Appendix B: Customer Preparation and Considerations

Customer participation

Successful planning and implementation of a Modular Messaging system require cross-functional participation from a variety of disciplines from within the customer organization.

The following disciplines may be represented by single or multiple individuals or organizations:

- Telephony management
- Voice mail management
- E-mail management
- Desktop computing
- Server management
- Help desk
- IP network management
- SMTP gateway
- Data network security
- User community

System design and data collection

In preparation for a Modular Messaging implementation, customers are required to provide specific information related to their voice and data network. As part of the Modular Messaging installation, the Data Collection Tool (DCT) is used to supply information required to implement the system. DCT is a standalone application, delivered on the Modular Messaging Application Server Software DVD. It is also available from the Avaya support Web site: http://www.avaya.com/support.

During the system planning phase and prior to installation, customers are required to complete the information requested in the DCT. Consultation with a Modular Messaging Software

Specialist is highly recommended. Upon completion, the DCT output file (.mmdct) is used to configure the Modular Messaging system.

Caution:

Several requirements of the DCT must have unique designations. They include server host names, IP addresses, and the name of the private Windows Domain. If these items are duplicated anywhere in the network, errors will occur. If a change is required to the Domain Name or Server Host Name after installation, all Modular Messaging software must be reloaded on all affected servers. This may result in a loss of data or require data restoration. Ensure that unique and accurate information is provided for each Modular Messaging system.

Information customers should be prepared to provide includes:

- Unique host names for all Modular Messaging servers (see Caution above)

  Note:

  Do not use the underscore character (_) in a MSS Host Name. The Aria TUI voice mail searches fail if you use the underscore (_) character. The IMAP RFC does not allow the underscore character (_) in host names.

- Corporate IP addresses, subnet-mask and default gateway information (see Caution above)
- Corporate networks domains, DNS, NTP and SNMP information (see Caution above)
- PBX/Call server type and method of integration to Modular Messaging
- Message Networking, SMTP protocol, and Web Client information
- Desired system feature functionality, including classes of service, mailbox size, message length, time zones and telephone user interface (TUI)
- Caller Application (Auto-Attendants), Enhanced Lists / Broadcast (System Distribution Lists)

If the option to join the Modular Messaging system to the Customer Domain was purchased, the following considerations also apply:

- All MASs and MSS will join the corporate domain
- Requires Windows Domain Controller and IP address
- Create computer and user accounts for the Modular Messaging system within the corporate domain
- Login and password requirements
- Additional information and requirements specific to your network will also be required

Existing system review

If migrating or replacing an existing voice messaging system, customers should be prepared to discuss important attributes of their existing messaging and private branch exchange (PBX) systems.

Items for consideration may include:

- Automated attendant and call processing mailboxes – these can often be hosted on the PBX or voice messaging servers
- Bulletin board or announcement only mailboxes
- Desired system feature functionality, including classes of service, mailbox size, message length, time zones and telephone user interface (TUI)
- Subscriber Mailbox Profiles including assigned class of service, zero out destination, and special features (Outcalling)
- Voice mail access numbers, Message Waiting Indicators, vectors, call center agents, hunt groups, call coverage paths and auto-dial buttons

When integrating the Modular Messaging system with the host private branch exchange (PBX), planners and customers must also consider the following:

- Switch hardware and software to support required provisioning
- Features supported by a particular integration type

  For more information, see Switch integration matrix on page 178.
- Programming of translations for networked PBXs or IP gateways for centralized deployments
- Any updates that the dial plan requires, especially when Modular Messaging is to be networked with a Message Networking system

For the latest switch integration information, see the configuration notes available on the Avaya Support Web site at http://www.avaya.com/support.

E-mail management

Avaya recommends an assessment of the network bandwidth and e-mail resources to ensure optimal network performance for message transport between desktop applications and the e-mail servers. If implementing a Modular Messaging system with a Microsoft Exchange or an IBM Lotus Domino message store, customers may need to make changes to the existing e-mail infrastructure.

Security processes

Prior to the implementation of a Modular Messaging system, the customer's security staff should review and approve the Modular Messaging deployment. Customers should engage the expertise of their security staff early in the implementation process. Security staff must consider how the Modular Messaging system will be incorporated into their routine maintenance of virus protection, patches, and service packs. Avaya recommends customer-provided virus protection for all Microsoft Windows servers. Additional information can be obtained at the Avaya Support website: http://www.avaya.com.

