OVERVIEW

The IPT Auto Config feature automatically performs the IPT station configuration functions that would otherwise require programming at the station using the IPT keypad.

For automatic configuration, the system administrator/technician programs IPedge/VIPedge server with station Auto Config data, and configures the DHCP server for IPTs to automatically discover the IPedge/VIPedge server.

The first time an IPT is connected, the user enters the DN and Password and the station is will be automatically configured with the system presets.

Note: The IPT must be an IP5000-series telephone with the “out-of-the-box” factory default settings. If the IPT has already been configured, it must first be reset to the factory default settings.

Note: For IPT Auto Config to function correctly the IP Telephones must be at firmware level 5Kx-M2P2 or higher.

IPT AUTO CONFIG

The IPT Auto Config feature automatically performs the IPT station configuration functions that would otherwise require programming at the station using the IPT keypad.

For automatic configuration, the system administrator/technician programs IPedge/VIPedge server with station Auto Config data, and configures the DHCP server for IPTs to automatically discover the IPedge/VIPedge server.

The first time an IPT is connected, the user enters the DN and Password and the station is will be automatically configured with the system presets.

Note: The IPT must be an IP5000-series telephone with the “out-of-the-box” factory default settings. If the IPT has already been configured, it must first be reset to the factory default settings.

Note: For IPT Auto Config to function correctly the IP Telephones must be at firmware level 5Kx-M2P2 or higher.

IPT AUTO CONFIGURATION

The IPT Auto Config feature automatically performs the IPT station configuration functions that would otherwise require programming at the station using the IPT keypad. For automatic configuration, the system administrator/technician programs IPedge/VIPedge server with station Auto Config data, and configures the DHCP server for IPTs to automatically discover the IPedge/VIPedge server. The first time an IPT is connected, the user enters the DN and Password and the station is will be automatically configured with the system presets.

Important! For IPT Auto Config to function correctly the IP Telephones must be at firmware level M2M0 or higher. The minimum IPT 5000-series firmware levers are: 5K4-M2P2 (or later) and 5k9-M2P2 (or later.) The telephone must also be initialized to factory default condition.

Automatic Server Discovery

In the factory default setting, an IPT will request an IP address from the DHCP server. The IPT will also request a vendor specific option which contains the system servers IP address and optionally VLAN configurations, such as Phone VLAN ID, PC port VLAN etc.

When VLAN configurations are offered from the DHCP server, the IPT releases the obtained IP address to the DHCP server, memorizes the configurations, and reboots to enable VLAN tagging. After reboot, the IPT will send a DHCP request (with phone VLAN ID) to obtain an IP address. This second DHCP request allows the DHCP server to recognize that the requesting device is connected (virtually) to the Phone VLAN, and to lease an IP address allocated for the VLAN subnet.

In the event the DHCP server is down or there is network trouble, the IPT will display an error message on the LCD screen. The IPT will ping the DHCP server periodically in an attempt to regain network connectivity.

When the IPT is unable to obtain the IP address from the DHCP option field, it will request the user login DN, then broadcast a server discovery message with the login DN. In this case, only IPT phones deployed on the same IP subnet (Node) as the IPedge server may be configured automatically.

Note: The IPT ignores the system server IP address and VLAN configurations provisioned from DHCP server when it boots without factory default mode. To re-provision from the DHCP server, the IPT phone must be manually reset (initialized) to factory defaults.

Automatic Login DN and Password Saving

The IPT phone user will be always prompted to enter a login DN at initial bootup. Once user enters the login DN, the IPT will contact the system server using the IP address obtained from the DHCP server. The system server will check for a valid DN, and the user may be prompted to enter password if password authentication is enabled for that DN. If the server accepts the login DN and password, the IPT will automatically save the login DN and password. During the login process, the LCD display and

user interface are exactly the same as the IP Phone User Mobility feature.

Multi-Node IPedge Systems

This section applies only to IPTs configured for survivability in a multi-node IPedge system. For VIPedge systems go to Automatic Data Provisioning.

There are a few different scenarios relevant to which system will be a first contact of registration from IPT.

IPT registers with primary IPedge server associated with the login DN

The primary IPedge server handles the login process and provides additional configuration data, if any, for that IPT. The IPT will keep connecting with the primary server after auto configuration.

IPT registers with secondary IPedge server associated with login DN, if it is programmed to have a secondary server address.

The secondary IPedge server handles the login process and provides the primary server address along with additional configuration data, if any, for that IPT. The IPT will switch back to the primary IPedge server following General Survivability specification after automatic configuration is done, however, if the primary server is not available, the IPT will keep staying on the secondary server.

