that it is not secure, you must first update the CentOS security policy to `LEGACY`.
>
> To view the current security policy, run the following command:
>
> ```
> update-crypto-policies --show
> ```
>
> To set the policy to `LEGACY`, run the following command:
>
> ```
> update-crypto-policies --set LEGACY
> ```
>
> Once this policy is set, you can proceed with the following instructions.

To use HTTPS/TLS on the PCoIP License Server:

1. Get a valid certificate and accompanying private key, and save them in JKS (Java Key Store) format. Ensure that the JKS file has a keystore password and storepass, and they both are the same.

> ✏️ **Using a self-signed certificate (not recommended)**
>
> Teradici recommends using a CA-signed certificate whenever possible, but you can use a self-signed certificate if required.
>
> If you must use a self-signed certificate, generate one using the following command. Replace `<password>` with your own password, and `<License Server address>` with the IP address or FQDN of the license server:
>
> ```
> keytool -genkey -keyalg RSA -alias teradiciLicenseServer -keystore
> teradiciLicenseServer.jks -storepass <password> -validity 365 -keysize 2048 -noprompt -dname
> "CN=<License Server address>, OU=Teradici PCoIP License Server, O=Teradici Corp,
> L=Vancouver, ST=BC, C=CA" -keypass <password>
> ```
>
> ```
> keytool -importkeystore -srckeystore teradiciLicenseServer.jks -destkeystore
> teradiciLicenseServer.p12 -deststoretype pkcs12
> ```
>
> PCoIP agents can't validate self-signed certificates for HTTPS connections unless the public certificate is installed on the machine's trust store. For more information, see the RHEL instructions on this page.

2. Create a new `/opt/flexnetls/certs` directory, and copy the `.jks` file into it. Do not place `.jks` file under `/opt/flexnetls/TERADICI/`, which may be overwritten by future upgrades.

3. Give the `.jks` file appropriate permissions:

   ```
   sudo chmod 440 /opt/flexnetls/certs/teradiciLicenseServer.jks
   ```

   ```
   sudo chown root.pcoip_license_server /opt/flexnetls/certs/
   teradiciLicenseServer.jks
   ```

4. Create an obfuscated password using Flexera's password obfuscation tool, replacing `<password>` with your password:

   ```
   cd /opt/flexnetls/TERADICI/
   ```

   ```
   java -jar flexnetls.jar -password <password>
   ```

   The output from this command shows the original password and the obfuscated password. Copy the obfuscated password (including `OBF:`) for use in the next step.

5. Configure the Local License Server settings to use the JKS:

   a. Open `/opt/flexnetls/TERADICI/local-configuration.yaml` in a text editor using sudo.

   b. Edit the following lines, replacing `<obfuscated password>` with the password you copied in the previous step. The configuration options are described next:

```
# local-configuration.

# HTTP listening port. Default is 7070. You can bind to an interface
with this syntax: '[127.0.0.1].7070'.
port: 7070

...

# HTTPS server mode
https-in:
  # Set to true to enable
  enabled: true
  # HTTPS listening port
  port: 7071
  # Path to keystore
  keystore-path: /opt/flexnetls/certs/teradiciLicenseServer.jks
  # Keystore password. You can obfuscate this with java -jar
flexnetls.jar -password your-password-here
  keystore-password: <obfuscated password>

...
```

The options are:

`port` : HTTP listen port. This is required to run the license server commands internally on the license server host. You can safely block this port externally.

`https-in/enabled` : HTTPS-in enable. Set this to true to enable HTTPS for incoming connections to the license server.

`https-in/port` : HTTPS-in port number. Set this to the HTTPS listening port for the license server.

`https-in/keystore-path` : Set this to the full path for the JKS file that will be used for encryption.

`https-in/keystore-password` : Set this to the keypass/storepass, *preferably the obfuscated password you created earlier*.

