

Getting Started with DTP Enterprise Pack

In this chapter:

- [Installation](#)
- [Enabling SSL](#)
- [Cross-origin Resource Sharing Configuration](#)
- [Licensing](#)
- [System Requirements](#)
- [Starting and Stopping Applications](#)
- [Setup and Configuration](#)
- [Branding Extension Designer and Policy Center](#)
- [Important Concepts and Terminology](#)

See the [Integration with DTP Enterprise Pack](#) chapter for additional information.

Installation

Make sure your system environment meets the [system requirements](#) before installation. Extract the files from the installation package. The package includes a script, `dtpservices.bat` for Windows and `dtpservices.sh` for Linux, which automates processes, such as starting up, stopping, and restarting the Extension Designer, Policy Center, and the database.

Upgrading from a Previous Version

See [Migrating PIE Slices to Extension Designer](#) if you are upgrading from a previous version.

Additional Installation Notes

- For Windows installations, we recommend using a third-party zip compression utility, such as WinZip, WinRar, or 7Zip to extract the distribution files for installation. Microsoft Windows' built-in Uncompress utility (from Windows Explorer) has many issues—for example, directory and file name size limitations and performance issues. If you extract the DTP Enterprise Pack distribution zip file using Windows Explorer, you may get a "Path too long" error message. The same error may also result if you open the distribution with 7Zip and drag the DTP Enterprise Pack folder from the 7Zip UI to the desktop.
- Install the pack as a local user with a local (not network-shared) home directory. The same local user should be used for installing Parasoft DTP.
- We strongly encourage you to install the pack into a dedicated directory, such as `$HOME/parasoft/dtpservices` or `C:\Parasoft\dtpservices`. **DO NOT install it into the same directory as Parasoft DTP**; if you do, upgrades to one product could impact the installation of the other product(s).
- The `installed.file.lst` file in the installation directory is used to track which installation files are modified and should be included in any backups.

Enabling SSL

SSL is not enabled in DTP Enterprise Pack by default. You will need to enable SSL if you need to secure the data transported between applications in your infrastructure. If you are using an SSL-enabled reverse proxy server, you do not need to enable SSL for Parasoft applications (see [Reverse Proxy Support](#)).

To enable SSL, you must first obtain an authority-signed certificate (CA) from a provider, such as VeriSign, Symantec, or GlobalSign.



Do Not Use a Self-signed Certificate

Unless you are implementing a reverse proxy infrastructure, only use authority-signed certificates when enabling SSL.

1. If you have the CA, open the `ssl.config.js` file in an editor. This file is located in the `<DTPSERVICES>/shared` directory.
2. Change the value of the `enabled` property to `true` and set the options to use your certificate. See the [node.js documentation](#) for a complete list of options. If the certificate was created with a passphrase, then be sure to include it in your configuration.
3. Save the file.

The same ports are used when SSL is enabled for DTP Enterprise Pack, but they will all use the HTTPS protocol. DTP Enterprise Pack will also use SSL-enabled ports to communicate with DTP. If you want to send data between DTP and Enterprise Pack applications over HTTPS, you must enable SSL for both systems to make sure they work properly.

If you enable SSL for Enterprise Pack, you must also enable SSL for the DTP interface (DTP APIs always run under SSL) so that Report Center, Extension Designer, and Policy Center use the same protocol (HTTP). If you disable SSL and are not using an SSL-enabled reverse proxy server, then passwords and other important information will transmit over the network unencrypted.

Cross-origin Resource Sharing Configuration

You can manually enable authentication to services across DTP Enterprise Pack by whitelisting hostnames in the <DTPSERVICES>/shared/whitelist.json file. The whitelist file is typically for special circumstances in which an extra set of domains need to be registered. Extension Designer creates its own internal whitelist automatically whenever the DTP Configuration is changed through the UI. Your manual entries to the whitelist file are appended to the internal whitelist.

This JSON file is an array of strings containing the hostname or IP address and port numbers (if applicable).

Example Whitelist JSON

```
[
  "54.219.185.79:8080",
  "54.219.185.79:8443",
  "ec2-54-219-185-79.us-west-1.compute.amazonaws.com:8080",
  "ec2-54-219-185-79.us-west-1.compute.amazonaws.com:8443"
]
```

If you are whitelisting the domain that is hosting DTP and DTP Enterprise Pack, the entries must also include ports for the DTP interface, DTP API, Enterprise Pack, and Policy Center. Ports should not be added, though, if you are using a reverse proxy (see [CORS with Reverse Proxy](#)). The whitelist generator adds domains to the whitelist based on the following information:

- hostname:port
- fully-qualified domain name:port
- IP address:port
- localhost:port

If one of these entries is missing you will get a CORS error when you try to access a resource that isn't part of the whitelist.

CORS with Reverse Proxy

If you are using reverse proxy on port 443 or 80 to forward your traffic to real server, add only the hostname to the whitelist. For example, you would add one of the following to the whitelist:

`https://mydtp.domain.com/`

`http://mydtp.domain.com,/ mydtp.domain.com`

Licensing

A Parasoft DTP Enterprise license is required. Contact your Parasoft representative if you have questions about your license.