IPT registers with IPedge server other than primary and secondary server.

Assuming that Network DN table and remote node's IP addresses are properly programmed for login DN, the IPedge server receiving login DN as Network DN can redirect the IPT to its primary IPedge server. After redirection, the primary IPedge server will take over the login process and provide additional configuration data.

If the IPT gets no response from the IPedge server, the IPT will keep retrying registration.

Errors during the login process can be due to several reasons shown below. See IP Phone User Mobility feature about error displays.

- Login DN is not created on IPedge server.
- Login DN is already in use for another user and transfer registration option is disabled.
- No IP endpoint license is left on IPedge server.
- Login password is incorrect.
- Terminal authentication failed when it is enabled.

Note: Once user changes any IPT data locally, it will no longer ask the user to enter login DN until a reset to factory defaults is performed.

Automatic Data Provisioning

The system server will send to the IPT; the primary server IP address and, if any, secondary server IP address. The IPT will save that information as well. On the next reboot, the IPT will start to register with the saved primary system server address instead of using system server address obtained from DHCP server.

The system administrator is able to customize IPT device configuration based on system policy, user preference and so on by saving the configuration data on the system server prior to IPT deployment. Before the IPT will be made ready, it will pull out those configuration data from system server, re-configure itself and then save. Some device configuration data requires the phone to reboot to reflect the change.

IPT AUTO CONFIGURATION

The normal IPT programming in Enterprise Manager must be done first.

- Create the station data for IPT phones
- Set IPT login password and enable password authentication per prime DN as required
- For stations with Survivability (IPedge system only) the same station data must be stored on both the primary and secondary servers

PREREQUISITES

Only IP 5000 series telephones, for use with IPedge/VIPedge servers can use the IPT Auto Config feature. All of the following perquisites must be completed before the IPT is connected to the network.

- IP Telephones must be at firmware level: 5Kx-M2P2 (or later)
- IP Telephone must be set to factory default (new, out of the box or reset to factory default)
- DHCP Server with Option 43 setup and online, reachable by all IPTs
- IPT programming in the IPedge/VIPedge database complete

Reset IPT Factory Default Settings Manually

To reset the LCD settings to Factory defaults

1. Press 3+6+9+Hold (simultaneously).
2. Press Volume ?
3. Press Hold to access Initializing Mode.
4. FB01 – Resets Terminal Data (This includes Handset Volume and Handset/Headset sidetone.)
    - FB02 – Resets LCD Contrast / Backlight data
    - FB03 – Resets Network data.
    - FB04 – Resets Analog CO settings (on IP5122-SDC only).
5. Press FBxx to turn on initialization FB will light red.
6. When FB's have been selected, press Hold to save the settings.
7. Lift the handset off-hook /on-hook to perform initialization. Telephone will reset.

DHCP SERVER SETUP

Two vendor specific options are supposed to be used for providing additional information for IPT. Vendor Specific Information option is used to provide the IPedge/VIPedge server's IP address and optionally VLAN configurations for IPT phones. The Vendor Class Identifier option allows some DHCP servers which are able to have different vendor specific information per vendor class to distinguish which vendor's device or application is requesting vendor specific information and to offer proper vendor specific information.

Vendor Specific Option Setup

The definition of the Vendor Class Identifier and Vendor Specific Information for IPT Auto Config is shown Table 1. The Vendor Specific Information is configured and transmitted as Type/Length/Value structure. For example:

Type1,Length1,Value1(Hex),Type2,Length2,Value2(Hex).....

This structure is provided for by RFC2132.

Table 1 DHCP Server Vendor Specific Options

DHCP Option	Type	Length	Value	Hex Presentation <Type><Length><Value>
Vendor Class Identifier	0x01	0x0f or 0x0e	TOSHIBA IPedge/VIPedge **Note:** Regarding whether there is NULL or not, there is a difference according to DHCP server's type. When there is NULL, Length becomes "0x0f". When there is not NULL, Length becomes "0x0e".	<With NULL> 01 0f 54 4f 53 48 49 42 41 20 49 50 65 64 67 65 00 <Without NULL> 01 0e 54 4f 53 48 49 42 41 20 49 50 65 64 67 65
Server IP Address	0x02	0x04	For example, 192.168.100.39	<The case of 192.168.100.39> 02 04 c0 a8 64 27
VLAN Enable/ Disable	0x03	0x01	0x00 : VLAN Disable 0x01 : VLAN Enable	<When VLAN Disable> 03 01 00 <When VLAN Enable> 03 01 01
Phone VLAN ID=	0x04	0x01 or 0x02	1 - 4094 **Note:** Length is difference between the value of VLAN-ID. When VLAN-ID is bigger than 255(0xff), Length is “0x02”. When VLAN-ID is smaller than 256, Length is “0x01”.	<When VLAN-ID=100> 04 01 64
PC Port Type	0x05	0x01	0x00 : Access 0x01 : Trunk	<Access> 05 01 00 <Trunk> 05 01 01
PC Port VLAN ID=	0x06	0x01 or 0x02	1 - 4094 **Note:** Length is difference between the value of VLAN-ID. When VLAN-ID is bigger than 255(0xff), Length is “0x02”. When VLAN-ID is smaller than 256, Length is “0x01”.	<VLAN-ID=101> 06 01 65