6. Restart the license server:

```
sudo systemctl restart flexnetls-TERADICI
```

7. When the server comes back up, verify that the system is listening on the configured HTTP and HTTPS ports (replace the ports in this example with your own as needed):

```
sudo netstat -tulpn | grep -e 7070 -e 7071
```

A positive response will look similar to the following example:

```
tcp6       0       0 :::7071                  :::*
LISTEN      3083/java
tcp6       0       0 :::7071                  :::*
LISTEN      3083/java
```

8. Verify that you can still view licenses:

```
pcoip-list-licenses
```

If you can view licenses, you will see output similar to the following example:

```
===========================================================================
Name            Count          Version        Type
Expiration
===========================================================================

Agent-Graphics  1              2019.0209      CONCURRENT
2019-02-09
Agent-Session   1              2019.0209      CONCURRENT
2019-02-09


Total number of features : 2



===========================================================================
Feature ID      Feature Name          Feature Version   Feature Count Used/
Available
===========================================================================
1               Agent-Graphics        2019.0209         0/1
2               Agent-Session         2019.0209         0/1
===========================================================================
```

```
Device Information:


---------------------------------------------------------------
Device Name                     Feature Registered(Used Count)
---------------------------------------------------------------
===============================================================================

        Total feature count        : 2
        Total feature count used   : 0
        Total uncounted features   : 0
===============================================================================
```

9. Verify that the license server setting in the Connection Manager is configured correctly.

   When using HTTPS, it should be configured as follows (replace `<License-Server-IP-or-FQDN>` with the IP or FQDN of your license server, and `<https-listen-port>` with the port number you specified in step 5):

   ```
   LicenseServerAddress = https://<License-Server-IP-or-FQDN>:<https-listen-
   port>/request
   ```

10. Verify that the PCoIP Agents can check out licenses.

    a. Move to a PCoIP Agent desktop machine that will use this license server.

    b. Verify that the License Server's firewall is open by opening a browser and visiting `https://<License-Server-IP-or-FQDN>:<https-listen-port>/api/1.0/health` .

       • If the page loads, the firewall configuration is correct.

       • If the page loads but throws a certificate error, the port is open but the certificate is invalid; see below for guidance.

       • If the page does not load, the port is most likely closed.

    c. Verify that the PCoIP Agent machine can view license information from the License Server:

    ```
    pcoip-validate-license
    ```

If a Certificate Fails to Validate

If the certificate fails to validate, it is likely because the Common Name for the certificate is invalid -- either incorrect, or not issued by a trusted Certificate Authority. Follow the instructions provided here to install or import certificates.

- On PCoIP Agent for Linux machines, follow the instructions here to install or import the certificate.

- On PCoiP Agent for Windows machines, follow the instructions here to install or import the certificate.

Managing PCoIP Session Licenses

PCoIP session licenses are purchased in bundles from Teradici. Each bundle is given an activation code at purchase, which controls activation and return of its session licenses. Licenses are validated by Flexera FlexNet Operations, and stored on the PCoIP License Server's trusted storage.

Activated licenses remain linked to their license server until they are returned. No other license server instance can activate licenses that are already allocated.

> ⚠️ **Caution: Licenses can be lost**
>
> If a system hosting a PCoIP License Server is destroyed or becomes corrupted, any licenses registered to it can no longer be returned and are effectively lost. If this happens, open a ticket with Teradici Global Support Services at the Teradici Support Center.

Activating Licenses in an Offline Environment

Since offline environments have no access to the internet, PCoIP session license activation is done indirectly. To activate licenses, you must have an internet-connected machine available and a means of transferring licensing files between the connected machine and your offline PCoIP License Server.

> ✏️ **What if you can't transfer files to an internet-connected machine?**
>
> If you are not able to transfer files from the PCoIP License Server to an internet-connected machine, do not follow these instructions. Teradici Global Support Services will facilitate license activation for you. Create a ticket with Teradici Support for assistance.
>
> When you create the ticket, select **Licensing** as the case reason and include the `VM_UUID` of the PCoIP License Server in your description. Run the following command to get the `VM_UUID`:
>
> ```
> pcoip-get-license-server-id
> ```

> 🔥 **Important: Access to teradici.flexnetoperations.com required**
>
> Before you can activate licenses with an offline license server, you must be given access to https://teradici.flexnetoperations.com. To request access, create a ticket with Teradici support. Be prepared to provide a valid activation key, and the name and email address of a contact person who should have access.

Offline license activation is accomplished by invoking `pcoip-activate-offline-license` twice; once to export a request file which you then supply to FlexNet Operations, and a second time to import FlexNet Operation's response.

This command requires the PCoIP License Server's administrative password. You can provide the password inline using `-p`. If you do not provide the password on the command line, you will be prompted for it.

