



# **Administration – Remote Worker**

## **Avaya Business Communications Manager Release 6.0**

Document Status: **Standard**

Document Number: **NN40171-600**

Document Version: **01.02**

Date: **October 2010**

© 2010 Avaya Inc.  
All Rights Reserved.

#### **Notices**

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

#### **Documentation disclaimer**

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

#### **Link disclaimer**

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

#### **Warranty**

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>

**Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.**

#### **Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

#### **Copyright**

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

#### **Third Party Components**

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

#### **Trademarks**

*The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.*

#### **Downloading documents**

For the most current versions of documentation, see the Avaya Support. Web site: <http://www.avaya.com/support>

#### **Contact Avaya Support**

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>

# Contents

---

<b>Customer Service</b>	<b>5</b>
Navigation	5
Getting technical documentation	5
Getting product training	5
Getting help from a distributor or reseller	5
Getting technical support from the Avaya Web site	5
<b>Getting started with remote worker support</b>	<b>7</b>
About remote worker support	7
Audience	7
Acronyms	8
Symbols and text conventions	8
Related publications	9
<b>Virtual private network configuration overview</b>	<b>11</b>
<b>Configuring the BCM for remote IP sets using VPN</b>	<b>13</b>
Setting up the BCM (01-vpn-config-em graphics)	13
<b>Setting up the secure router</b>	<b>17</b>
<b>Configuring the IP deskphone</b>	<b>19</b>
Configuring network settings on the IP deskphone	19
Configuring VPN settings on the IP deskphone	20
<b>Installing the pre-configured phone in a home office</b>	<b>21</b>
Verifying the VPN license	22
<b>Diagnostics</b>	<b>23</b>
Verifying the license type	23
Verifying the Secure Router port	23
Verifying the Secure Router user connection	23



## Customer Service

---

This section explains how to get help for Avaya products and services. Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to <http://www.avaya.com> or go to one of the pages listed in the following sections.

### Navigation

- “Getting technical documentation” on page 5
- “Getting product training” on page 5
- “Getting help from a distributor or reseller” on page 5
- “Getting technical support from the Avaya Web site” on page 5

### Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to <http://www.avaya.com/support>.

### Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at <http://www.avaya.com/support>. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

### Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

### Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at <http://www.avaya.com/support>.



# Chapter 1

## Getting started with remote worker support

---

This section contains information on the following topics:

- [“About remote worker support” on page 7](#)
- [“Audience” on page 7](#)
- [“Acronyms” on page 8](#)
- [“Symbols and text conventions” on page 8](#)
- [“Related publications” on page 9](#)

### About remote worker support

Avaya Business Communications Manager 6.0 (BCM 6.0) includes new options for remote worker support. You can connect your Avaya 1100 Series IP Deskphone to the Avaya BCM through a secure VPN tunnel, or by using the new remote worker feature. Using the remote worker feature, you can use the BCM system as an HTTP server, allowing you to distribute configuration files, license files, and firmware to IP clients.

This guide provides procedures for administrators to provision IP 1100 series phones to be supported in home offices in a remote worker configuration.

### Audience

This guide is intended for administrators who want to configure the IP 1100 series phones for remote worker support.

## Acronyms

This guide uses the following acronyms:

HTTP	hypertext transfer protocol
IP	internet protocol
LAN	local area network
NAT	network address translation
PAT	port address translation
PSK	pre-shared key
RTCP	realtime control protocol
RTP	realtime transfer protocol
UDP	user data protocol
VPN	virtual private network
WAN	wide area network

## Symbols and text conventions

These symbols are used to highlight critical information for the <Product Name short> system:



**Caution:** Alerts you to conditions where you can damage the equipment.

---



**Danger:** Alerts you to conditions where you can get an electrical shock.

---



**Warning:** Alerts you to conditions where you can cause the system to fail or work improperly.

---



**Note:** A Note alerts you to important information.

---



**Tip:** Alerts you to additional information that can help you perform a task.

---





**Security note:** Indicates a point of system security where a default should be changed, or where the administrator needs to make a decision about the level of security required for the system.



