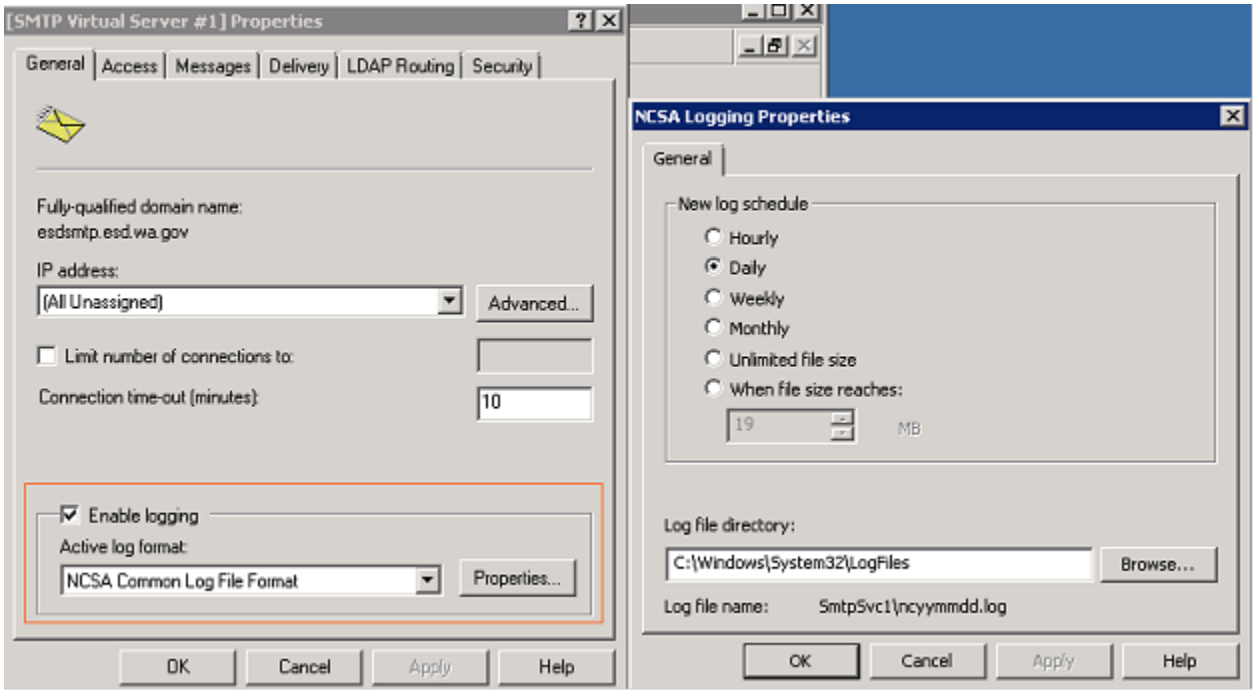
SMTPWatch Sample Script

Please note: this is a sample script provided by a customer agency Exchange administrator and is published for informational purposes only. Sample scripts are not supported by CTS. Please refer to the Agency Delegated Administrator Guide for supported scripts and commands.

This sample script creates and emails the administrator a report of applications using SMTP relay, and SMTP relay activity by IP address. NOTE: Replace all RED-faced text with your agency-specific information.

Instructions Provided by the Author:

1. Enable SMTP logging on your SMTP server, per the screenshot below, choosing "NCSA Common Log File Format"



2. Next, open the script and modify the following four variables (in red-faced font) to reflect the email address to send the email to, the SMTP relay server to use, the path of the SMTP log files, and the SMTP label that will show up in the subject and body of the email

```
# ---------------------------------------------------------------------------
# Global Variables
# ---------------------------------------------------------------------------
$email="user@AGY.wa.gov"
$smtpserver="agencysmptserver.AGY.wa.lcl"
$path="agencypath"
```

```
$smtpLabel="agency SMTP Label to display in the email subject and body of the email"
# ---------------------------------------------------------------------------
# Process SMTP logs
# ---------------------------------------------------------------------------
$datevar=(get-date).adddays(-2)
$body1=New-Object System.Collections.ArrayList
$body1.add("-----------------------------------------------------")
$body1.add("SMTP relay new - $smtplabel")
$body1.add("-----------------------------------------------------")
$header1=New-Object System.Collections.ArrayList
$smtplogs=get-childitem $path  | where-object {$_.lastwritetime -gt $datevar}
foreach ($line in $smtplogs)
   {
   $in=get-content $line.fullname
   $in=$in -notmatch "OutboundConnection" -notmatch "AGYSMTPServer"
   foreach ($line2 in $in)
    {

    $ip=$line2 | % { [regex]::Match($_,'([^,]+) \[').Groups[1].Value }
    $header1.add($ip)
    }
   }

$sum=$header1 | group-object $_ | sort-object count -descending
foreach ($line in $sum)
   {
   $body1.add($("{0,-20}{1,-7}" -f $line.count,$line.name))
   }

remove-item -force temp.csv

# ---------------------------------------------------------------------------
# Send email
# ---------------------------------------------------------------------------
$count1=$($body1.count)-3
$body="";$body1 | %{$body += "$_ `n"}
$mail = new-object System.Net.Mail.MailMessage
$mail.From = "$email"
$mail.To.Add("$email")
$mail.Subject = "SMTP watch - $count1 $smtplabel"
$mail.Body = $body
$(new-object system.net.mail.smtpClient("$smtpserver")).Send($mail)
```

3. Run the script in a scheduled task using credentials that would have access to the remote SMTP relay server logs and you will get an email including the number of devices using SMTP in the subject line. The item counts displayed in the report shows how many lines of SMTP logs contain each specified server.