Avaya IP Office

Remote Access Guidelines for Implementation and Maintenance Support

Introduction

The Avaya IP Office family is the latest advancement in converged voice and data technology from Avaya. IP Office combines high-end voice and data applications normally reserved for large enterprises with easy to use tools that allow the smallest of businesses to deliver cutting edge customer service. The Avaya IP Office family is designed to solve the complex communications challenges of the home office, small office and medium enterprise with simple yet powerful communications tools.

Avaya Remote Access Position

At Avaya, we believe that our customers deserve all the support necessary to help their business succeed. A critical component of the Master Reseller Agreement and more importantly our customers’ Maintenance Agreement stipulates that remote access be made available on Avaya IP Office.

Avaya is committed to providing world-class support at a competitive price. It is necessary that all Avaya IP Office systems sold have remote access capability for Avaya to achieve this goal. All customers are billed prevailing Time and Material (T&M) rates if they contact an Avaya Technical or Care Center team and do not have remote access. Charges are applied whether the customer has an Avaya maintenance contract or not unless the customer agrees to initiate and fund a Web Ex session. Remote access is a critical component of the Avaya Maintenance Service Agreement as stipulated as a requirement.

It is also important that customers who take advantage of SMBS Services Enhancement offers such as Remote Administration with an unlimited number of software translations or Subsequent On-line Training provide Avaya with remote access so that they can be properly cared for.

Remote Access Overview

An IP Office installation typically has two system components, the IP Office control unit with expansion units that stations and outside lines plug into, and a Server PC with applications, such as Voice Mail Pro. Remote access to each component is separate, with different requirements.

Remote access to the Server PC is the best method, as it also gives access to the IP Office system; and, if the IP Office control unit has to be rebooted, connection is maintained to the Server PC and remote programming can continue by Avaya’s remote technical team.

Changes to the IP Office configuration, which is the system programming for lines, stations, and system call flow, are done with an application in the PC called Manager. Manager extracts a copy of the working configuration from the IP Office system, imports it into the PC, and changes are made offline in Manager. The updated configuration is then sent back to the IP Office system to activate the changes. Some changes in the IP Office configuration require the IP Office system to be rebooted. If the remote programmer is connected via dial up to the IP Office system, this connection must then be re-established. When the changed configuration is sent to the IP Office system, a backup copy is kept on the PC with Manager that sends the configuration.
For future maintenance recovery in case of system failure, at the minimum the local PC Manager application should be opened and connected to the IP Office. A copy of the changed configuration on the local PC can then be loaded onto the IP Office control unit for the recovery of the system from the backup configuration.

Programming changes to the Voice Mail Pro are done in the application running on the Server PC. Both the IP Office configuration file and the Voice Mail Pro mdb call flow file can be emailed to the customer site for manual installation into the IP Office system or the Voice Mail Pro system. This is not true remote access, but a method to deliver system programming.

**What is a Virtual Private Network (VPN)?**

A Virtual Private Network or VPN is a secure, private communications tunnel between two devices or networks across a public network (like the Internet or PSTN Frame Relay). VPN can be implemented using hardware-based systems, firewall-based systems, or software-based systems. VPNs are designed to allow a computer to be securely connected to an office network or to allow two networks to be connected to each other. Even though VPN data travels across a public network, it is secure because it uses very strong encryption. If anyone “listens in” on the VPN communications, they will not understand it because all of the data is encrypted. VPNs also monitor all traffic to ensure that the packets of data never get altered while traveling across the public network.

A VPN server is a piece of hardware or software that can act as a gateway into a network. Generally, it is always on and listening for VPN clients to connect to it. A VPN client is, most often, software that resides on a computer. The VPN client initiates a call to the VPN server and logs in. The computer with the VPN client software can then communicate with the network it is connecting to.

Today, there are two types of VPNs: (1) IPSec VPNs and (2) SSL VPNs.

- IPSec works at the Network Layer of the OSI model and secures all data that travels between two endpoints without association to any specific application. When connected on an IPSec VPN, the client computer is virtually a full member of the network it is connecting to. The majority of IPSec VPNs require third-party hardware and/or software and the workstation or device must have an IPSec client software application installed.

