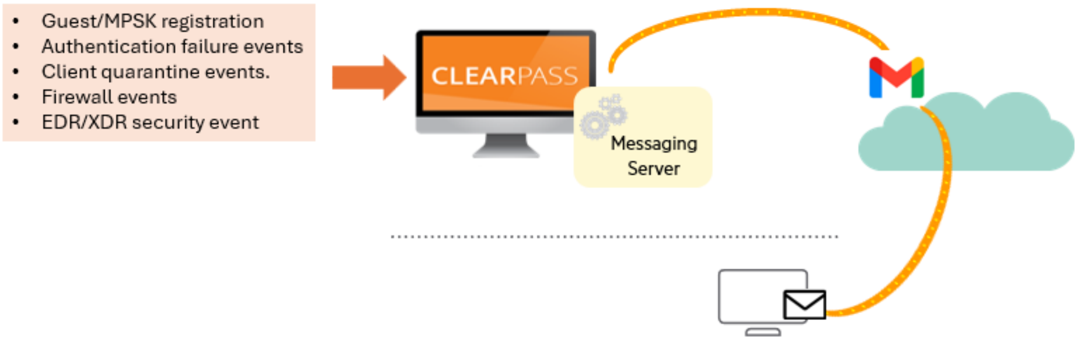
1 Table of Contents

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
29 Aug 2025	0.1	Ariya Parsamanesh	Initial creation

2 ClearPass using Gmail as Messaging Server

In this technote, I'll walk through using Gmail as a messaging server in ClearPass, particularly useful in lab environments where you're testing solutions that require email integration.



• Guest/MPSK registration
• Authentication failure events
• Client quarantine events.
• Firewall events
• EDR/XDR security event
CLEARPASS
Messaging Server

Here are some solutions that require email integrations.

- Trigger email delivery of credentials after MPSK registration.
- Guest access with sponsor approval
- Schedule automated delivery of Insight reports via email
- Authentication failure notification via email
- Use post-authentication enforcement profiles to trigger email notifications based on defined policy conditions.
- Email notifications for client quarantine events.
- Send email notifications when ClearPass detects a security event through its integration with an EDR/XDR platform (e.g., CrowdStrike).

2.1 Things you need

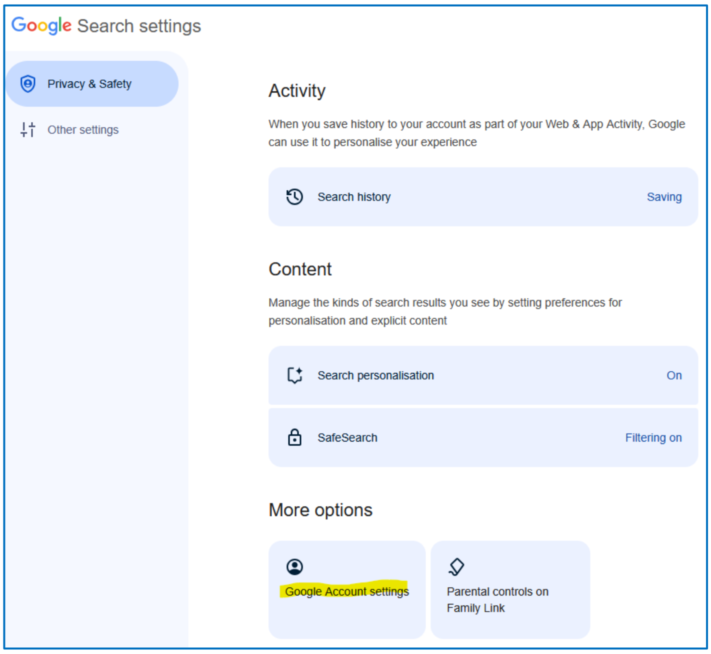
We need the following.

- ClearPass version 6.11.x or better
- Access to a SMTP server, here I am using Gmail.

2.2 Gmail Configuration

In the past, it was possible to use a Gmail account with legacy authentication methods, but this has since been disabled by default. Now, all Gmail account owners require modern authentication. In this setup, I've used an app password, which requires enabling 2-Step Verification.

To do this, first log in to your Google account, then navigate to Account Settings → Privacy & Security.



