

Avaya IP Office Platform Support Certified Exam

Avaya 78201X

Version Demo

Total Demo Questions: 22

Total Premium Questions: 222

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, IP Office Platform Overview	46
Topic 2, IP Office Platform Installation and Initial Configuration	28
Topic 3, IP Office Platform Configuration	90
Topic 4, IP Office Platform Maintenance and Troubleshooting	58
Total	222

QUESTION NO: 1

What is the additional security measure required for upgrading the IP Office 500 V2 using the Upgrade Wizard?

- A. Biometric authentication
- B. Firewall authentication
- C. Two-factor authentication
- D. Captcha authentication

ANSWER: C

Explanation:

Two-factor authentication is the required additional security measure. An IP Office upgrade is a privileged maintenance operation: it can replace core system software, restart telephony services, and affect the configuration and operation of the entire system. Requiring a second factor in addition to the administrator's normal sign-in credentials provides stronger assurance that the individual authorizing the Upgrade Wizard operation is the legitimate, authorized administrator. This protection is particularly important where management access is available across the network, since a password by itself may be exposed, reused, or compromised. The second factor supplies an additional independent verification step before a high-impact action proceeds, helping protect the IP Office 500 V2 from unauthorized software changes. This approach is consistent with Avaya's general emphasis on securing administrative access and using appropriate authentication controls for IP Office management. Consult the applicable release documentation and security guidance before beginning the upgrade, and ensure that the administrator has the required access and authentication method available. See the [Avaya IP Office support portal](#) and [Avaya IP Office product documentation resources](#).

QUESTION NO: 2

After the ignition process, what tool can be utilized to configure the IP500 V2 and Server Edition systems, in a step-by-step manner, for configuring Users, Groups, and Lines?

- A. Avaya Management Tool
- B. Configuration Manager
- C. Management Wizard
- D. Configuration Wizard

ANSWER: D

Explanation:

Configuration Wizard is the guided IP Office configuration facility used after the system has completed ignition and is accessible for administration. It presents configuration tasks in a structured, step-by-step workflow, making it appropriate for building the core telephony setup without manually navigating every configuration form. In particular, the wizard supports the initial definition of users and their extensions, hunt groups, and external line settings, along with the related basic system parameters required for those objects to operate together.

This is applicable to IP500 V2 control units and IP Office Server Edition environments because both use IP Office configuration data and the IP Office administration toolset. The wizard is especially useful during initial deployment or when a technician needs a guided method to create standard user, group, and trunk/line arrangements consistently. Once the guided work is complete, the resulting configuration can be reviewed and refined through the normal IP Office configuration interface where more advanced settings are required.

Avaya's product documentation and downloads are available through the [Avaya Support portal](#); use the IP Office documentation section for the release installed on the system. See also the [Avaya Documentation portal](#) for IP Office administration guides and configuration-wizard procedures.

QUESTION NO: 3

What are two options to install licenses for an Avaya IP Office™ release 11 system? (Choose two.)

- A. the ADI licenses that are installed locally on the Avaya IP Office™ system
- B. the Avaya IP Office™ system connecting to a Media Manager server hosting the appropriate licenses
- C. the PLDS license file that is installed locally on the Avaya IP Office™ system
- D. the Avaya IP Office™ system connecting to a WebLM server hosting the appropriate licenses

ANSWER: C D

Explanation:

Avaya IP Office Release 11 supports licensing either through a locally installed license file or through centralized licensing with Avaya WebLM. With local licensing, entitlement information is obtained through Avaya's Product Licensing and Delivery System (PLDS), and the resulting license file is uploaded to and stored on the IP Office system. IP Office then validates and uses the entitlements locally for the features, users, trunks, or applications that require them. This method is appropriate where the deployment does not use a centralized license server or where independent local operation is required.

Alternatively, IP Office can be configured to obtain its licenses from an Avaya WebLM server. WebLM provides centralized license management, allowing the server to host the applicable license entitlements while IP Office connects to it for license use. This is particularly useful when an organization manages licensing across systems or applications through a common licensing service. Avaya's IP Office documentation identifies locally installed PLDS license files and WebLM-hosted licenses as supported licensing approaches for Release 11. See the [Avaya IP Office Platform Release 11.1 documentation](#) and the [Avaya Support documentation portal](#) for IP Office licensing administration guidance.

