GUMBO MAIL

Enhancement Summary V1R4M0
Program Number 2A55SM2

Fourth Edition (February 2007)

GUMBO *Software, Inc.*

809 W Howe St
Seattle, WA 98119
United States of America

Phone: (206) 284-5078
E-mail: support2007@gumbo.com
Web: www.gumbo.com

Installation Instructions

Restoring the new release

Read the Enhancement Summary to determine if any changes affect your installation.

Follow these instructions to install Gumbo Mail V1R4M0 on your System i5:

Note: If you have downloaded this software from the web, instructions specific to installing from the download can be found in the file "readme.htm" which is included in the download.

1. Sign on to the system as the security officer (QSECOFR).

2. Verify that your machine is at i5/OS V5R3M0 or later by running:

   DSPDTAARA DTAARA(QGPL/QSS1MRI)

   Note: If you are running a version of i5/OS earlier than V5R3M0 you can not install Gumbo Mail V1R4M0 on your machine. You must install an earlier version of Gumbo Mail or upgrade the operating system.

3. Verify that user domain objects are allowed in the libraries GUMBOMAIL and QSRV, by running:

   WRKSYSVAL SYSVAL(QALWUSRDMN)

   Take option 5 to display the value. If the value is not *ALL, use option 2 to add libraries GUMBOMAIL and QSRV to the list of libraries where user domain objects are allowed.

4. Insure that i5/OS will be able to verify the signatures that we apply to our product's objects by installing our Signing Certificate and Root CA Certificate using Digital Certificate Manager. Alternately, insure that signature verification will not prevent the restore operation by running:

   WRKSYSVAL SYSVAL(QVFYOBJRST)

   Take option 5 to display the value. If the value is 3 or higher, use option 2 to temporarily change the value to 1.

5. Mount the distribution media in the appropriate device.

6. Submit the Restore Licensed Program (RSTLICPGM) command to batch:

   RSTLICPGM LICPGM(2A55SM2) DEV(device-name) LNG(2924)

   Note: "device-name" is the device the media was mounted on and is usually OPT01.
   Note: During the restore operation the system operator message queue may receive inquiry message CPA3DE4 "Directory not registered. (C G)". Unless you are using a directory naming convention similar to ours (that is the directory specified in the CPA3DE4's second level text is unrelated to our software), You can safely respond with a "G" to reestablish the relationship between the directory and the product. Typically the message will occur three times.

 © Copyright Gumbo Software, Inc. 2007.

7. Enter your permanent authorization code.
8. Determine which PTFs were included on the media by entering the following command:

   DSPPTF LICPGM(2A55SM2)

9. Visit www.gumbo.com to determine if newer PTFs are available.

Enhancements For Gumbo Mail V1R4M0

What's In This Section

This section provides information on Gumbo Mail enhancements for the current release, notes any customer code implications, and describes where to find more information when applicable.

S/MIME Signed Message Capability Added

Email produced by Gumbo Mail can now be, optionally, digitally signed using S/MIME Signed Message format. S/MIME (Secure / Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of email encapsulated in MIME. A signed message is an ordinary message with a digital signature added by the sender. The signature has two purposes: it identifies the sender, and it verifies that the content of the message has not been altered since the message was sent.

You create digitally signed email by specifying an **Application ID** when the email is created. There are two ways to accomplish this: at the command level and at the system (or LPAR) level. The command level overrules the system level. For command level, specify an **Application ID** directly on the send command's new **Signing key** (SGNKEY) parameter. For the system level, specify an **Application ID** on the CHGSM2DFT command's new **Signing key** (SGNKEY) parameter.

The shipped default values for the **Signing key** (SGNKEY) parameters are *DEFAULT and *NONE respectively.

Application ID refers to the name you have given to a digital certificate when placing it in the *OBJECTSIGNING Certificate Store using i5/OS's Digital Certificate Manager (DCM). DCM is option 34 of i5/OS. You can determine if DCM has been installed by running the Display Software Resources (DSPSFWRSC) command.

For complete information on setting up DCM, creating and storing certificates and adding **Application ID**s, goto the iSeries Information Center (http://www.iseries.ibm.com/infocenter).

*CURRENT Added to CC(), BCC(), And REPLYTO()

A new special value, *CURRENT, has been added to the CC(), BCC(), and REPLYTO() parameters of the GSENDMAIL command. When specified, the email address associated with the sending user profile is substituted.

Ping SMTP Mail Server (PINGMAIL) Command Enhanced

The Ping SMTP Mail Server (PINGMAIL) command has been enhanced to include a from address and to allow SMTP authentication username and password.

Previously, only one email address was accepted by the command and it was used as both the originator and the recipient of the test message. This limited some of the cases of SMTP server behavior that could be tested.

Some internet service providers require SMTP authentication before they will accept out going email from an account. To date, IBM has not implemented this in i5/OS's SMTP stack. When a username and password are specified, PINGMAIL uses them to perform SMTP

 © Copyright Gumbo Software, Inc. 2007.

authentication (PLAIN only). In many cases, you can use this feature to perform SMTP authentication for your System i5 and i5/OS's SMTP stack will then be able to use the connection to send email through the internet service provider.

Product Integrity Enhancements

Objects and the save files that contain them are digitally signed by Gumbo when they are created on our development system. You can verify that their contents have not been altered or corrupted since they were produced. You do this by first importing our root certificate authority (CA) and object signing certificates to your system and then running the Check Object Integrity (CHKOBJITG) command against them. For detailed instruction on importing certificates for signature verification using the CHKOBJITG command, see IBM's manual "Digital Certificate Manager RZAH-U000".

Note: We uniquely name our digital certificates to simplify their management on your system. If you have previously imported digital certificates from us with the same name as those included in this package, you do not need to repeat this step.

Certificates can be found in downloads that contain save files as well as in the product's /doc directory after it is installed.

Send Mail Component Corrections And Updates

- Removed requirement for a primary recipient. This allows all recipients to be specified as CCs or BCCs only.
- Implemented RFC3490 Internationalizing Domain Names in Applications (IDNA). This allows mailing to domains that contain non US-ASCII characters for example schöpe.de.
- Email address parser now supports use of characters outside the US-ASCII range.

OpenSsl Component Corrections And Updates

- Initial build. Portions of OpenSsl.org's OpenSsl library have compiled into a service program to generate asn.1 encoded Pkcs7 signatures rendered base 64.

Authorization Component Corrections And Updates

- Check Gumbo Mail Authorization (CHKSM2AUT) command added. The command exercises the product's authorization verification function. This allows you to determine whether the product is authorized for use. If the product is not permanently authorized, the generated messages allow you to determine when the temporary authorization will expire. You may specify a message queue to receive messages generated when the product is not permanently authorized.

Encryption Component Corrections And Updates

- Functions implementing the SHA-1 message digest algorithm have been added.

Mail Set Up Corrections And Updates

- Malformed SMTP commands cause PINGMAIL to always fail to send test message.

Space Management Component Corrections And Updates

- Added locking protocol to insure that pointer retrieved during space creation points at newly created space.
- Space locking now uses job default wait time.

 © Copyright Gumbo Software, Inc. 2007.