Cisco ASR 5000 Policy Provisioning Tool Installation and Administration Guide

Version 14.0

Last Updated August 17, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27221-01

Cisco ASR 5000 Policy Provisioning Tool Installation and Administration Guide

CONTENTS

About this Guide

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis.

This preface includes the following sections:

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electrostatic Discharge (ESD)	Warns you to take proper grounding precautions before handling ESD sensitive components or devices.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents text that appears on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter at the CLI, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* *`slot_number`* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**.

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by braces. They must be entered as part of the command syntax.
[**`keyword`** or *`variable`*]	Optional keywords or variables that may or may not be used are surrounded by brackets.

Command Syntax Conventions	Description
|	Some commands support alternative variables. These "options" are documented within braces or brackets by separating each variable with a vertical bar. These variables can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Go to http://www.cisco.com/cisco/web/support/ to submit a service request. A valid Cisco account (username and password) is required to access this site. Please contact your Cisco account representative for additional information.

Additional Information

Refer to the following guides for supplemental information about the system:

- *Cisco ASR 5x00 CDMA Command Line Interface Reference*
- *Cisco ASR 5x00 eHRPD / LTE Command Line Interface Reference*
- *Cisco ASR 5x00 GPRS / UMTS Command Line Interface Reference*
- *Cisco ASR 5x00 Thresholding Configuration Guide*
- *Cisco ASR 5x00 SNMP MIB Reference*
- *Web Element Manager Installation and Administration Guide*
- *Cisco ASR 5x00 AAA Interface Administration and Reference*
- *Cisco ASR 5x00 GTPP Interface Administration and Reference*
- *Cisco ASR 5x00 Product Overview*
- *Cisco ASR 5x00 Release Change Reference*
- *Cisco ASR 5x00 Statistics and Counters Reference*
- *Cisco ASR 5x00 Gateway GPRS Support Node Administration Guide*
- *Cisco ASR 5x00 HRPD Serving Gateway Administration Guide*
- *Cisco ASR 5x00 Mobility Management Entity Administration Guide*
- *Cisco ASR 5x00 Packet Data Network Gateway Administration Guide*
- *Cisco ASR 5x00 Packet Data Serving Node Administration Guide*
- *Cisco ASR 5x00 System Architecture Evolution Gateway Administration Guide*
- *Cisco ASR 5x00 Serving GPRS Support Node Administration Guide*
- *Cisco ASR 5x00 Serving Gateway Administration Guide*
- *Cisco ASR 5000 Session Control Manager Administration Guide*
- *Cisco ASR 5000 Packet Data Gateway/Tunnel Termination Gateway Administration Guide*
- Release notes that accompany updates and upgrades to the StarOS for your service and platform

Chapter 1
Policy Provisioning Tool Overview

This chapter provides an overview of the Policy Provisioning Tool (PPT) which is an integral part of the Cisco's Policy Control and Charging (PCC) Solution, designed to be used in conjunction with the Intelligent Policy Control Function (IPCF) on Cisco© chassis and the Subscriber Service Controller (SSC) on Cisco© UCS or IBM© Blade Center.

This chapter contains following sections:

PCC Solution Elements

This section provides a brief overview of PCC solution components.

The Cisco Policy and Charging Control (PCC) solution includes following functional entities:

- Intelligent Policy Control Function (IPCF)
- Subscriber Service Controller (SSC)
- Policy Provisioning Tool (PPT)

Intelligent Policy Control Function (IPCF)

This section briefly describes IPCF.

IPCF provides policy control and charging rule functions in a core network. IPCF acts as a Policy Charging and Rules Function (PCRF) supplemented with usage monitoring capability that enables policies around data consumption. IPCF interfaces with Policy Charging and Enforcement Function (PCEF) over standard **Gx** interface.

Cisco IPCF is compliant with 3GPP standard in operator's core network. It performs following key functions:

- Derive and authorize the QoS information for the service data flow for session as well as bearer use.
- Select appropriate charging criteria and mechanism apt for data usage.
- Provide network control regarding the service data flow detection and gating.
- Ensure that the PCEF user plane traffic treatment is in accordance with user's subscription profile.
- Correlate service and charging information across PCEF and Application Function (AF).

Important: For more information on IPCF function and supported interfaces, refer *Cisco ASR 5000 Series Intelligent Policy Control Function Administration Guide*.

Subscriber Service Controller (SSC)

This section briefly describes SSC.

SSC provides the SPR functionality for the Cisco PCC solution that is compliant with 3GPP R8, and uses an extended implementation of 3GPP Sh messaging for exchanging static as well as dynamic subscriber profile data with IPCF. SSC allows the enforcement of aggregate rules supporting volume usage across groups of subscribers sharing common account. It also provides optional decision center functionality.

SSC provides a centralized and simplified policy management for the network. It interfaces with IPCF over **Sp** interface which is based on standard **Sh** protocol, for subscriber profile and usage related transactions. SSC also supports a proprietary interface to receive event notification data from IPCF.

Important: For more information on SSC function and supported interfaces, refer *Cisco ASR 5000 Subscriber Service Controller Installation and Administration Guide*.

Policy Provisioning Tool (PPT)

This section briefly describes PPT.

The PPT is a GUI-based policy and profile management tool in the PCC solution that allows operators to perform subscriber policy provisioning and management functions.

The PPT interfaces with IPCF as well as SSC to provide centralized policy management interface for operators.

PPT Introduction

This section describes Policy Provisioning Tool (PPT) application.

Cisco Policy Provisioning Tool (PPT) is a Web-based client-server application that provides a comprehensive policy design experience to service providers or network operators. Using wizard-based implementation of policy use cases, PPT enables service providers to design policies for network usage and monitoring. These policies can then be used to monitor and control services rendered to subscribers as well as their network usage. PPT interfaces with other components of PCC solution such as IPCF and SSC to exchange data such as QoS profile or data plans.

PPT can be deployed to configure policies using a local library of user defined actions and conditions along with rules, rule bases, Access Point Names (APNs), and other data elements from Policy Control Enforcement Function (PCEF) such as Gateway GPRS Support Node (GGSN), Serving GPRS Support Node (SGSN) or Packet Data Serving Node (PDSN). PPT is designed to simplify policy use case configuration by importing relevant rules, flows and other data elements from PCEF. In most deployments the PCEF is located at a gateway that is responsible for enforcing policy and charging related decisions received from IPCF. PCEF performs service data flow detection as well as gate enforcement for the data flows.

PPT works in conjunction with other PCC solution components such as IPCF, SSC and PCEFs such as GGSN or PDSN to provide following functionality:

- Designing highly flexible, easily expandable and manageable policy use cases using a GUI based tool.
- Configuring policies using libraries containing rules, rule bases as well as APN and traffic type categories.
- Configuring and maintaining policies that can be used by IPCF and SSC to provide various services to the subscribers.
- Configuring data plans containing service usage limits and thresholds.
- Deploying policies across multiple IPCF instances and interfacing with multiple SSC instances in a PCC deployment.
- Configuring templates for notification messages to subscribers that can be sent thru e-mail as well as SMS using the SSC component of PCC solution.
- Configuring Quality of Service (QoS) profiles, that can act as a container for QoS parameters used to determine the availability and quality of services being offered.
- Maintaining a policy database.

Depending upon your business model and network configuration PPT can fetch policy related objects from PCEF as well as provision policy related objects to SSC and IPCF instances.

PPT can fetch following policy related information from PCEF:

- APN names
- Ruledef names
- Rulebase names

Important: User can use this information in policy configuration. But, the definition of these objects is not fetched i.e. the definition of the rule is not fetched. For the policy configuration, only the name is required.

PPT can provision following policy related IPCF objects:

- Map profiles

- Data Services
- Timedef
- Quality of Service (QoS) Profiles
- Profiles
- PCC Service
- Dynamic rules

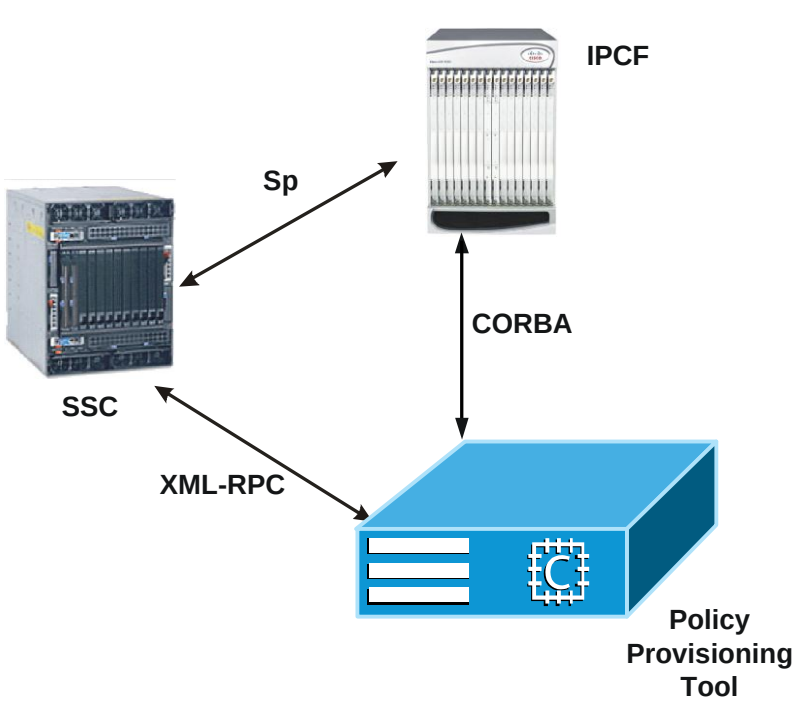
PPT can provision following policy related SSC objects:

- Data plans
- SMS and e-mail notification templates
- Subscription tiers
- Dynamic profile attributes
- Areas
- Regions
- Region lists

Important: PPT is a **policy provisioning** tool. It does not perform any functions related to subscriber profile provisioning, such as creating subscribers or associating data plans to subscribers. Such functions are performed by the SSC component of the PCC solution.

Following figure describes a network scenario where PPT is deployed with other PCC solution components such as IPCF and SSC.

Figure 1. Deployment Scenario



The client-server architecture of PPT provides a GUI based tool to quickly create new policies. Depending upon the business model, subscriber base and network configuration, following categories of policies can be created using PPT application:

- Subscriber profile based policies using subscriber attributes such as subscription tiers, IMSI and MSISDN.
- Volume based policies using maximum limits and thresholds.
- Access Point Name (APN) based policies using the network configuration.
- Speed based policies using Quality of Service (QoS) and throughput.
- Location based polices using home region roaming and base station id.
- Time based polices using time of the day, day of the week.
- Access type based policies using category of network access technology deployed, such as 2G, 3G or LTE.
- Subscriber session based policies using usage per session.
- Protocol based policies indicating allowed or restricted protocols such as P2P, FTP, HTTP.
- Content based polices indicating allowed or restricted content categories.
- URL based polices indicating allowed or blocked URLs.

Features and Functionality

This section describes features and functionality supported by PPT application.

Following features are described in this section:

- Synchronizing Policy Objects from Multiple IPCF, SSC and PCEF Instances
- High Availability (HA) Support in the PPT Application
- Viewing Manageability status of IPCF, SSC and PCEF Instances

Synchronizing Policy Objects from Multiple IPCF, SSC and PCEF Instances

This section briefly describes intelligent, on-demand policy objects synchronization between PPT and IPCF, SSC and PCEF instances.

While creating and maintaining policies, PPT application needs to synchronize with IPCF and SSC instances in the deployment to get latest values of all the policy related IPCF as well as SSC objects. If any PCEF instance is part of the PCC deployment then PPT application needs to synchronize with the PCEF such as GGSN or PDSN to get latest values of policy related PCEF objects.

Synchronization can be performed using a script as well as GUI. A synchronization script can be scheduled to be executed periodically. In the PPT Administration menu, users with administrative privileges can access the **Element Summary** GUI to perform synchronization as well as view its status. The synchronization process can be monitored by accessing SNMP traps related to scheduler and synchronization status.

Policy object synchronization allows PPT application:

- Faster access to configurations of all IPCF and SSC instances in the deployment.
- Access to changes performed directly by IPCF and SSC.

PPT application can synchronize following IPCF objects:

- Map profiles
- Data Services
- Timedef
- Quality of Service (QoS) Profiles
- Profiles
- PCC Service
- Dynamic rules

PPT application can synchronize following SSC objects:

- Data plans
- SMS and e-mail notification templates
- Subscription tiers
- Dynamic profile attributes
- Areas

- Regions
- Region lists

PPT application can synchronize following PCEF objects:

- APN names
- Ruledef Names
- Rulebase Names

PPT application synchronizes latest values of all these objects periodically and maintains these values in PPT database. It can be configured to perform synchronization process when Administrators initiate the process by using GUI.

High Availability (HA) Support in the PPT Application

PPT application can monitor processes associated with its components such as:

- Apache Web Server
- PostgreSQL Database Server
- PSMon
- Notification Server
- Scheduler
- Monitor Server

It can also re-start a failed process. Enhanced PPT architecture ensures availability and continuity of PPT application in a transparent manner, in case of hardware failure. This High Availability (HA) feature is implemented using Veritas© Cluster solution.

Three main components of a cluster solution are:

- Active node
- Stand-by node
- Shared Disk

The machines on which PPT is installed are configured as active or stand-by nodes in a cluster. The shared disk is used for data storage which is accessible by all active nodes in the cluster. These nodes share a floating IP address that is used by the client PPT application to securely connect to the PPT server. As each node contains configuration file for PPT application, PPT administer must ensure that both the files are synchronized periodically to avoid inconsistent configuration across PPT cluster.

Important: Same version of PPT application must be installed on active and stand-by nodes. The administrator account that owns and manages the PPT application must have same UID on all nodes.

The shared disk is used for data storage which is accessible by all active nodes in the cluster.

Important: It is not possible to upgrade a standalone PPT installation to the clustered installation supporting HA feature.

Viewing Manageability status of IPCF, SSC and PCEF Instances

This section briefly describes the manageability status of PCC solution components such as various IPCF and SSC instances that are interacting with PPT application. It also describes the manageability of PCEF instance.

In a PCC deployment, PPT application may need to communicate with multiple IPCF as well as SSC instances. PPT application can be configured to exchange information with various IPCF, SSC and PCEF instances. At any given instance some of these instances may not be in an active state, or reachable from the PPT application. Enhanced PPT architecture provides a mechanism that can monitor and display the current status of all configured IPCF, SSC and PCEF instances using a monitor server process for each such instance. PPT application database is always updated with the current status of each instance.

While configuring connections with existing IPCF, SSC and PCEF instances, their manageable status is indicated by green radio button. PPT application does not connect with an un-manageable IPCF, SSC or PCEF instance. Appropriate SNMP alarms are generated upon status change of any such instance.

PPT Architecture

Cisco's Policy Provisioning Tool is a client-server application. It comprises a server and web based GUI client.

PPT server includes following components:

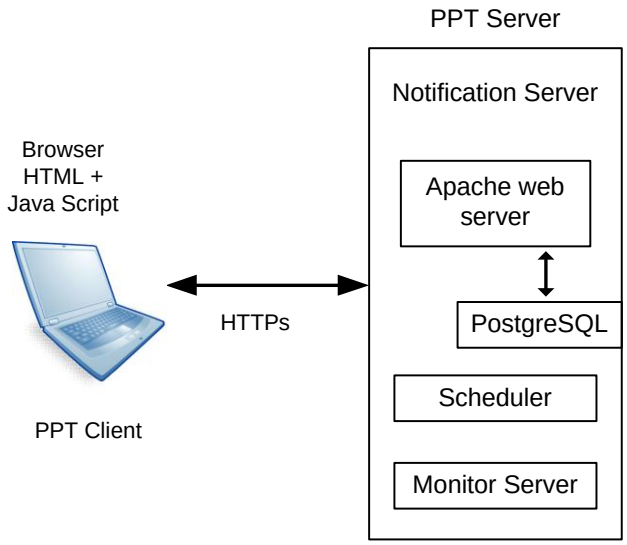
- Apache Web Server
- PostgreSQL Database Server
- PSMon
- Notification Server
- Scheduler
- Monitor Server

PPT client includes following components:

- Browser

Following figure describes PPT architecture:

Figure 2. PPT Architecture



Apache Web Server: Apache server is used to relay requests received from clients to the PPT server.

PostgreSQL Database Server: PostgreSQL RDBMS provides centralized database for most of the data being accessed by different components of PPT. It stores details of users accessing PPT application. Along with user details, it also stores information pertaining to elements such as IPCF and SSC nodes, audit logs of traffic types, rules and rule bases, Access Point Names (APNs), user defined conditions and actions along with configured policies.

PSMon: This is a script which runs as a daemon process on PPT server. It monitors the server components including Apache server, PostgreSQL, and Policy Provisioning Server. PSMon periodically examines state of PPT components and restarts the in-active components. The administrator can configure a PSMon configuration file that contains a list of

components to be monitored along with the time interval after which their state should be examined, and maximum number of retries for restarting a component.

Important: The PSMon configuration file **psmon.conf** is located in *<ppt-install-dir>/3rdparty/psmon* directory.