To activate licenses:

1. SSH into your PCoIP License Server machine.

2. Navigate to your home directory (or another directory that you have write permissions for). To navigate to your home directory, type:

   ```
   cd ~
   ```

3. Invoke `pcoip-activate-offline-license` with `-g`, the activation code, and the number of licenses to activate. Use `-p` to provide the PCoIP License Server's administrative password inline, or leave it off to be prompted for the password:

   ```
   pcoip-activate-offline-license -g -a <activation code> -c <license count>
   ```

   > 🔥 **Important: Activation codes are case-sensitive**
   >
   > The activation code you use here must *exactly* match the code you received from Teradici, including dashes and uppercase or lowercase letters.

> ✏️ **Note: License count (`-c`) sets the total number of active licenses for each activation code**
>
> The license count (`-c`) sets the *total number of licenses* that will be active for a given activation code. It does not add *c* additional licenses.
>
> For example, if you use `pcoip-activate-online-license -a 1234567890 -c 5` and then `pcoip-activate-online-license -a 1234567890 -c 10` , you will have 10 active licenses—not 15.

This will generate a file named `request.bin` and store it in the current working directory.

The contents of the `request.bin` file are displayed for transparency and debugging purposes; the response will look similar to this example:

```
The binary file /home/administrator/request.bin includes the following
information:
MessageType="Capability request"
Vendor=TERADICI
MessageTime="May 10, 2018 4:04:17 PM"
ResponseTime="May 10, 2018 4:00:10 PM"
IdentityName=Agents_RSA_2048_SHA2_256
HostUUID=abc12d3e-4a50-6789-1234-5e0678a90123
RequestHostIDType="VM UUID"
RequestHostID=123A4BCD-56F7-E82F-970A-B12CD3EFA45C
SourceIds=123A4BCD-56F7-E82F-970A-B12CD3EFA45C/VmUuid
IsServer=true
DesiredRights=(ActivationID=12344:1)
```

4. Transfer `request.bin` to a computer that has an internet connection using any acceptable method, such as a USB flash drive.

5. Submit `request.bin` to Flexnet Operations:

   a. Browse to https://teradici.flexnetoperations.com using the internet-connected machine and log in.

   b. Log in with the email address you set up as your Flexnet Activations contact.

   > ✏️ **Note: First-time only password reset**
   >
   > The first time you log in to Flexnet Operations, you will need to reset your password. Click **Password Finder** on the login page to reset the password.

> 🔥 **Important: Resolving login difficulties**
>
> If you experience difficulties logging in, contact Teradici for help. The owner of the activation code email address can also add you as a user on the account.

c. In the sidebar, find the *Devices* section and click Upload Capability Request:

d. Click **Browse** and provide the *request.bin* file you transferred from the PCoIP License Server.

e. Click **Send** to submit the request and download a response file.

If FlexNet Operations returns an error instead of a response file, there is a problem with your request file. Generate a new *request.bin* file and try again.

6. Transfer the received *response file* to the License Server machine using any acceptable method, such as a USB flash drive.

The **response.bin** file can only be used on the machine that generated the **request.bin** file.

7. Invoke `pcoip-activate-offline-license` again with `-r` and the response file received from Flexnet Operations:

```
pcoip-activate-offline-license -r 'path/to/response.bin'
```

> ✏️ **Note: `response.bin` expires after 7 days**
>
> The `response.bin` file expires after 7 days, after which it will be rejected by the License Server. If this occurs, repeat this procedure from the beginning with fresh `request.bin` and `response.bin` files.

8. Verify your license activations:

```
pcoip-list-licenses
```

Returning Licenses in Offline Environments

Licenses are registered to the license server where they are activated. In order to activate them on a different license server, they must first be *returned*, or released, back into the available license pool.

Licenses are returned by using `pcoip-activate-offline-license` to reduce the active license count, which activates the new (smaller) number of licenses and returns the remainder. To do this, follow the procedure for *Activating Licenses in an Offline Environment* and supply the reduced license count for `pcoip-activate-offline-license` in step 3.

For example, if activation code *1234-ABCD-EF12-3456* has 25 active licenses and you want to return 5, you set the number of active licenses to 20:

```
pcoip-activate-offline-license -g -a 1234-ABCD-EF12-3456 -c 20
```

> 🔥 **Tip: Returning all licenses**
>
> You can return all the active licenses by supplying a count of 0 (zero):
>
> ```
> pcoip-activate-offline-license -g -a 1234-ABCD-EF12-3456 -c 0
> ```

Viewing License Information

To view the current status of your managed licenses, use `pcoip-list-licenses` . This command provides information about the PCoIP session licenses that have been activated on the Teradici PCoIP License Server.