Google Search settings

Privacy & Safety

Other settings

Activity

When you save history to your account as part of your Web & App Activity, Google can use it to personalise your experience

Search history — Saving

Content

Manage the kinds of search results you see by setting preferences for personalisation and explicit content

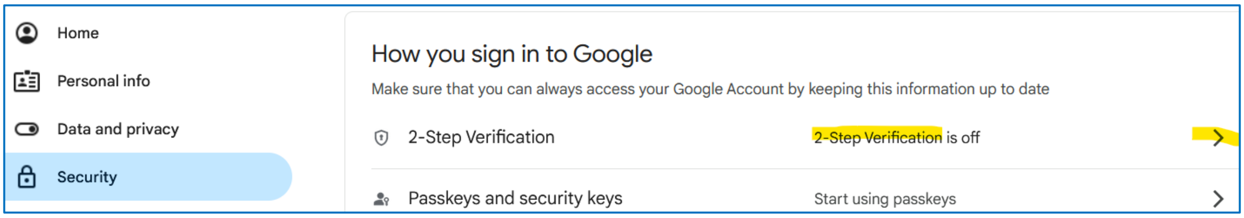
Search personalisation — On

SafeSearch — Filtering on

More options

Google Account settings

Parental controls on Family Link



Home

Personal info

Data and privacy

Security

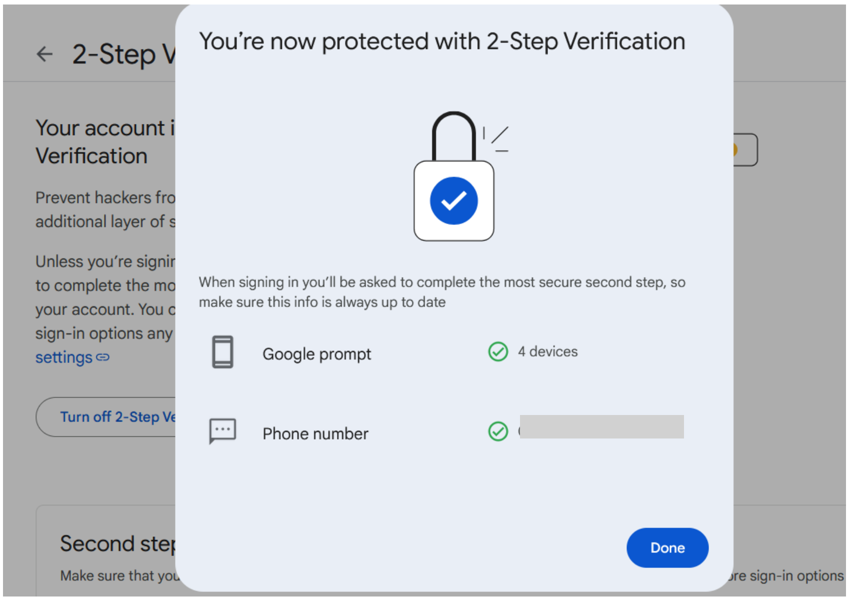
How you sign in to Google

Make sure that you can always access your Google Account by keeping this information up to date

2-Step Verification — 2-Step Verification is off

Passkeys and security keys — Start using passkeys

Here you can add the second factor for the authentication by adding a phone number.



You're now protected with 2-Step Verification

When signing in you'll be asked to complete the most secure second step, so make sure this info is always up to date

Google prompt — ✓ 4 devices

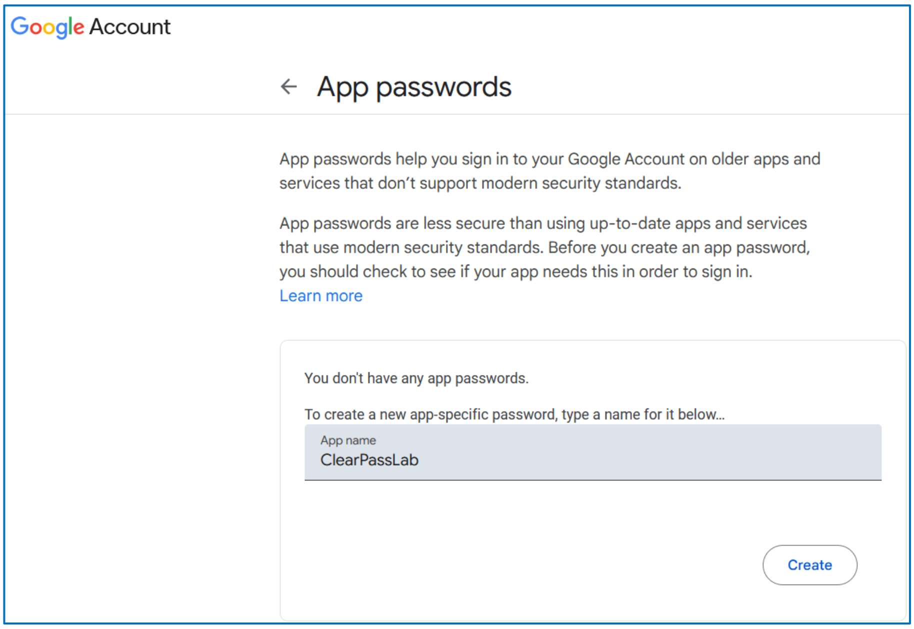
Phone number — ✓ [redacted]