**Warning:** Alerts you to ground yourself with an antistatic grounding strap before performing the maintenance procedure.



**Warning:** Alerts you to remove the <Product Name short> main unit and expansion unit power cords from the ac outlet before performing any maintenance procedure.

These text conventions are used in this guide to indicate the information described:

Convention	Description
<b>bold Courier text</b>	Indicates command names and options and text that you need to enter. Example: Use the <b>info</b> command. Example: Enter <b>show ip {alerts   routes}</b> .
<i>italic text</i>	Indicates book titles
plain Courier text	Indicates command syntax and system output (for example, prompts and system messages). Example: Set Trap Monitor Filters
<b>FEATURE HOLD RELEASE</b>	Indicates that you press the button with the coordinating icon on whichever set you are using.
separator ( > )	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.

## Related publications

Related publications are listed below. For more information about the Avaya Business Communications Manager 6.0 documentation suite, see *Documentation Roadmap* (NN40170-119).

*Avaya Business Communications Manager 6.0 Configuration — Telephony* (NN40170-502)

*Avaya Business Communications Manager 6.0 Configuration — Remote Worker* (NN40171-505)



# Chapter 2

## Virtual private network configuration overview

The virtual private network (VPN) feature provides VPN client capability to the following IP sets:

- Avaya 1120E IP Deskphone
- Avaya 1140E IP Deskphone
- Avaya 1150E IP Deskphone

There are four main steps to configure the Avaya Business Communications Manager (Avaya BCM) and the IP deskphone for virtual private network (VPN) use in a remote worker setup:

- 1 [Configuring the BCM for remote IP sets using VPN \(page 13\)](#)
- 2 [Setting up the secure router \(page 17\)](#)
- 3 [Configuring the IP deskphone \(page 19\)](#)
- 4 [Installing the pre-configured phone in a home office \(page 21\)](#)

The set up described in this guide uses a BCM50be equipped with an integrated secure router. As part of the installation, a firewall is configured. It is recommended that you connect to the equipment using the OAM port on the BCM to avoid the possibility of lockout.

The BCM and the integrated secure router each have a static IP address on the same network. The secure router serves DHCP addresses to additional hardware (such as the IP sets). The IP sets at the remote site receive DHCP addresses on this same network after they securely establish a connection using the VPN.

In the set up described in this guide, the BCM is connected directly to the Internet through the integrated secure router. A static IP address is assigned by the Internet Service Provider (ISP). The IP sets used in this set up are Avaya 1140E IP deskphones.

The following table provides the configuration details for the BCM network.

**Table 1** BCM network configuration details

Parameter	Value
<b>Local network</b>	
Subnet mask	255.255.255.0
Integrated secure router IP	172.16.1.1
BCM50be IP	172.16.1.2
Dynamic address range	172.16.1.120 to 172.16.1.125 (assigned by the integrated router to be used by IP sets)
<b>OAM LAN default values</b>	
OAM port	10.10.11.1
Subnet mask	255.255.255.255

**Table 1** BCM network configuration details

Parameter	Value
<b>Internet</b>	
BCM public IP	68.100.10.51

A computer connected to the OAM port is assigned a DHCP address of 10.10.11.2. Business Element Manager and Internet Explorer connect to the BCM on the OAM port.

# Chapter 3

## Configuring the BCM for remote IP sets using VPN

Complete the following procedures to configure the BCM to support IP sets that join the corporate network through a virtual private network.

