SMTPRelay.pcgus.com Operations & Troubleshooting Guide

Ver. 1.0

December 7, 2021

Raymund Codina

Table of Contents

[Overview of SMTP Relay Flow at PCG 3](#_Toc60992177)

[The Big Picture 3](#_Toc60992178)

[Mail Flow Components 3](#_Toc60992179)

[Adding IP Addresses to Relay Allow List 5](#_Toc60992180)

[Mail Flow Troubleshooting 8](#_Toc60992181)

[Starting Point: Troubleshooting PCG E-Mail Flow 8](#_Toc60992182)

[BEGIN HERE: Required Information for All E-Mail Incidents. 8](#_Toc60992183)

[Tier 2 Troubleshooting 9](#_Toc60992184)

[Troubleshooting Outbound Flow To Internet 10](#_Toc60992185)

[The MOST important key to solving this problem: 11](#_Toc60992186)

[Is the Mail Getting Out of O365 & Sent To the Internet? 11](#_Toc60992187)

[IMPORTANT NOTES FOR OUTBOUND TROUBLESHOOTING: 12](#_Toc60992188)

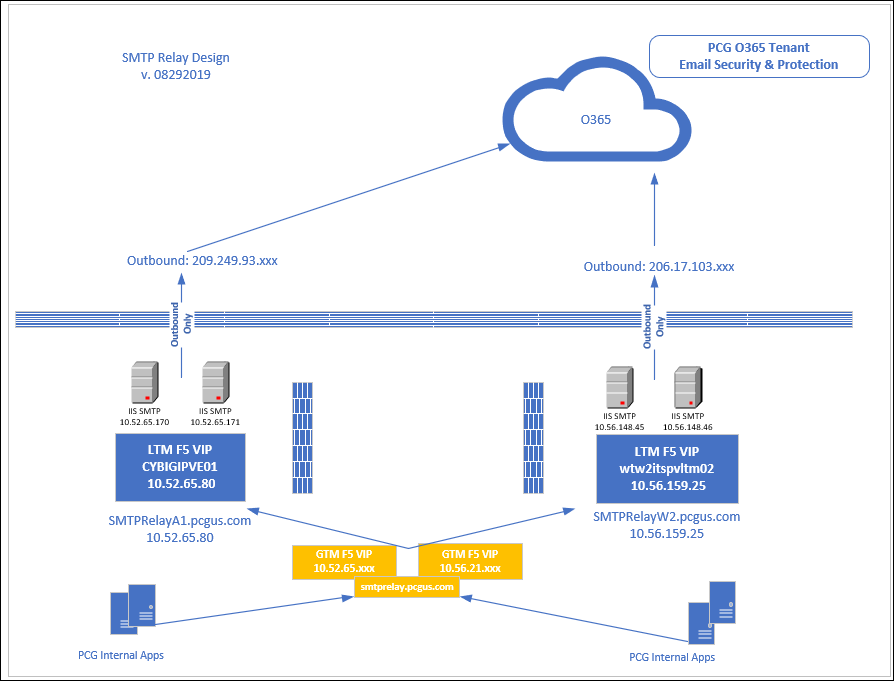
[Application E-Mails 12](#_Toc60992189)

# Overview of SMTPRelay Flow at PCG

The Corporate ITS email architecture and mail flow in on-premises datacenters SMTP mail relay services for Practice Areas. The mail relay servers are directly connected to PCG’s O365 tenant over a secured TLS1.2 connection. All email relayed over this connection follows all PCG email security and compliance standards.

## The Big Picture

Below is an overview of the flow of PCG e-mail through the various components discussed below.