Refer to the example on the next page.

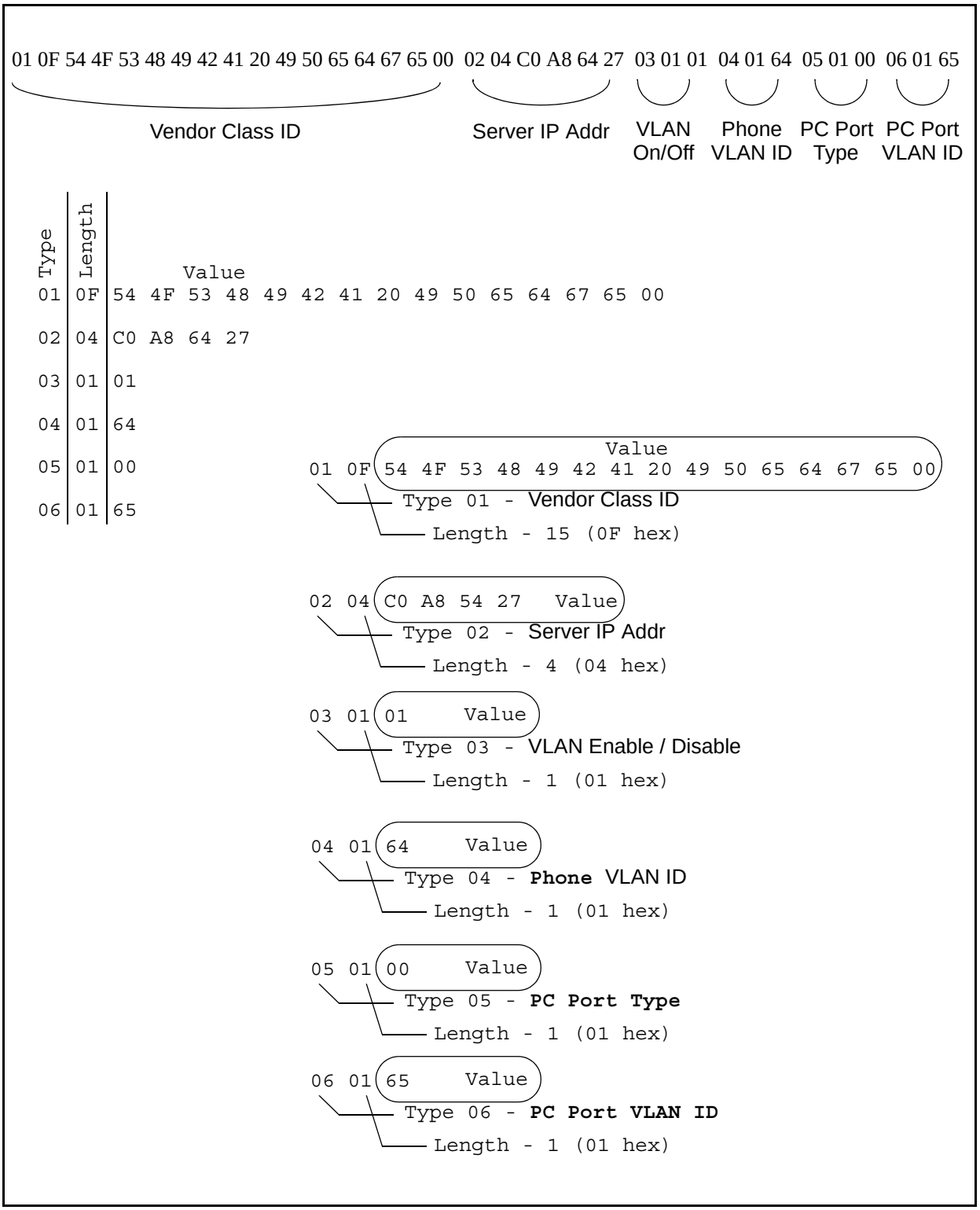


Figure 1 DHCP Server Vendor Specific Options Example

IPT Data Preparation

The station must be created in the IPedge/VIPedge database with the required settings before the IP Telephone is connected.

