



Avaya Unified Communications for Small Business Solution Guide

15- 602858

Release 1

Issue 1

May 2008

© 2008 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Hardware Documentation, Document number 03-600759.

To locate this document on our Web site, simply go to <http://support.avaya.com> and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not 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. Customer and/or 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. 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 through the following Web site:

<http://support.avaya.com>

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

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>

Software License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT <http://support.avaya.com/LicenseInfo/> ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s):

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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 identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's Web site at:

<http://support.avaya.com/ThirdPartyLicense/>

Interference

Using a cell, mobile, or GSM telephone, or a two-way radio in close proximity to an Avaya IP Telephone might cause interference.

Security

See <http://support.avaya.com/security> to locate and/or report known vulnerabilities in Avaya products. See <http://support.avaya.com> to locate the latest software patches and upgrades. For information about secure configuration of equipment and mitigation of toll fraud threats, see the Avaya Toll Fraud and Security Handbook at <http://support.avaya.com>.

Table of Contents

Solution Overview - Avaya Unified Communications for Small Business	4
Technical Specifications	6
Steps to Configure Avaya Unified Communications for Small Business.....	8
Steps to Configure VPN Phones	8
Steps to Configure tested VPN Gateways	10
Steps to Configure Phone Manager Pro Telecommuter Mode	11
Steps to Configure Mobile Twinning	13
Administration Tips	14
<i>VPN Phone</i>	14
<i>VPN Gateways</i>	14
<i>Phone Manager Pro Telecommuter mode</i>	15
<i>Mobile Twinning</i>	16
Critical Information & Product Interactions	17
<i>VPN Phone</i>	17
<i>VPN Gateways</i>	18
<i>Phone Manager Pro Telecommuter mode</i>	18
<i>Mobile Twinning</i>	19
Related Documents	22

Solution Overview - Avaya Unified Communications for Small Business

This document provides a reference on how to set up the Avaya Unified Communications for Small Business solution.

Unified Communications for Small Business consists of the following components:

- VPN Phone licenses
 - VPN Phone licenses enable the supported Avaya IP phone (with appropriate firmware) to be used without the need for an external gateway at the remote location. This capability allows a supported Avaya IP phone to be connected and used over a secure IPSec VPN from any broadband Internet connection. The user of the VPN Phone will experience the same functionality as IP telephony users co-located with the IP Office. Avaya has tested specific VPN Gateways for this solution, and those are documented in this guide.
- Phone Manager Pro licenses
 - Phone Manager Pro is an application that resides on a user's PC and provides call handling capability. Phone Manager Pro includes Telecommuter mode. In this mode, Phone Manager Pro users will require a data connection to the IP Office network via VPN. At log-in, the user will indicate the external number to be used when making and receiving calls. By having the speech part of the calls initiated from the IP Office, the cost for those calls is assigned to the IP Office.
- Mobile Twinning licenses
 - Mobile Twinning allows an external phone to be twinned with an internal IP Office extension. The twinned device can be any external phone such as a mobile or home phone. When a call rings at the IP Office extension, both the IP Office extension and the external device will ring simultaneously enabling the user to answer the call from either device. If answered on the external device, busy indication is shown of the IP Office extension to internal users. If unanswered, the call can follow the rules set up for that extension such as covering to voicemail.

This document describes the following:

Technical Specifications of the IP Office hardware and software components required.

Steps to Configure the VPN Phones

Steps to Configure the tested VPN Gateways

Steps to Configure Phone Manager Pro Telecommuter Mode

Steps to Configure Mobile Twinning

Troubleshooting measures and references to troubleshooting tools.

This document assumes that the Avaya IP Office components, both hardware and system software, have been installed and are in proper working order.

Where available, references to IP Office system documentation and other related documents are provided. All documents referenced are available on the Avaya support website: www.avaya.com/support.

Technical Specifications

- Phone Manager Pro Licenses
- Mobile Twinning Licenses
- VPN Phone Licenses

Avaya Unified Communications for Small Business requires the following hardware components and software versions in order to support the above licensing:

- **IP Office System Hardware:**

The solution is available for IP Office 500, IP412, IP406v2, and Small Office Edition properly equipped with Smart Card (for IP500) or Dongle (for IP400 systems) and equipped to support the type and quantity of telephones and lines/trunks needed per customer requirements.

- **Voice Compression Module (VCM) resources:**

In order to support IP telephones and trunks, VCM resources are necessary.

- **IP500:**

- The IP500 supports up to 128 VCM resources using (2) VCM 64 cards fully licensed. Both the VCM 64 and the VCM 32 is a Base Card that occupies an available slot in the IP500 chassis. Other VCM options for the IP500 are the IP400 VCM 4, 8, 16, 24, and 30 modules which require the Legacy Card Carrier.