### Setting up the BCM

Before you start this procedure, ensure you have

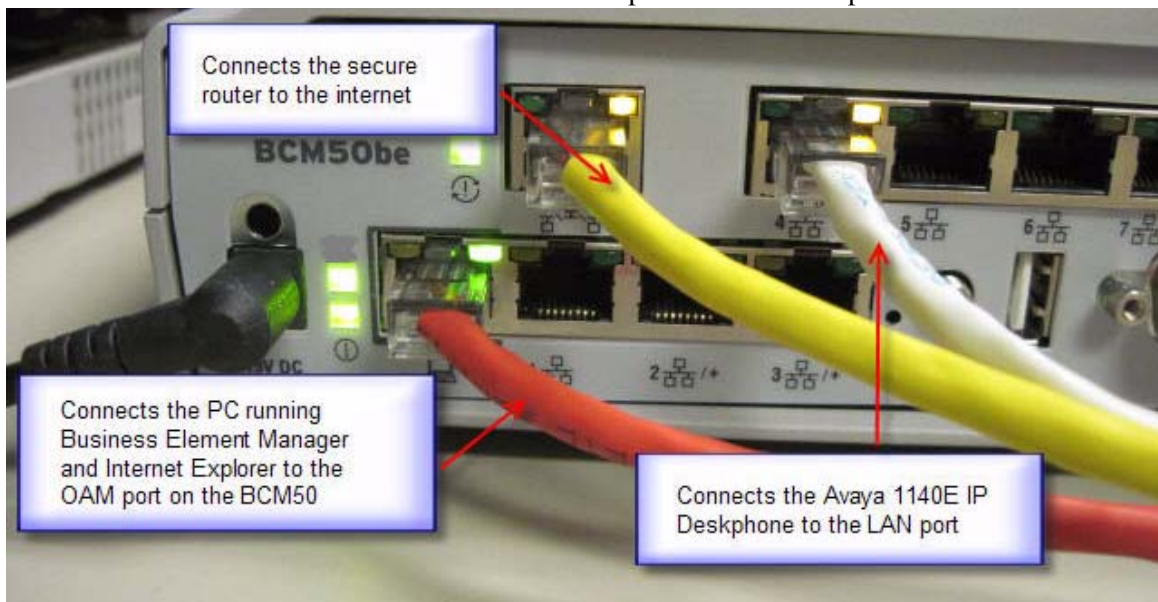
- enough licenses for all IP sets on the BCM
- a license file which enables the VPN on the IP set

1 Connect the cables as shown in the following figure.

The yellow cable connects the secure router to the Internet.

The red cable connects the PC that is running Business Element Manager and Internet Exporter to the OAM port.

The white cable connects the 1140E IP deskphone to the LAN port.



2 In the Business Element Manager, go to **Configuration > System > IP Subsystem > General Settings**.

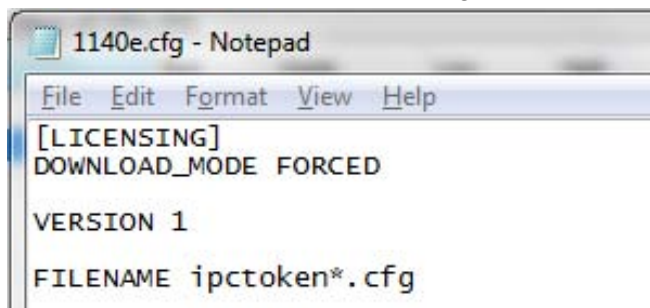
3 Configure the **IP settings**, **Public Network**, and **DNS Settings** fields.

- 4 Go to **Configuration > System > Keycodes**, and install the IP Client Seat license. For more information on keycodes, see *Keycode Installation Guide* (NN40010-301).



**Note:** You must have enough licenses for all the IP sets on the BCM.

- 5 Use a text editor to create an 1140e.cfg file.