Notification Server: This is a script which is responsible for generating SNMP v1 or v2 traps including the instances whenever a PPT component is started, stopped or restarted. It also sends traps for events related to Web server, Database and PSMon. The SNMP targets can be configured using the script **confSNMPTarget.sh** located in *<ppt-install-dir>/scripts* directory. PPT administrator can configure a maximum of five SNMP targets at a time, and for each target can specify whether it should receive SNMP v1 or v2 traps.

Important: Notification server checks for the Notification target file after every five minutes, hence changes made to the SNMP target configuration file would not take more than five minutes to come to effect.

Scheduler: Scheduler's responsibility is to trigger different operations at the scheduled time or periodically. One of these tasks is synchronization, the other is to cleanup log files created by PostgreSQL server. Synchronization can be scheduled using parameters from the *<ppt-install-dir>/etc/ppt.cfg* file.

Monitor Server: Monitor server is a background process. It stores the status of all the IPCF, SSC and PCEF instances that are configured in the PPT application. Any such instance can be either manageable or not-manageable, this information is stored in a PPT database. Monitor server process checks whether the configured IPCF, SSC or PCEF instances are manageable or not. If the configured IPCF, SSC or PCEF instances are un-manageable, then PPT client is not allowed to select them.

Browser: This is the only component required at the client side. It is an Internet browser, which requires the Java script and cookies enabled.

System Requirements

This section identifies the minimum system requirements for PPT software, that can be installed on Sun Solaris as well as Linux platform.

Linux Server Hardware Platform:

- Cisco UCS running OS version Cisco MITG RHEL v5.5
- Cisco UCS C210M2 Server
- 2 x Intel Xeon X5675 processors with 32 GB DDR3 RAM
- 2 of 300 GB SAS hard disk drives with 10,000 RPM
- Quad Gigabit Ethernet interfaces

RHEL Operating System Cisco MITG RHEL v5.5 OS is a custom image that contains software packages that are mandatory to support Cisco MITG external software applications. Users must not install any other applications on the platforms running Cisco MITG RHEL v5.5 OS. For detailed software compatibility information, refer *Cisco MITG RHEL v5.5 OS Application Note*.

Sun Server Hardware Platform:

- Sun Solaris or SPARC running OS version SunOS 10
- Sun Microsystems X4270
- 1 x 1.2 GHz 8 core UltraSPARC T2 processors with 16 GB RAM
- 2 x 146 GB SAS hard disk drives
- Quad Gigabit Ethernet interfaces

Ensure that the following patches are installed for Sun Platform:

> ***Important:*** Solaris 10 must be installed using the **End User System support 64-bit** software group and it must be specified during the installation of the operating system. This option installs the libraries required for proper operation of the PPT.

- The timezone patch 113225-07 or later and libc patch 12874-33 or later for extended daylight savings time (DST) support.
- Solaris 10 with Recommended Patch Cluster dated on or after July 16, 2007 and not later than Nov 2008. Ensure that the kernel patch is not later than the stable patch 137137-09

> ***Important:*** Solaris 10 Kernel patch beyond 137137-09 may result in kernel panic while executing or invoking system calls.

Client Platform:

The only requirement at the client side is a browser which supports Java script and cookies enabled. The recommended browsers include Internet Explorer 7 or later and Mozilla Firefox 3.5 or later.

Licenses

Policy Provisioning Tool is not a licensed product.

PPT Deployment and Interfaces

This section describers PPT deployment in a network and various interfaces it uses to communicate with other components of PCC solution such as IPCF and SSC.

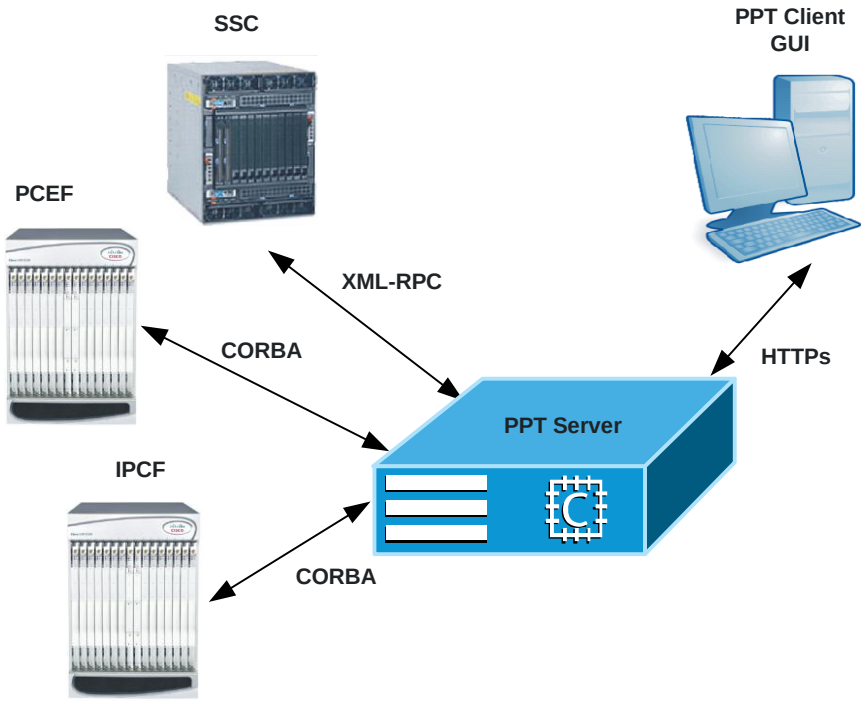
PPT in PCC Environment

In a given PCC environment PPT can be deployed with other components of Cisco PCC solution such as IPCF and SSC.

Following figure describes a network scenario where PPT is deployed along with other components of PCC solution in a network.

Important: In some deployments server components of PPT and Web Element Manager (WEM) applications may share a common hardware platform.

Figure 3. PPT Deployment Scenario



Interfaces

PPT supports following network interfaces for communication with other PCC elements:

- **XML-HTTPPs**: PPT is a client-server application. A browser based policy configuration interface is used to access the data stored on the PPT server. The secure HTTP interface is used by the browser based GUI of PPT to communicate the information with PPT server.

- **XML-RPC**: PPT requires objects such as data or service plans, subscription tiers, notification templates and subscriber profile attributes, to configure and maintain policies. The XML-RPC interface is used to fetch such objects from appropriate Subscriber Service Controller (SSC) instances.
- **CORBA**: PPT requires objects such as Quality of Service (QoS), Policy Charging and Control service, data service as well as time definitions, to configure and maintain policies. CORBA interface is used to fetch these parameters from appropriate instance of Intelligent Policy Control Function (IPCF). The CORBA interface can also be used to fetch objects such as rule definitions, rule bases and APN information from the PCEF, for configuring and maintaining policies.

Chapter 2
Installation Prerequisites

This chapter contains information about the hardware and software prerequisites before installating PPT in stand-alone or cluster mode.

Checklist

Before installing PPT, perform the following checks:

- Do I have the hardware required to setup PPT in cluster mode?
- Do I have VERITAS Cluster Solution 5.1 installed on the machines?
- Do I have the hardware connections made between the cluster nodes?
- Do I have the floating IP address which will be shared between the cluster nodes?
- Do I have the path which will be used as shared-dir path which will be shared between the cluster nodes?
- Do I have the username, password and user Id (UID) which will be used to create PPT administrator? The default value for PPT administrator is *pptadmin*. UID and password for PPT administrator should be same on both the cluster nodes.
- Do I have the directory path which will be used for backup-dir during PPT installation?
- Do I have the names to be used for disk group, disk volume, application resource, NIC resource and IP resource?

Hardware Requirements

This section describes the minimum hardware requirements for installing PPT in stand-alone or cluster mode.

For Stand-alone

This section describes the minimum hardware requirements for PPT software to be installed in stand-alone mode on Sun Solaris as well as Linux platform.

Linux Server Hardware Platform:

- Cisco UCS C210M2 Server
- 2 x Intel Xeon X5675 processors with 32 GB DDR3 RAM
- 2 x 300 GB SAS hard disk drives with 10,000 RPM
- Quad Gigabit Ethernet interfaces

Sun Server Hardware Platform:

- Sun Microsystems Netra x4270 Server
- 1 x 1.2 GHz 8 core UltraSPARC T2 processors with 16 GB RAM
- 2 x 146 GB SAS hard disk drives
- Quad Gigabit Ethernet interfaces

For Cluster

PPT can be configured in cluster with Active/Passive configuration. Hardware prerequisite are as follows:

- 2 UCS or Solaris 10 machines (Cluster Nodes)
    - Solaris
        - Sun Solaris/SPARC running OS version SunOS 10
        - Sun Microsystems Netra x4270 Server
        - 1 x 1.2 GHz 8 core UltraSPARC T2 processors with 16 GB RAM
        - 2 x 146 GB SAS hard disk drives
        - Quad Gigabit Ethernet interfaces
    - UCS
        - CISCO MITG RHEL release 5.5
        - UCS C210M2
        - 2 x Intel Xeon X5675

    - 32 GB DDR3 RAM
    - 4-16 x 600 GB SAS; 6 G, 10,000 RPM
    - Quad Gigabit Ethernet interfaces
- Up to 2 Internal disks (depending upon the fault tolerance for boot disk/OS)
- Qlogic QLE2462 4Gb dual port FC HBA / Qlogic QLE2560 8 Gbps FC 1 port
- FC Cables
- External Storage with multiple disks. It could be EMC or Storage Tek 2540 M2.

Software Requirements

This section identifies the minimum software requirements for installing PPT in stand-alone or cluster mode.

For Stand-alone

This section describes the minimum software requirements for PPT to be installed in stand-alone mode.

Linux Server Hardware Platform:

- **RHEL Operating System Cisco** MITG RHEL v5.5 OS is a custom image that contains software packages that are mandatory to support Cisco MITG external software applications. Users must not install any other applications on the platforms running Cisco MITG RHEL v5.5 OS. For detailed software compatibility information, refer *Cisco MITGRHEL v5.5 OS Application Note*.

Sun Server Hardware Platform:

- Solaris 10 must be installed using the End User System support 64-bit software group and it must be specified during the installation of the operating system. This option installs the libraries required for proper operation of the PPT.

Ensure that the following patches are installed for Sun Platform:

- The timezone patch 113225-07 or later and libc patch 12874-33 or later for extended daylight savings time (DST) support.
- Solaris 10 with Recommended Patch Cluster dated on or after July 16, 2007 and not later than Nov 2008. Ensure that the kernel patch is not later than the stable patch 137137-09.

> ***Important:*** Solaris 10 Kernel patch beyond 137137-09 may result in kernel panic while executing or invoking system calls.

For Cluster

In addition to the above software, Veritas Cluster Server 5.1 must be installed.

Chapter 3
Veritas Cluster Installation and Management

This chapter describes Veritas Cluster Installation and Management.

Veritas Cluster enables one system to failover to the other system. All related software processes are simply moved from one system to the other system with minimal downtime.

The cluster mode functionality enables PPT to provide high availability and critical redundancy support to retrieve data in failure of any one of the systems. Highly available clusters provide nearly continuous access to data and applications by keeping the cluster running through failures that would normally bring down a single server system.

The cluster setup offers several advantages over traditional single-server systems. These advantages include:

- Low entry price compared to traditional hardware fault-tolerant systems.
- Reduce or eliminate system downtime because of software or hardware failure.
- Provide enhanced availability of the system by enabling you to perform maintenance without shutting down the entire cluster.

This chapter contains following sections:

Configuring Veritas Volume Manager and Veritas Cluster

In veritas volume manager, external disks need to be configured and in veritas cluster PPT resources need to be configured.

Veritas Volume Manager

The number of disks in each group depends upon the size of disks in the external storage.

Please contact your system administrator for setting up the external storage to make the required number of disks (luns) accessible from both the cluster nodes. When the external storage disks are made accessible, you can see them connected using multipath command:

```
$ multipath -1

mpath6 (36006016069902d008892bc0dec14e111) dm-7 DGC,RAID 5

[size=300G][features=1 queue_if_no_path][hwhandler=1 emc][rw]

\_ round-robin 0 [prio=0][active]

\_ 8:0:0:1 sdi 8:128 [active][undef]

\_ 8:0:1:1 sdk 8:160 [active][undef]
```

Use the following steps for setting up the external storage disks into separate disk groups:

Step 1 Execute VxVM command to rebuild the disk lists with the new disks detected by the kernel.

```
$ vxdctl initdmp

$ vxdctl enable
```

Step 2 Execute VERITAS **vxdisk** command to see the new disk.

```
$ vxdisk -o alldgs list

DEVICE TYPE DISK GROUP STATUS

disk_0 auto:none - - online invalid

disk_1 auto:none - - online invalid

disk_2 auto:none - - online invalid

disk_3 auto:none - - online invalid

emc_clariion0_30 auto - - error
```

Step 3 Execute the following command to setup the disk:

```
$ /etc/vx/bin/vxdisksetup -i emc_clariion0_30
```

```
[root@pnextappsucs460-1 ~] # vxdisk -o alldgs list
```

Step 4 With the newly initialized disks, create disk group for PPT.

```
$ vxdg init ppt_dg ppt_dg01=emc_clariion0_30
```

Step 5 After adding the disk into respective disk groups, you can verify them by executing **vxdisk** command.

```
$ vxdisk -o alldgs list

DEVICE TYPE DISK GROUP STATUS

disk_0 auto:none - - online invalid

disk_1 auto:none - - online invalid

disk_2 auto:none - - online invalid

disk_3 auto:none - - online invalid

emc_clariion0_30 auto:cdsdisk ppt_dg01 ppt_dg online
```

VxVM ensures that the newly created disk groups are visible from both the cluster nodes. These disk groups can be used only from one node at a time. You have to import/deport a disk group from either node to use the disk groups and their volumes.

Step 6 Next step is to create volumes in the disk groups. Execute the following command to create one volume in each disk group.

```
$ vxassist -g ppt_dg make ppt_vol 299g
```

Step 7 Execute the following command to initialize the volumes with the **vxfs** file system. For better performance, use 4Kb block size and also enable the support for large files (more than 1 TB).

```
$ mkfs -t vxfs -o bsize=4096,largefiles /dev/vx/rdsk/ppt_dg/ppt_vol
```

Step 8 Create the mount point and execute the following command to mount the volumes.

```
$ mount -t vxfs -o largefiles /dev/vx/dsk/ppt_dg/ppt_vol /shared_ppt
```

Important: The /shared_ppt should be entered for **Shared Disk Path** in **Install Mode Configuration** screen during installation.

Veritas Cluster

This section describes PPT resource configuration in Veritas Cluster.

To explain how to configure PPT resources in Veritas Cluster, consider the following example:

- Shared disk path:/shared_ppt
- Shared IP: 10.4.83.151
- PPT shared directory: /shared_ppt

- PPT installation directory: /users/ppt
- PPT PostgreSQL data directory: /shared_ppt/3rdparty/postgres/data
- Shared IP address: 10.4.83.151 (could be on NIC eth0)
- Cluster nodes are: pnstextappsucs1 and pnstextappsucs3

Step 1 Execute the following commands to create Resource Group (named ha) for PPT and add nodes to it.

```
hagrp -add ppt-ha

hagrp -modify ppt-ha SystemList -add  pnstextappsucs1 1 pnstextappsucs3 2
```

Step 2 Execute the following commands to create Disk Group resource for PPT partition.

```
$ hares -add ppt-apps-dg DiskGroup ppt-ha

$ hares -modify ppt-apps-dg DiskGroup ppt_dg

$ hares -modify ppt-apps-dg Enabled 1
```

Step 3 Execute the following commands to create volume resource for PPT partition.

```
$ hares -add ppt-apps-vol Volume ppt-ha

$ hares -modify ppt-apps-vol DiskGroup ppt_dg

$ hares -modify ppt-apps-vol Volume ppt_vol

$ hares -modify ppt-apps-vol Enabled 1
```

Step 4 Execute the following commands to create mount resource for PPT partition.

```
$ hares -add ppt-apps-mnt Mount ppt-ha

$ hares -modify ppt-apps-mnt MountPoint /shared_ppt

$ hares -modify ppt-apps-mnt BlockDevice /dev/vx/dsk/ppt_dg/ppt_vol

$ hares -modify ppt-apps-mnt FSType vxfs

$ hares -modify ppt-apps-mnt FsckOpt %-y

$ hares -modify ppt-apps-mnt MountOpt largefiles

$ hares -modify ppt-apps-mnt Enabled 1
```

Step 5 Execute the following commands to create application resource for PPT processes.

```
$ hares -add ppt-app Application ppt-ha

$ hares -modify ppt-app User pptadmin

$ hares -modify ppt-app StartProgram "<ppt-install-dir>/pptctl start"

$ hares -modify ppt-app StopProgram "<ppt-install-dir>/pptctl forcestop"
```

```
$ hares -modify ppt-app PidFiles "<ppt-install-dir>/3rdparty/psmon/psmon.pid"

$ hares -modify ppt-app Enabled 1
```

Step 6 Execute the following command to set the **Critical** attribute of the above created application resource to **0**.

```
$ hares -modify ppt-app Critical 0
```

Step 7 Execute the following commands to create the NIC resource.

```
$ hares -add ppt-nic NIC ppt-ha

$ hares -modify ppt-nic Device eth0

$ hares -modify ppt-nic Enabled 1
```

Step 8 Execute the following commands to create the IP resource.

```
$ hares -add ppt-ip IP ppt-ha

$ hares -modify ppt-ip Device eth0

$ hares -modify ppt-ip Address 10.4.83.151

$ hares -modify ppt-ip NetMask 255.255.255.0

$ hares -modify ppt-ip Enabled 1
```

Step 9 Execute the following commands to set the resource dependencies.

```
$ hares -link ppt-app ppt-apps-mnt

$ hares -link ppt-apps-mnt ppt-apps-vol

$ hares -link ppt-apps-vol ppt-apps-dg

$ hares -link ppt-app ppt-ip

$ hares -link ppt-ip ppt-nic
```

Step 10 Execute the following command to create AutoStartList and add the node in the list.

```
$ haconf -makerw
$ hagrp -modify ppt-ha AutoStartList pnstextappsucs1
$ haconf -dump
```

Verifying the Cluster Setup

Once VCS is installed and PPT resources are configured in VCS setup, cluster setup needs to be verified.

