Integration with DTP Enterprise Pack

In this section:

Installation

DTP Enterprise Pack is an installation option when you install DTP. See New DTP Installations for instructions or Upgrading if you are upgrading to the latest version of Enterprise Pack.

Requirements

See Requirements.

Installation Directory and User Account

You should use the same local user to install enterprise pack with DTP. This is to enable full integration and avoid potential issues in some environments. The user should have a local home directory, not a network shared directory.

By default, Enterprise Pack is installed in [DTP_HOME]/dtpservices, but you can install the applications on different servers if necessary. They should both, however, be installed on the same network.

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.\

Enabling Access to Policy Center

Policy Center and all Policy Center Practice artifacts are deprecated and will reach their end of life in a future release. Policy Center is disabled by default and must be re-enabled if you want to continue using it. Edit the PSTRootConfig.xml configuration file located in the <DTP_INSTALL>/conf/ directory and make the following modifications:

1. Uncomment the `<visible-apps>` node.
2. Uncomment the child `<policy-center>` node and set the value to `true`. To disable Policy Center, you can set the value to `false` or comment the node back out.
3. Save the file and restart DTP (see Stopping DTP Services and Starting DTP Services).

One Policy Center Per DTP Deployment

For the full duration of your DTP and Policy Center implementation, you should only integrate one DTP server with one instance of Policy Center. This is because Policy Center requires DTP's project list to be consistent so that accurate information is displayed. The following scenarios describe potential issues regarding this requirement and how to resolve them:

Scenario	Resolution
Moving DTP to new server	If you are migrating to new DTP, be sure to move the Enterprise Pack installation at the same time so that all internal data is consistent.
Lost DTP and data	If DTP data is lost, reset the Policy Center database when DTP is brought back online. All previously stored data will no longer be valid.
Set testing against production	A separate Enterprise Pack installation should be deployed for each environment.

Setting Default Ports for Connected Services

You can specify a default host and port for applications connecting to DTP using the services API. This enables you to redirect users to the appropriate URL if you need to enforce SSL, for example. DTP Enterprise Pack applications, for example, use the services API to communicate with Report Center.

1. Open the DTP_HOME/conf/PSTRootConfig.xml configuration file in an editor.
2. Locate the `<default-server-url>` element and provide a valid URL:

```
<default-server-url>http://example.host.com:port</default-server-url>
```

3. Save the file.

Enabling Single Sign-on

If you are using Policy Center 3.2 or later in your organization, you can enable a cookie that allows users to log into Policy Center from your primary DTP server. The single sign-on cookie is disabled by default. To enable:

1. Open the <DTP_install_dir>/conf/PSTSecConfig.xml configuration file and either uncomment or add the `<pst-cookie>` element:

```
<pstsec-config>
        ...
                <pst-cookie>
                        <domain>companydomain.com</domain>
                </pst-cookie>
        ...
</pstsec-config>
```

2. Save your changes and restart the DTP server. See Starting DTP Services.

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 (HTTPS). 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.