If the DN is a Survivability station (IPedge systems only) the same set of station data must be stored on both the primary IPedge server and the secondary IPedge server. Enterprise Manager will automatically insert the proper IP addresses for both Primary and Secondary IP address into the station data.

Security

If system administrator wants to authenticate the end user by password before they start using the IPT, a login password must be set and password authentication must be enabled per Prime DN.

Enterprise Manager implements the IPT Automatic Configuration programming into following three groups according to the parameter characteristic, operation and limitation. Refer to Table 2.

Table 2 Auto Config Station Parameters

Configuration Name	Parameter Name	Default value
Station ID	Prime DN	
Auto Login Password (1)	IP Phone Login Password	Disabled
Auto Login Password (2)	Security Code	No data
Discovery Mode	Discovery Mode	Broadcast
Primary Server Address	Primary Server	Primary server IP
Secondary Server Address	Secondary Server	0.0.0.0
User Mobility Language		English

IPT CREATION IN ENTERPRISE MANAGER

Use the information above to setup the DHCP server and the IP Telephones. The following steps detail the IPT programming in the IPedge/VIPedge server. Most of the programming is the same as standard IP Telephone database programming.

1. In Enterprise Manage select **Station > Station Assignment**.
2. Assign the Prime DN(s).
3. Program IPTs.
4. For Survivable IPTs assign a Secondary IP address.

Station Creation Cases

Basic IPT Deployment

- Enterprise Manager saves IPedge/VIPedge server IP address into the Primary server IP address parameter
- Enterprise Manager will keep secondary server parameter 0.0.0.0 (IPedge systems only)

- Reboot is not necessary because no phone is connected

Survivable DN (IPedge system only)

- Enterprise Manager saves IPedge server IP address into the Primary server IP address parameter
- Enterprise Manager saves the survivability secondary IPedge server IP address to Secondary sever IP address parameter
- Same data saves to the survivability secondary server
- Reboot is not necessary because no phone is connected

IPT AUTO CONFIGURATION

IPT Auto Config page is an individual page that gathers all IPT Auto Config parameters and features in one place that allow administrator to configure the IPT more conveniently, refer to Table 3.

The page supports single IPT and multiple IPT operation. Enterprise Manager automatically reboots the IPT when a parameter change requires a restart to reflect change.

Table 3 Auto Config Parameter Default Values

Parameter Name	Configuration Name
IP Phone Login Password	Auto Login Password
Security Code	Auto Login Password
Server Discovery Mode	Discovery Mode
Base UDP port for IPT Media Channel	Dynamic RTP Port Base
Primary Server Address	Primary Server Address
Secondary Server Address	Secondary Server Address
User Mobility Language	User Mobility Language

Enterprise Manager Controls

In Enterprise Manager select **Station > IPT Auto Config** to access the IPT Auto Config page.

There are three buttons implemented for the IPT Auto Config feature. Refer to Figure 2. The IPTs are selected by DN.

1. **Edit** - launches Edit Dialog for selected IPTs.
2. **Reset** - resets selected IPTs to Factory Default value.

3. **Restart** - reboots the selected IPTs.

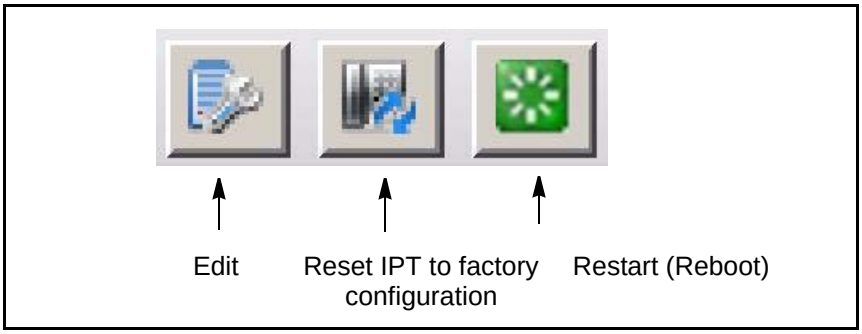


Figure 2 IPT Auto Config Icons

IPT Selection

IPTs can be selected by:

- Check-mark to select a single DN
- Check-Mark to select multiple DNs
- Enter Range of DNs
- The administrator can enter a range of DNs, following the Enterprise Manager conventions:
  - Range: 2000-2020
  - Single: 2031, 2037 or 2034 2088
  - Combine: 2000-2020 2031 2088 2177-2277
  - Range does not combine with check list. Range override check list.
- Check a single box to Select All DNs in the specified IPedge/VIPedge server

  All DNs means all Primary DN programed as IPT type stations. All others are ignored. All DNs option overrides the check box list.