This command requires the PCoIP License Server's administrative password. You can provide the password inline using `-p` . If you do not provide the password on the command line, you will be prompted for it.

```
pcoip-list-licenses
```

The information returned by `pcoip-list-licenses` includes:

- The number of licenses that have been activated
- The number of licenses that have been used
- The expiration dates of features or session licenses.

Migrating Licenses to Another Server

A license may only be used on one license server instance at a time. To migrate licenses, you must return them on the first PCoIP License Server and then activate them on the second.

Viewing the contents of `request.bin` and `response.bin`

In some cases, you may need to view the contents of the `request.bin` or `response.bin` files generated by the license activation procedure, either as a debugging tool or a securty measure.

The contents of the `request.bin` file are displayed automatically when running `pcoip-activate-license -g` . To view the contents of `response.bin`, run `pcoip-activate-offline-license` with the `-v` option and the path to the file to inspect:

```
pcoip-activate-offline-license -v <response-file>
```

A result for `response.bin` looks like this example:

```
The binary file /home/administrator/123A4BCD-56F7-E82F-970A-B12CD3EFA45C.bin
includes the following information:
MessageType="Capability response"
ServerIDType=String
ServerID=BACK_OFFICE
SourceIds=BACK_OFFICE
Lifetime=86400
ResponseTime="May 10, 2018 2:43:53 PM"
LastResponseTimeMilliseconds=0
RequestHostID=123A4BCD-56F7-E82F-970A-B12CD3EFA45C
RequestHostIDType="VM UUID"
HostUUID=abc12d3e-4a50-6789-1234-5e0678a90123
MachineType=Unknown
EnterpriseID=12345678
```

Locating License Server Files

License server files are in the following locations. Directories are denoted with a trailing '/'.

File or directory	Location
Log files	`/var/log/flexnetls-TERADICI/`
Server configuration file	`/opt/flexnetls/TERADICI/local-configuration.yaml`
Service configuration files	`/etc/systemd/system/flexnetls-TERADICI.service` `/etc/systemd/system/flexnetls-TERADICI.service.d/flexnetls.conf`
Executable files	`/opt/flexnetls/TERADICI/`
Trusted storage	`/var/opt/flexnetls/TERADICI`
Support bundle file	`/tmp/pcoip-license-server-support-bundle-<datetime>.tar.gz`
Temporary files	`/opt/flexnetls/TERADICI/`

✏️ **Changing the temporary file location**

If needed, you can change the temporary file location by editing `opt/flexnetls/TERADICI/local-configuration.yaml` and providing a new path in the `jni-helper-directory` property.

Using a Failover PCoIP License Server

> ⚡ **Configuring failover requires a temporary internet connection**
>
> You must temporarily open a connection to the public internet for *both* primary and backup license servers while following this procedure. Once the failover pair is registered, the internet connection can be closed and is not needed again. The procedure on this page indicates when to open and close the internet connections.
>
> The primary and backup servers must always have connectivity with each other.

You can add a second standalone PCoIP License Server to your system, which will act as a backup in case the main PCoIP License Server fails. The two servers are registered as a pair called a *failover pair*, in which the main server periodically updates the backup server to keep it in sync.

In a failover situation, when the main PCoIP License Server is down or is unreachable, the backup PCoIP License Server can validate sessions.

> 🔥 **Important: Failover requires manual changes in PCoIP Connection Managers and PCoIP Agents**
>
> Switching from the main to the backup PCoIP License Server requires manual configuration changes in your PCoIP Connection Managers and your PCoIP agents. The change is not automatic. See Failover behavior for more information.

> ✏️ **Note: Backup PCoIP License Servers do not synchronize data**
>
> The backup PCoIP License Server does not synchronize data with the main PCoIP License Server, so information about usage will be unreliable as long as failover lasts.

1: Install the Backup PCoIP License Server

First, install the new PCoIP License Server that will act as your backup. **Do not** register it with Teradici yet (we'll do that later). Keep the following guidelines in mind:

- The two PCoIP License Servers must be the same version.

- Both PCoIP License Servers should be configured identically, with some allowable differences. For example, you can specify different PORT values for the two PCoIP License Servers.

- The two servers should be in different physical locations if possible, or at least on independent hypervisors. One incident or failure should not be able to take down both servers.