- SSL (Secure Socket Layer) VPNs require only a standard web browser with SSL capabilities built in to function. SSL VPNs also allow more precise access control because they provide tunnels to specific applications rather than to the entire corporate LAN. It is also easier to provide different access rights to different users. However, as was pointed out above, SSL VPNs access applications through a web browser which means that they only work for web-based applications. It is possible to web-enable other applications so that they can be accessed through SSL VPNs, however, doing so adds complexity. And, having direct access only to web-enabled applications means that users are unable to use the VPN for file sharing (downloading) or file backups.

**Avaya has chosen IPSec VPN technology for its remote VPN connectivity option.** As technology advances, SSL VPN and other technology may also become recommended options.

**Recommended Remote Access Methods**

Avaya customers are accountable for the reliability of the remote access method chosen. If a customer needs support from an Avaya Service center, it is the customers’ responsibility to know how to connect and enable the remote access if they choose to leave it unattended. Avaya recommends dedicated, unassisted remote access to ensure the integrity of the support it provides its valued customers but understands that some end users prefer to only make connection when support is required. If for whatever reason the
customer cannot enable remote access based on their current set-up, then Avaya will provide services based on the prevailing Time and Material (T&M) rates whether or not an Avaya Maintenance Agreement is in effect.

Avaya makes the following recommendations to support remote access capabilities. It should be noted that these guidelines are a work in progress and as new technologies and capabilities become available, these guidelines will be updated accordingly. Customers without remote access devalue the advantages they are entitled to with an Avaya Service Contract and incur incremental costs and potentially may experience delays in service.

**DANGER WARNING!!!**: *(Use RDC with caution -- RDC can cause multiple sessions of Delta Server and other applications -- This will cause data base corruption in CBC, CCC, and Call Accounting.)*

<table>
<thead>
<tr>
<th>Option Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Option #1**                     | **VPN Connection (IP SEC)** Customer establishes an Avaya approved VPN hardware/software configuration on their provided router gateway equipment (setup charges may apply). This provides continuous connectivity providing a path for SNMP trap alarms out and remote access to the Avaya Global Technical Services (GTS) organization and other approved remote connectors.  
Additionally, on the Server PC, customer provided (purchased and configured) remote control software will be needed: DameWare, PC Anywhere or RDC – refer to the Notes section below for details. |
| **Option #2**                     | **Dial Up To A Modem on the Server** Dial up to a Modem configured/connected on the Server PC with a dedicated (copper) line to the modem. This capability allows access to the Server PC applications, and access to the IP Office system via the Manager application residing on the local Server PC connected to the IP Office system. A Remote Access Server (RAS) dial in configuration must be created on the customer PC if using DameWare or RDC. PC Anywhere does not need a Remote Access Server configuration. No additional remote access equipment is needed in the IP Office system. This option requires a dedicated outside line connected to the modem.  
**NOTE #1**: In this configuration, there cannot be any alarming provided from the IP Office or the Server PC to Avaya. The SNMP traps require a dedicated connection for this to function. The remote maintenance call is extended when the failure information for the location isn’t available. There is no facility in the IP Office for retaining any IP Office alarms in storage.  
**NOTE #2**: For remote control of the PC, either DameWare or PC Anywhere software needs to be installed on the on-site Server PC, or, if the PC is running XP Professional or Windows 2003 Server, an RDC account can be created on the Server PC. Set-up options are the accountability (investment/labor) of the customer.  
**NOTE #3**: If VoiceMail Pro and a HP Server are deployed, this is the preferred and documented method to use as a dedicated modem and line is required. Refer to the HP Server Offer Definition resident on the [Avaya Enterprise Portal > Sales & Ordering > Under Indirect Channel Resources select Global Services Reference Library > Offer Definitions](https://www.avaya.com).
### Option #3

**Direct Dial-Up to IP Office**

Direct to IP Office (no server or by-passing the server). Dial up (copper line) using an internal modem port on Avaya IP Office with dedicated trunk port (403, 406, and 412 only) or port one (1) of IP Office Small Office Edition (SOE) or port one (1) of ATM trunk module on 403, 406 or 412. This option requires a dedicated outside line connected to the IP Office trunk port. This line cannot be used for inbound calls but can be used for outbound customer calling. (NOTE: If the customer has DID associated with their modem and directed to the internal modem.) This is direct to the IPO communication system when there is no voicemail server or PC connected to the system.