Warning Dialog

A warning dialog will display when the administrator presses the Save, Reboot or Reset to Factory default button. The user needs to confirm for Enterprise Manager to continue the operation.

Edit dialog

The Edit Dialog has wizard like features that allow user to set the configuration and manipulate multiple IPTs.

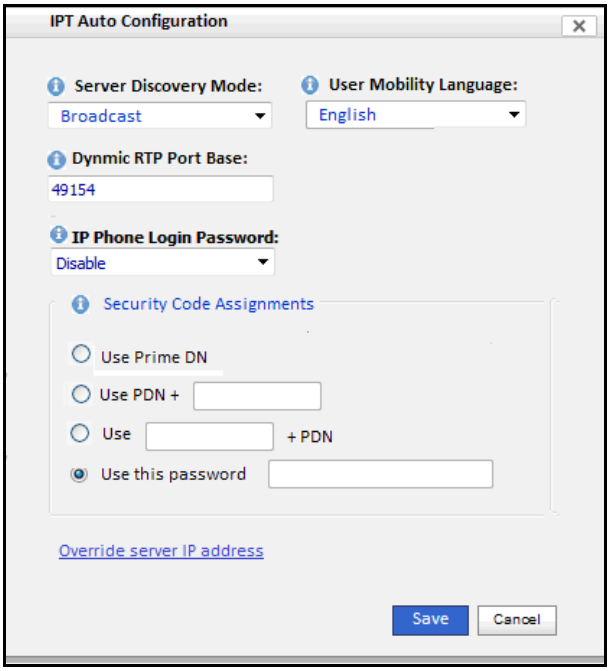
The Primary Server IP address and Secondary Server IP address (secondary address is for IPedge systems only) are managed by Enterprise Manager and are hidden from the user by default. The administrator can modify them manually, click on **Override server IP address**.

Important! The default value of the Primary Server Address for each IPT station is 255.255.255.255. This address flags the IPedge/VIPedge server that IPT Auto Config is disabled for DN with this address. To

enable IPT Auto Config to overwrite the IP address.

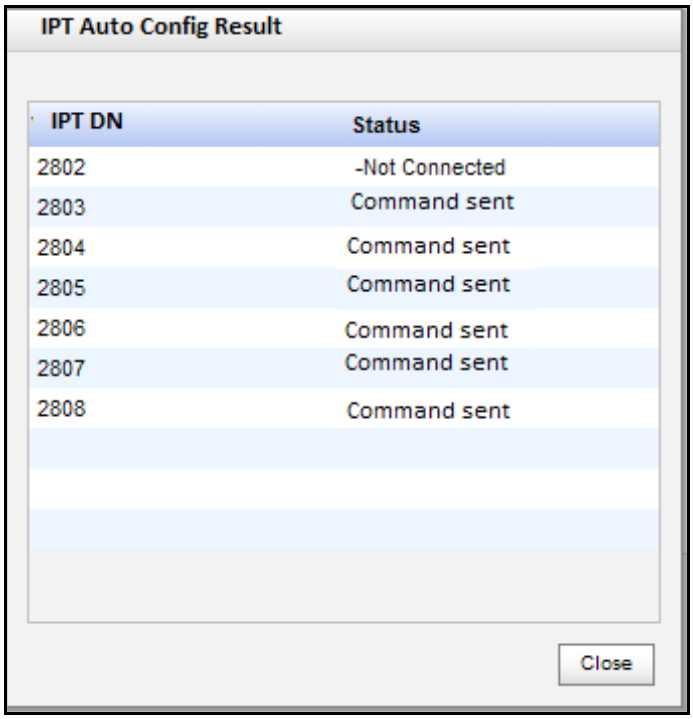
Parameters that belong to the auto provisioning are downloaded to each IPT when the IPT is online. To download this provisioning data to each IPT, Enterprise Manager performs the following:

- Ask for confirmation if one of the provisioning data is changed.
- Enterprise Manager automatically reboots IPT after data is saved.
- If only Dynamic RTP Port Base or IP Phone Login Password is changed then reboot is not necessary and Enterprise Manager will not ask for confirmation.