Step 1 The following command can be used to verify that the configuration.

```
hastatus -sum
```

This command will provide the summary of HA resources. Output would be similar to the one shown below:

```
[root@pnqaems-ucs1 ~]# hastatus -sum

-- SYSTEM STATE

-- System State Frozen

A pnqaems-ucs1 RUNNING 0

A pnqaems-ucs2 RUNNING 0

-- GROUP STATE

-- Group System Probed AutoDisabled State

B ems-rg pnqaems-ucs1 Y N OFFLINE

B ems-rg pnqaems-ucs2 Y N OFFLINE

B mur-rg pnqaems-ucs1 Y N OFFLINE

B mur-rg pnqaems-ucs2 Y N PARTIAL

B ppt-rg pnqaems-ucs1 Y N ONLINE

B ppt-rg pnqaems-ucs2 Y N OFFLINE
```

Veritas Cluster Files

Veritas Cluster log and config files can be used for troubleshooting and monitoring the VCS.

The below mentioned log and config files are useful:

- **Log File:** The log file contains the veritas logs like some resource has stopped on one node and some resources have started on other node. Log file name is appended by letters. Letter A indicates the first log file, B the second, C the third, and so on. The engine log is located at /var/VRTSvcs/log/engine_A.log.
- **Config File:** The cluster configuration information is stored in this file. This file also includes service group and resource dependency clauses. The config file is located at /etc/VRTSvcs/conf/config/main.cf.

Chapter 4
Installing the PPT Software

This chapter provides information and procedures to install and configure Policy Provisioning Tool (PPT) a component of Cisco Policy Charging and Control (PCC) solution.

PPT provides a GUI based as well as console based installer that can be used for installing, configuring and upgrading the PPT application. It installs all the components of client-server application.

The installer also creates users with appropriate access privileges that are required to administer the PPT deployment.

PPT provides necessary scripts for post installation configuration and administration tasks such as:

- Viewing status of processes related to PPT components.
- Starting or stopping the processes related to PPT components.
- Generating backup of PPT database as well as configuration files.
- Vacuuming the database.
- Cleaning the database.
- Generating support detail information such as different categories of logs and output of system commands.

Important: Most of these scripts except the PPT Component Control (pptctl) script, are located in<*ppt-install-dir*>*/scripts* directory along with their read me files, where as the **pptctl** script is located in <*ppt-install-dir*>directory.

This chapter includes the following sections:

Before You Begin

This section includes the information required to initiate the installation process.

This section includes following sub-sections:

- Unpacking the PPT Application Archive
- Choosing a Method for Installing PPT Application
- Configuring Environment Variables for PostgreSQL
- PPT Network and Protocol Considerations
- Default TCP Port Utilization

Unpacking the PPT Application Archive

This section lists the contents of PPT installation archive.

PPT installation package is distributed as a zip archive. Copy this archive in a temporary directory on the PPT server. This archive contains following files:

- inst
- Readme
- setup.bin

> ***Important:*** Installer installs PPT application along with all its components in <*ppt-install-dir*> directory.

Root access privileges are required for executing **`./inst`**.

> ***Important:*** The `./inst` script installs PPT application components using console or GUI method. You can view help by using the command `./inst - help`.

Choosing a Method for Installing PPT Application

This section lists the PPT components to be installed and available installation methods.

> ***Important:*** Installation procedure can be performed only by users with root administrative privileges.

PPT client and server application along with its components can be installed using either GUI or console based installation method.

Requirements for GUI based method are:

- Root access privilege to the PPT server with a display terminal and an active X-Windows application such as Xming or eXceed.

- Network connectivity to PPT server via Telnet or SSH using X-windows client from remote work station.

A user with root access privilege for PPT server, but without access to remote network connectivity or X-windows application can use the console based installation method to install PPT application.

Configuring Environment Variables for PostgreSQL

This section lists environment variables required for PostgreSQL database component of PPT application.

PostgresSQL RDBMS is installed by the PPT installer. Following environment variables determine the interaction of PostgreSQL database with underlying file system to process, store and retrieve the information contained within the database tables. Ensure that these variables are set accordingly.

For Solaris: Update the values of the following variables in */etc/system* file and reboot the server:

- shmsys:shminfo_shmmax=0x20000000
- shmsys:shminfo_shmmin=1
- shmsys:shminfo_shmmni=256
- shmsys:shminfo_shmseg=256
- semsys:seminfo_semmap=256
- semsys:seminfo_semmni=512
- semsys:seminfo_semmns=512
- semsys:seminfo_semmsl=32

For Linux: Update the values of the following variables in */etc/sysctl.conf* file and reboot the server:

- kernel.shmmax=536870912
- kernel.shmall=2097152

PPT Network and Protocol Considerations

This section lists the network and protocol requirements for PPT application.

For proper installation and operation of PPT application, following network and protocol considerations must be implemented:

- The Network Address Translation (NAT) or Port Address Translation (PAT) protocol should not be enabled between IPCF and PPT servers.
- If a firewall is installed between PPT server and the IPCF, then a port must be opened in this firewall that can be used by PPT server to access IPCF platform. Refer Default TCP Port Utilization section for more information.
- If a firewall is installed between PPT server and PPT clients, then a port must be opened in this firewall that can be used by PPT clients to access PPT server. Refer Default TCP Port Utilization section for more information.

Default TCP Port Utilization

This section briefly describes TCP port utilization and lists ports available for communication.

PPT application uses TCP ports to communicate with other components of PCC solution such as IPCF and SSC as well as for communication between PPT server and clients. If a firewall is configured in the deployment, and any PPT client or some other components of PCC solution with which PPT needs to communicate are beyond this firewall, then TCP ports need to be opened in the firewall to ensure communication. Following table lists required TCP ports and their usage.

Table 1. Default TCP Port Utilization Table

Port Number	Communication Type	Usage
TCP Port:		
443	PPT Client to PPT Server (Secured)	Used for XML-HTTPS client-server communication. This port is configurable.
14131	PPT Server to IPCF	Used for CORBA communication. This port is configurable.
9292	PPT Server to SSC	Used for XML-RPC communication. This port is configurable.

PPT Installation Methods

There are two modes in which PPT can be operated.

- **Stand-alone Mode:** This is normal operation mode.
- **Standby/Cluster Mode:** If this mode is used then user should provide the IP address which will be used by PPT client to communicate with PPT server. This mode is to be used for enabling High Availability feature in PPT.

> ***Important:*** Since configuration file is on the nodes and not on the shared disk, so changes done on one node need to be synchronized on other node. The onus of synchronization is on the user. While adding PPT administrator, user has to make sure that the same user is being added on both the nodes. The password and UID of the user on both nodes should be same. The system time and timezone on both the cluster nodes must be same or NTP synchronized. Else session related issues will take place after switchover. PostgreSQL username and password should be same on both the nodes.

This section list various PPT installation methods that can be used.

- GUI Based Installation Mode
- Console Based PPT Installation

GUI Based Installation Mode

Following task describes how to install PPT using the GUI based installation wizard.

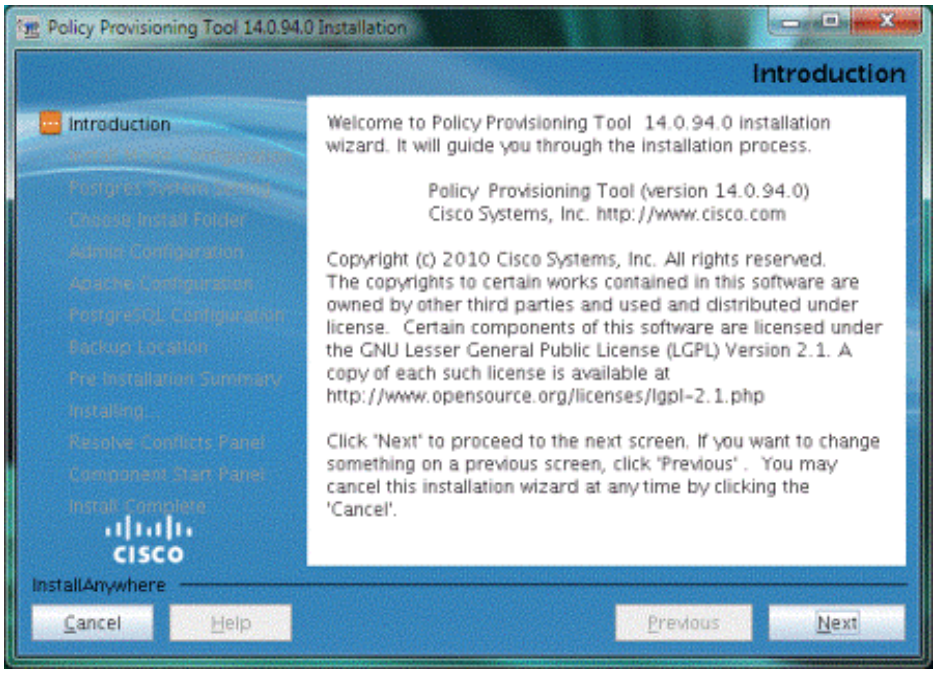
Step 1 Log-in as a user with root administrative privileges to the server where you want to install PPT application.

Step 2 Access the directory that contains files extracted from PPT installation archive.

Step 3 Execute the installation script by issuing following command:

```
./inst
```

The PPT Installer displays introduction screen:



Step 4 Click **Next** to proceed.

Step 5 Proceed with the installation process by following on-screen prompts to configure required installation parameters. Refer following table for description of such parameters.

Step 6 **GUI Based Installation Parameters**

Parameter	Description	Default Value
Install Mode Configuration		
Mode Selection	On this screen, the Stand-alone installation or Cluster mode installation can be selected. ***Important:*** For Cluster mode installation, Veritas Cluster Server needs to be installed and configured. For more information, refer to *Veritas Cluster Installation and Management* chapter.	For Stand-alone: N/A For Cluster: Host IP Address and Shared Disk Path
Postgres System Setting		
N/A	This section is informational and contains no configurable parameters. Information pertaining to these variables is located in the Configuring PostgreSQL Database System Environment step of the Before You Begin section in this chapter.	N/A
Choose Install Folder		
Directory Path	The directory path on the server where the PPT is to be installed. This directory path can be manually entered in the field provided or selected using the **Browser**.	*/<ppt-install-dir>/* which is */users/ppt* by default for Linux.

Parameter	Description	Default Value
PPT Administrator Account Configuration		
PPT Administrator Account	This is an account with administrative privileges that owns and manages the PPT application.	N/A
Admin Login	Enter the administrator login name. ***Important:*** This is the OS level administrator user of PPT application. The admin login can be an existing user, or it can be a new user that is created during installation.	pptadmin
Admin Password	Enter the administrator password. If the administrator user already exists, then password is not required. The password is case sensitive. ***Important:*** If a new user is created, password is mandatory.	N/A
UID	The user ID which should be used to create PPT administrator. ***Important:*** During installation care has to be taken that UID for PPT administrator should be same on both the cluster nodes. For this reason the UID will be accepted from user during installation. This UID will be used to create PPT administrator user. If the UID is already assigned to some other user a dialog will pop-up and user will be asked to enter a different UID. If PPT administrator already exists on the node then the UID will be displayed automatically on the screen. While doing installation on second node the user is supposed to enter the same UID during installation. If PPT administrator already exists then, PPT administrator will have to be deleted and again created using the new UID provided during installation.	N/A
Apache Server Configuration		
Apache Port (HTTPS)	This is a TCP port that will be used by the Apache server for secure communication with PPT client. Specify an integer value, default value is 443. ***Important:*** All connections between PPT server and client must be of SSL type such as HTPPS. Non-secure connections are not allowed.	443
PostgreSQL Configuration		

Parameter	Description	Default Value
User Name	Enter a username for the Postgres database administrator. ***Important:*** User name of PostgreSQL administrative account must be different from all other Postgers related roles or account names.	pptadmin
Password	Enter a password for the Postgres database administrator. The password is case sensitive.	N/A
Port	Enter the port number on which the Postgres server should listen to connections from client applications. Default port number is 5432. ***Important:*** If you specify a port number other than the default port then all client applications, including PSQL must specify the same port for communication. ***Caution:*** If PPT and ASR5k Web Element Manager (WEM) are co-located on single hardware platform, then ensure that ASR5k WEM is installed before PPT and PostgreSQL component of PPT is not listening on port 5432. As this port is reserved for ASR5k WEM.	5432
Backup Location		
Backup directory location	The backup will be taken at this location. ***Important:*** This path must be on the local disk where PPT is being installed or on shared disk.	For Stand-alone mode, the default path is *<ppt-install-dir>/backup_dir* . For Cluster mode, the default path is *<shared-directory-path>/backup_dir* .
Pre-Installation Summary		
	This section is informational and contains information of configurable parameters. Verify all the installation configurations and, click **Install** to proceed with installation.	N/A
Installing Policy Provisioning Tool Panel		
	This panel displays the PPT application installation progress bar and contains no configurable parameters.	N/A
Component Start Panel		

Parameter	Description	Default Value
Select the components to be started	Select the PPT software component that needs to be started as part of the installation. The option to start all PPT components after installation is available. ***Important:*** Successful installation of the PPT application requires the **Apache Server** to be started. Default setting is to enable or start Apache server. Though prompts are provided to disable the server, it is highly recommended not to modify the default values.	Enabled
Start components after system reboot	Select this option so that PPT components will start automatically, each time the server on which it is installed, is rebooted.	Enabled
Install Complete Panel		
	This panel displays information regarding successful completion of installation, along with the commands to start PPT application via command line interface. You can also find the PPT installation log file at the mentioned path on this panel. The installation log is stored in a file **Policy_Provisioning_Tool_InstallLog.log file**, located in <*ppt-install-dir*> directory.	N/A

Step 7 This step is specific to Cluster mode. Please read the note below to perform the operation.

Important: If the installation is done on node 1 then /var/.com.registry.xml file is created on node1. When PPT is installed on node 2, it is important to install same version of PPT on node 2. During PPT upgrade, installer will refer to the registry file located at /var/.com.registry.xml on the individual node. This is required since the upgrade is always done on standby node which does not have access to the shared disk.

Step 8 Click **Done** to exit the GUI based installation wizard.

After the installation is complete, you can access PPT application GUI by entering following URL in the address bar of the browser in client machine:

```
https://<ip_address>:<port_number>/

https://<host_name>:<port_number>/
```

where *ip_address* and *host_name* is the IP address of the machine where PPT server component is installed and *port_number* is the port number to which apache server is listening for the client requests. In case of the default port, URL should be limited to the *ip_address* or *host_name* only.

Important: Contact Cisco support for default Username and Password in order to login to the PPT application after installation.

Console Based PPT Installation

Following task describes how to install the PPT application using console:

Step 1 Log-in with administrative access privilege to the server where you want to install PPT application.

Step 2 Access the directory that contains files extracted from PPT installation archive.

Step 3 Execute the installation script by issuing following command:

```
./inst -i console
```

Installer displays a series of messages as listed below:

```
Extracting the JRE from the installer archive...

Unpacking the JRE...

Extracting the installation resources from the installer archive...

Configuring the installer for this system's environment...

Launching installer...

Preparing CONSOLE Mode Installation...
```

Step 4 Enter **N** (Next Step) to proceed.

Step 5 Proceed with installation by following on-screen prompts to configure required installation parameters. Refer table *GUI based Installation Parameters* for detailed description of these parameters.

After successfully installing the PPT application, installer displays following messages:

```
Install Complete

----------------

Policy Provisioning has been successfully installed to:

<ppt-install-dir>

Installation logfile located at:

<ppt-install-dir>/PolicyProvisioning_InstallLog.log

Start Policy Provisioning component as:

cd <ppt-install-dir>

./pptctl start

./pptctl stop
```

After the installation is complete, you can access PPT application GUI by entering following URL in address bar of the browser from client machine:

```
https://<ip_address>:<port_number>/

https://<host_name>:<port_number>/
```

where *ip_address* and *host_name* is the IP address of the machine where PPT server is installed and *port_number* is the port number to which apache is listening for the client requests. In case of default port number, the URL should be limited to the *ip_address* or *host_name* only.

Important: Contact Cisco support for default Username and Password in order to login to the PPT application after installation.

Chapter 5
Verifying the PPT Installation

This chapter briefly describes post-installation verification procedures for PPT server as well as client components.