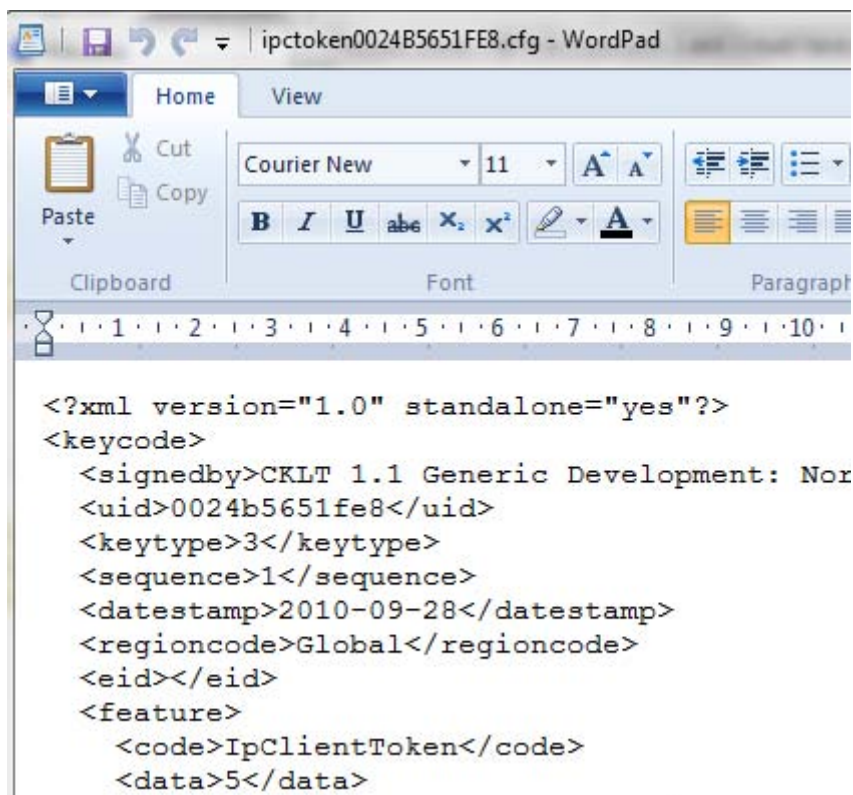
```
[LICENSING]
DOWNLOAD_MODE FORCED

VERSION 1

FILENAME ipctoken*.cfg
```

- 6 Rename the license file that enables the VPN on the IP set to ipctoken0024B5F693D2.cfg.

You must rename the license token file to match the MAC address of the specific phone that you are setting up. Ensure the file name matches the case of the MAC address printed on the back of the set.



```
<?xml version="1.0" standalone="yes"?>
<keycode>
  <signedby>CKLT 1.1 Generic Development: Nor
  <uid>0024b5651fe8</uid>
  <keytype>3</keytype>
  <sequence>1</sequence>
  <datestamp>2010-09-28</datestamp>
  <regioncode>Global</regioncode>
  <eid></eid>
  <feature>
    <code>IpClientToken</code>
    <data>5</data>
```

- 7** Go to **Configuration > Resources > Telephony Resources**.
- 8** In Telephony Resources panel, in the Configured Devices column, click **IP Sets**.  
The IP Terminal Global Settings panel appears in the lower pane.
- 9** In the IP Terminal Settings pane, configure the settings.
- 10** Upload the 1140e.cfg files to the BCM.
- 11** Upload the iptoken\*.cfg file to the BCM.





---

# Chapter 4

## Setting up the secure router

---

Complete the following procedure to set up the secure router for VPN.

You must be logged into the BCM50 and into the secure router interface to complete this procedure.