- **IP412:**

- The IP412 supports up to 60 VCM resources using (2) VCM 30 modules.

- **IP406v2:**

- The IP406v2 supports up to 30 VCM resources using (1) VCM 30 module.

- **Small Office Edition:**

- Built-in VCM resources (either 3 or 16) depending on Small Office Edition system model used.

- **Core Software:**

IP Office Release 4.1.9 (at minimum) using IP Office Manager 6.1.9

The solution relies on IP Office R4.1.9 (at minimum) for the VPN Phone License, available for specific IP hard phones, and the Telecommuter mode of the Phone Manager Pro User application. The administration of IP Office Release 4.1.9 requires using Manager 6.1.9 version.

- **User Software:**

Phone Manager Release 4.1.14

It is with this release of Phone Manager and in conjunction with IP Office Release 4.1.9, that the Telecommuter mode capability is available for Phone Manager Pro users. Telecommuter mode is built into Phone Manager Pro and is enabled on a per user basis through Manager. Those users with Telecommuter mode privileges designated will, at log-in, indicate the telephone number to be used.

- **Minimum PC requirements for Phone Manager Pro:**

64MB RAM

60Mb of free disk space

Pentium III 800MHz or Celeron3 800Mhz or Athlon B 650MHz

For further details on operating systems see **IP Office Technical Tip No. 198 – Minimum PC Specification required for IP Office Applications:**

http://support.avaya.com/elmodocs2/ip_office/tech/Global_IP_Office_Technical_Tip_198.pdf

- **Mobile Twinning:**

Mobile Twinning is programmed within Manager, the administration tool for IP Office. Mobile Twinning is enabled on a per user basis and is set within the User configuration form Twinning tab for that user.

- **Supported IP hardphone:**

5610, 5620, 5621, 4610, 4620, 4621 firmware 2.8.24 using VPN firmware version 2.3252

As noted above, the VPN Phone License is included in the Unified Communications for Small Business solution. The VPN Phone License is supported only on specific IP telephones for the IP Office. Local power is required for the IP phone. Note that the 4625 IP phone, though supported on IP Office, does *not* support the VPN Phone License on IP Office.

- **Compatible VPN Gateway:**

Avaya Security Gateway or third-party IPSec compliant (not included) security device is required at the IP Office site in order to support the remote VPN Licensed IP hard phone. It is not possible to terminate the VPN tunnel directly on the IP Office. The following VPN Gateways were tested:

- Juniper Secure Series Gateway 5
- Kentrox Q2300 Router
- Netgear FVS338 Router

- Netgear FVX538
- Adtran NetVanta 3305
- Sonicwall Tz170 Standard/Enhanced VPN Router
- Additional VPN Gateways are highlighted in the **Global IP Office Technical Bulletin No. 090 – General Availability (GA) of IP Office R4.1 Software:**
<http://support.avaya.com/japple/css/japple?temp.documentID=329924&temp.productID=129487&temp.releaseID=328264&temp.bucketID=264968&PAGE=Document>

Steps to Configure Avaya Unified Communications for Small Business

This section describes the steps necessary to configure the following components:

- VPN Phones
- Tested VPN Gateways
- Phone Manager Pro Telecommuter mode
- Mobile Twinning

The configuration steps below assume that the IP Office components, both hardware and system software (including importing the necessary Licenses), have been installed and are in proper working order. For details on system installation and administration:

See **IP Office Installation Manual** (Ref. No. 15-601042) for details:
<http://support.avaya.com/japple/css/japple?temp.documentID=328674&temp.productID=129487&temp.releaseID=328264&temp.bucketID=160259&PAGE=Document>.

See **IP Office Manager: 01. Using Manager** (Ref No. 39DHB0002UKAA) for details:

<http://support.avaya.com/japple/css/japple?temp.documentID=328686&temp.productID=129487&temp.releaseID=328264&temp.bucketID=159898&PAGE=Document>

See **IP Office Manager: 02. Configuration Settings** (Ref No. 39DHB0002UKAB) for details:


<http://support.avaya.com/japple/css/japple?temp.documentID=328688&temp.productID=129487&temp.releaseID=328264&temp.bucketID=159898&PAGE=Document>

Steps to Configure VPN Phones –

The following Avaya IP phones are supported for VPN deployment on the IP Office:

5610, 5620, 5621

4610, 4620, 4621

1. Launch and log into Manager
2. Select **License**  configuration form
3. Confirm that the License(s) for VPN Phone is Valid
4. Select **Extension** configuration form.
5. Select the **VoIP** tab.

6. Enable **VPN Phone Allowed**.
7. Click **OK**.
8. Repeat this for any other existing IP extensions that are going to be converted to VPN connection.
9. Save the configuration back to the IP Office system.