- The clocks of the main PCoIP License Server and backup PCoIP License Server must be accurate, synchronized, and in the same time zone. If they are not, unpredictable behavior can occur.

- You must configure the main PCoIP License Server with the failover information *before* the backup server is registered with Teradici. If the backup PCoIP License Server is registered with Teradici before configuration is complete, create a ticket with Teradici Support for assistance.

1A: Open a Temporary Internet Connection

Open a temporary internet connection for *both* the primary and backup servers. You will be directed to close this connection after step 6, below.

> ⚡ **Establishing the internet connection is required**
>
> You must open the internet connection when following this procedure. If the two PCoIP License Server machines cannot reach the internet, the failover registration will not work and the failover pair will not be established.

2: Set the Host ID of the Backup Server on the Main Server

The main PCoIP License Server needs to know the backup server's ID, which will be used to register with Teradici and create a failover pair. We'll get the ID from the backup server and then add that ID to the configuration file on the main server.

1. Start the backup PCoIP License Server.

2. On the backup PCoIP License Server, run the following command and note the backup server's host ID in the response:

   ```
   pcoip-get-license-server-id
   ```

3. Stop the *backup* PCoIP License Server.

   ```
   sudo systemctl stop flexnetls-TERADICI.service
   ```

4. Switch to the *main* PCoIP License Server and start it.

```
sudo systemctl start flexnetls-TERADICI.service
```

5. On the *main* PCoIP License Server, use a text editor to edit **/opt/flexnetls/TERADICI/ local-configuration.yaml**. Set the `backup-hostid` to the backup server's host ID you recorded in step 2.

> ✏️ **Host IDs must be of the same type**
>
> The host ID for both the main server and backup server must be the same type (for example, you can use two VM UUIDs or two Ethernet MAC addresses, but not one of each).

6. Save and exit the editor.

7. Shut down the *main* PCoIP License Server.

```
sudo systemctl stop flexnetls-TERADICI.service
```

At the end of this process, *both PCoIP License Servers should be shut down*.

3: Register the PCoIP License Servers

Next we'll create the failover pair by registering the servers with Teradici.

1. Start the *main* PCoIP License Server.

```
sudo systemctl restart flexnetls-TERADICI.service
```

2. Run the following command:

```
pcoip-list-licenses
```

You don't need the output of this command; we're using it to push the configuration to Teradici, which will find the new backup server ID in your configuration and create a failover pair association.

3. Once you see a valid response from `pcoip-list-licenses`, start the backup PCoIP License Server.

4: Enable Failover Support on the Backup Server

Next, we'll change a few settings on the backup server, configuring it to act as a backup and sync with the main server.

> 🔥 **Important: About `flexnetlsadmin.sh`**
>
> The following sections use the PCoIP License Server Administrator command-line tool, which is a utility provided at `/opt/flexnetls/TERADICI/admintools/flexnetlsadmin.sh`. You can invoke it by providing its full file path on the command line.
>
> If you'd like to invoke the tool as `flexnetlsadmin.sh` (omitting the full path), add `/opt/flexnetls/TERADICI/admintools` to your machine's $PATH variable and restart your console application.
>
> The examples that follow use the shorter command form, as if you had modified your system $PATH. If you haven't, replace `flexnetlsadmin.sh` with `/opt/flexnetls/TERADICI/admintools/flexnetlsadmin.sh` in all of these sample commands.

> ✏️ **Passwords**
>
> You will be prompted for a password when using these commands. The password is the PCoIP License Server administrative password, as set by `pcoip-set-password`.

On the *backup* server, use `flexnetlsadmin.sh` to set the following PCoIP License Server policy settings:

- `fne.syncTo.mainUri` : Set this to the URI of the main PCoIP License Server, using the format: `https://<licenseServerHostName>:<port>/fne/bin/capability`.