Policy Provisioning Tool (PPT) is a client- server application. For proper functioning of the application you need to verify that both the server and client components are installed properly, are compatible with each other and required server processes are running on the PPT server.

This chapter includes following sections:

Server Verification

This section briefly describes how to verify that server component of PPT application is installed completely and is compatible with client component.

Perform following verifications for the PPT server component:

- Check the version of the installed PPT server software component. By issuing the command **`pptctl version`**. Ensure that it matches with version of client component of PPT application, to avoid client –server compatibility issues. Refer to *PPT Components Control Script* section of the *Administrative Scripts* chapter for more information.
- Ensure that processes related to the PPT server components such as PostgreSQL RDBMS, Apache and Notification Servers as well as PsMon are active and running by issuing the command **`pptctl status`**.

Client Verification

This section briefly describes how to verify that client component of PPT application is installed completely and is compatible with server component.

Perform following verifications for PPT client component:

- Using recommended browser access the PPT application by invoking the URL

  https://<ip_address>:<port_number>/

  https://<host_name>:<port_number>/

  where, *ip_address* and *host_name* is the IP address of the machine where PPT server is installed and *port_number* is the port number to which apache is listening for the client requests.
- Ensure that PPT log-in page is accessible.
- Log-in to PPT application with the username and password provided by Cisco Support.
- Verify the version of the PPT application by clicking the *About* link from the top navigation bar. It should match with the version of PPT server derived in previous section.

Chapter 6
PPT Administration

This chapter describes how to configure and administer the PPT application.

Policy Provisioning Tool (PPT) is an element of Cisco Policy Charging and Control (PCC) solution. PPT acts as a GUI based policy management tool used by service providers to design, implement and maintain policies. These policies can be used to provide various services to subscribers as well as control network usage via differential policies for different subscribers.

PPT application provides a GUI based wizard to perform following activities in the policy configuration and management process:

- Mapping attributes to a subscriber profile. This profile is used as a benchmark for applying policy to existing subscribers.
- Configuring session based usage monitors for the policy.
- Associating single or multiple data plans with the policy.
- Configuring the business logic for the policy using rules, rule bases as well as user defined actions and conditions.
- Generating a summary of the configured policy.
- Committing or transferring the configured policy to relevant IPCF instance.

Important: Refer on-line help of PPT application for more information and tasks related to configuration and maintenance of policies as well as configuration of IPCF and SSC instances in the PPT application.

PPT is an integral part of PCC solution and works in conjunction with other PCC components such as Intelligent Policy Control Function (IPCF) and Subscriber Service Controller (SSC) for policy management. PPT administration includes tasks such as:

- Configuring IPCF instances in the PPT application for provisioning IPCF related policy parameters such as QoS profiles or dynamic rules.
- Configuring SSC instances in the PPT application for provisioning SSC related policy parameters such as data plans or subscription tiers.
- Configuring PCEF instances in the PPT application for provisioning PCEF related policy parameters such as APN names, Ruledef names and Rulebase names.
- Administering users for the PPT application.
- Generating application monitoring information such as audit trail and debug information.

This chapter includes following sections:

- Synchronization
- User Administration
- Change Password
- Debug Information
- Audit Trail

Important: On user login, **Administration** or **Subscriber Service Management** page is displayed based on configuration present in the database. If IPCF and SSC are configured then **Subscriber Service Management** page is displayed. If either IPCF or SSC is not configured, then the default page is **Administration** page.

IPCF Setup

This section describes how to configure an IPCF instance in the PPT application.

The Intelligent Policy Control Function (IPCF) provides policy control and charging rule function in a core network. IPCF is supplemented by usage monitoring capability that is enabled by the policies related to data consumption and usage monitoring.

PPT acting as an integral part of the PCC solution, allows service providers to create, update and monitor policies using local libraries of rules and rule bases, as well as Access Point Names (APNs) that exist with Policy Control and Enforcement Function (PCEF).

Important: For detailed information and configuration examples of IPCF, refer the *IPCF Administration Guide*.

To configure an IPCF instance in the PPT application, following information is required:

- **IPCF Name**: This is the name of IPCF instance. User can specify any name by which this IPCF instance is to be identified.
- **IP Address**: This is the IP or IOP address for CORBA to communicate with Cisco© chassis running the IPCF instance. This IP address can be retrieved by executing **`show orbem status`** command on chassis. A sample output of this command is shown below:

```
Service State : On

Management Functions : FCAPS

IOP Address : 10.4.10.35

SSL Port : 12125

TCP Port : 12126

Session Timeout : 300 secs

Max Login Attempts : 3

IIOP Transport : On

Number of Current Sessions : 0

Number of Operations Completed : 504

Number of Events Processed : 0

Avg Operation Processing time : 7396 usecs

(last 1000) : 7519 usecs
```

- **Port Number**: This is the TCP port over which the CORBA could communicate with an IPCF instance. This port number must be identical to the IIOP port setting on the IPCF. It can also be retrieved using the **`show orbem status`** command.

Important: IP address and Port number of the chassis can be obtained from IPCF administrator.

Caution: If PPT and Web Element Manager (WEM) are co-located on single hardware platform, then ensure that WEM is installed before PPT and PostgreSQL component of PPT is **not** listening on port 5432 as this port is reserved for WEM.

- **Application Server ID**: This is the ID by which the PPT instance is identified by IPCF server. The application server id can be retrieved by executing **`show orbem client table`** command on Cisco© chassis.

  Application server Id is set on the IPCF chassis by executing commands similar to following set of commands using Command Line Interface (CLI) in EXEC Mode:

  ```
  [local]asr5000#configure

  [local]asr5000(config)#orbem

  [local]asr5000(config-orbem)#client id client_id password password
  ```

  This information can be retrieved by executing the **`show configuration`** command. The sample output of this command is shown below:

  ```
  orbem

  iiop-transport

  client id STARENT encrypted password 5c4a38dc2ff61f72
  ```

  Caution: If PPT and WEM are co-located on a single hardware platform, then ensure that, for the CORBA management both PPT and WEM are using different application server ids.

- **Application Server Password**: This is the password set for the ORBEM client configuration as shown in the above sample set of command lines. It is used by PPT application to communicate with the IPCF instance.

  Important: Application server ID and password information can be obtained from the IPCF administrator.

- **Node Type**: A PCC deployment can contain multiple IPCF instances. An IPCF instance can be designated as a **Primary** or **Secondary**. At any given instance only one IPCF instance can be designated as Primary, where as multiple IPCF instances can be designated as Secondary. PPT communicates with Primary IPCF instance to exchange information such as PCC and data service, user defined conditions and actions, timedefs and traffic types.

Important: An IPCF instance can be configured in the PPT application even if it is not active or manageable, provided that correct values of all the configuration parameters mentioned above are available.

SSC Setup

This section describes how to configure an SSC instance in the PPT application.

Subscriber Service Controller (SSC) is a component of PCC solution. It acts as a Subscriber Profile Repository (SPR) for maintaining subscriber profile and service usage data. SSC uses centralized Policy Charging and Rules Function (PCRF) along with the SPR data store to assist policy implementation. SSC handles session state and account details information for subscribers. SSC also manages the event notification function for the PCC solution by sending e-mails and text messages to subscribers. SSC interacts with other components of PCC solution such as Customer Relationship Management (CRM), Operation Support System (OSS), and Billing Support System (BSS) for subscriber related information.

PPT interacts with an SSC instance using an XML-RPC interface and HTTP as a data transport mechanism.

To configure an SSC instance in the PPT application, following information is required:

- **SSC Name**: This is the name entered to identify the SSC machine where the profile controller of an SSC instance is installed.
- **Main SSC IP Address**: This is the IP address of the host on which SSC profile controller is running.

  Important: SSC supports geo-redundancy with multiple SSC instances in different geographical locations. Each SSC instance can be accessed by the PPT application, by using IP address of the host on which profile controller of SSC is running. For the PPT application, only one SSC instance can be configured as a **Primary** instance and all other SSC instances are configured as **Secondary**.

- **Port Number**: This is the port using which the XML-RPC could communicate with profile controller interface of the active SSC instance. Default value for this port is 8080.
- **Standby SSC IP Address**: This is the IP address of host machine on which profile controller of the standby SSC instance is running.

  Important: In a geo-redundant setup, there will be two physical SSCs each addressable with a different IP address. In case of a failover to the redundant SSC, administrator has to manually change the standby node to active in the PPT application. There is no automatic detection of SSC instance fail-over. Once the main node start working normally, administrator has to manually change the node back to Active. Primary SSC can also be active SSC if only the geo-redundancy is configured on SSC. IP address and Port information can be retrieved through the Apache configuration file *httpd.conf* or, it can be obtained from SSC administrator.

- **Node Type**: Select **Primary** or **Secondary** from drop-down list.

  Important: When configuring an SSC node into the system, it has to be designated as primary/secondary. Primary node is like a reference node and all data which is displayed to the user is fetched from the node which is designated as the primary. While configuring an object on any of the nodes, it is mandatory to configure on the primary. So, user can configure on primary and secondary nodes but it is mandatory to configure on primary. The assumption is that all nodes added into PPT will have the same configuration.

Important: An SSC instance can be configured in the PPT application, even if it is not active or manageable, provided that correct values of all the configuration parameters mentioned above are available.

PCEF Setup

This section describes how to configure an PCEF instance in the PPT application.

Policy and Charging Enforcement Function, the logical function in 3GPP network is responsible for enforcing the policy and charging as per PCC rules.

PCEF, typically located at the gateway is responsible for enforcing the policy and charging related decisions received from PCRF. PCEF performs service data flow detection as well as gate enforcement for the data flows.

The functions done by PCEF are mainly to:

- Detect service data flows.
- Perform gate control over flows.
- Bearer binding as well issue bearer procedures.
- QoS enforcement based on the authorized policy decision.
- Perform charging based on the charging decision supplied by PCRF.

IPCF interfaces with Policy Charging and Enforcement Function (PCEF) over standard Gx interface. IPCF handles operation of PCC Rule and activate/deactivate/install/modify/remove the PCC rules at PCEF. PCC rule operation may fail on PCEF due to various reasons. In such failure cases PCEF sends back a Charging Rule Report containing PCC rules failed and corresponding failure cause.

Important: PPT server will fetch APNs, ruledef and rulebase directly from PCEF and cannot be configured/modified using PPT application client.

To configure an PCEF instance in the PPT application, following information is required:

- **PCEF Name**: This is the name of PCEF instance. User can specify any name by which this PCEF instance is to be identified.
- **IP Address**: This is the IP or IOP address for CORBA could communicate with Cisco© chassis running the PCEF instance. This IP address can be retrieved by executing **`show orbem status`** command on chassis. A sample output of this command is shown below:

```
Service State : On

Management Functions : FCAPS

IOP Address : 10.4.10.35

SSL Port : 12125

TCP Port : 12126

Session Timeout : 300 secs

Max Login Attempts : 3

IIOP Transport : On

Number of Current Sessions : 0
```

```
Number of Operations Completed : 504

Number of Events Processed : 0

Avg Operation Processing time : 7396 usecs

 (last 1000) : 7519 usecs
```

- **Port Number**: This is the TCP port over which the CORBA could communicate with an PCEF instance. This port number must be identical to the IIOP port setting on the PCEF. It can also be retrieved using the **`show orbem status`** command.

  Important: IP address and Port number of the chassis can also be obtained from PCEF administrator.

  Caution: If PPT and Web Element Manager (WEM) are co-located on single hardware platform, then ensure that WEM is installed before PPT and PostgreSQL component of PPT is **not** listening on port 5432. As this port is reserved for WEM.

- **Application Server ID**: This is the ID by which the PPT instance is identified by PCEF. The application server id can be retrieved by executing **`show orbem client table`** command on Cisco© chassis.

  Caution: If PPT and WEM are co-located on a single hardware platform, then ensure that, for the CORBA management both PPT and WEM are using different application server ids.

- **Application Server Password**: This is the password used by PPT application to communicate with the PCEF.

  Important: Application server ID and password information can be obtained from the PCEF administrator.

- **IPCF Controller**: This is the IPCF that could communicate to the PCEF and conveys the policy and charging related decisions. The relation between PCEF and IPCF could be many to 1 i.e., multiple PCEF's communicating to one IPCF.

Synchronization

This section describes various synchronization approaches.

PPT has to synchronize the IPCF/SSC/PCEF instances on the known/configured IPCFs, SSCs and PCEFs. The following are the reasons for synchronization:

- PPT has faster access to the configuration on all IPCFs/SSCs/PCEFs.
- Any changes made directly on the IPCF CLI or on the SSC or on the PCEF are also available at the PPT with some delay.
- PPT can do configuration comparisons across different IPCFs/SSCs/PCEFs.
- Reduce network traffic between the PPT server and IPCFs/SSCs/PCEFs.
- Synchronization helps in optimization of condition groups and action sets.

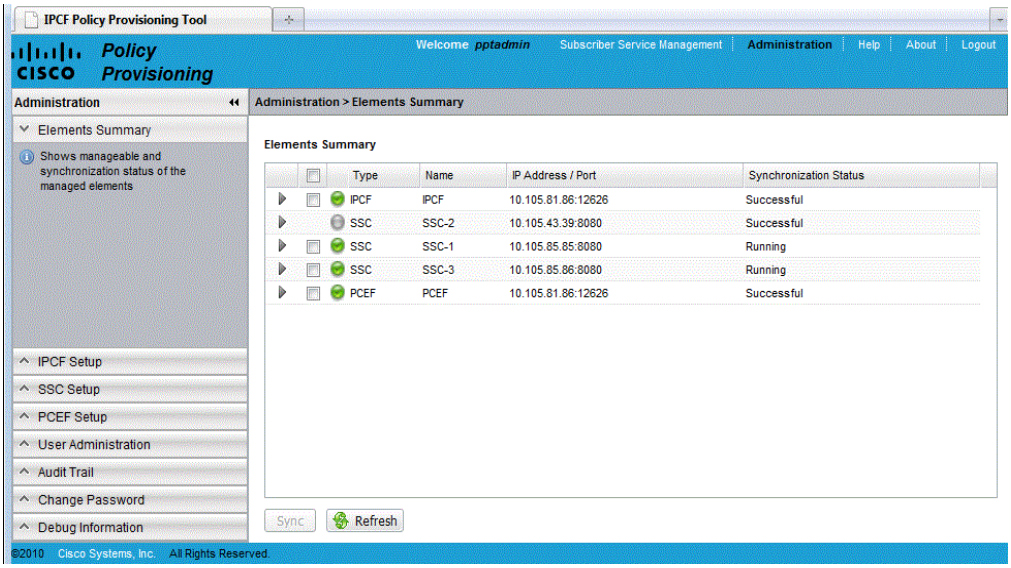
The following are various approaches used for synchronization:

- Manual Synchronization
- Automatic Synchronization

Manual Synchronization

Manual synchronization synchronizes IPCF/SSC/PCEF data when request is received from user. The possibilities could be to synchronize with all IPCFs/SSCs/PCEFs or only the selected IPCFs/SSCs/PCEFs. This type of synchronization can be supported through GUI and/or shell script.

The following figure displays Synchronization screen.



You can select an element to be synchronized and click **Sync** to synchronize. In the above figure, the **Synchronization Status** of SSC-1 and SSC-3 is **Running**, i.e., the synchronization is under process. For rest of the elements the status is **Successful**, i.e., the synchronization is complete.

Advantages:

Manual synchronization can be used at any time when there is a need to synchronize with IPCFs/SSCs/PCEFs. For example., if the operator does some changes directly on IPCFs/SSCs/PCEFs or knows that some changes have been done, then, manual synchronization can be done to get the changes in PPT.

Automatic Synchronization

Automatic synchronization takes place only when IPCF/SSC/PCEF state changes to manageable. It can happen that there are many state changes like manageable - unmanageable, unmanageable - manageable within a short time period. These changes can be due to network issues or they could be genuine state changes because of software malfunctioning on the IPCF/SSC/PCEF platform. To handle this scenario and to avoid repeated synchronization attempts because of this:

- API checks the 'last successful synchronization attempt time' and if it is more than an hour then only state change synchronization take places.
- The 'short time period' is configurable and the default is 1 hour.

Also when a new manageable IPCF/SSC/PCEF instance is added in PPT, the synchronization takes place automatically. Also when an IPCF/SSC/PCEF instance is deleted from PPT, then all the information related to that IPCF/SSC/PCEF instance is removed from the PPT database.

User Administration

This section describes how to administer users and generate audit trail as well as debug information.

For each user accessing the PPT application, a unique ID and password is provided. PPT application categorizes users as administrator and operator. Administrator user has the privileges to perform all the possible operations in the PPT application, where as only viewing privileges are provided to the operator user. The Operator user cannot add, delete, or modify any service or configuration using PPT application.

While adding a new user for the PPT application, the **Session Timeout** is set for the user. This time is set in number of minutes which ranges from 1 to 1440 minutes. With this session timeout setting, a user session expires when no request-response happens between the PPT client and PPT server during the prescribed time interval.In such a scenario the user has to login again and initiate a new session to access the PPT application.

Important: PPT installation creates a default user. The login credentials of this user can be used to create other users and assign administrator or operator roles to them. It is recommended that you change the password of the default user on first login. Contact Cisco support for the default username and password. The default session timeout for this user is 15 minutes.