Further details on VoIP Extension phone administration can be found in the **IP Office Manager: 02. Configuration Settings** (Ref. No. 39DHB0002UKAB), Extension Settings | VoIP:

<http://support.avaya.com/japple/css/japple?temp.documentID=328688&temp.productID=129487&temp.releaseID=328264&temp.bucketID=159898&PAGE=Document>

Details on VPN phone installation can be found in the following documents:

IP Phone Installation Manual (Ref No. 15-601046), VPN Phones:

<http://support.avaya.com/japple/css/japple?temp.documentID=328676&temp.productID=129487&temp.releaseID=328264&temp.bucketID=160259&PAGE=Document>

VPNremote for 4600 series IP Telephone Pre-deployment, User Installation and Configuration Quick Start

<http://support.avaya.com/elmodocs2/vpn/19-601608.pdf>

Steps to Configure tested VPN Gateways

Avaya has tested the following VPN Gateways:

- Juniper Secure Series Gateway 5
- Netgear FVX538
- Kentrox Q2300 Router
- Netgear FVS338 Router
- Adtran NetVanta 3305
- Sonicwall Tz170 Standard/Enhanced VPN Router

In support of the Unified Communications for Small Business solution, Avaya Solution & Interoperability Test Lab tested the VPN Phone and Phone Manager Pro Telecommuter mode with the following VPN Gateways:

- Juniper Secure Series Gateway 5
- Netgear FVX538

The Juniper Secure Series Gateway 5 Application Note is posted to avaya.com:

Configuring the Juniper SSG as an IPSec VPN Head-end to Support the Avaya VPNremote Phone and Avaya Phone Manager Pro with Avaya IP Office - Issue 1.0

<http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/ipo-jun-ssg5.pdf>

The NETGEAR FVX538 ProSafe VPN Firewall Application Note is posted to avaya.com:

Configuring the NETGEAR FVX538 ProSafe VPN Firewall as an IPSec VPN Head-end to Support the Avaya VPNremote Phone and Avaya Phone Manager Pro with Avaya IP Office – Issue 1.0

<http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/ipo-ntgr-fvx538.pdf>



Testing of the VPN Phone had previously been conducted and Global IP Office Technical Tips were created for the following VPN Gateways:

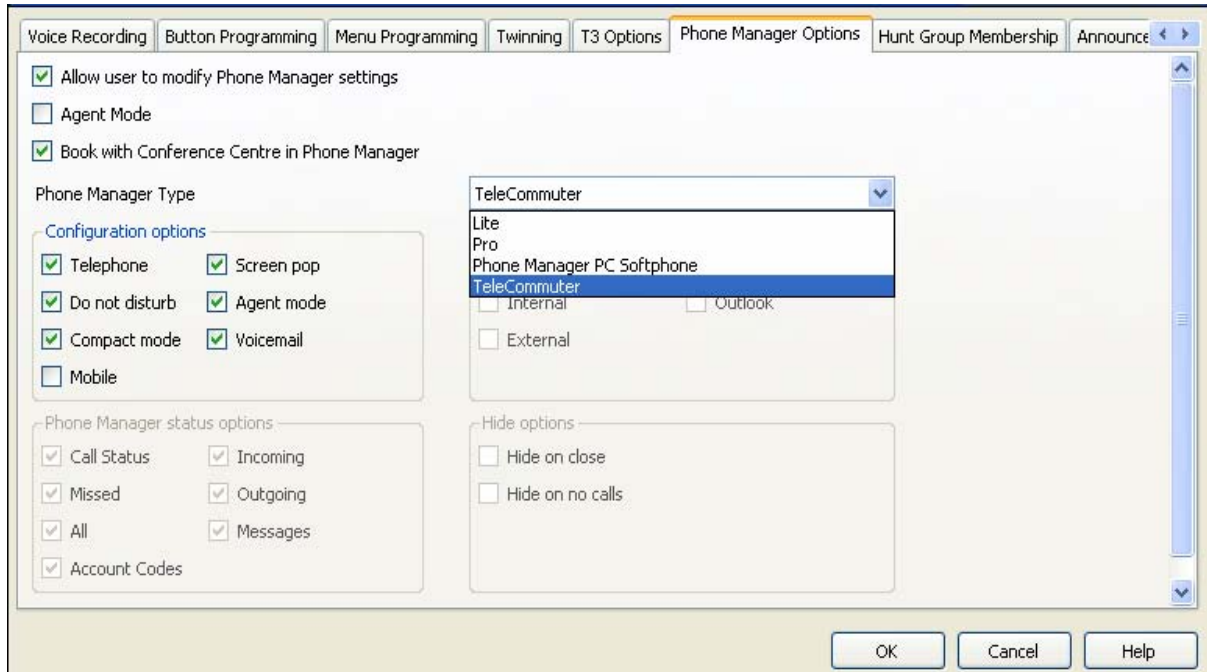
- Kentrox Q2300 Router
 - Global IP Office Technical Tip No. 185
 - September 2007
- Netgear FVS338 Router
 - Global IP Office Technical Tip No. 184
 - August 2007
- Adtran NetVanta 3305
 - Global IP Office Technical Tip No. 186
 - September 2007
- Sonicwall Tz170 Standard/Enhanced VPN Router
 - Global IP Office Technical Tip No. 190
 - September 2007
- Netgear FVX538
 - Global IP Office Technical Tip No. 196
 - January 2008