System Requirements

Operating System	Windows (64-bit only): <ul style="list-style-type: none">• Windows 7• Windows 8• Windows 10• Windows Server 2008• Windows Server 2012• Windows Server 2016 Linux: <ul style="list-style-type: none">• Any Linux distribution similar to /compatible with Ubuntu 14.04/14.10 or later or RedHat Enterprise Server 6.x or later. Solaris: <p>Solaris installation is not supported. If your DTP is installed on Solaris/Sparc, you can install the DTP Enterprise Pack on a separate Windows or Linux system. Parasoft does not support Solaris on x86 platform. Contact your sales representative or support for additional questions.</p>
Hardware	<ul style="list-style-type: none">• Same as DTP (see System Requirements)• At least 4 GB RAM free. An additional 4 GB RAM is recommended.

Software	<ul style="list-style-type: none"> Parasoft Development Testing Platform Server 5.3.2. Parasoft DTP Engines 10.2.x or later connected to Parasoft DTP
Browser	<ul style="list-style-type: none"> Microsoft Internet Explorer 11* Microsoft Edge Google Chrome Mozilla Firefox <p>* Extension Designer cannot be run in Compatibility mode. To disable this mode:</p> <ol style="list-style-type: none"> Open Internet Explorer's settings menu and choose Compatibility View settings Remove the Extension Designer from list (if it is there) and/or disable Display intranet sites in Compatibility View if Extension Designer is being viewed from the local network
Network	<ul style="list-style-type: none"> Ports 8314 and 8315. Extension Designer will use any open ports up to 8399. Each service creation will check port availability before assigning a port to the service. Port 1883 available on DTP Server Port 8316 for Mongo DB database <p>We recommend installing the Enterprise Pack and DTP on the same server. If they must be installed on different servers, they should both be installed on the same network.</p> <ul style="list-style-type: none"> On Windows, they should use the same domain (Active Directory) and the server's FQDN (Fully Qualified Domain Name) should be resolved by a DNS name server. On Linux, the domain name must be configured and the server's FQDN should be resolved by a DNS name server.

Starting and Stopping Applications

- Open a command prompt and navigate to the Enterprise Pack installation directory.
- Run the `dtpservices` script for your operating system with the `start` argument:

Windows:

```
dtpservices.bat start
```

Linux:

```
dtpservices.sh start
```

The `start` argument starts Extension Designer, Policy Center, and database will start.

To stop DTP Enterprise Pack applications, run the `dtpservices` script with the `stop` argument:

```
dtpservices.bat stop
```

The following table lists all available commands:

Command	Output
<code>dtpservices.bat start</code>	Starts all servers and the database
<code>dtpservices.bat stop</code>	Stops all servers and the database
<code>dtpservices.bat install-addon</code>	<p>Installs deployed slices into DTP. This command is only available if DTP and Extension Designer are installed as the same user on the same machine.</p> <p>For Windows, the <code>DTP_HOME</code> environment variable is set if DTP is installed on the machine. For Linux, <code>PST_HOME</code> is set under <code>\$HOME/.pstrc_<hostname></code>.</p>
<code>dtpservices.bat status</code>	Reports the status for DTP Enterprise Pack applications and services. If you are experiencing issues with Extension Designer, Policy Center, or any of your flows, run this command to verify that components and services are running.



Potential Errors When Stopping on Linux

In some unexpected instances, you may see the following message when running the `stop` on Linux:

"Time out on DTP Enterprise Pack process termination. Please kill all processes manually. (Refer to the documentation)"

This message only triggers if any of the children processes of the main DTP Enterprise Pack application (typically one of the service processes) started but was not killed completely. These processes must be terminated before starting DTP Enterprise Pack again.

1. Run following command:

```
pgrep node or pgrep -f <installation home>/nodejs/bin/node
```

This command will print out all processes that DTP Enterprise Pack started.

2. Run the kill command using the same argument to kill these process:

```
pkill node
```

or

```
pkill -f <installation home>/nodejs/bin/node
```

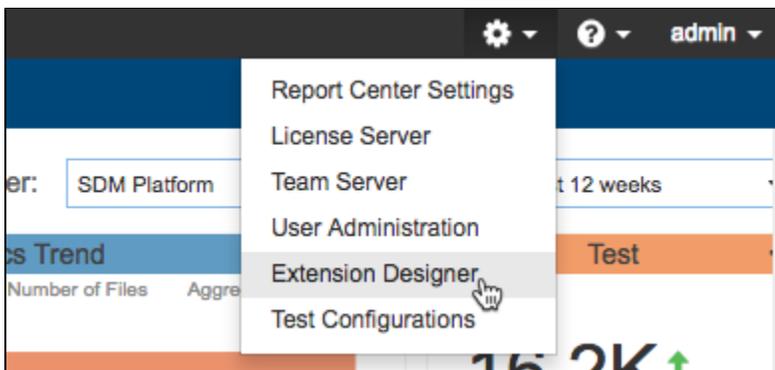
Accessing Enterprise Pack Applications

Enter the host and port number in a browser address bar to open Extension Designer and Policy Center. The following examples use the default ports, but the actual port number depends on the availability of the port. See [System Requirements](#):

- `http://<host>:8314` - Extension Designer.
- `http://<host>:8000` - Policy Center.