## Mail Flow Components

Below are the components that comprise the PCG SMTPRelay Email Service

1. **Office 365 (Exchange Online)**
   1. Primary location of all existing and new PCG Mailboxes
   2. Hosted in Microsoft Cloud.
   3. Provides inbound/outbound spam/AV scanning service.
   4. Provides e-mail encryption services.
2. **SMTP Relay Pools**
   1. Name of SMTP Relay: smtprelay.pcgus.com
   2. F5 Load balanced / Fault tolerant between 2 datacenters
      1. AUN1 LTM F5 VIP – 10.52.65.80
         1. AUN1CORPVAP018 - 10.52.65.170
         2. AUN1CORPVAP019 - 10.52.65.171
      2. WTW2 LTM F5 VIP – 10.56.159.25
         1. WTW2CORPVAP010 - 10.56.148.45
         2. WTW2CORPVAP011 - 10.56.148.46
3. **F5 GTM**
   1. Name: smtprelay.gslb.pcgus.com
   2. smtprelay.pcgus.com CNAME record pointing to NLB.
4. **Certificate Requirements**
   1. Entrust CA Subject Name: smtprelay.pcgus.com required on each server to authenticate a secure connection to our O365 tenant



1. **IIS SMTP Server Folder Structure and how SMTP service works**

The message store of the SMTP service is created when you install the service on IIS. SMTP utilizes this directory structure to process mail. The folders below in **C:\Inetpub\Mailroot** directory structure is listed below:

* ***Pickup:*** The SMTP service processes messages from the Pickup folder as outbound messages or as messages for delivery. If the message is intended for users that are members of the local domain managed by the SMTP service, the SMTP service moves the message to the Drop folder.
* ***Drop****:* Incoming messages intended for the local domains are placed in the Drop folder. This is true for all recipients because the SMTP service does not maintain a mailbox for each recipient.
* ***Queue****:* Messages that cannot be immediately delivered are moved by the SMTP service to the Queue folder from the Pickup folder. The SMTP service repeatedly attempts to deliver messages stored in the Queue folder.
* ***Badmail****:* The Badmail folder stores messages that could not be forwarded to the recipient, even after attempts have been made for a predefined number of times. Another characteristic of messages in the Badmail folder is that the messages cannot be returned to the senders of these messages by SMTP. This means that administrators must handle messages residing in the Badmail message store.

1. **O365 Mail Flow Connector – OnPrem SMTP Relay**
   1. This connector lets Office 365 accept email messages directly from the SMTP Relay servers.
   2. It is restricted/allowed to the below externally NATd addresses which are the on-premises SMTP Relay Pool of servers.
      1. 206.17.103.241
      2. 206.17.103.249
      3. 209.249.93.4

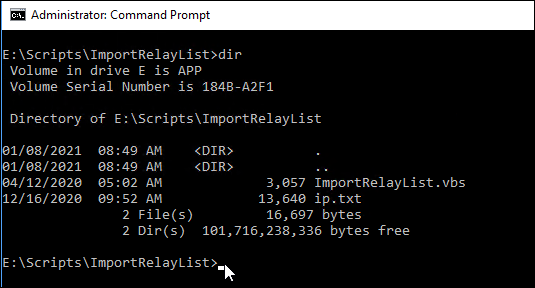
# Adding IP Addresses to Relay Allow List

Server/application host IPs must be added to the SMTP server’s Relay Restrictions Allow List to be able to relay mail. **Note: these procedures are manual, and automation/scripting still needs to be developed to simplify.**

The current script utilizes the **ImportRelayList.vbs** script to import the list of IP addresses in **IP.txt** file

To add IP addresses, Go to:

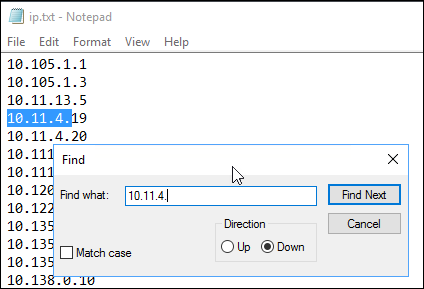
1. You will need to log on each server below to execute the script
   1. AUN1CORPVAP018 - 10.52.65.170
   2. AUN1CORPVAP019 - 10.52.65.171
   3. WTW2CORPVAP010 - 10.56.148.45
   4. WTW2CORPVAP011 - 10.56.148.46
2. Open CMD prompt in Administrator Mode



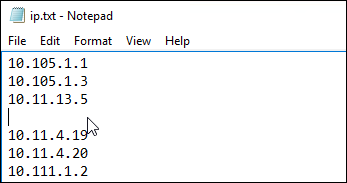
Pro tip: To open an administrative Command Prompt window in the current folder, use this hidden Windows 10 feature: Navigate to the folder you want to use, then hold Alt and type F, S, A (that keyboard shortcut is the same as switching to the File tab on the ribbon, then choose Open command prompt as administrator).