QUESTION NO: 4

A customer wants to restrict certain users from dialing out after 5 PM, limiting them to only dialing emergency numbers and internal extensions. Which two programming options can you use to achieve this?

- A. Source Number
- B. Time Profiles
- C. System Short Codes
- D. Account Codes
- E. User Permissions

ANSWER: A C

Explanation:

Source Number and **System Short Codes** are the relevant IP Office programming mechanisms for implementing targeted call restrictions. A source number can be used to identify the originating user or extension to which a restriction applies. This lets an administrator scope the restriction to the selected users rather than applying a blanket restriction to every extension in the system. The source-number match is therefore the basis for distinguishing the users whose external dialing must be controlled.

System Short Codes provide the dial-plan logic used to intercept and handle dialed digits. They can be programmed to bar outbound patterns while allowing the explicitly required emergency-number patterns and internal extension dialing. The associated restriction logic can be arranged around the required operational period so that the affected users are prevented from placing normal external calls after the defined cutoff while permitted calls continue to complete. Together, source-based identification and system short-code digit handling provide a flexible way to apply time-sensitive, user-specific dialing control in IP Office.

QUESTION NO: 5

What displays the progress of a software upgrade on an expansion system?

- A. Web Manager Dashboard
- B. System Tab
- C. System Monitor Program
- D. IP Office Manager on the expansion system

ANSWER: A

Explanation:

Web Manager Dashboard is correct. In an IP Office Server Edition solution, upgrades are managed and monitored centrally through Web Manager. When an upgrade is initiated for an expansion system, the Web Manager Dashboard provides the operational view of the upgrade activity and its progress. This centralized status display is especially important in a multisystem Server Edition deployment because the expansion system is a component of the overall solution and may restart during software installation. The dashboard lets the administrator follow the upgrade state without needing to connect separately to the expansion server while the process is underway. Administrators should allow the upgrade and associated reboot processes to complete before performing follow-up administration or configuration actions. Avaya's official documentation resources for IP Office and Server Edition administration, deployment, and maintenance are available through the [Avaya Documentation portal](#) and the [Avaya Support portal](#). These resources provide the release-specific upgrade procedures and compatibility guidance that should be reviewed before upgrading a Server Edition solution.

QUESTION NO: 6

Once the Avaya IP Office™ Server Edition is installed, which application can be used to install the required licenses for the system?

- A. System Status Application
- B. Manager Application
- C. Monitor Application
- D. one-X® Portal

ANSWER: B

Explanation:

Manager Application is the appropriate application for installing and administering IP Office licenses after an Avaya IP Office Server Edition deployment. Avaya IP Office Manager is the administration client used to connect to the IP Office system configuration, retrieve its current settings, and access the licensing functions. From Manager, an administrator can add the license file or keys supplied for the deployment and then save/merge the updated configuration back to the system. The system validates the licenses and displays their status, allowing the administrator to confirm that the required Server Edition, user, trunk, and feature entitlements are available and valid. This makes Manager central to post-installation system administration as well as licensing, configuration backup, extension programming, and feature management. Licensing must be applied to the IP Office configuration so that the relevant capabilities are enabled for operation. Avaya's IP Office documentation and support resources identify Manager as an IP Office administration tool and provide the supporting product documentation for configuration and license administration. See the [Avaya Documentation Portal](#) and the [Avaya Support site](#) for IP Office Manager and Server Edition documentation.

QUESTION NO: 7

Within the Configuration Wizard, which specific field must be populated first, before any other fields become visible?