  For example (replace the *backup host name*, *main PCoIP License Server host name*, and *port numbers* in this example with your own):

  ```
  flexnetlsadmin.sh -server https://localhost:7071 -authorize admin -
  passwordConsoleInput -config -set fne.syncTo.mainUri=https://
  <MainLicenseServerHostName>:7071/fne/bin/capability
  ```

- `fne.syncTo.enabled` : Set this value to `true` . For example (replace the *host name* and *port number* in this example with your own):

```
flexnetlsadmin.sh -server https://localhost:7071 -authorize admin -
passwordConsoleInput -config -set fne.syncTo.enabled=true
```

5: Configure Response Reference Information on the Main Server

Capability responses returned to client devices can include the URI for the main and backup PCoIP License Servers. Configure one or both of these policy settings to include the corresponding URIs in the response reference information:

- **To include the main PCoIP License Server URI in client reponses:** set the `licensing.main.uri` value using `flexnetlsadmin.sh`. For example (replace these host names and port numbers with your own):

```
flexnetlsadmin.sh -server https://localhost:7071 -authorize admin -
passwordConsoleInput -config -set licensing.main.uri =https://
<MainLicenseServerHostName>:7071/fne/bin/capability
```

- **To include the backup PCoIP License Server URI in client reponses:** set the `licensing.backup.uri` value using `flexnetlsadmin.sh`. For example (replace these host names and port numbers with your own):

```
flexnetlsadmin.sh -server https://localhost:7071 -authorize admin -
passwordConsoleInput -config -set licensing.backup.uri=https://
<BackupLicenseServerHostName>:7071/fne/bin/capability
```

6: Activate Licenses on the Main Server

If no licenses were activated on the main PCoIP License Server at startup, activate them now. The active licenses will be automatically synced to backup PCoIP License Server.

When this is done, **close the internet connection for both the primary and the backup PCoIP License Server**. Note that the primary and backup servers must still be connected to one another.

> ✏️ **Synchronizing changes from the main server to the backup**
>
> If you make changes on the main server that need to be synchronized with the backup, restart the flexnetls-TERADICI.service on the backup:
>
> ```
> systemctl restart flexnetls-TERADICI.service
> ```

> ⚡ **Disconnect internet**
>
> Be sure to close the internet connections now. Neither server will need access to the public internet again.
>
> *Note that the primary and backup servers must still have connectivity with each other*, even after the internet connections are closed.

7: Verify Failover Configuration

After both servers have received their license rights, verify the failover scenario role of each PCoIP License Server. Each server's failover role is included in capability responses delievered to it.

Use the `flexnetlsadmin.sh` tool from each server machine to verify its failover role. As usual, replace the URI and port information here with your own.

- From the **main** PCoIP License Server:

  ```
  flexnetlsadmin.sh -server https://localhost:7071 -authorize admin -passwordConsoleInput -status
  ```

  You should see a backup server specified in the response to this command.

- From the **backup** PCoIP License Server:

  ```
  flexnetlsadmin.sh -server https://localhost:7071 -authorize admin -passwordConsoleInput -status
  ```

  This response *should not* contain a backup server item.

Failover Behavior

If the primary PCoIP License Server fails or loses connectivity, the backup PCoIP License Server will automatically begin validating PCoIP sessions.

PCoIP Connection Managers and PCoIP agents do not automatically switch to a backup PCoIP License Server; they must be configured to point to the backup server for the duration of the failover event, and then reverted once normal service is restored.

For detailed PCoIP License Server configuration information, see the following documentation:

- Connection Manager license configuration
- Graphics Agent for Windows license configuration
- Graphics Agent for Linux (Ubuntu) license configuration
- Graphics Agent for Linux (RHEL/CentOS) license configuration
- Standard Agent for Windows license configuration
- Standard Agent for Linux (Ubuntu) license configuration
- Standard Agent for Linux (RHEL/CentOS) license configuration

Command Reference

For detailed information about all of these commands, including options and special forms, view the embedded man page documentation on the license server machine:

```
man <command-name>
```

You may use -p or -n flags to provide password for scripting license server commands. Teradici recommends omitting the -p and -n flags if possible, as they can cause the provided values to be logged into /var/log/secure and bash history. The PCoIP License Server provides the following commands for configuring the license server and managing licenses in offline environments:

pcoip-activate-offline-license

Activates licenses when the PCoIP License Server is not connected to the internet. See *Activating Licenses in an Offline Environment*. This command is also used to return licenses; see *Returning Licenses in Offline Environments*.