The privilege, session timeout, and password for the users added through PPT application can be modified later, however the user ID once configured, is not allowed to be modified.

Important: Refer on-line help of PPT application for tasks related to user administration such as adding or modifying user credentials.

Change Password

PPT administrator can reset the application password of any other user using the **Modify** button in **User Administration** option. A logged-in user can change his or her password using **Change Password** option.

Debug Information

The debug information can be used for troubleshooting as well as monitoring purpose. PPT application logs information related to processes associated with its components such as Apache and notification server, PostgreSQL database.

Debug Information provides following options to generate this data:

- **Level 1**: Choosing this option, user can access application, installation as well as web server logs. The following is the list of the commands for level 1:
  - `getLogDir`
  - `getFile`
  - `getDirectory`
  - `executeCommand`
  - `getDirectory`
- **Level 2**: Choosing this option user can access all level 1 logs along with database logs.

PPT application generates the **pptsupportDetails.tar** archive containing detailed logs as per the selected level. This tar archive contains certain log files, PPT and PsMon configuration files as well as output of some system commands.

pptsupportDetails.tar archive includes following log categories:

- PostgresSQL database log
- Apache web server log
- PPT server installation log

pptsupportDetails.tar archive also includes output of following system commands:

- netstat – an
- ifconfig –a
- df –k
- ipcs
- ps-eaf
- env
- "prstat 1 1" (SunOS) / "top -d 1 -n 1 -b" (Linux)
- "cat /etc/release" (SunOS) / "cat /etc/redhat-release" (Linux)
- /opt/VRTSvcs/bin/hares -state
- /opt/VRTSvcs/bin/hagrp -state

Important: For more information on support details, refer section *Get Support Details Script* in chapter *Administrative Scripts*.

Audit Trail

This section describes an audit trail of user activities in the PPT application.

Audit trail allows you to generate a trail of user activity in the PPT application. Depending upon the business model and assigned privileges, a user can perform following type of activities using PPT application:

- Accessing PPT application by logging in to the PPT server.
- Setting up IPCF and SSC instances in PPT application for communicating with IPCF and SSC deployments.
- Administering users.
- Accessing debug information and audit trail.
- Configuring user defined actions and conditions.
- Configuring rules, profiles and policies.
- Configuring subscription tiers and notification templates.
- Executing various PPT scripts and services.
- Accessing profile attributes QoS profiles and traffic types.

You can generate a time based, operation specific audit trail of activities performed by any user. This audit trail can be generated using following parameters as filters:

- **User Id**: Filters activities performed by user ids. You can list activities performed by all the users by selecting value **Any** for this parameter.
- **Operation Type**: Filters activities performed by the category or type of operations permissible in PPT application. You can list activities performed by all operation categories, irrespective of user's privilege by selecting value **Any** for this parameter. Depending upon your business model following operation categories are available - login, logout, user administration, IPCF and SSC setup, change password, session, traffic types, configuration of rules, policy, subscription tiers, user defined conditions and actions.
- **Log Severity**: Filters activities by severity of logs associated with the activities. You can list all the activities that are logged, by selecting value **Any** for this parameter. The log severity is categorized as debug, information, warning, error and critical.
- **To**: Filters activities by upper limit or end of date and time stamp associated with the activities. Format of date and time stamp is DD/MM/YYYY HH:MM.
- **From**: Filters activities by lower limit or the beginning of the date and time stamp associated with the activities. Format of date and time stamp associated with the activities is DD/MM/YYYY HH:MM.

> ***Important:*** You can access the record of activities from a particular date up to the last available record in the database, by keeping the **To** field blank and entering a particular date in **From** field. Alternately, you can access the record of all activities from the beginning up to a particular date, by keeping **From** field blank and enter a particular date in **To** field. If both **From** and **To** fields are kept blank then all records in the database are fetched.

An audit trail displays following information:

- **User Id**: Name of the user who has performed this activity.
- **Operation Type**: The category of the activity that was performed.

- **Time stamp**: Date and time when this activity was performed.
- **Log**: Brief description of the activity.

Objects and Notifications

This section lists SNMP objects and notifications generated by the PPT application.

Simple Network Management Protocol (SNMP) objects and notifications provide information about the network status to system administrators. Alarms can also be used for troubleshooting the issues. Objects or alarms mostly indicate status of various PPT server or client component such as web server or database. SNMP objects are used to manage and monitor the PPT services in the PCC deployment.

Following is the list of supported objects and notifications:

Table 2. Objects

Objects	Description
cPPTNotifTimeStamp	This object indicates the time when the notification was generated.
cPPTBackupDirPath	This object indicates the backup directory path where backup operation has failed.
cPPTAvailBackupDiskSpace	This object indicates the available space on backup disk.
cPPTIpcfName	This object indicates the name of IPCF.
cPPTIpcfAddressType	This object indicates the address type of cPPTIpcfAddress object.
cPPTIpcfAddress	This object indicates the IP address of IPCF. The type of this address is determined by the value of cPPTIpcfAddressType object.
cPPTIpcfUnmanageableCause	This object indicates the reason for IPCF being unmanageable in PPT.
cPPTSscName	The object indicates the name of SSC.
cPPTSscAddressType	This object indicates the address type of cPPTSscAddress object.
cPPTSscAddress	This object indicates the IP address of SSC. The type of this address is determined by the value of cPPTSscAddressType object.
cPPTSscUnmanageableCause	This object indicates the reason for SSC being unmanageable in PPT.
cPPTEnableNotif	This variable specifies whether the system produces the notifications. A 'false' value will prevent these notifications from being generated.
cPPTSynchronizationFailureCause	This object indicates the reason for failure of synchronization operation.
cPPTPcefName	This object indicates the name of PCEF.
cPPTPcefAddressType	This object indicates the address type of cPPTPcefAddress object.
cPPTPcefAddress	This object indicates the IP address of PCEF. The type of this address is determined by the value of cPPTPcefAddressType object.
cPPTPcefUnmanageableCause	This object indicates the reason for PCEF being unmanageable in PPT.
cPPTPreviousHostname	This object indicates the host name of cluster node on which PPT was running before cluster failover event occurred.
cPPTCurrentHostname	This object indicates the host name of cluster node on which PPT is running after cluster failover event occurred.

Table 3. Notifications

Notifications	Description
cPPTWebserverStartNotif	This notification is generated when Webserver process is started. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTWebserverStopNotif	This notification is generated when Webserver process is stopped. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTWebserverRestartedNotif	This notification is generated when Webserver process is restarted. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTDatabaseStartNotif	This notification is generated when Database process is started. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTDatabaseStopNotif	This notification is generated when Database process is stopped. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTDatabaseRestartedNotif	This notification is generated when Database process is restarted. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTPSMonStartNotif	This notification is generated when Process Monitoring process is started. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTPSMonStopNotif	This notification is generated when Process Monitoring process is stopped. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTPSMonRestartedNotif	This notification is generated when Process Monitoring process is restarted. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTCriticalConditionNotif	This notification is generated when Database process is down due to critical error condition and cannot be restarted by Process Monitoring process. No new logins will work, existing logins will be invalidated. Database process needs to be restarted manually to resume normal working of PPT. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTDBBackupDestinationNotAccessibleNotif	This notification is generated when PPT backup operation has failed. The reason for failure is that the destination directory is not accessible. Value of object cPPTBackupDirPath indicates the destination directory which is inaccessible via PPT. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.

Notifications	Description
cPPTDBBackupNotEnoughDiskSpaceNotif	This notification is generated when PPT backup operation has failed. The reason for failure is that the destination directory is not accessible. Value of object cPPTBackupDirPath indicates the destination directory which is inaccessible via PPT. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTMonitorServerStartNotif	This notification is generated when Monitor Server process is started. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTMonitorServerStopNotif	This notification is generated when Monitor Server process is stopped. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTMonitorServerRestartedNotif	This notification is generated when Monitor Server process is restarted. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTIpcfUnmanageableNotif	This notification is generated by Monitor Server when IPCF state changes from manageable to unmanageable. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time. Value of cPPTIpcfName object indicates the name of IPCF which is unmanageable via PPT. Value of cPPTIpcfAddrType object indicates the type of IP address contained in cPPTIpcfAddr object. Value of cPPTIpcfAddr object indicates the IP address of IPCF which is unmanageable via PPT. Value of cPPTIpcfUnmanageableCause object indicates the reason for IPCF to be unmanageable via PPT.
cPPTIpcfManageableNotif	This notification is generated by Monitor Server when IPCF state changes from unmanageable to manageable. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time. Value of cPPTIpcfName object indicates the name of IPCF which is manageable via PPT. Value of cPPTIpcfAddrType object indicates the type of IP address contained in cPPTIpcfAddr object. Value of cPPTIpcfAddr object indicates the IP address of IPCF which is manageable via PPT.

Notifications	Description
cPPTSscUnmanageableNotif	This notification is generated by Monitor Server when SSC state changes from manageable to unmanageable. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time. Value of cPPTSscName object indicates the name of SSC which is unmanageable via PPT. Value of cPPTSscAddrType object indicates the type of IP address contained in cPPTSscAddr object. Value of cPPTSscAddr object indicates the IP address of SSC which is unmanageable via PPT. Value of cPPTSscUnmanageableCause object indicates the reason for SSC to be unmanageable via PPT.
cPPTSscManageableNotif	This notification is generated by Monitor Server when SSC state changes from unmanageable to manageable. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time. Value of cPPTSscName object indicates the name of SSC which is manageable via PPT. Value of cPPTSscAddrType object indicates the type of IP address contained in cPPTSscAddr object. Value of cPPTSscAddr object indicates the IP address of SSC which is manageable via PPT.
cPPTSchedulerStartNotif	This notification is generated when Scheduler process is started. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTSchedulerStopNotif	This notification is generated when Scheduler process is stopped. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTSchedulerRestartedNotif	This notification is generated when Scheduler process is restarted. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time.
cPPTSynchronizationFailedOnIpcfNotif	This notification is generated by synchronization server when synchronization operation fails on manageable IPCF. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time. Value of cPPTIpcfName object indicates the name of IPCF on which synchronization operation has failed. Value of cPPTIpcfAddrType object indicates the type of IP address contained in cPPTIpcfAddr object. Value of cPPTIpcfAddr object indicates the IP address of IPCF on which synchronization operation has failed. Value of cPPTSynchronizationFailureCause object indicates the reason for failure of synchronization operation.

Notifications	Description
cPPPTSynchronizationFailedOnSscNotif	This notification is generated by synchronization server when synchronization operation fails on manageable SSC. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time. Value of cPPTSscName object indicates the name of SSC on which synchronization operation has failed. Value of cPPTSscAddrType object indicates the type of IP address contained in cPPTSscAddr object. Value of cPPTSscAddr object indicates the IP address of SSC on which synchronization operation has failed. Value of cPPTSynchronizationFailureCause object indicates the reason for failure of synchronization operation.
cPPTSynchronizationFailedNotif	This notification is generated by synchronization server when synchronization operation fails due to some internal error in PPT. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time. Value of cPPTSynchronizationFailureCause object indicates the reason for failure of synchronization operation.
cPPTPcefUnmanageableNotif	This notification is generated by Monitor Server when PCEF state changes from manageable to unmanageable. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time. Value of cPPTPcefName object indicates the name of PCEF which is unmanageable via PPT. Value of cPPTPcefAddrType object indicates the type of IP address contained in cPPTPcefAddr object. Value of cPPTPcefAddr object indicates the IP address of PCEF which is unmanageable via PPT. Value of cPPTPcefUnmanageableCause object indicates the reason for PCEF to be unmanageable via PPT.
cPPTPcefManageableNotif	This notification is generated by Monitor Server when PCEF state changes from unmanageable to manageable. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time. Value of cPPTPcefName object indicates the name of PCEF which is manageable via PPT. Value of cPPTPcefAddrType object indicates the type of IP address contained in cPPTPcefAddr object. Value of cPPTPcefAddr object indicates the IP address of PCEF which is manageable via PPT.

Notifications	Description
cPPTSynchronizationFailedOnPcefNotif	This notification is generated by synchronization server when synchronization operation fails on manageable PCEF. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time. Value of cPPTPcefName object indicates the name of PCEF on which synchronization operation has failed. Value of cPPTPcefAddrType object indicates the type of IP address contained in cPPTPcefAddr object. Value of cPPTPcefAddr object indicates the IP address of PCEF on which synchronization operation has failed. Value of cPPTSynchronizationFailureCause object indicates the reason for failure of synchronization operation on PCEF.
cPPTClusterFailoverNotif	This notification is generated when cluster failover event occurs. Value of cPPTNotifTimeStamp object indicates the time when this notification was generated. This will be system's current time. Value of cPPTPreviousHostName object indicates the host name of cluster node on which PPT was running before cluster failover event occurred. Value of cPPTCurrentHostName object indicates the host name of cluster node on which PPT is running after cluster failover event occurred.
cPPTMIBCompliance	The compliance statements for entities which implement the CISCO PPT MIB.
cPPTNotifMgmtGroup	A collection of objects related to notification management on PPT.
cPPTNotifGroup	A collection of notifications which indicate change in the state of PPT processes and change in the state of IPCF and SSC managed by PPT.
cPPTEnableNotifGroup	The collection of objects which are used to enable a group of notifications.

Important: For more information on PPT objects and notifications, please refer the *IPCF PPT Application MIB* chapter of the *Cisco ASR5000 Series SNMP MIB Reference* guide.

Chapter 7
Administrative Scripts

This chapter lists and describes the administrative scripts provided by PPT application.

Policy Provisioning Tool (PPT) provides various scripts. Most of these scripts perform administrative operations such as database backup, restore, and vacuuming, as well as resetting superuser password. Some scripts provide log information for troubleshooting purpose. All of these scripts, except the PPT Components Control (pptctl) Script, are located in the "*scripts*" folder in the PPT installation directory <*ppt-install-dir*>.

This chapter includes information on the following scripts:

- PPT Components Control Script
- Set Superuser Password Script
- Database Backup and Restore Script
- Update Backup Interval Script
- Database Cleanup Script
- Database Vacuum Script
- SNMP Target Configuration Script
- Get Support Details Script
- User Session Cleanup Script
- Migrating 12.1 PPT Data to 14.x PPT Cluster

Important: The user must have PPT administrator privileges to execute these scripts.

PPT Components Control Script

PPT Components Control (pptctl) script is used to control the PPT components by performing following operations:

- **start**: Starts the specified process or all processes.
- **stop**: Stops the specified process or all processes.
- **restart**: Restarts the specified process or all processes.
- **forcestop**: Forcefully stops the specified process or all processes.
- **status**: Checks current status of the specified process or all processes.

Caution: If a process name is not mentioned along with the action, then the respective action is taken for all processes related to policy provisioning application.

Syntax

```
pptctl [ postgres | apache | psmon | notif_server | monitor_server| scheduler ] [ start | stop | restart | forcestop | status ] | [ version ] | [ --help ]
```

-- help
This option describes script usage.

postgres [start | stop | restart | forcestop | status]
start/ stop/ restart/ forcestop the Postgres server.

apache [start | stop | restart | forcestop | status]
start/ stop/ restart/ forcestop the Apache server.

psmon [start | stop | restart | forcestop | status]
start/ stop/ restart/ forcestop the Process monitor.

notif_server [start | stop | restart | forcestop | status]
start/ stop/ restart/ forcestop the Notification server.

monitor_server [start | stop | restart | forcestop | status]
start/ stop/ restart/ forcestop the Monitor server.

scheduler [start | stop | restart | forcestop | status]
start/ stop/ restart/ forcestop the Scheduler.

version

Displays the version of currently installed PPT application.

Usage Description

- Execute the following script to start all the services associated with PPT application:

  ./pptctl start

  The sample output is displayed below:

  ```
  Starting Postgres Server ...

  Starting Apache Server ...

  Starting Notif Service ...

  Starting Monitor Server ...

  Starting Scheduler...

  Starting PSMon Service...
  ```

- Execute following script to view version of installed PPT application:

  ./pptctl version

  The sample output is displayed below:

  ```
  Policy Provisioning Tool (version 14.0.93.0)
  ```

- Execute the following script to stop the Apache Web server by force:

  ./pptctl apache forcestop

  The sample output is displayed below:

  ```
  This will stop all currently running apache requests, if any.

  Stopping apache...
  ```

Set Superuser Password Script

This script is used to reset the superuser password in the Policy Provisioning Tool (PPT) database.

Syntax

```
./set_superuser_password [ --help ]
```

--help

This option describes script usage.

Usage Description

A user with administrative privileges can execute this script without any options, as shown below:

```
./set_superuser_password.sh
```

The script prompts the user to enter a password. This password is stored in the database. The sample output is shown below:

```
Please enter the password for superuser.

password:new_password

Password for superuser changed successfully.
```

Caution: If an existing password is specified, when prompted to enter the new superuser password, following messages are displayed:

```
Password update for superuser failed.

New password cannot be same as old password.
```

Database Backup and Restore Script

This script is used to perform PPT database backup and restore operations.