- A. Network Configuration
- B. System Configuration
- C. Ignition Configuration
- D. User Configuration
- E. Country

ANSWER: E

Explanation:

Country must be selected first in the IP Office Configuration Wizard. This initial value establishes the regional operating context that the wizard uses to present the remaining configuration fields and defaults. In particular, IP Office must apply the appropriate telephony locale, including dialing conventions, tones, and other country-dependent settings, before it can safely expose the rest of the initial system configuration workflow. Consequently, the wizard initially limits the available input and then reveals the additional fields after a valid country selection has been made. This behavior helps ensure that subsequent configuration values are appropriate for the installation's regulatory and dialing environment. The country selection is therefore a prerequisite within the wizard itself, rather than a general configuration area such as network, system, ignition, or user configuration. For official IP Office product documentation and current installation/support resources, consult the [Avaya Support portal](#) and the [Avaya Support resources page](#).

QUESTION NO: 8

You have purchased a pre-configured Avaya IP Office™ Application Server. The server has both Voicemail Pro and one-X® Portal installed on it.

Which tool could be used to verify if both services are running?

- A. one-X® Portal interface: https:// < server Address > :9443
- B. Web Control: https:// < server address > :7071
- C. Manager Application
- D. Monitor Application

ANSWER: B

Explanation:

Web Control at `https://<server address>:7071` is the appropriate tool because it is the IP Office Application Server's centralized administration interface. Its status and service-management views identify the applications installed on the server and show their operational state. An administrator can therefore use one location to verify that both the Voicemail Pro service and the one-X Portal service are started and running. This is particularly useful on a pre-configured Application Server, where multiple IP Office applications share the same appliance or virtual server and must be checked at the server level rather than only through an individual end-user application interface. Web Control also supports further administrative actions, such as starting or stopping supported services and accessing relevant server configuration and diagnostic information, subject to the administrator's permissions. Avaya's IP Office documentation describes Web Control as the browser-based management interface for Application Server components and service status. Consult the [Avaya Documentation Portal](#) for the IP Office release-specific Server Edition and Application Server guides, and the [Avaya Support portal](#) for product documentation and support resources.

QUESTION NO: 9 - (SIMULATION)

Where can password rules and complexities be set for Users?

A From the Manager application go to Advanced > Security Settings and open General Settings

B From the User Portal go to settings and change the security settings

C. From the Web Manager, go to Call Management > Security.

D From the Manager application open your system configuration and select a user in the Users section and open the Security tab

ANSWER: See the explanation for the answer

Explanation:

Correct answer: A — From the Manager application, go to Advanced > Security Settings and open General Settings.

This is the system-wide location for configuring user password policy and complexity requirements, such as password length, complexity, and related password rules. The Security tab on an individual user is used for settings specific to that user, not the global password-rule policy.

QUESTION NO: 10

Which two profile licenses, that are used for user configuration, can support the Avaya Workplace client for Desktop (Desktop/Tablet VoIP client)? (Choose two.)

A. Office Worker User

B. Power User

C. Basic User

D. Remote Worker User

ANSWER: A B

Explanation:

Office Worker User and **Power User** are the applicable IP Office user-profile licenses for using the Avaya Workplace desktop/tablet VoIP client. An Office Worker profile is intended for an IP Office user who needs desktop productivity and unified-communications functions, including a supported soft-client experience. This allows the user to register and use the Avaya Workplace client for calling through the IP Office system rather than relying solely on a physical extension.

A Power User profile includes the Office Worker-level communications capability and adds broader mobility and advanced unified-communications features. Consequently, it also provides the user-profile entitlement needed to use Avaya Workplace as a VoIP endpoint. In IP Office administration, the selected user profile determines the licensed applications and endpoint capabilities available to that user, so assigning either of these profiles is the relevant licensing step before configuring the client and its extension details.

Avaya's IP Office documentation describes user-profile licensing and associated application capabilities in the [IP Office Release 11.1 documentation](#). Product and client documentation is also available through the [Avaya Support portal](#).

QUESTION NO: 11

A customer is planning a Small Community Network between two IP Office systems across a WAN. The design must provide reliable inter-site call routing and sufficient media-processing capacity for simultaneous calls.

Which two items are essential to plan? (Choose two.)

A. IP Routes

- B. VCM channels
- C. PRI trunks
- D. Advanced Edition
- E. H.323

ANSWER: A B

Explanation:

IP Routes are required so that each IP Office system can reach the remote system through the correct network path. **VCM channels** must be calculated to provide sufficient voice-compression and media-processing capacity for the expected concurrent inter-site calls.