Result Dialog A dialog box listing the IPT Auto Config operation results. This example shows that station 2802 was not connected. It was not configured.

Stations 2803~2808 were configured.



Maintenance Procedures

Reset or Reboot IPT

Reset IPT local data to Factory Default value:

1. Select DN, DNs, enter range of DNs or All DNs in selected server.
2. Click on the **Reset to Factory Button**.
3. Confirm warning dialog.
4. Display result dialog.

To manually reset an IPT, see Reset IPT Factory Default Settings Manually

Reboot IPT phone:

1. Select DN(s) in selected server.
2. Select **Restart Phone** icon.
3. Click on **Confirm** in the warning dialog.
4. The result dialog will be displayed.

Edit Configuration

Edit non-auto provisioning parameters:

1. Select DN, DNs, enter range of DNs or All DNs in selected server.

2. Select Enable/Disable IP Phone Login Password or modify Dynamic RPT Port Base
3. Click on the **Save** icon.

Enterprise Manager will skip the reboot step if the IP Phone Login Password and Dynamic RPT Port Base are the only parameters changed.

Edit Auto Provisioning Parameters

1. Select DN, DNs, enter range of DNs or All DNs in selected server.
2. Edit Server Discovery Mode, User Mobility Language
3. Click on the **Save** icon.
4. Confirm warning dialog.
5. Enterprise Manager will save the data and reboot IPT if IPT is online.

Set User Password

1. Select DN, DNs, enter range of DNs or All DNs in selected server.
2. Select one of the four options:

- Use Prime DN
- Use PDN + digit
- Use digit + PDN
- Use specific password.

3. Click on the **Save** icon.
4. Confirm warning dialog.
5. Enterprise Manager will save the data and reboot IPT if IPT is online.

Change Primary Server IP Address

This section applies only to multi-node IPedge systems. For VIPedge systems go to IPT VLAN.

This procedure is used when it is necessary to change the IP address of a Primary IPedge server. Note that the IP Telephones will be out of service while the IPTs and then the IPedge server reboot.

Note: This procedure is for a Survivability Primary server that is the Primary server of a multi-node enterprise system.

1. Change the DHCP server configuration to the new IPedge server IP address within DHCP Vendor Specification data.
2. Login to the Enterprise Manager on the server that will get the new IP address.
3. Select **Station > IPT Auto Config**.
4. Select All DN or enter range of DNs in the server.
5. Click on the **Edit** icon.
6. Click **Override server IP address**.
7. Enter the new IP address of the server in the Primary Server Address field.

8. Click on **Submit** and Click on **Confirm** in the warning dialog.
9. Enterprise Manager save the data and reboot the IPTs. Note that it this time the IPTs will not be able to process calls. The IPTs will be trying to register to the new IP address.
10. Select **Application > Webmin** select the server. Select **Networking > Network Configuration > Network Interfaces** and change the IP address to the new value.
11. Restart the IPedge server.
12. Log out Enterprise Manager.

Important! If this is the Primary server in a multi-node IPedge system, the Member nodes will need to have the Primary server IP address changed. Login to each member node 'Locally' to change the Primary server IP address on the Server Management page.

Change IP Address of a Member Node

This procedure is used when it is necessary to change the IP address of a IPedge Member server. Note that the IP Telephones will be out of service while the IPTs and then the IPedge server reboot.

1. Select All DN or enter range of DNs in member server.
2. Click on **Override server IP address**.
3. Enter the new IP address in the Primary Server IP address field.
4. Click **Save** and confirm the warning dialog.
5. Enterprise Manager will save the data and reboot the IPT.
6. Select **Application > Webmin** select the server. Select **Networking > Network Configuration > Network Interfaces**.
7. Change member server IP address to new value from Network Configuration.
8. Restart the member IPedge server.
9. Login to Enterprise Manager. Select **Administration > Enterprise > Servers**. Select the member server, click on the **Edit** icon. Go to Server page and change the member server IP address.

Important! If this is a Member server in a multi-node system the Member node address will need to be changed on the Primary server. Login to the primary node. Detach the member node then, attach the node using the new IP address.

Change Secondary Server IP Address

This procedure is used to change the Secondary server assignment in the IPT. This changes the IP address the IPT will register to if the primary survivability server becomes unavailable.

Note: The DN of the IPTs must be programmed on the secondary server and enough licenses to support the “fail over” IPTs must be present in the IPedge server.

1. Select All DN or enter range of DNs in member server.
2. Click on **Override server IP address**.
3. Enter the new IP address in the **Secondary Server Address** field.
4. Click on **Save** and confirm the warning dialog.
5. Enterprise Manager will save the data and reboot the IPTs.