1. Open **ip.txt** file in Notepad and search for IP address to be added.

Ie. IP address to be added is 10.11.4.15



1. Insert and add IP address, then save file



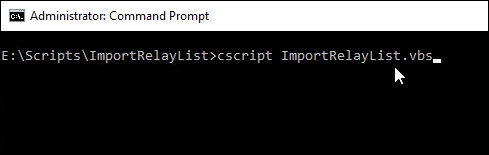
1. The **IP.txt** file will need to be copied to other servers

**xcopy .\ip.txt \\aun1corpvap019\e$\scripts\importrelaylist\ /c /f /y**

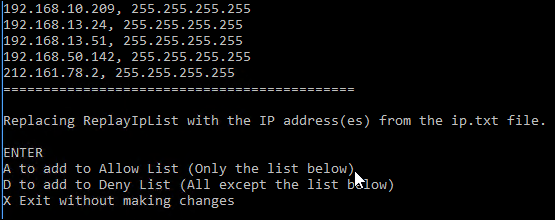
**xcopy .\ip.txt \\wtw2corpvap010\e$\scripts\importrelaylist\ /c /f /y**

**xcopy .\ip.txt \\wtw2corpvap011\e$\scripts\importrelaylist\ /c /f /y**

1. Execute the following command…. >**cscript ImportRelayList.vbs**



1. Enter **A**…. (Add to Allow List)



1. This will also need to be individually executed on each server:
   1. AUN1CORPVAP018 - 10.52.65.170
   2. AUN1CORPVAP019 - 10.52.65.171
   3. WTW2CORPVAP010 - 10.56.148.45
   4. WTW2CORPVAP011 - 10.56.148.46

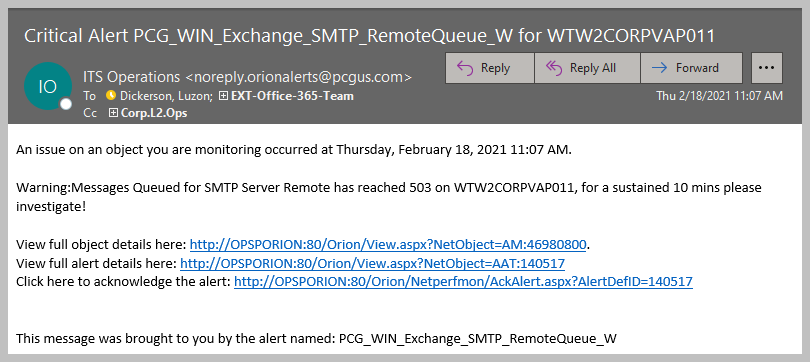
# Mail Flow Troubleshooting

Now that you understand the structure/topology of the PCG SMTPRelay email infrastructure, it’s time to look at the functional aspects a little deeper. **Keep in mind the SMTPrelay is an OUTBOUND ONLY connection**. It is not designed to receive incoming mail.

# Starting Point: Troubleshooting Orion Email Alerts

Orion has been setup to monitor various services on the uptime and availability of the SMTP server.

The most critical to note is monitoring the **SMTP Server Remote Queue Length.** This is the performance monitor that indicates how many messages are currently in queue to be delivered. The threshold is set to 500 messages sustained for over 10 minutes.

The email will appear as follows:  


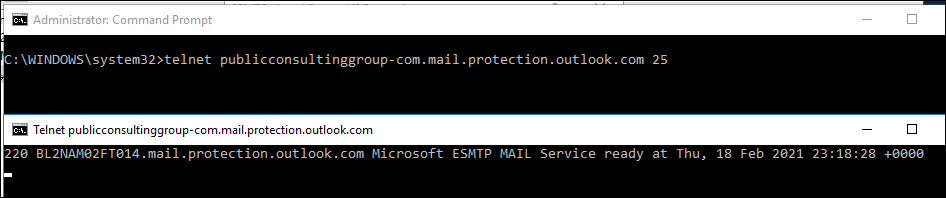
## BEGIN HERE: Required Information for All Orion E-Mail Alerts.