PRI trunks are not required for an SCN because the systems communicate across the IP network. Advanced Edition is not a prerequisite for basic SCN connectivity, and H.323 is not itself a planning substitute for routing and VCM resource capacity.

QUESTION NO: 12

Which two applications can invoke Secure Digital (SD) card commands?

- A. IP Office Manager
- B. Avaya Aura® System Manager
- C. IP Office Web Manager
- D. IP Office System Monitor
- E. Avaya Control Manager

ANSWER: A D

Explanation:

IP Office Manager and IP Office System Monitor can invoke Secure Digital (SD) card commands. IP Office Manager is the principal administration client for an IP Office system and provides the SD-card command functions used by an administrator to manage card-based system software and related maintenance operations. These commands are performed against the selected IP Office control unit and therefore require an appropriate connection and administrator access to the system.

IP Office System Monitor can also invoke SD-card commands as part of its support and diagnostic role. System Monitor connects to the IP Office control unit to obtain operational information and can send supported maintenance commands, making it useful when an engineer is troubleshooting or performing controlled platform-level actions. In practical support work, both tools are installed as part of the IP Office administration suite and are used with care because SD-card actions can affect the system's installed software, operational state, or recovery process. Avaya's IP Office product-support resources and documentation are available through [Avaya Support: IP Office](#); product and deployment information is also available at [Avaya IP Office](#).

QUESTION NO: 13

A customer reports a delay of 5 seconds in receiving calls over analog trunks on the target phone. What could be the cause of this problem?

- A. Improper configuration of the system Locale.
- B. High level is set on Incoming Call Route.
- C. Ring delay is not configured on system telephony settings.

D. IP Office is not receiving the ICLID from PSTN.

ANSWER: D

Explanation:

IP Office is not receiving the ICLID from PSTN. is the correct cause. On an analog trunk, calling-line identity information is normally delivered by the public network in the interval associated with the initial ringing signal. IP Office can defer alerting or routing presentation briefly while it waits for that incoming caller identification data, allowing the call to be matched and displayed with the caller's number where available. If the PSTN does not supply ICLID, supplies it in an unsupported format, or the analog line is not correctly provisioned for the service, IP Office waits for the caller-ID interval to expire before it presents the call to the target telephone. This can be perceived as an approximately five-second delay before the phone rings. The appropriate investigation is therefore to verify that caller identification is enabled and delivered by the carrier, confirm the analog trunk's caller-ID and locale-related signaling expectations, and test the line directly if necessary. Avaya's IP Office maintenance documentation discusses analog-line caller-ID operation and related diagnostic considerations: [Avaya IP Office Maintenance Guide](#). Current Avaya product documentation and support resources are available through the [Avaya Support portal](#).

QUESTION NO: 14

During the installation of a Server Edition, the New Hardware screen detects the presence of a second hard drive. For which application is this additional hard drive typically used?

- A. One-X® Portal
- B. Call Detail Records
- C. Avaya Contact Recorder
- D. Voicemail Pro
- E. Web Services

ANSWER: D

Explanation:

Voicemail Pro is correct because a Server Edition deployment commonly uses a second physical disk as the dedicated storage location for voicemail messages and related Voicemail Pro data. Keeping message storage on a separate drive from the operating system and core application partitions provides additional capacity for retained messages and helps isolate the rapidly changing voicemail-store workload. During installation, the New Hardware process can detect the additional drive and configure it for this purpose, rather than leaving voicemail messages on the primary system disk. This arrangement is especially important on systems with significant voicemail traffic, since mailbox greetings, recordings, and user messages can consume storage over time. It also supports more manageable maintenance and recovery practices because the application's message store is separated from the server's core software installation. Avaya's IP Office Server Edition documentation describes Voicemail Pro as a Server Edition application and covers the server storage and installation requirements used to support its voicemail services. See the [Avaya Documentation portal](#) and the [Avaya Support site](#) for the applicable IP Office Server Edition installation and maintenance documentation.

QUESTION NO: 15

An IP Office system is configured to send alarm notifications by email through an SMTP relay. The relay rejects the notifications because it does not permit anonymous submission.