Syntax

backupAndRestore.sh [**backup** <backup_dir_path>] | [**restore**] | [**--help**]

backup

Takes the backup of the PPT database and configuration files including *ppt.cfg* and *psmon.cfg* and stores it in *backup_dir_path* location.

restore

Restores PPT database and configuration files such as *ppt.cfg* and *psmon.cfg*. For this restore operation, this script prompts for a backup filename. Provide absolute path for the backup file that is to be restored.

Caution: To restore the database no other parameters except **restore** are required.

--help

This option describes script usage.

Usage Description

Execute this script with listed options. For backup option <*backup_dir_path*> is mandatory. The script generates backup of PPT database and application configuration files. It creates a tar ball and compresses these files. This tar archive is created at the location specified by the user.
Backup and restore operations for the PPT application:

- Can be performed on the same version of PPT application, i.e., if backup is generated from the version x.y of PPT application then it can be restored on version x.y only.
- Are permitted across the platform , i.e. backup can be generated from the application on Solaris platform and this backup can be restored on the Linux platform and vice versa.
- Upon execution this script generates complete backup, incremental backup feature is not enabled for this version of PPT application.

SNMP traps are generated to indicate un-successful backup. Details of traps can be found in Trap Details table below. For detailed information regarding SNMP traps, refer *CISCO-PPT-MIB.my* file located at the *<ppt-install-dir>/mib* directory. SNMP traps are generated for specific error conditions and success or failure messages for these operations are recorded.

Table 4. Trap Details

Trap Name and Probable Cause	Solution
starPPTDBBackupDestinationNotAccessible: Backup directory is not accessible or PPT administrator does not have enough permissions to access it.	Provide complete path of backup directory,
starPPTDBBackupNotEnoughDiskSpace: The disk on which backup is to be taken is full.	Ensure that enough space is available on the disk where backup is being generated.

For example, to generate backup of the database, execute the following command:

`./backupAndRestore.sh backup` *`backup_dir_path`*.

This command generates backup of PPT database and copies configuration for PPT application and PSMon, by generating a tar archive. This tar file is created at the location *`backup_dir_path`*.

Running the Backup and Restore script via CRON

During PPT installation a cron entry for backup script is added.Default backup time interval is configured as 1 day. This time interval can be modified using the script: *<ppt-install-dir>/scripts/updateBackupInterval.sh*. By default, backup is generated at midnight each day. If backup interval is modified by user, then backup operation will be performed at following time intervals:

- hourly - start of the hour
- daily - at midnight
- weekly - at midnight on the weekday configured by user
- monthly- at midnight on 1st day of month

Update Backup Interval Script

This script is used to update the database backup interval in the CRON utility. This interval is configured for the regular database backup.

Syntax

updateBackupInterval.sh [**--help**]

--help

This option describes script usage.

Usage Description

Execute the script without any option. For example:

./updateBackupInterval.sh

The script prompts user to specify backup interval. The valid options include: **1** - hourly, **2** - daily, **3** - weekly, and **4** - monthly. If weekly option is selected then, the script prompts for the day of week on which to generate the backup. In such case the valid options are: 0 - Sun, 1 - Mon, 2 - Tue, 3 - Wed, 4 - Thu, 5 - Fri, and 6 - Sat. Depending on the user input, backup interval in cron entry for PPT backup is modified. The sample output is shown below:

```
======================================

Please select any one of the following

options for backup interval

1 - hourly

2 - daily

3 - weekly

4 - monthly

======================================

Enter your option and press [ENTER]:3

[0]Sun, [1]Mon, [2]Tue, [3]Wed, [4]Thu, [5]Fri, [6]Sat

Enter the weekday and press [ENTER]:1

Cron updated successfully. Crontab contents are as follows

0,5,10,15,20,25,30,35,40,45,50,55 * * * * sh
/root/users/ppt//cronjobs/sessCleanup.sh
```

```
0 0 * * 1 /root/users/ppt//scripts/backupAndRestore.sh backup
/root/users/ppt/backup_dir
```

Database Cleanup Script

This script is used to perform the cleanup of PPT database. However the cleanup is performed for the Audit table only.

Syntax

dbcleanup [**--days** *number_of_days*] | [**--help**]

--help

This option describes script usage.

--days

Number of days for which the data is to be retained. Default is 30 days, minimum is 2 days, and maximum is 30 days. Therefore the *number_of_days* ranges from 2 to 30.

Usage Description

Execute this script with the **--days** option followed by the number of days for which records are to be retained. For example, to delete all records older than 5 days use following command:

```
./dbcleanup.sh --days 5
```

If the script is executed without any option, it asks for confirmation to delete data older than 30 days. To change this number of days, enter 'yes'. Enter the number of days for which the data is to be retained. Script deletes records from the database that are older than the specified number and displays success or failure message.
Sample output, generated without any option is given below:

```
Number of days prior to which data is to be deleted is not specified.

Using default value: 30 days.

Do you want to change the number of days? (yes/no):yes

Number of days:5

30 records deleted from database, which were older than 5 days.
```

Caution: Data purged by executing this script will not be recovered.

Database Vacuum Script

This script is used to perform the vacuuming on PPT database.

Syntax

vacuum [**--help**]

--help

This option describes the script usage.

Usage Description

Execute the script without any option. For example:

./vacuum.sh

It asks for confirmation. If you wish to continue then, enter 'yes'. Script performs vacuum operation on the database and displays success or failure message. The sample output is shown below:

```
Vacuuming will be done for database.

Proceed (yes/no):yes

Password:postgres_password

Vacuum was done successfully.
```

Caution: When prompted for the password, if you enter an incorrect password to access Postgres database, then following message is displayed:

```
Vacuum operation failed: vacuumdb: could not connect to database pptdb: FATAL:
password authentication failed for user "pptadmin".
```

SNMP Target Configuration Script

This script is used to add as well as delete SNMP targets to PPT database. These targets are used by Notification Server (NotifServer) to send traps.

Syntax

configSnmpTarget.sh [**--help**]

--help

This option describes the script usage.

Usage Description

Execute this script without any option. For example:

./configSnmpTarget.sh

The script displays a list of SNMP targets currently configured in database and prompts the user to **Add** or **Delete** a target or to **Exit** this script. Choosing **Add** option prompts the user for IP address, port, SNMP version 1 or SNMP version 2c and community name. Choosing **Delete** option prompts user for IP address and port value. Depending on success or failure, appropriate message is displayed.

Important: Maximum of five SNMP targets can be configured.

The sample output of this script is shown below:

```
The list of SNMP targets configured is as follows. Maximum of 5 targets
can be configured.

================================================

IP address - Port number - SNMP version - Community

 ================================================

 127.0.0.1 -     162          - 1 -        public

Select option to Add/Delete SNMP target (Add/Delete/Exit):Add

Please enter SNMP target details

IP address:1.2.3.4

Port: 667

SNMP version (1 / 2c):2c

Community: test

SNMP target added successfully
```

```
The list of SNMP targets configured is as follows. Maximum of 5 targets
can be configured.

================================================

IP address - Port number - SNMP version - Community

 ================================================

 127.0.0.1 -     162          - 1 -        public

 1.2.3.4 -       667          - 2c -       test

Select option to Add/Delete SNMP target (Add/Delete/Exit): Exit
```

Get Support Details Script

This script is used to collect support details information for the PPT application.

Purpose of this script is to collect debug information for PPT application. It collects different log files and captures output of certain system commands that would help in troubleshooting of a particular issue. This script collects required information and prepares a *gzip* file named <*project_name*>*supportDetails.tar.gz* file in the */tmp* directory.

Important: While reporting any issue with PPT application, attach this *gzip* along with the problem report (PR).

The *gzip* file name and the directory in which this *gzip* file is created, are configurable via an XML file

Syntax

```
./getSupportDetails.pl [ --level = level_number ] [ --xmlfile = xml_filename ] [ --outputDir = outpur_dir_path ] [ --verbose ] [ --help ]
```

`--level = level_number`

Specifies the debug level to be executed. Default: 1 and Max: 2.
Level 1 debug includes following information:

- Recent log files
- Current status of the product indicating whether it is in active or hanged state.
- Current Config files of the product
- Installation logs
- Database logs, if available
- Web server logs, if available
- Operating system information. For Solaris, it collects the OS version and patch information and for Linux, only OS version is captured
- Crontab entries
- Output of following commands, depending upon the configuration:
    - netstat -an
    - ifconfig -a
    - df -k
    - ipcs
    - ps -eaf
    - env
    - "prstat 1 1" (SunOS) / "top -d 1 -n 1 -b" (Linux)
    - "cat /etc/release" (SunOS) / "cat /etc/redhat-release" (Linux)
    - /opt/VRTSvcs/bin/hares -state
    - /opt/VRTSvcs/bin/hagrp -state

Level 2 debug includes logs from level 1 along with the database dump.

--xmlfile = ***xml_filename***

Specifies the XML file to be used to collect the log information. Default xml file is **getSupportDetails.xml** located in same directory as the script. This XML file allows the user to configure the *gzip* file name and directory where gzip file is to be stored.

> ***Caution:*** Do not update or change any other configuration parameters in this XML file, as it may lead to un-expected results.

--outputDir = ***output_dir_path***

Uses specified directory *output_dir_path* as destination to collect logs. Default: */tmp/* as output directory to collect logs.

--verbose

Displays information of the logs being collected.

--help

This option describes the script usage.

Usage Description

To execute this script for level 2 debugging with XML file name testXML, execute the following command:

```
./getSupportDetails.pl --level=2 --xmlfile=/tmp/testXML.xml
```

User Session Cleanup Script

This script is used to terminate the session of a particular user.

Syntax

user_session_cleanup [**--help**] | [**- u** *<user_name>*]

--help

This option describes script usage.

-u *<user_name>*

Prompts to specify the username as command line interpreter, whose session is to be terminated.

Usage Description

At any given instance, PPT application client allows only single login per user. If a user does not perform a clean log out, then their session remains valid and the application client prevent them from logging in again till completion of session time-out. Default value of the session time-out, which is configurable using administration menu from the application client is 15 minutes.

To terminate session associated with specific user:

- Log in with administrative privileges.
- Execute the script with u option and name of the user whose session you want to terminate.
- The script displays session details for this user and asks for confirmation to terminate the session.

```
./user_session_cleanup

Please enter the username
for which session is to be terminated.

Username:test

User session details
are as
follows:============================================================

Username     |
   IP address   | Session Expiry Time
=================================================================

test        |
 64.103.156.106  |   2012-03-22 06:43:34
=================================================================
=


Do
you wish to terminate the session? (yes/no):
```

If you want to terminate the session, enter *yes* or else *no*.

- On receiving confirmation, the script terminates session and removes session information from PPT database.

Migrating 12.1 PPT Data to 14.x PPT Cluster

This script is used to migrate v12.1 data to v14.x PPT cluster installation.

Syntax

upgrade_to_ha [**-f** *<backup_file_name>*] | [**--help**]

-f *<backup_file_name>*
Prompts to specify the name of backup file generated as the result of backup operation performed on installed v12.1 PPT application.

--help
This option describes script usage.

Usage Description

To migrate v12.1 data to v14.x PPT cluster installation:

Step 1 Login with administrative privileges on the system where data migration is required.

Step 2 Execute the following commands to create PPT v12.1 data backup in the backup directory.

su *<12.1-ppt-admin-user>*

cd *<12.1-install-dir>*

./scripts/backupAndRestore.sh backup *<backup-directory>*

PPT backup will be created in the backup-directory. The filename will have the following format:*backup_file-<PPT-version>-<YYYYMMDDHHSS>-<timezone offset from GMT>.tar.gz*

where, backup-file is the default file name which can different if overridden during v12.1 installation.

Step 3 Install v14.x in cluster mode and run the script **upgrade_to_ha** to migrate v12.1 PPT data to v14.x cluster PPT.

Step 4 Execute the following commands to migrate the data backup from v12.1 to v14.x.

su *<14.x-ppt-admin-user>*

cd *<14.x-install-dir>*

<ppt-install-dir>/scripts/upgrade_to_ha -f *<absolute-path-of-backup-file>*

where, *<absolute-path-of-backup-file>* is the absolute path of v12.1 data backup (including file name) which was taken earlier in Step 2.

Chapter 8
PPT Logs

This chapter describes various log files maintained by PPT application.

These log files can be used for troubleshooting and monitoring the PPT application. This chapter includes the following sections:

- Installation Logs
- Running Logs

Important: The default log severity level is set to warning. PPT administrator can change this severity by updating the **LOG_LEVEL** in the ppt.cfg file located at the *<ppt-install-dir>/etc* directory. For more information on log configuration, refer to *PPT Configuration File* chapter.

Installation Logs

This section describes PPT installation logs.

Installation logs are created during the installation of PPT server software. These logs are maintained in <*Install_logs*> directory inside PPT installation directory. PPT segregates the installation logs as per version of installed PPT application.

Following is the list of log files created at the time of installation in the xx.x.xx.x directory:

- console log

  This is a debug level log file created during PPT installation and is helpful for troubleshooting and debugging related issues. For example if xx.x is the version of installed PPT application, then installation logs for this version are maintained in <*ppt-install-dir*>*/Install_logs/xx.x* directory.

- postgres log

  This log file contains messages specific to Postgres installation that can be helpful for troubleshooting and debugging related issues. For example if xx.x is the version of installed PPT application, then installation logs for this version are maintained in <*ppt-install-dir*>*/Install_logs/xx.x* directory.

- PPT_Installer log

  This log file is generated by the **InstallAnyhere** and contains details regarding installation steps and actions performed during installation. For example if xx.x is the version of installed PPT application, then installation logs for this version are maintained in <*ppt-install-dir*>*/Install_logs/xx.x* directory.

- PolicyProvisioningTool_InstallLog.log

  This log file is generated by **InstallAnywhere** and captures all events of installation process. It contains logs pertaining to the extraction of files from installer binary and records success or failure status of each event.

> ***Important:*** The PolicyProvisioningTool_InstallLog.log log file corresponding to the current PPT software installation is stored at the PPT installation directory <*ppt-install-dir*>, however this log file is moved to <*ppt-install-dir*>*/Install_logs/xx.x.xx.x* directory once the PPT software is upgraded to different version. xx.x.xx.x stands for the PPT version being upgraded.

Running Logs

Running logs are created and maintained by PPT server for all the services and processes that are currently active.

Running log files are automatically created and maintained by PPT application.

Following is the list of running log files:

- ipcfpp.log_ipcfpp

  This file contains PPT logs generated via Apache and PPT scripts. This file is located in *<ppt-install-dir>/server/logs* directory.

- traceback_info.log

  This file is used to log trace back generated when an exception occurs in PPT. This file is located in *<ppt-install-dir>/server/logs* directory.

- scheduler.log_scheduler

  This file contains the logs generated by the scheduler process of PPT application. This file is located in *<ppt-install-dir>/server/logs* directory.

- postgres.log

  Postgres logs contains information regarding the requests of database transaction received from PPT application. The log files are maintained at *<ppt-install-dir>/3rdparty/postgres/pg_log* folder. These log files are labeled as postgresql-%Y-%m-%d_%H%M%S.log, where %Y, %m, %d, %H, %M, %S indicates year, month, day, hour, minute and seconds respectively. Rollover support is enabled for this log file which means that once the log file reaches 10 MB a new log file is created. PPT application can maintain up to 10 such log files.

  > ***Caution:*** It is highly recommended not to modify the log file name, log file location in the Postgres configuration file located at *<ppt-install-dir>/3rdparty/postgres/data/postgresql.conf*. Such modifications may lead to un-expected behavior of logging functionality as well as installation and upgrade of PPT application.

- Apache logs

  Apache logs contains information regarding the requests received from clients to the PPT server. The following log files are created and maintained at *<ppt-install-dir>/3rdparty/apache/logs*:

  - error_log

    The error log contains messages sent from Apache for errors encountered during the course of operation. This log is very useful for troubleshooting Apache issues on the server side.

  - deflate_log

    The server output being sent to client over HTTP is compressed to reduce network traffic. The deflate_log file records the compression log for each request/response.

  - access_log

    Apache server records all incoming requests and all requests processed to this log file.

  - ssl_request_log

This file contains logs similar to those present in access_log but contains additional information for each request like, client host IP, SSL version, cipher algorithm being used.

Chapter 9
PPT Configuration File

This chapter describes various parameters that can be configured according to the user requirements. The configuration file *ppt.cfg* is located at <*ppt-install-dir*>/*etc* directory.

The following table describes some of the parameters that can be modified.

Table 5. Configuration Parameters

Parameter Name	Description	Range	Default Value	Remarks
LOG_LEVEL	Level of the logging.	debug, info, warning, error or critical Min = debug Max = critical	Default = warning	The values are case sensitive. Changing the value of LOG_LEVEL requires Apache, Scheduler, Monitor server and Notification server to be restarted.
MAX_LOG_FILE_SIZE	The size of each individual log file.	Min = 0 Max = 20 MB	Default = 10 MB	Setting this value to 0 will disable to log file rollover feature and a single log file of unlimited size will be created. Changing the value of MAX_LOG_FILE_SIZE requires Apache, Scheduler, Monitor server and Notification server to be restarted.
LOG_FILE	The name of the log file.	NA	Default = <*ppt-install-dir*>/*server/logs/ipcfpp.log_ipcfpp*	Changing the value of LOG_FILE requires Apache, Monitor server and Notification server to be restarted.
TRACE_BACK_FILE	The name of the trace back file.	NA	Default = <*ppt-install-dir*>/*server/logs/traceback_info.log*	Changing the value of TRACE_BACK_FILE requires Apache, Scheduler, Monitor server and Notification server to be restarted.