Logic & best practices dictate that any problem must be defined before it can be solved. Therefore, to ensure that a clear picture of the problem is captured, the questions and sub-questions below must be asked and answered before moving on to ANY further troubleshooting.

1. **Before doing ANYTHING:** Is there a known, ongoing issue?
   1. If **YES**, note it, continue troubleshooting, and see if it maps to current incident.
   2. If **NO**, continue troubleshooting below.
2. **Next: Look at the Queues.** 
   1. On desktop, Launch the icon labeled **SMTP Perfmon.msc** for each DC pair.

* 1. Is the Remote Queue Length over > 500?
     1. Value stuck or changing? If changing, there could have been an email blast that is just taking time to process deliveries.
     2. If stuck, check network connectivity issues to Microsoft. The destination is:
        + **publicconsultinggroup-com.mail.protection.outlook.com**
     3. To verify, perform a telnet into port 25 of the destination address as follows.



* 1. A 220 response indicates an active/good connection.
  2. A blank blinking cursor that eventually errors with cannot make connection is a problem. The Network Team will need to be engaged.

1. **Data-Gathering After Initial Problem Definition:** 
   1. When Did It Start?
   2. **Collect Data. Update Ticket and send to Tier2.**

**IMPORTANT: Updating the ticket the information you have gathered is critical to faster problem resolution and you may have ticket returned to you if you do not include the results of your troubleshooting. Please do not simply pass an incident along blindly without performing due diligence and including all relevant information.**

**DECISION:**

1. **ID Problem as Internal, Outbound, or Combination.**
2. **Proceed to appropriate Tier 2 troubleshooting section next.**

# Starting Point: Troubleshooting PCG E-Mail Flow

The good thing about most e-mail flow problems is that they are usually the result of a relatively small set of common causes. Identifying the cause and eliminating others is often the real challenge. However, this challenge can be minimized, and incident resolution significantly increased by following a standard, repeatable troubleshooting methodology. This document follows such a method for managing PCG e-mail incidents.

## BEGIN HERE: Required Information for All E-Mail Incidents.

Logic & best practices dictate that any problem must be defined before it can be solved. Therefore, to ensure that a clear picture of the problem is captured, the questions and sub-questions below must be asked and answered before moving on to ANY further troubleshooting.

1. **Before doing ANYTHING:** Is there a known, ongoing issue?
   1. If **YES**, note it, continue troubleshooting, and see if it maps to current incident.
   2. If **NO**, continue troubleshooting below.
2. **Next: Define the Primary Problem. What’s Wrong?**
   1. Problems Sending?
      1. To Internal Recipients?
      2. To External Recipients?
   2. Problems Receiving?
      1. From Internal Recipients?
      2. From External Recipients?
   3. Some combination of A & B?
   4. Problems with all the above?
3. **Data-Gathering After Initial Problem Definition:** 
   1. When Did It Start?
   2. Has this happened before with **this** caller/user? If YES, what was resolution?
   3. Can you replicate the problem?
   4. **Collect Data. Update Ticket and send to Tier2.**

**IMPORTANT: Updating the ticket the information you have gathered is critical to faster problem resolution and you may have ticket returned to you if you do not include the results of your troubleshooting. Please do not simply pass an incident along blindly without performing due diligence and including all relevant information.**