- 1 In the router interface, go to **Main Menu > LAN > IP tab**.
- 2 In the LAN TCP/IP area, configure a static address for the router.
- 3 Configure DHCP for a range of dynamic addresses.
- 4 Go to **Main Menu > WAN**.
- 5 In the WAN IP tab, set the WAN IP of the router to the static IP assigned by your ISP.
- 6 Go to **Main Menu > WAN**.
- 7 In the SUA/NAT tab, set NAT to **SUA Only**.
- 8 On the SUA Server tab, ensure the Default Server is set to 0.0.0.0.
- 9 Go to **Main Menu > WAN**.
- 10 On the Firewall tab, create a firewall rule for UDP on port 4016.
- 11 In the Summary tab, select the **Enable Firewall** checkbox.
- 12 Click **Apply**.
- 13 Got to **Main Menu > System > VPN**.
- 14 In the Client Termination tab, select the Enable Client Termination checkbox.
- 15 In the Authentication area, select the **Local User Database** and **User Name and Password/Pre-Shared Key** check boxes.
- 16 In the Encryption area, select the five ESP check boxes.
- 17 In the IKE Encryption and Diffie-Hellman Group area, select all the check boxes.
- 18 In the Assignment for Client IP area, select the **Use Static Addresses** check box.
- 19 In the VPN -Client Termination - Advanced tab, in the NAT Traversal area, select the **Enabled** checkbox.
- 20 Got to **Main Menu > Auth Server**.
- 21 In the Local User Database tab, create a user account for each IP set that you want to have connected through the VPN. Select a line in the Local User Database table.
- 22 Click Edit.
- 23 In the User Edit screen, select the **Active** checkbox.
- 24 Complete the fields with the user information, including user ID and password.
- 25 Create the IP Sec User Profile.

- 26 In the Remote User area, type a unique Static IP for each new user account you create. You must assign one static IP to each user.
- 27 In the Split Tunneling drop-down list, select **Disabled**.
- 28 Click **Apply**.

---

# Chapter 5

## Configuring the IP deskphone

---

Complete the following procedures to configure the phone that you want to deploy to a remote worker for use with VPN.

Before you complete this procedure, ensure you have set the registration password in Business Element Manager. To set the registration password, go to Resources > Telephony Resources > IP Terminal Global Settings Tab > Enable global registration password checkbox > global password field.

### Configuring network settings on the IP deskphone

- 1 Unpack and plug in the phone.  
A large Avaya logo flashes when the LEDs in the corners of the phone extinguish.
- 2 When the small Avaya logo appears, immediately and quickly press the softkeys from left to right.  
A tone sounds.
- 3 Using the phone keypad, type the Administration password: **Color\*set**.
- 4 Press Network Configuration.
- 5 Press Auto.
- 6 In the configuration screen, press the AllMan key to select all check boxes.
- 7 Scroll down the screen and deselect the following check boxes. To scroll, use the navigation button. To select or deselect check boxes, press the enter button in the middle of the navigation button.
  - EAP Settings
  - VPN
  - S1 IP
  - S2 IP
  - Provision Server
- 8 Press **Config**.  
If the phone has no EAP, ignore this field and configure the remaining settings.
- 9 In the S1 IP and S2 IP fields, type the numeric IP address of the BCM for S1 and S2.
- 10 In the Provision field, type the IP address prefixed by http://.



**Note:** To type the colon (:) and slash (/) characters, use the number 1 key on the dial pad.

---

- 11 Verify that the cable is properly connected.
- 12 Press **Apply**.

The phone resets. At this time, the phone may automatically download any new firmware that it requires.
- 13 In the Registration Password screen, type the registration password.
- 14 In the Select a DN for this set screen, type a DN for the set.

The phone is now active on the local network.
- 15 Verify that the phone has downloaded its license file by navigating to **Services > Local Diagnostics > License Information**. Verify that the license appears and is valid.

### Configuring VPN settings on the IP deskphone

- 1 Navigate to the Configuration screen on the phone.
- 2 Use the navigation key on the phone to scroll to the VPN section.
- 3 Highlight VPN and deselect the checkbox.
- 4 Press **Config**.
- 5 In the VPN field, select the check box.
- 6 Press the right arrow on the navigation button to move to the next field.
- 7 Type the user name and password that you defined in Business Element Manager.
- 8 Scroll to the VPN Server 1 and VPN Server 2 fields, and type the IP address assigned by your ISP.