Customer responsibility for system security

No telecommunications system can be entirely free from the risk of unauthorized use. Customers have ultimate control over the configuration and use of the product and are solely responsible for ensuring the security of their systems.

Customers who administer and use the system can tailor the system to meet their unique needs. Therefore, customers are in the best position to ensure that the system is secure to the fullest extent possible. Customers are responsible for keeping themselves informed of the latest information for configuring their systems to prevent unauthorized use. Customers must regularly implement security patches, hot fixes, and anti-virus updates. System managers and administrators are also responsible for reading all recommendations, installation instructions, and system administration documents provided with the product. This information can help them understand the features that might introduce risk of toll fraud, and the steps they must take to reduce that risk.

Avaya does not guarantee that this product is immune from or will prevent unauthorized use of telecommunications services or facilities accessed through or connected to this product. Avaya is not responsible for any damages or charges that result either from unauthorized uses or from incorrect installations of the security patches that are made available periodically. To aid in combating these crimes, Avaya maintains strong relationships with its customers and supports law enforcement officials in apprehending and successfully prosecuting those responsible.

Report suspected security vulnerabilities with Avaya products to Avaya by sending e-mail to securityalerts@avaya.com. Reported vulnerabilities are prioritized and investigated. Any corrective actions resulting from the vulnerability investigation are posted at http://www.avaya.com/support. Whether immediate support is required, report all toll fraud incidents perpetrated on Avaya services to Avaya Corporate Security at securityalerts@avaya.com.

In addition to recording the incident, Avaya Corporate Security is available for consultation on:

- Product issues
- Investigation support
- Law enforcement
- Education programs

For more information about system security, see the “Modular Messaging and Security” section of the media.

Recommendations for configuring Data Execution Prevention (DEP)

Data Execution Prevention (DEP) prevents your system from viruses and other security threats that results from running malicious code. Data Execution Prevention must not be mistaken as a firewall or antivirus program as it does not prevent harmful programs from being installed on your system. Instead, DEP performs additional checks on memory, and prevents code execution from data pages.

There are two types of Data Execution Prevention, "Software Enforced" and "Hardware Enforced." Hardware-enforced DEP detects code that is running and raises an exception when execution occurs. Software-enforced DEP prevents malicious code from taking advantage of exception-handling mechanisms in Windows.

Configuration of DEP

Microsoft Windows supports the following four system-wide configurations for both hardware-enforced and software-enforced DEP.

- **OptIn**: On systems with processors that can implement hardware-enforced DEP, DEP is enabled by default for limited system binaries and programs that "opt-in." With this option, only Windows system binaries are covered by DEP by default.
- **OptOut**: DEP is enabled by default for all processes. You can manually create a list of specific programs that do not have DEP applied by using the System dialog box in Control Panel. You can also use the Application Compatibility Toolkit to "opt-out" one or more programs from DEP protection. System compatibility fixes, or shims, for DEP do take effect.
- **AlwaysOn**: This setting provides full DEP coverage for the whole system. All processes always run with DEP applied. The exceptions list to exempt specific programs from DEP protection is not available. System compatibility fixes for DEP do not take effect. Programs

that have been opted-out by using the Application Compatibility Toolkit run with DEP applied.

- **AlwaysOff**: This setting does not provide any DEP coverage for any part of the system, regardless of hardware DEP support. The processor does not run in PAE mode unless the **/PAE** option is present in the `Boot.ini` file.

Avaya recommends that the existing default settings in the MAS image must only be used to configure the DEP settings. The default DEP setting is **OptOut** with no exceptions. As there are no exceptions, all Modular Messaging services are being monitored for DEP.

If the system-wide DEP policy is set to **OptOut**, programs that have been exempted from DEP protection will be exempted from both hardware-enforced and software-enforced DEP.

The `Boot.ini` file settings are as follows:

`/noexecute=policy_level`, where, `policy_level` is defined as **AlwaysOn**, **AlwaysOff**, **OptIn**, or **OptOut**.

Existing `/noexecute` settings in the `Boot.ini` file are also not changed if a Windows operating system image is moved across computers with or without hardware-enforced DEP support.

During installation of Windows XP SP2 and Windows Server 2003 SP1 or later versions, the **OptIn** policy level is enabled by default unless a different policy level is specified in an unattended installation. If the `/noexecute=policy_level` setting is not present in the `Boot.ini` file for a version of Windows that supports DEP, the behavior is the same as if the `/noexecute=OptIn` setting was included.