**NOTE #1:** In this configuration, there cannot be any alarming provided from the IP Office or the Server PC to Avaya. The SNMP traps require a dedicated connection for this to function. The remote maintenance call is extended when the failure information for the location isn’t available. There is no facility in the IP Office for retaining any IP Office alarms in storage.

**NOTE #2:** Refer to the **NOTES** Section below for related information on the Secure Access & Control (SAC) service offer.

### NOTES:

- **Web Ex:** Customers can initiate and fund a Web Ex in the event other remote access options are not readily available.

- **Network Addresses:** GTS SOCKS supported IP address ranges need to be used in order for the Avaya GTS remote connection tools to function properly. Avaya B-B VPN will use 172.16-17.x.y addresses and Dial-Up PPP will be assigned 10.1-3.x.y or 10.121-127.x.y addresses. These need to be unique addresses within Avaya and cannot be arbitrarily assigned.

- **DameWare:** 3rd party application supplied with each IP Office application CD and is a free install. This software needs to be installed on any PC in which the application requiring support is running. For example, if VoiceMail Pro is installed on a separate PC from the Manager, then DameWare needs to be installed on both PCs for access to both applications.

- **PC Anywhere:** Third party application that is licensed to the host and client. PC Anywhere is not provided by or licensed through Avaya. This software needs to be installed on any PC in which the application requiring support is running. For example, if VoiceMail Pro is installed on a separate PC from that of Manager, then PC Anywhere needs to be installed on both PCs for access to both applications. Avaya technical support resources will use PC Anywhere to aid in the troubleshooting of certain issues, but the BusinessPartner must provide connectivity to the site and username and password information.

- **SAC Lite:** Avaya Global Services makes available the Secure Access & Control (SAC) service offer which provides for remote servicing of communications products attached to a customer’s converged network by greatly enhancing security associated with remote access by Avaya Services personnel. SAC Lite is a subset of the SAC Offer that is targeted at customers that require a simple, very low-cost VPN remote servicing solution. Protection against unauthorized access to the customer’s computing systems that share a local area network (LAN) with communications systems is realized through adoption of secure IP-VPN connectivity obviating the need for analog modems and telephone lines. Combined with strong, centralized authentication, authorization and accounting, SAC Lite reduces the potential for unauthorized access to network elements and provides a detailed audit trail of remote accesses to the customer’s products in the Avaya network.

### Avaya Web Conferencing

Avaya Web Conferencing (AWC) can be used by Avaya remote programmers or maintenance personnel to access the Server PC (if Internet access is available on the customer-provided PC). This option can be used when one of the approved methods noted above fails for whatever reason, however Avaya offers no guarantees. If the customer does not utilize one of the approved methods and Avaya cannot access the customers’ solution via AWC, then the customer is responsible for T&M charges associated with not meeting the remote access requirements.
It should be noted that there are occasions where the customer server may have access to the Internet, Java may be installed and enabled but it still may not work due to other settings in the PC. It is important that the contact at the customer site have the expertise to troubleshoot and correct the issue on the server as Avaya is not responsible for troubleshooting the customers’ server. If Avaya must dispatch a Technician to resolve problems that cannot be resolved due to poor connectivity, the customer would be charged prevailing T&M rates.

The Server PC must be able to access the Internet preferably with a high-speed connection. Again, to establish the AWC session, the customer must provide a technically astute individual to work with Avaya service personnel. The customer connects to the AWC site. The remote programmer will initiate an AWC session. AWC provides control of the Server PC without additional software on the Server PC or an Administrator login, as it is a customer initiated connection to the AWC site. This capability allows access to the Server PC applications, and access to the IP Office system via the Manager application. No additional remote access equipment is needed in the IP Office system. There is no remote alarming using Avaya Web Conferencing.

Customer Responsibilities

The Sales Team for the IP Office solution must work with the customer to select the method desired for remote access. The customer is solely accountable to enable remote access. If Avaya cannot gain access to the customers’ solution, then services will be provided based on the then current prevailing Time and Material (T&M) rates whether or not an Avaya service agreement is in effect.