IP Office Global Technical Tips are located on the **IP Office: Technical Articles & Technical Tips** site:

<http://support.avaya.com/japple/css/japple?PAGE=ProductArea&temp.productID=129487&temp.bucketID=162326&temp.releaseID=306419&x=10&y=6>

Steps to Configure Phone Manager Pro Telecommuter Mode

1. Launch and log into Manager
2. Select **License**  configuration form
3. Confirm that the License(s) for Phone Manager Pro is Valid
4. Select **User**  configuration form
5. Select specific User
6. Select **Phone Manager Options** tab



- a. **Phone Manager Type:** select **TeleCommuter**
 - b. Complete other Phone Manager Option settings per User requirements.
 - c. When complete, select **OK**.
 - d. Repeat steps for any other Users.
7. Save the configuration back to the IP Office system.




Further details on Phone Manager installation can be found in the **IP Office Installation Manual** (Ref. No. 15-601042), System Components | Applications | Phone Manager:

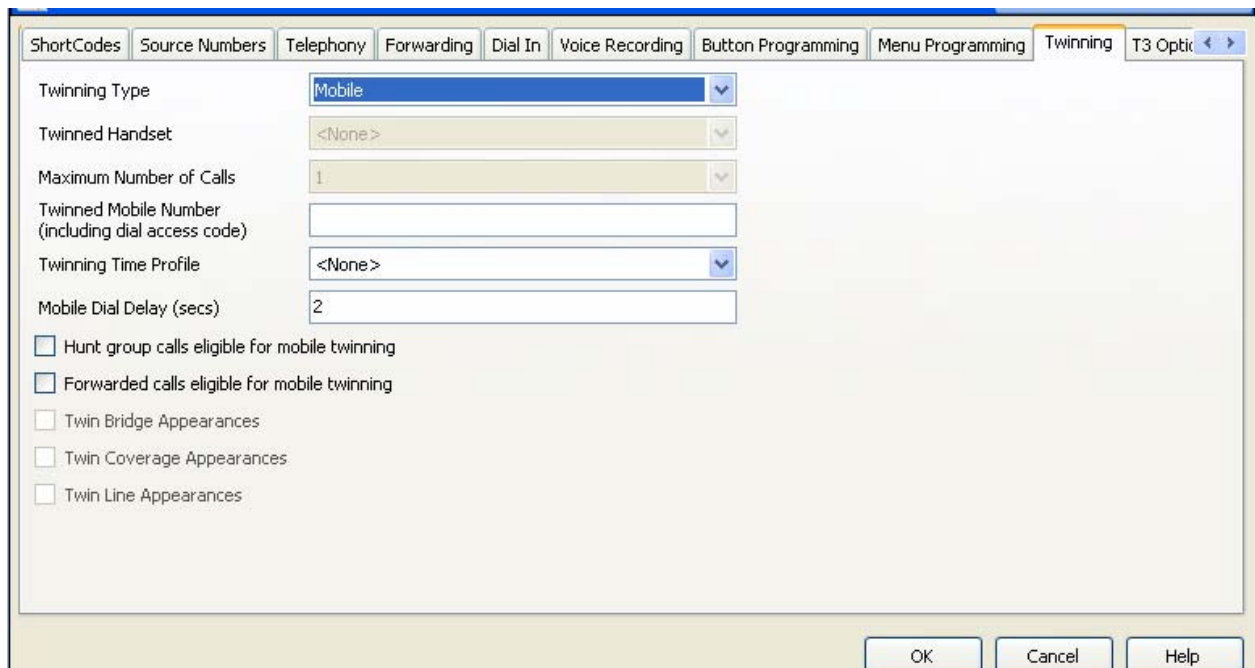
<http://support.avaya.com/japple/css/japple?temp.documentID=328674&temp.productID=129487&temp.releaseID=328264&temp.bucketID=160259&PAGE=Document>

Further details on Phone Manager administration can be found in the **IP Office Manager: 02. Configuration Settings** (Ref. No. 39DHB0002UKAB), User Settings | Phone Manager Options:

<http://support.avaya.com/japple/css/japple?temp.documentID=328688&temp.productID=129487&temp.releaseID=328264&temp.bucketID=159898&PAGE=Document>