**Note:** The IP address is also the Public Address of the BCM.

---

- 9 Press **Apply**.
- 10 Disconnect the power and Ethernet cables.
- 11 Dispatch the phone to the remote worker.

## Chapter 6

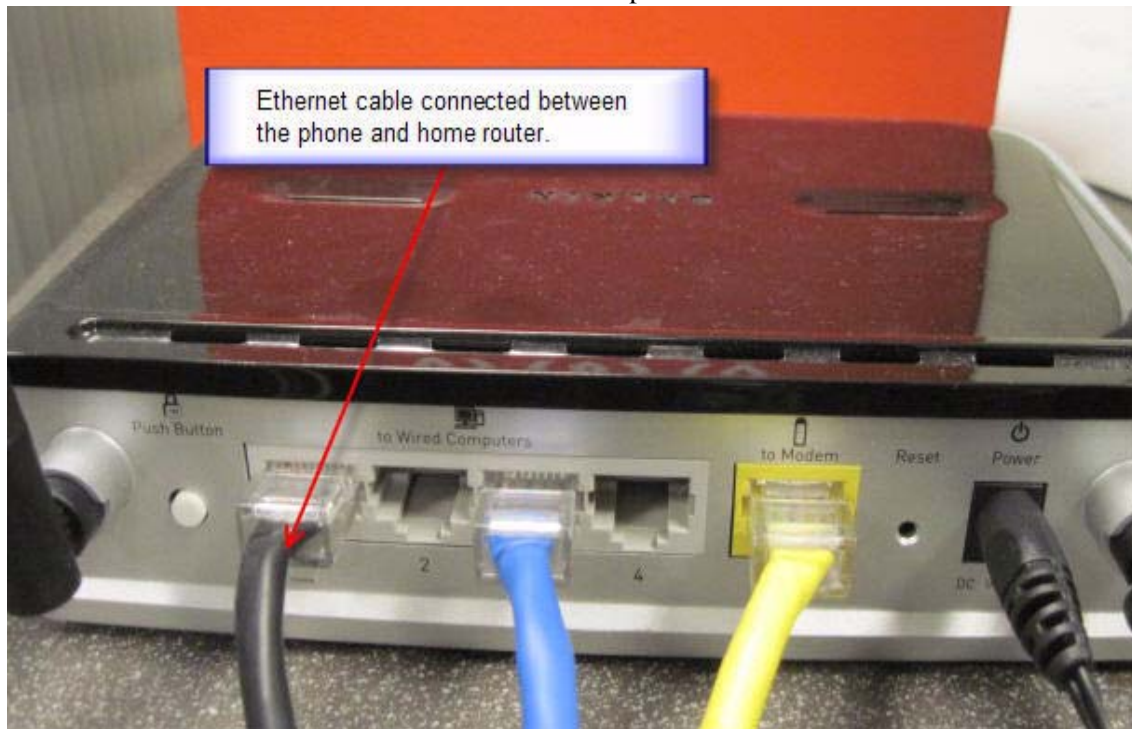
### Installing the pre-configured phone in a home office

---

This procedure can be completed by a remote worker in their home office when they receive their pre-configured IP deskphone.

Before you start this procedure, ensure you have an Ethernet cable.

- 1 Attach one end of the Ethernet cable to the Network port on the phone.
- 2 Attach the other end of the Ethernet cable to a free port on the home router.



- 3 Power up the IP phone.
- 4 Wait for set to boot.
- 5 When prompted, provide the password as assigned by your administrator.