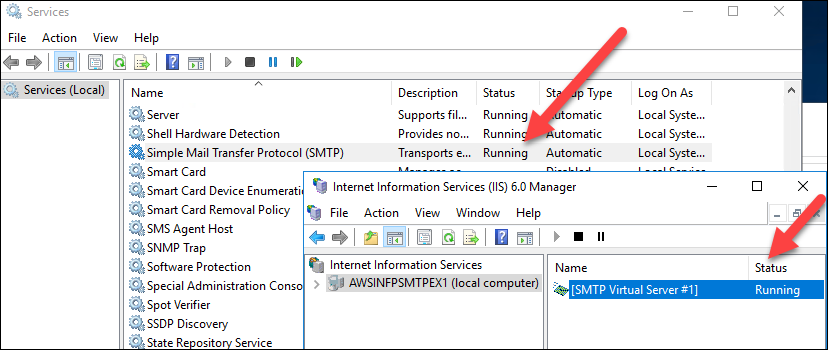
**DECISION:**

1. **ID Problem as Internal, Outbound, or Combination.**
2. **Proceed to appropriate Tier 2 troubleshooting section next.**

# Tier 2 Troubleshooting

These are usually the simplest to define and resolve, as they only involve services on the SMTP Server. Below are the recommendations for troubleshooting internal mail issues.

1. Review all required standardized troubleshooting data gathered above.
2. Gather any error messages user has reported trying to relay mail.
3. Are services running on the SMTP Servers?
4. Check Queue: Are there any other identical/similar incidents?
   * 1. How many? – Define scope of problem.
     2. Were they resolved?
        + If YES: Gather solution and attempt to repeat.
        + If NO: Inform colleagues and continue troubleshooting below.
5. **IMPORTANT:** Are there NDR/Bounce Records? Get them from users!
6. Confirm & document what IS and IS NOT working. (Isolate the problem to eliminate non-problematic areas.)
7. The most common would be that the host is not listed in the Relay Allow List receiving the following error.
   1. **Error code: 550 5.7.1 Unable to relay for….**
   2. Resolution: Follow instructions above to add host IP address to Relay Allow List.
   3. Validation: Have user/application re-try sending mail.
8. Verify the SMTP Server Services are running
   1. Login to SMTP Relay Servers
      1. AUN1CORPVAP018 - 10.52.65.170
      2. AUN1CORPVAP019 - 10.52.65.171
      3. WTW2CORPVAP010 - 10.56.148.45
      4. WTW2CORPVAP011 - 10.56.148.46
   2. Check the following services to ensure they are Running as shown below?
      1. Server Services - Simple Mail Transfer Protocol (SMTP)
      2. Internet Information Services (IIS) 6.0 Manager – SMTP Virtual Server



1. Can you telnet into port 25 from the host server submitting the SMTP relay request by executing the command below.



* The above indicates a successful network connection.
* If blank, there is an issue with the network or firewall.

1. Checking Queue Backlog - Messages that cannot be immediately delivered are moved by the SMTP service to the Queue folder from the Pickup folder. The SMTP service repeatedly attempts to deliver messages stored in the Queue folder
   1. Alerting: Orion monitoring is set to Alert
      1. Polling every 5 minutes
      2. if the Queue exceeds > 500 messages
      3. condition to exist more than 30 min
   2. Troubleshooting: This could be caused by several variables.
      1. Connection to O365. You can access the Service Health page on the [Microsoft 365 Admin Center](https://admin.microsoft.com/Adminportal/Home?source=applauncher#/servicehealth) for any advisories.
      2. This connection requires an updated certificate so check if the certificate mentioned in the components sections is up-to-date.
   3. Resolution: You can observe the queues clear if issue resolved.

**DECISION: Issue Resolved? Y/N?**

**If YES, close incident.**

**If NO, update ticket with ALL required/gathered information & escalate to Tier 3.**

# 

# Troubleshooting Outbound Flow To Internet

Begin here if the mail problem is determined to be outbound-only.

Mail flow of email out to the Internet has recently become much less complex. It is now easy to troubleshoot and resolve these issues and more by simply using the Message Trace feature in Exchange Online, to identify where it is being blocked or otherwise not passing through.