Change Primary Server IP Address

This procedure is used to change the Primary server assignment in the IPT. This changes the IP address the IPT will register to during normal operation.

1. Select All DN or enter range of DNs in member server.
2. Click on **Override server IP address**.
3. Enter the new IP addresses in the **Primary Server Address** field.
4. Click on **Save** and confirm the warning dialog.
5. The same data will also be saved on Primary Server IP address field in secondary server.
6. The affected IPTs will reboot.

Change Primary Server IP Address on Survivability Server

If a survivable secondary server has changed IP address.

1. Select DNs that are assign to failover to the target server.
2. Click on **Override server IP address**.
3. Enter new IP addresses on Secondary Server IP address field.
4. Click on the **Save** icon and confirm the warning dialog.
   The same data will also be saved on Secondary Server IP address field in secondary server.
5. The IPTs will reboot.

Change Secondary Server to a Strata CIX System

A Strata CIX system can be the survivability secondary system.

1. Select All DN or enter range of DNs in member server.
2. Click on **Override server IP address**.
3. Enter new IP addresses on Secondary Server IP address field.
4. Click on **Save** and confirm the warning dialog.
5. Enterprise Manager save the data and reboot the IPT.

IPT VLAN

DHCP server will be the initial provisioning server. Because Enterprise Manager reads data directly from the IPT, the IPT must be online. The IPedge system does not store this information. The Enterprise Manager database will store the data not current but last from last synchronized.

Change Phone VLAN ID

1. Change the DHCP server configuration to have a new Phone VLAN ID within the DHCP Vendor Specific Information option field. Newly deployed IPT phones will get updated Phone VLAN ID.
2. Use Enterprise Manager to change the Phone VLAN ID for the IPT DN affected by the VLAN design change. IPT phones will reboot right after the data change. IPT phones won't reconnect to IPedge Server until a VLAN-aware LAN switch is re-configured. Make sure that all IPT phones are connecting to the IPedge server during this programming. Otherwise, system administrator will have to change the Phone VLAN ID for offline IPT phones locally.
3. Change the VLAN-aware LAN switch configuration according to new VLAN design. After that, the LAN switch will forward VLAN-tagged frames with new VLAN ID sent from IPT phones, thus IPT phones will reconnect to IPedge server.

Move IPT to Another VLAN

1. Using Enterprise Manager, change the Phone VLAN ID for all IPT DN to new value for new VLAN segment. IPT phones will reboot right after data change. IPT phones won't reconnect to IPedge Server until those are moved to new VLAN segment. Make sure that all IPT phones are connecting to IPedge server during this programming. Otherwise, system administrator has to change Phone VLAN ID for offline IPT phones locally.
2. Move the IPT phones to the new VLAN segment. After moving, the IPTs will reconnect to the IPedge server.

Enterprise Manager Personal Administration

The IPT user can use the Enterprise Manager Personal Administration (EMPA) to assign and change:

- User Mobility Language - The User Mobility Language is combined with LCD Display Language
- Login password and security code (Preferences) -.

Change User Mobility Language

EMPA uses the **Phone Display Language** field to control the LCD display language as well as user mobility language.

1. The user changes the Phone Display Language, EMPA populates the value to both LCD display language and user mobility language parameters.
2. The EMPA will display a Warning message to alert user reboot the phone. User clicks on **OK** to save the change and reboot the phone.

   User clicks **Cancel** to abandon the change.

Change LCD Display Language

EMPA uses the **Phone Display Language** field to control the LCD display language as well as user mobility language.

1. The user changes the Phone Display Language, EMPA populates the value to the LCD display language.
2. The User clicks on **OK** to save the change and reset the phone.

   User clicks **Cancel** to abandon the change.

Turn off Login Password Setting

When the phone login password is turned off no password is required for log in. This parameter does not require the phone to reboot.

The IPT User can turn off the login password requirement.

1. Login to EMPA.
2. Select the **Preferences** tab.
3. Click on **Change password**.
4. Uncheck the **Turn on phone login password** box.
5. Click on the **Save** icon.

Turn on Login Password (no security code set)

The IPT User can turn on the login password requirement.

1. Login to EMPA.
2. Select the **Preferences** tab.
3. Click on **Change password**.
4. Check-mark the **Turn on phone login password** box.
5. Enter the new Password and Confirm Password.
6. Click on the **Save** icon.
   If the New Password and Confirm Password fields are blank, the user will receive an error message.
7. Click on **OK** to continue save the change phone.
   Click on **Cancel** to abandon the change.