Steps to Configure Mobile Twinning

1. Launch and log into Manager
2. Select **License**  configuration form
3. Confirm that License(s) for Mobile Twinning is Valid
4. Select **System**  configuration form
5. Select **Twinning** tab
 - a. **Send Original Party Information for Mobile Twinning:** *Default = On.* When on, the IP Office will attempt to send the ICLID information provided with the incoming call to the twinning destination. Depending on the services provided by the line provider, this information may not be allowed in which case it may either be removed or the twinned call blocked. If this occurs, the **Calling Party Information for Mobile Twinning** field should be used to send information that is acceptable to the line provider.
 - b. **Calling Party Information for Mobile Twinning:** *Default = Blank (Disabled).* This field is useable when **Send Original Part Information for Mobile Twinning** is off.
6. Select **User**  configuration form
7. Select specific User
8. Select **Twinning** tab



- a. **Twinning Type:** select **Mobile**
- b. **Twinned Handset:** blank

- c. **Maximum Number of Calls:** blank
 - d. **Twinned Mobile Number:** *Default = Blank*. This field sets the destination number for mobile twinned calls. This can be an external or internal number. It is subject to normal short code processing and should include any external dialing prefix if necessary. For details on entering an SCN number, refer to Manager Help.
 - e. **Twinning Time Profile:** *Default = <None> (Any time)*. This field allows selection of a time profile during which mobile twinning will be used.
 - f. **Mobile Dial Delay:** *Default = 2 seconds*. This setting controls how long calls should ring at the user's primary extension before being routed to ring at the twinning destination number. This setting may be used at the user's choice however it may also be a necessary control. For example, if the twinning number is a mobile device that has been switched off, the mobile service provider may immediately answer the call with their own voicemail service. This would create a scenario where the user's primary extension does not ring or rings only briefly.
 - g. **Hunt group calls eligible for mobile twinning:** *Default = Off*. This setting controls whether hunt group calls ringing the user's primary extension should also be presented to the mobile twinning number.
 - h. **Forwarded calls eligible for mobile twinning:** *Default = Off*. This setting controls whether calls forwarded to the user's primary extension should also be presented to the mobile twinning number.
 - i. When complete, select **OK**.
9. Save the configuration back to the IP Office system.

Further details on Mobile Twinning administration can be found in the **IP Office Manager: 02. Configuration Settings** (Ref. No. 39DHB0002UKAB), User Settings | Twinning
<http://support.avaya.com/japple/css/japple?temp.documentID=328688&temp.productID=129487&temp.releaseID=328264&temp.bucketID=159898&PAGE=Document>

Administration Tips

VPN Phone

Within Manager, by default, the Extension | VoIP setting for VPN Phone Allowed is set to Off. The field will be unavailable if there are no available licenses.

VPN Gateways

Please refer to Application Notes and IP Office Global Technical Tips.

Phone Manager Pro Telecommuter mode

- **Continuous Mode**

A key consideration for telecommuter operation is the trunk types involved. During Phone Manager log-in as a remote telecommuter, the user is able to select whether for that location they should select **Continuous Mode** or not. Continuous Mode changes the behavior of Phone Manager and must be used when trunks without reliable disconnect are in use or suspected to be in use between the IP Office and the user location.

- **Off**

If **Continuous Mode** is not selected, the IP Office will only call the remote location number when required, that is when making or receiving an IP Office call. For example when making a call using Phone Manager, the IP Office will call the remote location, when answered it will make another call using the number requested in Phone Manager. You can end the call through either Phone Manager or by replacing the handset.

- In this mode, it is possible for the remote location phone to make and receive non-IP Office calls. IP Office calls can be distinguished by their indication in the Phone Manager call details display.

- Calls will not succeed if the IP Office detects that a trunk using analog loop start or analog loop start emulation is being used.

- Pages calls are not redirected. Intercom and dial direct calls are redirected as normal calls.

- **On**

If **Continuous Mode** is selected, once you complete the Phone Manager login, the IP Office will call the remote location number and when answered the user should leave the connection open (off-hook). This will occur as part of either the test call if requested or after you click **OK**. Phone Manager is then used exclusively to make and answer calls, with the IP Office connecting the speech path to the remote location phone handset as and when required.

- This option should be used whenever analog loop start trunks or analog loop start emulation trunks are in use or suspected to be in use. This may include cellular connected to cellular gateways on analog trunks.

- If the IP Office has a mix of trunks, it may be advisable using outgoing group ID's, short codes and ARS forms to configure a specific dialing prefix that ensure that calls are routed via trunks that provide reliable disconnect and so remove the need for Off Hook Station operation.

- **Request Test Call**

If selected, the IP Office will attempt to make a test call to the remote location number. This option is unavailable if **Continuous Mode** is selected.

Mobile Twinning

Calls routed to the secondary device remain under control of the IP Office and can be pulled back to the primary if required. If either leg of an alerting twinned call is answered, the other leg is ended.