For reference, please see and use the outbound mail flow diagram below as well as the full description of the process in the section above entitled **Outbound (Non-PCG Recipients) Mail Flow.**

1. Gather all required standardized troubleshooting data info above if not already done.
2. What is the mail address of PCG user reporting problems?
3. Are there problems sending to **all** Internet addresses, or just to specific addresses/domains?
   1. If the latter, gather ALL addresses where problems are reported.
   2. Please gather & provide SPECIFIC example(s) of messages sent to problematic external domains.
4. If the user has received any NDR’s collect them from the user.
   1. Have them forward NDR to service desk agent and attach to ticket.
   2. If in a remote session, open the NDR, copy the headers, and add them to the ticket.
   3. More Information: [About NDRs & What They Mean.](https://support.office.com/en-us/article/Email-non-delivery-reports-in-Office-365-51daa6b9-2e35-49c4-a0c9-df85bf8533c3)
5. Was the user able to reach the external recipient by other means (i.e. phone/SMS) and confirm non-delivery of PCG email?
   1. If answer to 5 is ‘Yes’, ask the external recipient to check with their IT department and ask the following (if possible):
      1. Is there any ongoing problem with the recipients’ IT systems?
      2. Have they possibly blocked our email domain?
      3. Record results in ticket.
6. Testing:
   1. Using your own PCG email, try and send a test email to problematic external recipient(s).
   2. If you have access to another non-PCG email (personal, Gmail, etc.) try to send a test message to problematic external recipient.
   3. Record all results.

### The MOST important key to solving this problem:

* **How far is email getting out along the chain?**
* **Where is email being stopped?**

### Is the Mail Getting Out of O365 & Sent To the Internet?

All outbound email exits to the Internet through Office 365. This includes all user, application, and mail relayed from apps/servers inside the PCG network.

1. The first place you should go once you have your information about the problem sender/recipient is the Exchange Message Trace Console. This is the message tracking center of O365. Plug in the known values and see what the results tell you about the mail you’re working on.
2. Quick instructions may be found here:
   1. [Run a Message Trace and View Results](https://technet.microsoft.com/en-us/library/jj200712(v=exchg.150).aspx)
   2. [Find and fix email delivery issues as an Office 365 for business admin.](https://support.office.com/en-us/article/Find-and-fix-email-delivery-issues-as-an-Office-365-for-business-admin-e7758b99-1896-41db-bf39-51e2dba21de6)
3. Quick Reference for Exchange Online Message Trace Fields:
   1. **Sender** field. This is the email of the user having problems sending to the internet.
   2. **Recipient:** field. This is the target recipient or domain
   3. **Date Sent:** This allows you to set shorter or longer search ranges, based on when the user reported the problem. You can also specify a custom date/time range if necessary.

**NOTE: If multiple users are having problems sending to a specific address or domain, you can use the “\*” character as a wildcard to specify all email to/from a specific domain (i.e. \*@pcgus.com).**

1. Once you get your results, you can review the messages, confirm whether they even arrived, and if so, how it/they were handled.

### IMPORTANT NOTES FOR OUTBOUND TROUBLESHOOTING:

In addition to the technical aspects, there are a few general things you should keep in mind whenever approaching these types of problems:

1. Outbound troubleshooting is best performed using a combination of NDR’s and Message Tracking at O365 to determine any specific path problems. Most issues can be quickly identified and resolved this way.
2. More information is always better than less.
3. Remember: Narrow the problem down by identifying it and then assessing its exact scope. Then attack the problem.
4. Be ready for finger-pointing between the vendors.
5. Don’t be surprised if after narrowing a problem down through our own troubleshooting that you have to **prove** it to one or more vendors before they’ll address it. However, as long as we’ve done our due diligence it’s not too difficult.
6. If you aren’t getting the vendor assistance you need, do not be afraid to ask for escalation within their support structure.

# Application E-Mails

In addition to user emails, the many servers and applications that send out hundreds of emails per day may encounter issues. Below is a basic troubleshooting checklist when a problem with an application email or mailbox is reported:

1. Is a 3rd party application trying to send email that is having problems?
2. If an internal server, what is the Name/IP of the sending or problematic server?
3. To where or what addresses is it sending emails?
4. What are the ‘from’ addresses in the problematic emails?
5. Is the problem with individual addresses, or entire domains?

**DECISION: Issue Resolved? Y/N?**

**If YES, close incident.**

**If NO, update ticket with ALL required/gathered information & escalate to Tier 3.**