Task	Command
Generate request file	`pcoip-activate-offline-license -g -a <activation code> -c <license count>`
Process response file	`pcoip-activate-offline-license -r <path/to/response.bin>`
Display contents of response file	`pcoip-activate-offline-license -v <path/to/response.bin>`

pcoip-list-licenses

Provides information about the PCoIP session licenses that have been activated on the Teradici PCoIP License Server. See Viewing License Information.

```
pcoip-list-licenses
```

This command was formerly `pcoip-view-license` . To ensure backward compatibility, both commands will work.

pcoip-set-password

Sets the PCoIP License Server's administrative password. See Setting the License Server's Administrator Password.

```
sudo pcoip-set-password
```

pcoip-support-bundler

Gathers information useful to Teradici support in troubleshooting and diagnosing problems. See Creating Support Bundles.

```
sudo pcoip-support-bundler
```

pcoip-get-license-server-id

Returns the unique ID of the PCoIP License Server machine. This may be required in debugging or support situations.

```
pcoip-get-license-server-id
```

Additional Tools

Teradici maintains a Github repository with open-source tools that augment usage of the PCoIP License Server. The tools in this repo are provided as-is, with no expectation of support. Users are encouraged to submit bug reports in github, and are welcome to fork projects and submit pull requests.

The repo is available at https://github.com/teradici/pcoip-license-server.

Getting Support

If you are having trouble, help is always available. Here's how to contact Teradici support and connect with the Teradici user community.

Contacting Support

If you encounter problems installing or using Teradici technology, you can:

- Check for updated release notes, which may address the issue you are experiencing. Release notes are published on Teradici Support.

- Browse the Teradici Knowledge Base.

- Submit a support ticket.

The Teradici Community Forum

The PCoIP Community Forum allows users to have conversations with other IT professionals to learn how they resolved issues, find answers to common questions, have peer group discussions on various topics, and access the Teradici PCoIP Technical Support Service team. Teradici staff are actively involved in the forums.

To join the Teradici community, visit the Teradici Community Forum.

Creating Support Bundles

Support bundles include relevant log files, current configuration, and license server and operating system information that are useful for Teradici Support in diagnosing problems and recommending actions. You may be asked by your Teradici Support representative for a support bundle while troubleshooting.

Support bundles are created using the `pcoip-support-bundler` command. You must have superuser (sudo) permissions to use this command.

This command requires the PCoIP License Server's administrative password. You can provide the password inline using `-p` . If you do not provide the password on the command line, you will be prompted for it.

To generate a support bundle:

1. Invoke the `pcoip-support-bundler` command.

   ```
   sudo pcoip-support-bundler
   ```

   > ✏️ **Running with an empty password**
   >
   > It is possible to run this command using a blank password (using `-p` with no argument). In this case, the bundler will exclude some information from the generated support bundle.

2. Find the generated .tar.gz output in the `/tmp` directory:

   ```
   /tmp/pcoip-license-server-support-bundle-<date-time>.tar.gz
   ```

> ⚠️ **Understand the data the support bundler collects**

Support bundles will collect the following files or command output:

- `/opt/flexnetls/TERADICI/*` (except flexnetls.jar)
- `/opt/flexnetls/TERADICI/admintools/*` (except flexnetlsadmin.jar)
- `/var/log/flexnetls-TERADICI/*`
- `var/log/audit/*`
- `/var/log/messages*`
- `/etc/init.d/flexnetls-TERADICI`
- `/etc/default/flexnetls-TERADICI`
- `/etc/*-release`
- `/etc/issue`
- `pcoip-configure-proxy.py -v`
- `pcoip-view-license.py -p`
- `flexnetlsadmin.sh -server -config`
- `flexnetlsadmin.sh -server -status`

The output of the following system commands is collected:

- `id license_server`
- `groups license_server`
- `yum list installed`
- `who`
- `dmesg`
- `ss -ax`
- `semodule -l`
- `sestatus`
- `ps wwauxfZ`
- `netstat -Wnap`
- `firewall-cmd --list-all`
- `iptables-save`
- `df -hk`
- `ip addr`

Troubleshooting General Issues

My PCoIP session licenses have disappeared

Your licenses have most likely expired. Contact Teradici Sales to re-activate your licenses.

My installation is taking a long time to complete

Offline systems can expect installation times of up to 10 minutes. If you are experiencing delays longer than this, or if your installation is quitting with a timeout error, check the system logs for errors and contact Teradici Support.

I forgot my PCoIP License Server administrative password

If you forget the PCoIP License Server administrative password, you will no longer be able to run most administrative commands. You will still be able to adjust proxy settings and change the listening port.

The PCoIP License Server administrative password is not recoverable. To restore administrative access, you must:

1. Destroy the PCoIP License Server's trusted storage folder (`/var/opt/flexnetLS/ TERADICI`)

2. Reinstall the PCoIP License Server

3. Set a new PCoIP License Server administrative password

4. Reactivate any licenses that were previously activated on the PCoIP License Server. The activation code (or keys) used must be identical to the original activations in order to preserve your licenses.