- **Time Profiles:**

In a user template, time profiles are used with users to control when features such as RAS, automatic voice recording, mobile twinning and user rights are enabled or disabled.

- **Button Programming Actions**

The **Emulation | Twinning** action can be used to control mobile twinning operation. Set on the primary extension, when that extension is idle the button can be used to set the twinning destination and to switch twinning on/off. When a twinned call has been answered at the twinned destination, the button can be used to retrieve the call at the primary extension.

- **Short Code Features**

The following short code actions are available for use with mobile twinning.

- **Set Mobile Twinning Number.**
- **Set Mobile Twinning On.**
- **Set Mobile Twinning Off.**
- **Mobile Twinned Call Pickup.**

- **Caller ID**

The options on the **System | Twinning** tab can be used to control which caller ID is sent with calls sent to the twinned destination. The use of those options may be restricted by the trunk type carrying the twinned call and the services provided by the line provider.

- **Mobile Twinning in a Small Community Network**

In order for mobile twinning to be used with SCN extensions as the destination, a short code or short codes must be added in order to route the calls to the correct SCN link. For example, a primary user at site A wants to twin with an extension at Site B, the two sites being linked by an IP trunk in Outgoing Group Id of 1. At Site A, add the system short code **8N/Dial/N/1**. For the primary to twin with extension 300 at Site B, the mobile twinning number should be entered 8300.

Critical Information & Product Interactions

VPN Phone

1. The VPN Phone requires an external VPN Gateway as outlined in this document. The VPN Phone cannot terminate directly into the IP Office via VPN IPsec Licensing option.
2. IP Phone will reboot when multiple log ins are attempted. Log in at an IP Phone. Log in at another IP Phone with the same user credentials (extension/password). The original logged-in IP Phone will reboot and the new IP Phone will register with IP Office. This behavior is seen with both the IP Phones and the VPNremote Phones.
3. It takes a very long time for the VPN Phone to reboot. There is no visual indication to the user while the phone is in the process of rebooting.
4. If the user name is greater than 8 characters, it will override the VPN remote logo on the phone display.
5. Route Based VPN is not a supported configuration for VPNremote Phones with Juniper SSG.
6. VPNremote Phones can only support preshare or certificate for Phase 1 negotiations.
7. It is recommended by the VPNremote Product House to set the Phase 1 and Phase 2 timers to 5 days.
8. The configuration used for testing uses a single Phone Configuration File Server to simultaneously support both non-VPN phones and VPN phones avoiding the need to maintain a separate file server for each firmware type. The IP telephone script files maintained on the Phone Configuration File Server, combined with the GROUP ID feature of the IP telephones, is used to a VPN phone. This file – **46xxupgrade.scr** needs to be placed in the **C:\Program File\Avaya\IP Office\Manager** folder.
9. Integration Testing Notes with **Netgear FVX 538**
 - a) Direct Media Path:
No audio was observed for calls between VPNremote phones using the NETGEAR FVX538. Direct Media path should not be allowed for the VPNremote phones.
 - b) VPNremote Phone Reboots when Phase 1 Lifetime Timer expires:
When the Phase 1 lifetime timer expired on the NETGEAR FVX538, the Avaya VPNremote Phone would reboot. The following messages would be displayed on the Avaya VPNremote Phone:
Time Elapsed (in seconds)
Exchanging keys
Lost VPN connection

Rebuilding tunnel. Please wait.

The user can press the "Reboot" softkey or the VPNremote Phone will reboot after 5 minutes. The recommendation from the VPNremote Product House is to set the Phase 1 and Phase 2 timers to 5 days.

- c) Replay Attack:
Replay Attack is not a configurable option on the NETGEAR FVX538.

10. Integration Testing Notes with **Juniper Secure Services Gateway 5 & Netgear FVX538**

- a) IKE ID Type on Avaya VPNremote Phone
The "IKE ID Type" field was set to "**FQDN**" on the Avaya VPNremote Phone as described in IP Office Global Technical Tip No.196, **Configuring a VPN Remote IP Phone with a Netgear FVX538 VPN Router**.
<http://support.avaya.com/japple/css/japple?PAGE=ProductArea&temp.productID=129487&temp.bucketID=162326&temp.releaseID=306419&x=10&y=6>
- b) VPN Client
Juniper NetScreen-Remote and NETGEAR VPN Client does not support No PFS for Phase 2 negotiations.

VPN Gateways

Refer to above **VPN Phone Critical Information & Product Interactions**

Phone Manager Pro Telecommuter mode

1. Telecommuter mode is only available with Phone Manager Pro.
2. While logged in to Phone Manager as a remote telecommuter:
 - a) Outgoing calls to an internal IP Office number or to collect voicemail are started using Phone Manager. It signals to the IP Office which connects a call to the remote location number and then to the internal number required.
 - b) Outgoing calls to a number external to the IP Office are also started using Phone Manager. It signals the IP Office which connects a call to the remote location number and then a call from the IP Office to the required external number as if it had been dialed from your normal IP Office extension. This will also be subject to your IP Office user dialing restrictions, if any.
 - c) Incoming calls to the user's normal IP Office extension are redirected to the

remote location number and accompanied by the caller details in Phone Manager call details display.