Sales teams will order IP Office equipment, such as an internal modem card or additional ATM 4 port card, depending on the method of remote access selected. HP Servers provided by Avaya are equipped with a modem inside the HP Server.

Depending on the remote access method selected, the customer is to provide a modem for the customer Server PC, dial up copper line, and any additional software needed for the Server PC. PC Anywhere can be sold on the Server PC if customer does not have a copy to install. DameWare is the remote control software recommended by Avaya IP Office Technical support. Access to the Server also gives access to the IP Office system.

Unless specifically negotiated in the contract, the customer is responsible for all programming and configurations in the customer Server PC and the remote access application selected.

All sales colleagues are encouraged to consult with the Avaya SMBS Project Coordinator and/or IPO Software Specialist to help select the appropriate remote access method.

IPO Software Specialist/Programmer Responsibilities

- Verify remote access option selected.

Implementation Team Responsibilities

The Avaya Technician is required to:

- Verify that a remote dial access capability exists. — When dial up is the selected option, the customer is responsible for providing a dedicated dial-up loop start line.
- Install dial modem for remote access capability.—on Avaya HP servers – on customer provided Servers; it is the customer responsibility to set up the modem and remote access capability, such as logins, passwords, and configuration on their Server.
Avaya Proprietary

- Verify connectivity of remote access modem to the appropriate support center. —when the VPN option is used by the customer, the customer will be responsible for configuring the customer provided VPN equipment and software. Technician will verify VPN connection with support center.
- Register the Avaya IP Office and applications hardware.
  - The Registration Team will require the following items:
    - SAP Order #
    - Installation location
    - Modem telephone number & password or IP Address and password —when the VPN option is chosen, the settings and configuration of the VPN
    - Model number of the Server —on Avaya HP servers
    - Serial #. There is a label on the Server as well as the outside of the original shipping box. — on Avaya HP servers
    - To register IP-Office systems (and HP Servers) call 1-800-552-3293.
    - Check with the SMBS Project Coordinator for Avaya IP Office, they can assist you with this registration if they haven’t completed it already.

The BusinessPartners’ technical staff is required to use the Product Registration Tool (see below for registration process information). In the “Comments” section on the screen requesting remote access line information, a notation should be made regarding pertinent information in connection with the remote access.

Avaya IP Office – Product Registration

The Product Registration Tool (https://prodreg.avaya.com) ensures proper registration of Avaya IP Office solutions. IP Office solutions must be registered when they are sold with an (1) Avaya Maintenance Agreement, (2) HP Server or when (3) In-Warranty Support is ordered.

Information regarding the tool can be obtained on the Avaya Enterprise Portal > Support > Installation & Maintenance > Product Registration.

Conclusion

Avaya has a strong commitment to its BusinessPartners and customers and the price we charge to support a customers’ business is predicated on having remote access. If a customer experiences problems and they do not have remote access, delays in repairing the system will likely occur and required dispatches of Field Engineers is billable as they are out of scope to the customers’ Maintenance Agreement when remote access isn’t available. Dispatching a Field Technician can be costly for our customers and Avaya. Dispatches result in incremental expense and inconvenience for all.

Our goal is to ensure customers have maximum confidence in the Avaya communication solution and service plan that they invested in. Having access to the customers’ systems provides us with the valuable information we need to successfully diagnose the system and take corrective action as well as support subsequent training and administration requests quickly with minimum disruption to their business.

Contacts

- Avaya Technology & Consulting (ATAC) organization
  - 888-297-4700  atac@avaya.com (Must state “SERVICES”)

- Avaya Global Technical Services (GTS)
  - BusinessPartner Technicians: 877-295-0099 (SMBS customers would call 800-628-2888, enterprise customers would call 800-242-2121)
  - Avaya Field Service Technicians: 800-552-3293 or 800-248-1234

Avaya Inc. – Proprietary.

Use pursuant to the terms of your signed agreement or Avaya policy.
Developed By:

James W. Allen
Avaya IPO Software Specialist
407 838 4234
allenjw@avaya.com

Kim Bennett
Global Technical Service (GTS) – New Product Development
720 444 5267
kbenndtt@avaya.com

Debbie Brandt
SMBS Services Offer Management
908 953 6025
debbieboyce@avaya.com