> 🔥 **Do not destroy the PCoIP License Server machine**
>
> If you destroy the license server machine, the licenses will be lost.

I've changed some configuration settings but the changes have not been applied

Configuration changes require a restart of the PCoIP License Server service to take effect. To restart the service, use this command:

```
sudo systemctl restart flexnetls-TERADICI
```

My password fails when using the `-p` option

If your password contains reserved Linux characters like the pipe (`|`), the shell may interpret them as operators instead of string characters and break the command. In order to prevent the shell from interpreting operators, enclose your password in single quotes.

When I activate additional licenses under an existing activation code, the number of activated licenses I get is wrong

When you supply an activation count (`-c`) to `pcoip-activate-*-license` , you are setting the *total* number of licenses that should be active under that code. If you have 10 licenses and want to activate 5 more, you should run the activation command with `-c 15` (not `-c 5`).

The PCoIP agent reports that there are no available licenses

If the PCoIP agent reports that that no licenses are available, consider the following possibilities:

- The PCoIP License Server may be incorrectly configured and unable to communicate with your PCoIP agents. The PCoIP License Server should be available at `https://<license-server-address>:<port(default=7070)>/request` .

- PCoIP agents must be configured to use the same port number as your PCoIP License Server. By default, this is 7070. If you change the listening port on the PCoIP License Server, you must also configure your PCoIP agents to use the new value.

- The PCoIP License Server may not have enough free licenses. Use `pcoip-list-licenses` to verify your available license count.

Troubleshooting Error Messages

ERROR: Connection to server failed or refused

Check that the license server service is running:

```
sudo systemctl is-active flexnetls-TERADICI
```

If it is, ensure that the listening port is open (the default listening port is 7070). To quickly check that the correct listening port is open, use a browser to visit the following URL:

```
https://<license-serve-ip-address>:<port>/api/1.0/health
```

Job for flexnetls-TERADICI.service failed because the control process exited with error code

If you see this error message, the server needs to be killed and restarted. To kill and restart the system, use these commands:

```
sudo pkill -u pcoip_license_server
sudo systemctl restart flexnetls-TERADICI
```

Too many failed logins

This error means that the provided password has been incorrect 3 consecutive times while attempting to access the PCoIP License Server trusted storage. If the incorrect password has been provided 3 or more times consecutively, the license server will block access to administrative commands for 10 minutes, or until the license server is restarted.

FNE License Server has not been configured for HTTPS

This can happen when the `/opt/flexnetls/TERADICI/flexnet.certs` file is missing or invalid. Updating or re-installing the license server should fix the issue. See Updating PCoIP License Server in an Offline Environment for detailed instructions.

Contact Teradici Support if the issue persists after reinstalling.

ACTIVATION_ID_COUNT_EXCEEDED

This error means you are attempting to activate more licenses than the activation code allows. Most likely, one or both of these conditions has been met:

- Some or all of the licenses for this activation code have already been activated on other PCoIP License Server instances, and there are not enough still available to complete your request. To activate these licenses on the current PCoIP License Server instance, you must first return them on the other instances.
- You have specified a larger license count than the given activation code manages.

ACTIVATION_ID_INVALID

This error means you have provided an invalid activation code. Make sure you have entered the activation code string correctly, including any symbols like dashes (-).

`response.bin` is rejected

The `response.bin` file generated by FlexNet Operations expires after 24 hours. Once expired, the file can no longer be used to validate licenses using `pcoip-activate-offline-license`. If this occurs, submit your `request.bin` to FlexNet Operations again and use the new `response.bin` file.

Troubleshooting Errors in Logs

PCoIP License Server logs are located in `/var/log/flexnetls-TERADICI/` .

Network is Unreachable

Check the firewall to make sure the license server has network access.

Name or service unknown

The specified server address could not be resolved. Ensure that the server is a valid target and the DNS is properly configured.

Unable to connect to compliance.teradici.flexnetoperations.com

This error occurs because the License Server cannot reach Flexnet operations in offline environments. The License Server does not need to reach this service in an offline context, and the error can be safely ignored.

No logs are present, or the PCoIP License Server doesn't start

If there are no license server logs available, or if the service won't start, you can view additional system logs by entering the following command:

```
journalctl -u flexnetls-TERADICI
```