- d) Your normal internal IP Office extension is logged off while in Telecommuter mode. When you close Phone Manager you will be logged back into your extension unless you are set to forced login or another user has logged in at the extension.
 - e) Accessing IP Office short code features using dialing digits is not supported.
 - f) The remote location phone is assumed to be a single line phone. If call waiting is enabled in your IP Office configuration it can be used for a single additional call when an existing call via the IP Office is connected.
3. Integration Testing General Notes:
- a) During integration testing, the Hot Desking feature of IP Office was used with Phone Manager Pro. The Phone Manager Pro users have an internal IP Office extension with a hard phone. While logged in to Phone Manager as a telecommuter, the internal IP Office extension is logged off.
 - b) Integration testing resulted in remote worker, when using the Phone Manager Pro in Telecommuter mode, **does not** have the same functionality as a telephone co-located with the IP office. **Phone Manager limitations are:**
 - 1. Single Line appearance.
 - 2. No bridged call appearances at the Phone Manager Pro or of the Phone Manager Pro extension at other IP Office users when in this mode.
 - 3. Mobile Twinning feature is not available when using the Phone Manager Pro.
 - 4. Phone Manager Pro has single line appearance. If call waiting is enabled, the user can place the first call on Hold, otherwise the call goes to voice mail.

Mobile Twinning

Mobile twinning is only applied to normal calls. It is **NOT** applied to:

- Intercom, dial direct and page calls since these are answered automatically.
- Calls alerting on line appearance, bridged appearance and call coverage buttons.
- Returning held, returning parked, returning transferred and automatic callback calls.
- Follow me calls.
- Additional calls when the primary extension is active on a call or the twinning destination has a connected twinned call.

User BLF indicators and application speed dials set to the primary user will indicate busy when they are connected to a twinned call including twinned calls answered at the mobile twinning destination.

- **Account Codes**
If account codes are used, the user can not enter an account code when they answer a call at the external telephone.
- **Analog Lines**
These types of lines do not provide call progress signaling. Once a twinned call has been sent to an analog line, the IP Office assumes that it has been answered and stops ringing the primary extension.
- **User Rights Settings | Twinning**
Within Manager | User Rights configuration form, the Twinning tab can be used to set and lock the following settings relating to the use of mobile twinning. Use of mobile twinning requires entry of a mobile twinning license.
 - **Mobile Dial Delay**
Sets and locks the dial delay applied to calls eligible for mobile twinning.
 - **Hunt group calls eligible for mobile twinning**
Sets whether mobile twinning calls is applied to hunt group calls.
 - **Forwarded calls eligible for mobile twinning**
Sets whether mobile twinning calls is applied to forwarded calls.
- **User Rights Settings | Phone Manager**
Within Manager | User Rights configuration form, the Phone Manager tab can be used to set and lock which parts of Phone Manager the associated users can use or adjust. Mobile Twinning settings is included in these options to allow/deny the user access to modify Mobile Twinning settings.
- **Settings within SoftConsole**
 1. Click the required user in the SoftConsole directory panel.
 2. Click checkmark.
 3. Click **Forwarding**. The Forwarding window opens.
 4. Select **Mobile Twinning**.
 5. In the Mobile Twinning field, enter the telephone number that you want to 'twin' to the user's extension. Telephone numbers must be entered with no spaces.
 6. Click **OK** to save your changes.
- **Settings within VoiceMail Pro**
 - Both the internal and external telephones ring when a call is received. The call can be answered from either telephone.
 - If the feature Do Not Disturb (DND) is active for the user, any callers to the Internal extension number will hear the busy tone and the external telephone will not ring. If a caller is entered in to the DND exception list, for example using the application Phone Manager, only the internal telephone will ring.
 - If any of the forward options are active, both the external and the telephone where the calls are forwarded to will ring.
 - If the Follow Me option is active, only the telephone that the calls are forwarded to will ring. The external telephone number will not ring.

Within Voicemail Pro you can administer the mobile twinning features using call flows. Mobile twinning can be turned on or off and the external twinning number entered.

In a call flow the Generic action is used to control Mobile twinning. Within the Generic action details are entered in the specific tab. In the generic 'free format' field, the following syntax can be added.

- **CFG:Set MattR twinning_type Mobile**

For example, used to turn the Mobile twinning on for the named extension MattR. The extension number can be entered instead of the named extension. If mobile twinning has been previously used and then turned off, the previous mobile twinning number will become active.