Which two settings must be configured to allow IP Office to authenticate to the SMTP relay? (Choose two.)

- A. Enable SMTP Authentication.
- B. Configure the SMTP user name and password.

- C. Configure an SNMP community string.
- D. Configure the IP Office System password.
- E. Configure only the alarm-recipient email address.

ANSWER: A B

Explanation:

SMTP Authentication must be enabled so that IP Office attempts to log on to the SMTP relay rather than submitting mail anonymously. The corresponding **SMTP user name and password** must also be configured with credentials accepted by that relay.

The alarm-recipient address determines who receives a notification after the SMTP server accepts it; it does not authenticate IP Office. SNMP settings are unrelated to SMTP relay authentication, and an IP Office system password is not used as SMTP credentials.

QUESTION NO: 16

A customer reports that after they rebooted the IP Office, some users are not receiving calls as they did before. Which two tools can you use to identify the last system changes made?

- A. Web-Manager
- B. Monitor
- C. Manager
- D. System Status Application

ANSWER: C D

Explanation:

Manager and **System Status Application** can be used to investigate recent IP Office system changes after an unexpected behavior change following a reboot. Manager is the primary administration client for retrieving and reviewing the IP Office configuration. It provides access to configuration information and saved configuration history, enabling an administrator to compare the active configuration with prior versions and determine what was changed before the restart. This is particularly useful when call routing, users, groups, short codes, or incoming call routes no longer operate as expected.

System Status Application complements that review by providing current platform and operational status information, including system events and details that help establish the timing and context of changes or a restart. Used together, the configuration history available through Manager and the system-status information from System Status Application support a structured investigation: identify the latest configuration activity, correlate it with the reboot or reported service impact, and then verify the affected call-handling settings. Avaya describes these administrative and diagnostic functions in its IP Office platform documentation. See the [Avaya IP Office documentation reference](#) and the [Avaya Documentation portal](#).

QUESTION NO: 17

A Hot Desking user must be able to log on at an available desk telephone and continue to receive calls presented to the hunt groups to which the user normally belongs.

Which two areas should be configured? (Choose two.)

- A. Extension settings
- B. Hunt Group settings in the user record
- C. ARS table settings

D. SMTP settings

E. Incoming Call Route settings

ANSWER: A B

Explanation:

The physical destination telephone must be prepared in the **Extension** configuration for Hot Desking. In addition, the user's applicable **Hunt Groups** should be configured in the user record so that hunt-group calls follow the user when the user is logged on at a hot-desk extension.

An ARS table controls outbound routing and does not prepare a desk phone for a Hot Desking login. SMTP settings are unrelated to user mobility, and an Incoming Call Route determines treatment of calls arriving on trunks rather than user hunt-group membership.

QUESTION NO: 18

A support engineer needs to determine the reason that an IP Office telephone is failing to register intermittently. The engineer needs a live protocol trace of the registration signalling between the endpoint and IP Office.

Which application is most appropriate for collecting this trace?

A. IP Office System Monitor

B. System Status Application

C. IP Office Manager

D. Voicemail Pro Client

ANSWER: A

Explanation:

IP Office System Monitor is the appropriate application for collecting live signalling traces. It can be connected to the IP Office system and configured with relevant protocol filters so that the engineer can examine registration attempts, responses, failures, and timing.

System Status Application provides live status and resource information but is not the primary protocol-trace tool. Manager is used to administer configuration, while Voicemail Pro Client is used to administer voicemail call flows and mailboxes.

QUESTION NO: 19

Where should the firmware files (.bin) for an IP telephone be placed on the system SD card?