Parameter Name	Description	Range	Default Value	Remarks
NUMBER_LOG_FILES	If log file rotation is in place we need to specify the number of files we should rotate between.	Min = 1 Max = 10	Default = 10	If value of MAX_LOG_FILE_SIZE is set to 0 then, value of NUMBER_LOG_FILES is ignored and single file of unlimited size is created. Changing the value of NUMBER_LOG_FILES requires Apache, Scheduler, Monitor server and Notification server to be restarted.
SCHEDULER_LOG_FILE	The file name of the scheduler log file.	NA	Default = <*ppt-install-dir*>*/server/logs/scheduler.log_scheduler*	Changing the value of SCHEDULER_LOG_FILE requires Scheduler to be restarted.
TCP_TIMEOUT	TCP timeout value for IPCF/SSC/PCEF reachability checking requests in seconds.	Min = 1 Max = 5	Default = 1	Changing the value of TCP_TIMEOUT requires Apache and Monitor server to be restarted.
KEEP_ALIVE_POLLING_INTERVAL	Polling interval for IPCF/SSC/PCEF keep alive requests in seconds.	Min = 5 Max = 60	Default = 30	Changing the value of KEEP_ALIVE_POLLING_INTERVAL requires Monitor server to be restarted.

Scheduler

The user can specify a variety of different expressions on each field, and when determining the next execution time, the scheduler finds the earliest possible time that satisfies the conditions in every field. This behavior resembles the **Cron** utility found in most UNIX like operating systems.

The following table lists all the available fields applicable in schedules.

Table 6. Available Fields in Schedules

Field	Description	Value Range	Default Value
HOUR	Hour field.	Min = 0 Max = 23	Default = 0
MINUTE	Minute field.	Min = 0 Max = 59	Default = 0

Important: The time format is HH:MM:SS. Changing the value of any field requires Scheduler to be restarted.

The following table lists all the available expressions applicable in schedules.

Table 7. Available Expressions in Schedules

Expression	Field	Description
*	any	Schedules are executed on every value.
a-b	any	Schedules are executed on any value within the a - b range. ***Important:*** The value of **a** must be smaller than value of **b**.
a-b/c	any	Schedules are executed whenever value reaches **c** which is within a - b range.
x,y,z	any	Schedules are executed on any matching expression. It can combine any of the above expressions.

Here are some examples for the schedulers:

- HOUR=0 MINUTE=0, the synchronization job will be executed everyday at 00:00:00 (This is default configuration).
- HOUR=* MINUTE=20, then the synchronization job will be executed everyday at 20 minutes of every hour.
- MINUTE=0-3, then the synchronization job will be executed everyday at 00:00:00, 00:01:00, 00:02:00 and 00:03:00.

Synchronization

It could happen that there are many state changes like manageable - unmanageable, unmanageable - manageable within a short time period. This state change can be due to network issues or they can be genuine state changes because of software malfunction on the IPCF/SSC/PCEF platform. To handle this scenario and to avoid repeated synchronization attempts because of this state change, synchronization will take place only if synchronization has not been done in recent past. This attribute defines the time period before which the synchronization should have taken place for state change trigger to be considered.

SHORT_TIME_PERIOD_BET_STATE_CHANGE_SYNC value is in seconds. The value range is given below:

- Min = 0 (Disable)
- Max = 86400 (1 day)
- Default = 3600 (1 hour)

Changing the value of SHORT_TIME_PERIOD_BET_STATE_CHANGE_SYNC requires Monitor server to be restarted.

Postgres

This section contains attributes which are related to log files generated by PostgreSQL server. Log file rollover facility in PostgreSQL server is being used and new log file will be created when existing log file reaches a limit of 10 MB. The log files are generated in *<ppt-install-dir>/3rdparty/postgres/pg_log* directory and the log file name is of the format postgresql-%Y-%m-%d_%H%M%S.log where %Y, %m, %d, %H, %M, %S stand for year, month, day, hour, minute and seconds respectively. Log file location, name and size are configurable via PostgreSQL configuration file. PostgreSQL does not support cleanup of old log files, for this purpose a cleanup script is provided in PPT. This section allows user to configure the number of log files to be retained and the time at which cleanup script should be executed.

Setting the value of NUMBER_OF_LOG_FILES to 0 will disable cleanup of log files generated by PostgreSQL server. The value range is given below:

- Min = 0
- Max = 50
- Default = 10

The user can configure the number of files to be retained after cleanup and the time at which the Postgres log file cleanup script is executed. The following table lists all the available fields applicable in schedules.

Table 8. Available Fields in Schedules

Field	Description	Value Range	Default Value
HOUR	Hour field.	Min = 0 Max = 23	Default = 1
MINUTE	Minute field.	Min = 0 Max = 59	Default = 0

Important: The time format is HH:MM:SS. Changing the value of any field requires Scheduler to be restarted.

The following table lists all the available expressions applicable in schedules.

Table 9. Available Expressions in Schedules

Expression	Field	Description
*	any	Schedules are executed on every value.
a-b	any	Schedules are executed on any value within the a - b range. ***Important:*** The value of **a** must be smaller than value of **b**.
a-b/c	any	Schedules are executed whenever value reaches **c** which is within a - b range.

Expression	Field	Description
x,y,z	any	Schedules are executed on any matching expression. It can combine any of the above expressions.

Here are some examples for the schedulers:

- HOUR=0 MINUTE=0, the cleanup script will be executed everyday at 00:00:00 (This is default configuration).
- HOUR=* MINUTE=20, then the cleanup script will be executed everyday at 20 minutes of every hour.
- MINUTE=0-3, then the cleanup script will be executed everyday at 00:00:00, 00:01:00, 00:02:00 and 00:03:00.

Cluster

This section contains the attributes being used by PPT in cluster mode. The value of HOST_IP is configured during PPT installation in cluster mode. In standalone mode, this value is ignored. HOST_IP is part of varbind information for traps generated by PPT application. The default host IP is 127.0.0.1.

Changing the value of HOST_IP requires Apache, Monitor server and Notification server to be restarted.

Chapter 10
Upgrading the PPT Software

This chapter provides the procedure to upgrade Policy Provisioning Tool (PPT) application using GUI-based as well as the console-based methods.

Important: Only users with root level privileges can perform upgrade.

PPT application upgrade is an automated procedure to replace an existing version of PPT application by a later or higher version.This procedure is performed by PPT installer program. During upgrade procedure, if PPT application is already installed, then the installer displays appropriate message indicating version of existing PPT installation. In such case installer provides a choice either to continue with upgrade procedure or to abort it.

PPT application does not provide any automated mechanism to revert to its earlier version. This can be achieved by un-installing existing PPT application and installing the earlier version. Refer chapters *Uninstalling PPT Software* and *Installing PPT Software* for detailed instructions.

Caution: Un-installing PPT application removes PPT database related files from the deployment. However, PPT back-up containing database dump and PPT configuration files, that are updated every mid-night by default, are not removed during un-installation process if they are located outside PPT installation directory. These backup files are compatible with version of PPT application and cannot be used with earlier or later versions of PPT application.

This chapter includes the following sections:

Unpacking the PPT Files

PPT installation package is archived as a single zipped file with a .zip extension. You need to copy this file on PPT server and then extract it.

Following task describes how to extract PPT installer:

Step 1 Access the directory in which the PPT installer archive is copied.

Step 2 Unzip the file by issuing following command:

```
unzip <file_name>.zip
```

The *file_name* is name of the downloaded PPT installation archive. For Linux machine, the file name is *ppt_<version_number>_rhel_x86.zip*; and for Sun Solaris machine, the file name is *ppt_<version_number>solaris_sparc.zip*.

PPT installation archive contains following files:

- README
- setup.bin
- inst

Pre-upgrade Steps in Cluster Mode

The following steps should be performed before upgrading the PPT in cluster mode:

Step 1 Execute the following command to disable the resource on the standby node. This will make sure that the resource group does not failover in between the upgrade and result in any sort of data corruption.

```
$ hagrp -disable <resource group name> -sys <node2>
```

Step 2 Execute the following command to verify that the cluster has been disabled.

```
$hagrp -state | grep ppt-ha
```

Expected output.

```
ppt-ha State <node1> |OFFLINE|

ppt-ha State <node2> |OFFLINE|
```

Step 3 Execute the following command to set the 'Critical' and 'Enable' attribute of the ppt-app resource to '0'. This will ensure that only the PPT application can be brought offline on the active node with the storage and network resources still online.

```
$ hares -modify <resource-name> Enabled 0

$ hares -modify <resource-name> Critical 0
```

Step 4 Execute the following command to verify that the above changes have been done.

```
$ hares -state | grep ppt-app
```

Expected output.

```
ppt-app State <node1>
OFFLINE

ppt-app
State <node2> OFFLINE
```

Step 5 Execute the following commands to synchronize the main.cf file on both the cluster nodes.

```
$haconf -makerw - to make in writeable

$haconf -dump makero - to sync the config and make it readonly
```

Refer to Performing the PPT Upgrade for further steps on how to upgrade PPT application.

Performing the PPT Upgrade

This section provides information about available upgrade methods and how to use them to upgrade an existing PPT application.

Important: Standalone PPT installation cannot be upgraded by cluster PPT installation and vice versa. Also existing standalone PPT installations cannot be added into cluster mode.

This section contains following sub-sections:

- Available PPT Upgrade Methods
- Upgrading PPT Using the GUI-based Installation Wizard
- Upgrading PPT Using the Console-based Installation Wizard

Available PPT Upgrade Methods

An existing PPT application along with its components such as Apache web server, PostgreSQL database engine, Notification sever and PsMon can be upgraded using either a GUI based or a console based method.

GUI-based Upgrade: This is commonly used upgrade method. Following are the requirements for GUI-based upgrade:

- Administrative access to the PPT server and attached display terminal, with active X-Windows application such as Xming or eXceed.
- Network connectivity to PPT server via Telnet or SSH, using some X-Windows client on remote workstation.

Console-based Upgrade: This upgrade method is used when either X-Windows application or remote network connectivity to PPT server using Telnet or SSh is not available.

Upgrading PPT Using the GUI based Installation Wizard

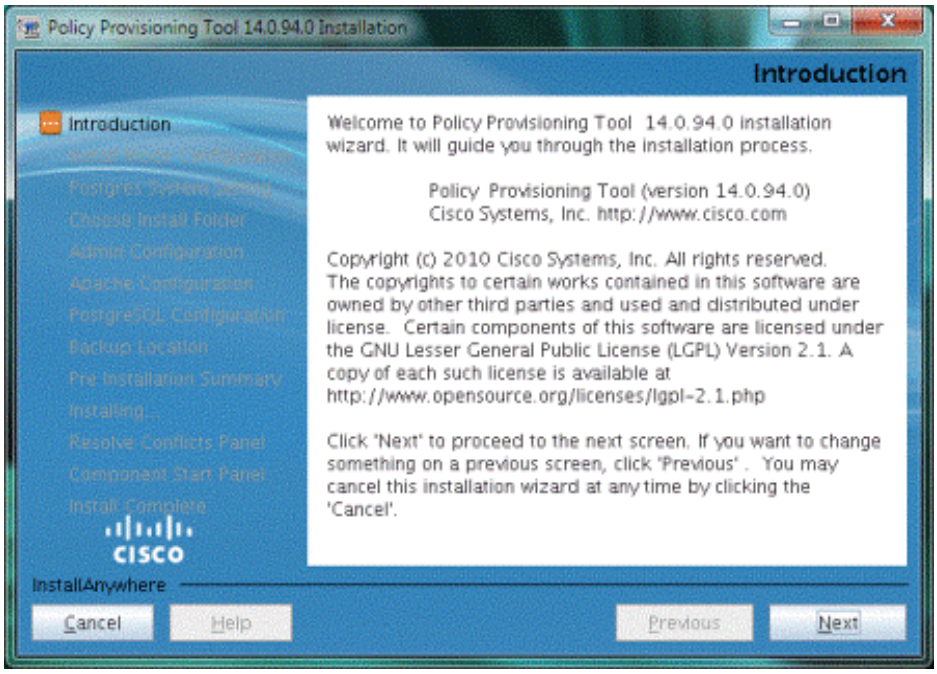
Following task describes how to upgrade PPT application using GUI based method:

Step 1 Access the directory where extracted PPT installation files are located.

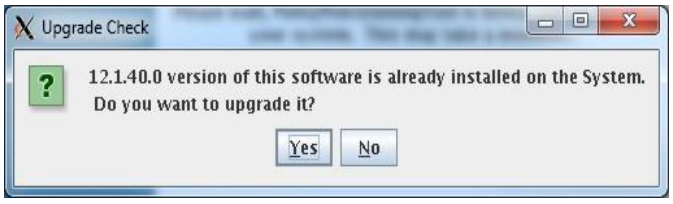
Step 2 Execute the following command to start PPT setup:

```
./inst
```

The PPT Installer screen appears:



Step 3 Click **Next** to proceed. PPT installer checks for any existing version of the PPT software. If such version is found, then following dialog box opens:



Step 4 Click **Yes** if you want to continue with upgrade.

Step 5 Follow instructions displayed by PPT installer to configure and update required parameters. Refer *GUI Based Installation Parameters* table from *Installing the PPT Software* chapter, for descriptions of configurable parameters.

Step 6 Click **Done** to exit the GUI-based installation wizard.

After completion of upgrade process, you can access PPT application GUI by entering following URL in the address bar of the browser in client machine:

```
https://<ip_address>:<port_number>/

https://<host_name>:<port_number>/
```

where *ip_address* and *host_name* is the IP address of the machine where PPT server software is installed and *port_number* is the number of port to which apache is listening for the client requests. Installer assumes the default port if *port_number* is not provided with URL.

Important: Contact Cisco support for default Username and Password in order to login to the PPT application after the upgrade.

Upgrading PPT Using the Console based Installation Wizard

Following task describes how to upgrade PPT application using console based method:

Step 1 Access the directory where extracted PPT installer archive is located.

Step 2 Execute the following command to start setup file:

```
./inst -i console
```

PPT installer displays a series of messages as shown below:

```
Extracting the JRE from the installer archive...

Unpacking the JRE...

Extracting the installation resources from the installer archive...

Configuring the installer for this system's environment...

Launching installer...

Preparing CONSOLE Mode Installation...

     .   .   .

     .   .   .

     .   .   .

PRESS <ENTER> TO CONTINUE:
```

Step 3 Press the “Enter” key to proceed. A series of messages appear as shown below:

```
User Checking...

Upgrade Checking...

Version number <xx.x.xx.x> of the software is already installed on the System.

     Do you want to upgrade it? (Y/N):
```

Step 4 Enter “Y” (Yes) to proceed with upgrade.

Step 5 Follow the instructions displayed by PPT installer to configure and update required parameters. Refer *GUI Based Installation Parameters* table from Installing the *PPT Software chapter* for description of configurable parameters.

After successful upgrade, PPT installer displays following messages:

```
Install Complete

----------------

Policy Provisioning has been successfully installed to:

/users/<ppt-install-dir>
```

```
Installation log file "/PolicyProvisioning_InstallLog.log" can be viewed from the
same location.

Start Policy Provisioning component as:

cd /users/<ppt-install-dir>

./pptctl start

./pptctl stop
```

After completing the upgrade process, you can access PPT application GUI by entering following URL in the address bar of the browser in client machine:

https://<ip_address>:<port_number>/

https://<host_name>:<port_number>/

where *ip_address* and *host_name* is the IP address of the machine where PPT server software is installed and *port_number* is the port number to which apache is listening for the client requests. Installer assumes default port, if port number is not provided with the URL.

Important: Contact Cisco support for default Username and Password in order to login to the PPT application after installation.

Post Upgrade Steps in Cluster Mode

After completing upgrade on standby node shift the PPT application on active node.

Following task describes post upgrade steps in cluster mode:

Step 1 Run the script provided as part of PPT installer (*install_postgres*). This script will upgrade the database schema. This script should be run on active node.

Step 2 Execute the following command to set the **Enable** attribute of the ppt-app resource.

```
$ hagrp -enable <resource group name> -sys <node2>

$ hagrp -switch <resource group name> -to <node2>
```

Step 3 Upgrade PPT on node which was previously active (node1).

Step 4 Execute the following command to set the **Critical** attribute of the ppt-app resource.

```
$ hares -modify <resource-name> Critical 1
```

Step 5 Execute the following command to verify that the above changes have been done.

```
$ hares -state | grep ppt-app
```

Expected output.

```
ppt-app State <node1> OFFLINE

ppt-app State <node2> ONLINE
```

Chapter 11
Uninstalling the PPT Software

This chapter provides step-by-step procedure to uninstall PPT application using console as well as GUI based uninstallation wizard.

This chapter includes the following sections:

Caution: Uninstallation removes PPT database related files from the server. However, PPT back-up files such the database dump and PPT as well as PsMon configuration files, that are updated every mid-night by default are not removed during uninstallation process if these files are located outside PPT installation directory. These backup files are compatible with version of PPT application and cannot be used with earlier or later versions of PPT application.