- **CFG:Set MattR twinning_type Internal**

For example, used to turn the Mobile twinning off for MattR.

- **CFG:Set MattR mobile-twinning-number \$KEY**

For example, used to set the mobile twinning number.

Related Documents

Following is a list of documents that have been referenced throughout this document. Other helpful documents have also been provided. These documents relate to installing, additional administration, troubleshooting, and use of the components that comprise the Unified Communications for Small Business solution. These documents are available from the Avaya support Web site, www.avaya.com/support.

IP Office Installation Manual (Ref. No. 15-601042):

<http://support.avaya.com/japple/css/japple?temp.documentID=328674&temp.productID=129487&temp.releaseID=328264&temp.bucketID=160259&PAGE=Document>).

Further details on Phone Manager Installation can be found in the **IP Office Installation Manual** (Ref. No. 15-601042), System Components | Applications | Phone Manager

For details on operating systems and PC requirements see **Global IP Office Technical Tip No. 198 – Minimum PC Specification required for IP Office Applications:**

[http://support.avaya.com/elmodocs2/ip_office/tech/Global IP Office Technical Tip 198.pdf](http://support.avaya.com/elmodocs2/ip_office/tech/Global_IP_Office_Technical_Tip_198.pdf)

Details on VPN phone installation can be found in the following documents:

IP Phone Installation Manual (Ref No. 15-601046), VPN Phones:

<http://support.avaya.com/japple/css/japple?temp.documentID=328676&temp.productID=129487&temp.releaseID=328264&temp.bucketID=160259&PAGE=Document>

VPNremote for 4600 series IP Telephone Pre-deployment, User Installation and Configuration Quick Start

<http://support.avaya.com/elmodocs2/vpn/19-601608.pdf>

Configuring the Juniper SSG as an IPSec VPN Head-end to Support the Avaya VPNremote Phone and Avaya Phone Manager Pro with Avaya IP Office - Issue 1.0

<http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/ipo-jun-ssg5.pdf>

Configuring the NETGEAR FVX538 ProSafe VPN Firewall as an IPSec VPN Head-end to Support the Avaya VPNremote Phone and Avaya Phone Manager Pro with Avaya IP Office – Issue 1.0

<http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/ipo-ntgr-fvx538.pdf>

IP Office Manager: 01. Using Manager (Ref No. 39DHB0002UKAA):

<http://support.avaya.com/japple/css/japple?temp.documentID=328686&temp.productID=129487&temp.releaseID=328264&temp.bucketID=159898&PAGE=Document>

IP Office Manager: 02. Configuration Settings (Ref No. 39DHB0002UKAB):

<http://support.avaya.com/japple/css/japple?temp.documentID=328688&temp.productID=129487&temp.releaseID=328264&temp.bucketID=159898&PAGE=Document>

Further details on VoIP Extension phone administration can be found in the **IP Office Manager: 02. Configuration Settings** (Ref. No. 39DHB0002UKAB), Extension Settings | VoIP

Further details on Phone Manager administration can be found in the **IP Office Manager: 02. Configuration Settings** (Ref. No. 39DHB0002UKAB), User Settings | Phone Manager Options

Further details on Mobile Twinning administration can be found in the **IP Office Manager: 02. Configuration Settings** (Ref. No. 39DHB0002UKAB), User Settings | Twinning

IP Office Global Technical Tips are located on the **IP Office: Technical Articles & Technical Tips** site:

<http://support.avaya.com/japple/css/japple?PAGE=ProductArea&temp.productID=129487&temp.bucketID=162326&temp.releaseID=306419&x=10&y=6>

Global IP Office Technical Bulletin No. 090 – General Availability (GA) of IP Office R4.1 Software:

<http://support.avaya.com/japple/css/japple?temp.documentID=329924&temp.productID=129487&temp.releaseID=328264&temp.bucketID=264968&PAGE=Document>

Phone Manager User Guide (Document No. 15-600988):

<http://support.avaya.com/japple/css/japple?temp.documentID=328664&temp.productID=129487&temp.releaseID=328264&temp.bucketID=160257&PAGE=Document>

Mobile Twinning Quick Reference Guide (Reference No. 15-601403):
http://support.avaya.com/elmodocs2/ip_office/R3.2/ipo_mobile_twinning_qrg.pdf

Telephone **User Guides** and **Quick References Guides** for 5610, 5620, 5621, 4610, 4620, and 4621:
<http://support.avaya.com/japple/css/japple?PAGE=ProductArea&temp.productID=129487&temp.bucketID=160257&temp.releaseID=306419&x=17&y=4>

(C) 2008, Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by (R), (TM) or (SM) are registered marks, trademarks, or service marks, respectively, of Avaya Inc., with the exception of FORTUNE 500 which is a registered trademark of Time Inc. All other trademarks are the property of their respective owners.

3/2008