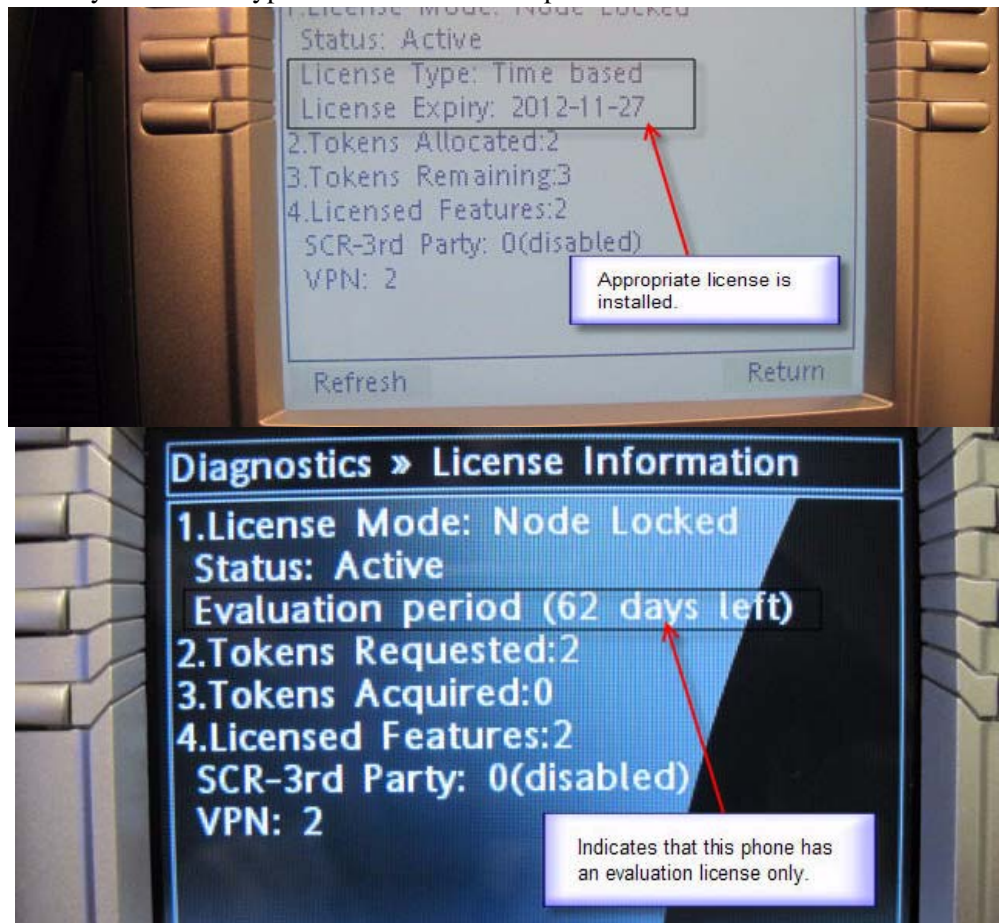
**Note:** When you are prompted for the password, a Connect VPN Failed message appears. You do not need to take any action at this time.

- 6 Press **OK**.  
Set is now active using the VPN.
- 7 Check for a dial tone.

### Verifying the VPN license

It is possible that the phone is in Evaluation Mode if the license was not properly configured. Without verification, this may not be detected until the Evaluation License is about to expire and you are notified of its expiration date. Complete this procedure to verify the license on your IP phone.

- 1 Go to **Services > Local Diagnostics > License Information**.
- 2 Verify the license type that is installed on a phone.



# Chapter 7

## Diagnostics

---

Complete the following procedure to verify some key diagnostics on the phone.

### **Verifying the license type**

- 1 From the main screen on the phone, quickly press the Services key twice.
- 2 Navigate to Local Diagnostics > License Information.
- 3 Confirm the license type installed.

### **Verifying the Secure Router port**

- 1 In the Secure Router interface, confirm that UDP is being forwarded on port 4016. (\*\* current picture is incorrect \*\*).

### **Verifying the Secure Router user connection**

- 1 In the Secure Router interface, confirm that the user is connected on VPN > SA Monitor.