Pre-uninstallation Steps in Cluster Mode

The following steps should be performed before uninstalling the PPT in cluster mode:

Step 1 Execute the following command to disable the resource on the standby node. This will make sure that the resource group does not failover in between uninstallation process and result in any sort of data corruption.

```
$ hagrp -disable <resource group name> -sys <node2>
```

Step 2 Execute the following command to set the **Critical** and **Enable** attribute of ppt-app resource to '0'.

```
$ hares -modify <resource-name> Enabled 0

$ hares -modify <resource-name> Critical 0
```

Refer to GUI Based PPT Uninstallation Wizard and Console Based Uninstallation Method for further steps on how to uninstall PPT application.

Uninstallation Methods

This section describes the methods that can be used to uninstall PPT application.

The PPT application along with its components such as the Apache web server and PostgreSQL database engine, can be uninstalled using either a GUI based or a console based method.

GUI based method: This is commonly used uninstallation method. Following are the requirements for GUI-based uninstallation:

- Administrative access to the PPT server and attached display terminal, with an active X-Windows application such as Xming or eXceed.
- Network connectivity to PPT server via Telnet or SSH, using some X-Windows client on remote workstation.

Console based method: This uninstallation method is used when, neither X-Windows application nor remote network connectivity to the PPT server using Telnet or SSh is available.

Important: PPT installation and uninstallation method are not interdependent, i.e., PPT application can be installed using GUI and uninstalled using console and vice versa.

GUI Based PPT Uninstallation Wizard

This section provides instructions for uninstalling the PPT application using a GUI based uninstallation method.

Important: The uninstallation process must be executed by a user with root access privileges. This process removes all the database entities pertaining to the build that is being uninstalled. After uninstallation, it is not possible to recover these database entities.

Step 1 Log into the server on which PPT application is installed, using root username and password.

Step 2 Default installation directory is */users/ppt*, access this directory by entering following command:

```
cd /<ppt-install-dir>
```

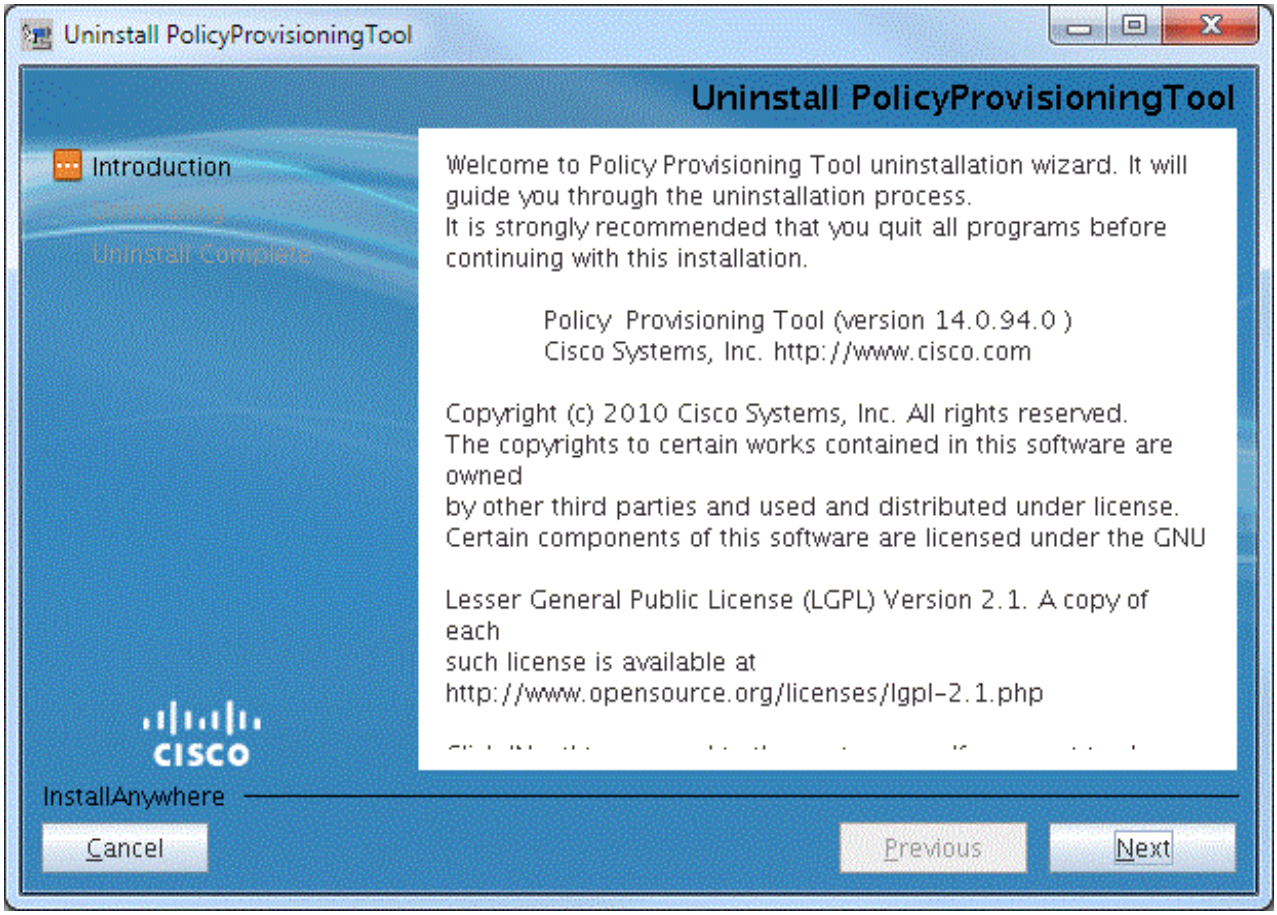
Step 3 Access */Uninstall_PolicyProvisioningTool* sub-directory by entering the following command:

```
cd Uninstall_<ppt-install-dir>
```

Step 4 Execute the uninstall script by entering the following command:

```
./Uninstall_<ppt-install-dir>
```

Uninstall Policy Provisioning Tool screen appears as shown below:



Step 5 Click **Next**. Uninstallation wizard identifies the processes to be stopped.

Step 6 Click **Next** and follow the instructions.

Step 7 Click **Finish** to complete the uninstallation process.

Console Based PPT Uninstallation Method

This section provides instructions for uninstalling the PPT application using the console-based uninstallation method.

Important: The uninstallation process must be executed by the user with root access privileges. This process removes all the database entities pertaining to the build that is being uninstalled. After uninstallation, it is not possible to recover these database entities.

Step 1 Log into the server on which the PPT application is installed. Use the root username and password.

Step 2 Access the directory in which PPT is installed, the default installation directory is */users/ppt*, by entering the following command:

```
cd /<ppt-install-dir>
```

Step 3 Access the */Uninstall_PolicyProvisioningTool* sub-directory by entering the following command:

```
cd Uninstall_<ppt-install-dir>
```

Step 4 Execute the uninstall script by entering the following command:

```
./Uninstall_PolicyProvisioningTool
-i console
```

Console based uninstallation displays a welcome message.

Step 5 Enter **N** to proceed. A message appears listing the application processes to be uninstalled.

Step 6 Enter **N** to proceed with the uninstallation. A number of messages are displayed indicating the progress of uninstallation process.

Step 7 Press **Enter** to complete the uninstallation process.

Post-uninstallation Steps in Cluster Mode

The following steps should be performed after uninstalling PPT application in cluster mode:

Step 1 After uninstalling PPT from the Active Node, enable the resource on the standby node and disable it on current active node. This will make sure that the resource group does not failover in between uninstall and result in any sort of data corruption.

```
$ hagrp -enable <resource group name> -sys <node2>

$ hagrp -disable <resource group name> -sys <node1>
```

Step 2 Switchover the resource group to Standby Node.

Step 3 Uninstall PPT from the Standby Node.

Chapter 12
Troubleshooting the PPT

You may face issues while working with a Policy Provisioning Tool (PPT) application, as well as while installing or un-installing it. For troubleshooting such issues PPT application provides following categories of support data:

- Installation logs
- Running logs
- Audit Trail
- Debug Information

Following log files can also be used for troubleshoot issues related to PPT GUI, database and installation respectively:

- Console.log
- Postgres.log
- PPT_Installer.log

Important: These files are stored in *<ppt-install-dir>/install_logs/<PPT_version>* directory.

Following troubleshooting sections provide information about possible cause and work around if available for such issues. The issues are categorized as:

Issues Pertaining to Installation

Problem:	Installer window does not appear.
Possible Cause(s):	• If you received the *"ERROR: could not initialize interface awt - exception: java.lang.InternalError: Cannot connect to X11 window server using ':0.0' as the value of the DISPLAY variable."* message, the display settings of your terminal program may be incorrect, or the X-Windows client (e.g. Exceed and Xming) is not running on the client machine. • The */var/tmp* directory may be full.
Action(s):	• Verify the display settings of the terminal application on the client machine are correct. • Verify that Exceed is installed properly on the client machine. • Determine the status of the */var/tmp* directory by entering the **df -k** command. If it is at or near capacity, choose another directory for the *Host Base Directory* parameter setting. This parameter can be set via the installation process.

Problem:	During installation, PPT installer displays following message *"Unable to install Policy Provisioning Tool <version> over Policy Provisioning Tool: Installed product has newer version."*
Possible Cause(s):	• A later version of the PPT as compared to the version that you are attempting to install is already present on the machine. • A previously installed version of the PPT was not installed successfully, or was un-installed incorrectly.
Action(s):	• Completely un-install the current version and install the desired version.

Issues Pertaining to PPT Startup

Problem:	Postgres does not start.
Possible Cause(s):	• A postgres lock file, *.s.PGSQL.xxxx.lock* is present in the */tmp* directory prior to starting postgres. Here xxxx is the port number • Shared resources are not released after another Postgres instance was terminated. • The PostgreSQL system environment variables were not configured properly prior to installation.
Action(s):	• If the lock file is present, delete it using the **`rm .s.PGSQL.xxxx.lock`** command. • Determine if a previous Postgres instance is still using system resources by entering the **`ipcs`** command. If it is, then clear the resources by entering the **`ipcrm`** command. • Ensure that the PostgreSQL system environment variables were configured properly using the information in *Installing the PPT Software* chapter of this guide.

Problem:	PostgreSQL server does not start. Logfile shows entries similar to those given below: *[2012-05-24 10:57:43 IST] [16939] FATAL: could not create log file "../pg_log/postgresql-2012-05-24_105743.log": No such file or directory.*
Possible Cause(s):	• Check whether PPT administrator was created manually. • If **Yes**, then may be parameters like home-dir and *groups* (root, users) were not configured properly which resulted in PostgreSQL data directory permissions mismatch. • This problem can be observed in both standalone and HA/cluster mode.
Action(s):	• Uninstall PPT, delete PPT administrator user (from both nodes in case of HA/cluster mode) and install PPT again.

Problem:	PPT application processes not generating traps. *ipcfpp.log_ipcf log* file contains following error message, *Error while resolving the local host name. Error {errorno 8} node name or service name is not known*
Possible Cause(s):	This may happen because of in-correct configuration in *../etc/nsswitch.conf* file.

Action(s):	• With root access privilege, edit the */etc/nsswitch.conf* file. • Search for the following host entry **`hosts: nis dns [NOTFOUND=return] files`**In the host entry the *files* option may not be present. • Change the above mentioned entry as follows: **`hosts: nis dns files [NOTFOUND=return]`**. • Above mentioned change states to use the host name for, IP address to host name mapping from the file */etc/host* if the host name is not available in nis or dns. • Save the changes in */etc/nsswitch.conf* file. • Access the *etc/host* file and ensure that for every host name an IP address entry is present. • If such association does not exists, then add appropriate <host name> <IPaddress>, where host name is a string returned by **`host name`** command and IP address can be retrieved using **`ifconfig –a`** command. • For the UCS machine, execute following command **`/etc/init.d/network restart`**. This command is not required for the Solaris machine. • Verify that the traps are being sent by monitoring PPT logs.

Issues Pertaining to Login

Problem:	Could not login to PPT.
Possible Cause(s):	Invalid user name or password.
Action(s):	Verify that the username and password you are entering is correct. Contact Cisco support for further assistance.

Problem:	Post login window opens after successful login, but focus is not given to it.
Possible Cause(s):	Mozilla Firefox is being used and Java Script settings are not done as required for this site.
Action(s):	Click **Tools** menu -> **Option** sub menu -> **Content** tab -> Click the **Enable JavaScript** check box -> Click the **Advanced** button -> Click the **Raise or lower windows** check box -> Click **OK**.

Problem:	Using Internet Explorer, login to PPT is successful; but immediately an error message "User session is invalid. Please re-login" is displayed . On attempting to re-login, an error message "User already logged-in" is displayed.
Possible Cause(s):	The username that is being sent in HTTP request is empty. This happens as the PPT server lag time is more than 15 minutes the default idle time-out configured for the PPT application client.
Action(s):	In this scenario where PPT server lag time is more that client idle time-out, the username in the HTTP request will be checked and user will receive the session in-valid message. This user session needs to be cleaned using the script .*scripts**user_session_cleanup*.

Issues Pertaining to the Web Browser

Problem:	PPT application does not invoke on client machine or takes too long to load.
Possible Cause(s):	A non-recommended Web browser is being used.
Action(s):	Use the recommended Web browser, Internet Explorer (7 or later version) or Firefox (3.5 or later version). Install it, if it is not present.

Problem:	PPT client shows old information which must have changed with the newer installed version or build.
Possible Cause(s):	Old information might be populated from the browser cache.
Action(s):	Cleanup the temporary Internet cache of your browser and re-invoke the PPT client application.

Issues Pertaining to CORBA Communication

Problem:	IMG is unmanageable.
Possible Cause(s):	• The PPT cannot communicate with the Cisco IPCF due to network issues. • There is an ORBEM client identification mismatch between the IPCF and PPT. • The ORBEM client on the IPCF is disabled. • There is an IIOP port configuration mismatch between the IPCF and PPT. • The IIOP transport parameter on the IPCF is not enabled. The IPCF is unmanageable.
Action(s):	• Ensure ICMP connectivity between IPCF and the PPT Server using the **ping** <*ppt_server_ip_address*> command from the IPCF command prompt. Refer to the *Command Line Interface Reference* for more information on using this command. • Verify that the ORBEM client identification on the IPCF matches with that configured on the PPT. The configuration of this parameter on the IPCF can be determined by entering the **`show configuration | grep client`** command. On the PPT, check for the ASID (Application Server ID) and Port on the view IPCF screen. Change these settings as needed. • Check the status of the ORBEM client on the IPCF by executing the **`show orbem client id`** <*client_id*> command on the IPCF. The "State" should be *"Enabled"*. If the "State" is *"Disabled"*, execute the **`activate client id`** <*client_id*> command in the ORBEM Configuration Mode and check the status again-- it should now be *"Enabled"*. • Verify that the configuration of the IIOP port on the IPCF matches that configured for the PPT. The configuration of this parameter on the IPCF can be determined by entering the **`show configuration | grep "TCP-port"`**. On the PPT, check for the ASID (Application Server ID) and Port on the view IPCF screen. Change these settings as needed. • Verify that the IIOP transport parameter is enabled on the chassis by entering the **`show orbem status | grep iiop-transport`** command. If it is not, enable using the instructions found in the Intelligent Policy Control Function Administration Guide.

Issues Pertaining to the Process Monitor (PSMON)

Problem:	PPT processes are not restarted after a crash.
Possible Cause(s):	• PSMON is not running • Invalid PSMON configuration • The PSMON may have given up after performing multiple retries in a specific duration
Action(s):	• Verify that PSMON is running by entering the **`./pptctl status psmon`** command. • Verify that PSMON is configured with the proper entries to start PPT processes. These entries may not be available if they were not selected for monitoring during the installation process. • The PSMON tries to restart the processes for "numretry" time within a duration of "tmintval" (refer to *etc/psmon.conf*) per process. If the process still does not start, PSMON no longer monitors this process. Please check the *<ppt-install-dir>/3rdparty/psmon/psmon.log* for details. Try restarting the process using the *pptctl* script.

Issues Pertaining to XML-RPC Communication

Problem:	SSC is unmanageable
Possible Cause(s):	• The PPT cannot communicate with the SSC due to network issues. • There is an SSC Port configuration mismatch between the SSC and PPT
Action(s):	• Ensure that the ICMP connectivity between the SSC and PPT using the **`ping`** <*ssc_ip_addr*> command from the PPT shell prompt. • Verify that the configuration of the SSC port matches with that configured for the PPT. The configuration of this parameter on SSC can be determined by entering the command **`grep Listen 3rdparty/apache/conf/httpd.conf`**. On the PPT, check for the SSC port on the View SSC detail screen. Change these settings as required. • Verify that the apache server is running on SSC using command **`sscadm status`**.

Issues Pertaining to Uninstallation

Problem:	Un-installing the PPT failed with error java.lang.OutOfMemoryError.
Possible Cause(s):	Memory heap size fell short.
Action(s):	• Open the file <ppt-install-dir>/Uninstall_PolicyProvisioningTool/Uninstall_PolicyProvisioningTool.lax • Search for the key string "lax.nl.java.option.java.heap.size.max". The value would be "134217728" (128MB). • Change this value to "268435456" (256MB). • Save the file and rerun to the un-installer.