If SSL is enabled, the protocol will be `https` (see [Enabling SSL](#)).

You will also be able to access Enterprise Pack applications from the settings menu in DTP.

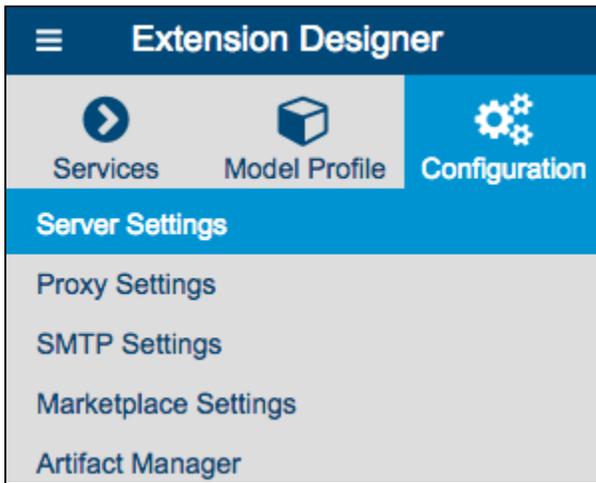


Setup and Configuration

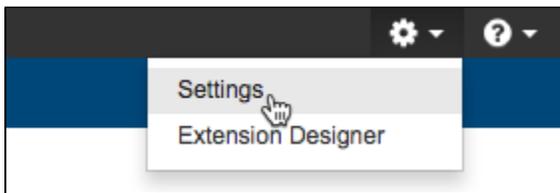
Extension Designer and Policy Center must be configured for use within your DTP environment. This includes:

- Connecting to DTP
- Configuring security settings
- Configuring DEP to use your email server
- Connecting to Marketplace (for downloading and installing extensions)

The configurations are set in the Server Designer Configuration tab.



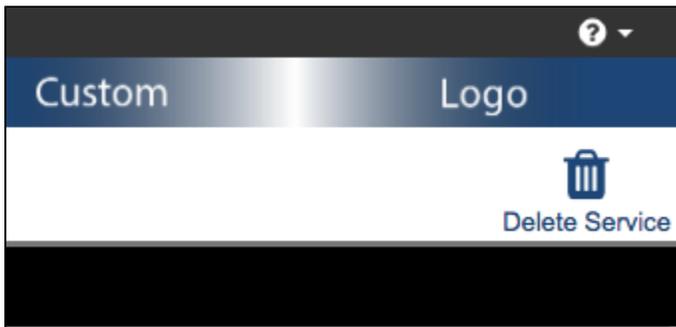
You can also access this tab from Policy Center by choosing **Settings** from the gear icon menu.



See [Server Settings](#) for instructions.

Branding Extension Designer and Policy Center

You can add a custom logo to the header of Enterprise Pack applications. To add a custom logo, replace the png at `/public/lib/custom-logo.png` with your company logo.



The image file must be named "custom-logo.png". The dimensions of the image container is 300px by 35px.

Important Concepts and Terminology

The following table provides working definitions of concepts and terms associated with DTP Enterprise Pack applications.

Service	In the context of this technology, a service is a group of one or more flows or artifacts that can perform specialized tasks. Services can provide custom REST endpoints, custom widgets for DTP, custom practices for Policy Center, trigger actions in third-party system, etc. Services in DTP Enterprise Pack should not be confused with web services or components that are more generally described as services.
Flow	Flows are one or more nodes that can perform specialized tasks. Flows can be grouped into services to more evenly distribute data processing across endpoints, which results in more stable execution.
Node	Nodes are the basic building blocks for creating flows and services that can perform specialized tasks.
Artifact	Artifacts are complete services or flows that can be downloaded and installed from the marketplace (see Downloading and Installing Artifacts) or created locally and uploaded to Extension Designer.

Policy	Policies are non-functional requirements that can be automatically monitored in an exception-based manner. See Core Policy Center Concepts for additional information.
Practice	A practice can be any means of automatically assessing the software being produced, such as static analysis, metrics analysis, code coverage, and unit testing. See Core Policy Center Concepts for additional information.
Gate	Gates measure compliance to one or more policies at a particular point in time. If the policy expectations are not met, the gate can prevent the software from proceeding to the next phase of the SDLC. See Core Policy Center Concepts for additional information.
Model	If you want to perform custom calculations within the context of a flows or services , you can create a model, which defines the template for the data used to perform the specific type of calculation. Specific instances of a model are called profiles , which can be used in a flow to carry out the custom calculation. See Working with Model Profiles for additional information.
Profile	Each instance of a model is a profile. Profiles must be paired with flows that can consume the data associated with the specific type of calculation. See Working with Model Profiles for additional information.