A. /backup

B. /primary

C. /dynamic

D. /lvmail

E. /temp

ANSWER: B

Explanation:

The correct location is **/primary**. On an Avaya IP Office system using an SD card for system storage, the primary partition is the active, operational software area used by the system. IP telephone firmware binary files must be made available from this active area so that IP Office can serve the appropriate firmware to supported telephones during their boot and upgrade process. Placing the files in **/primary** ensures that the running system can locate the binaries when it receives a telephone firmware request and can deliver the matching version configured for the endpoint type. This location is also consistent with the normal IP Office SD-card workflow: current system resources required in day-to-day operation are held in the primary area, while other SD-card areas are intended for separate operational functions. After copying firmware to the active location, an administrator should confirm that the firmware file name and version correspond to the relevant Avaya telephone model and that the system's firmware settings select that version where applicable. Avaya's IP Office documentation and support resources are available through the [Avaya Support portal](#) and the [Avaya Support documentation page](#).

QUESTION NO: 20

Given an IP Phone that is not working, which of the following is an example of " Top-Down Troubleshooting " ?

- A. Validate that the gateway IP address is present in the IP Phone configuration.
- B. Attempt to ping the IP Phone and make a call if the ping is successful.
- C. Replace the patch cord of the IP Phone, and if it boots up, make a call.
- D. Check for an indicator light where the IP Phone is connected and listen for a dial tone.
- E. Attempt to make a call from the IP Phone and, if the call cannot be completed, ping the IP Phone.

ANSWER: E

Explanation:

Attempt to make a call from the IP Phone and, if the call cannot be completed, ping the IP Phone is an example of top-down troubleshooting because it begins with the service the user is trying to use: IP telephony calling. A call attempt tests the highest, user-visible level of operation, including the phone's registration and its ability to use the call-control service. If that application-level function fails, pinging the endpoint moves the investigation down to basic Internet Protocol network reachability. This ordered approach helps isolate whether the fault is related to the telephony service itself or to lower-level connectivity required by that service. Top-down troubleshooting proceeds from the application or service experience toward the underlying network and physical components, testing lower layers only as needed to narrow the fault domain. Avaya's LAN administration troubleshooting guidance describes using a structured troubleshooting approach for IP telephones and their LAN connectivity. See the [Avaya IP Telephone LAN Administration troubleshooting guidance](#). For additional product support resources, consult the [Avaya Support portal](#).

QUESTION NO: 21

What are the two essential requirements when planning for a Small Community Network (SCN)? (Choose two.)

- A. PRI trunks
- B. Advanced Edition
- C. IP Routes
- D. VCM channels
- E. H.323

ANSWER: C D

Explanation:

IP Routes and **VCM channels** are essential when planning an Avaya IP Office Small Community Network. An SCN connects separate IP Office systems across an IP network so that users can make calls, use centralized services where configured, and apply network dialing between sites. Each system must have the required IP routing information so that

traffic intended for another IP Office is directed through the appropriate network interface, gateway, and destination path. Careful route planning also ensures that each site can reach every required remote system and avoids ambiguous or unintended call paths.

VCM channels provide the media-processing capacity needed for calls whose audio must be handled across IP connections, including the codec conversion and compression resources required by the particular endpoints and links. The planner must calculate simultaneous intersite call demand and ensure that adequate VCM capacity is available on the applicable IP Office systems. This capacity planning is particularly important where calls traverse WAN links or involve endpoints using differing codec requirements. Avaya's SCN planning guidance identifies IP routing and VCM resource availability as core prerequisites for a functional, scalable networked deployment. See the Avaya documentation at [Avaya IP Office documentation](#) and the [Avaya Support portal](#).

QUESTION NO: 22

A Server Edition Primary Server has failed and is being replaced. The replacement is to be restored using a backup taken from the failed server, with minimal changes required for connected systems and applications.

Which two conditions should be met before the restore is performed? (Choose two.)

- A. Install the same software version as the original server.
- B. Use the same IP address as the original server.
- C. Use a temporary IP address until after the restore.
- D. Install a later software release before restoring the backup.
- E. Use only the same server name as the original server.

ANSWER: A B

Explanation:

The replacement should use the **same IP address** as the failed server so that IP Office systems, endpoints, applications, and administration clients can continue to reach the restored server without widespread addressing changes. It should also have the **same software version** installed as the server from which the backup was created, ensuring that the backup data is restored to a compatible platform.

A different temporary address can complicate recovery and require additional reconfiguration. The server name alone does not replace the network identity expected by connected components, and installing a later release before the restore can introduce backup-format and compatibility issues.