The IPT must be on line to reflect the changes.

Change Security Code

The IPT User can set or modify the security code. When security code field is blank no change is made.

1. Login to EMPA.
2. Select the **Preferences** tab.
3. Click on **Change password**.
4. Enter the new Password and Confirm Password.

5. Click on the **Save** icon.
   If the New Password and Confirm Password fields are blank, the user will receive an error message.

Note: The IPT must be on line to reflect the changes.

CAPACITY

The number of IPTs that can be automatically configured simultaneously is limited only by the number of endpoint licenses.

AVAILABILITY

IP5000-series telephones on IPedge systems with R1.1 software. The IP Telephones must be software level M2M0 or later. Only the licensed IPTs will Automatically Configure.

RESTRICTION

The DHCP server must be able to offer the vendor specific information for the IPT Auto Configuration feature to operate. If the DHCP Vendor Specific Information option code is already used for another purpose on this network and the DHCP server does not have the ability to offer different vendor specific information per vendor class, the IPT Auto Config feature cannot be used.

- IPv6 is not supported.
- Until the auto configuration process is done, display language on LCD screen is English.
- When a user changes an IPT configuration by local configuration mode, server data cannot be updated. The IPT will sync with the IPedge server data again after either doing a remote configuration or rebooting the phone.
- The system doesn't guarantee values of IPT local data when local configuration (3+6+9+Hold) conflicts with remote (Enterprise Manager or EMPA) configuration.
- When the IPT program update function is executed during the Auto Config function, the Auto Config data is saved to the IPT and the IPT will be started up with the Auto Config data, and it's not guaranteed that Enterprise Manger monitors the progress of Program Update. In this case, Administrator has to abort Program Update manually.

R1.0 to R1.1 and LATER

For IPedge systems running R1.0 software the following instructions need to be followed in sequence to upgrade to R1.1 system software. Refer to the IPedge Install manual for software update procedures.

1. Backup the R1.0 IPedge Enterprise Manager database to a DVD or USB drive.

Note: This step only applies for ISO update; this step is not required for Program update.

2. Update the IPedge server software to R1.1 software.
3. Restore the IPedge Enterprise Manager database configuration to the server.

Note: This step only applies for ISO update; this step is not required for Program update.

4. For all previously configured IPT stations (in Phase 1.0) update the station record to add valid IPT Auto Configuration data to the station record. The following IPT station configuration needs to be updated on the server:

A. Server Discovery Mode
B. Primary Server Address
C. Secondary Server Address
D. IPT Login Password
E. User Mobility Language

5. Update IPT firmware from version corresponding to Phase 1.0 to version corresponding to Phase 1.1.

HARDWARE No additional IPedge hardware is necessary for this feature.

FEATURE INTERACTION

Feature Name	Descriptions
Survivability (IPedge only)	• When a login DN is programmed to have General survivability option, both primary IPedge and secondary IPedge servers can be a server to handle the initial login process and auto configuration for that DN. • Failover does not work during IPT Auto Config.
IP Phone User Mobility	• Transfer registration can be applied when login DN is already being used for another user and Transfer registration option is enabled for the login DN. • Multi-node login feature (IPedge only) can be applied to redirect an IPT to the right server for login DN: 1. When the Login-DN is different from the Station-ID saved in the IPT, IPT Auto Config Data of IPT registration is invalid (IPT does not save the data which is downloaded from the server during the boot-up process). The reason is to prevent IPT reboots at each Login then, users would have to enter the DN/Password again. 2. Even though the Login-DN is different from the Station-ID saved, Remote Configuration is allowed. In this case, the IPT local data is overwritten by the Login-DN configuration data after the phone reboots. 3. When the Login-DN is different from Station-ID saved in the IPT, if the IPT is manually restarted from Enterprise Manager without any data change by Remote Configuration, the IPT gets started up as same Login-DN again. In this case, user is not required to Login and enter a Password.
NAT Traversal	• For automatic configuration of remote IPT phone behind NAT, DHCP server (typically NAT router) needs to be set up on the remote site. • With DHCP server setting on remote site, DHCP Vendor Specific Information option must contain global IP address of main site, where IPedge server hosting remote IPT is deployed, as an IPedge server address.
Terminal Authentication	Terminal Authentication to login DN can be applied during IPT Auto Config when it is enabled.
Private Network Numbering Plan	In a situation where several nodes are deployed on a single site hosted by a single DHCP server and they have the same prime DN, user may have to enter Node ID preceded by login DN.