Done

Once you have enabled the two-factor authentication you need to sign out and back sign in again.

And back to the security setting. Then you need to go to this URL to add your first App password.

https://myaccount.google.com/apppasswords



App passwords

App passwords help you sign in to your Google Account on older apps and services that don't support modern security standards.

App passwords are less secure than using up-to-date apps and services that use modern security standards. Before you create an app password, you should check to see if your app needs this in order to sign in.
Learn more

You don't have any app passwords.

To create a new app-specific password, type a name for it below...

App name
ClearPassLab

The password will be displayed only once, make sure you copy it as we'll need it for ClearPass configuration.

2.3 ClearPass Configuration

Here is our task list

1. Retrieve Gmail SMTP certificates
2. Add google SMTP certificate chain to certificate trust list of ClearPass
3. Ensure the google SMTP certificates have the SMTP usage specified in ClearPass
4. Configure the messaging server

We'll start by using OpenSSL to retrieve the Gmail SMTP certificates used in TLS mode. TLS uses well known port of 587 and gmail's well known SMTP FQDN is smtp.gmail.com

Using the following command will list all the whole certificate chain.

```
$ OpenSSL s_client -starttls smtp -connect smtp.gmail.com:587 -showcerts
CONNECTED(00000003)
depth=2 C = US, O = Google Trust Services LLC, CN = GTS Root R1
verify return:1
depth=1 C = US, O = Google Trust Services, CN = WR2
verify return:1
depth=0 CN = smtp.gmail.com
verify return:1
---
Certificate chain
 0 s:CN = smtp.gmail.com
   i:C = US, O = Google Trust Services, CN = WR2
-----BEGIN CERTIFICATE-----
MIIEWDCCA0CgAwIBAgIRAKCdiixpEEwQENwyy81diLUwDQYJKoZIhvcNAQELBQAw
OzELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczEM
MAoGA1UEAxMDV1IyMB4XDTI1MDgxMTE5MjIyM1oXDTI1MTEwMzE5MjIyMlowGTEX
MBUGA1UEAxMOc210cC5nbWFpbC5jb20wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNC
AAQna5AYWMRgguxiOSLTkews0U6zXi8vXQHsXb1vfuNAPo511djmWNloA9X6wvG7
soJZOVIKRBFnFY289EmO+XWJo4ICQjCCAj4wDgYDVR0PAQH/BAQDAgeAMBMGA1Ud
JQQMMAoGCCsGAQUFBwMBMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYEFKm5fseSUbBh
oPuLybPXVxkqcLzuMB8GA1UdIwQYMBaAFN4bHu15FdQ+NyTDIbvsNDltQrIwMFgG
CCsGAQUFBwEBBEwwSjAhBggrBgEFBQcwAYYVaHR0cDovL28ucGtpLmdvb2cvd3Iy
MCUGCCsGAQUFBzAChhlodHRwOi8vaS5wa2kuZ29vZy93cjIuY3J0MBkGA1UdEQQS
MBCCDnNtdHAuZ21haWwuY29tMBMGA1UdIAQMMAowCAYGZ4EMAQIBMDYGA1UdHwQv
```

```
MC0wK6ApoCeGJWh0dHA6Ly9jLnBraS5nb29nL3dyMi83NXI0WnlBM3ZBMC5jcmww
ggEFBgorBgEEAdZ5AgQCBIH2BIHzAPEAdwAS8U40vVNyTIQGGcOPP3oT+Oe1YoeI
nG0wBYTr5YYmOgAAAZiazGo9AAAEAwBIMEYCIQCDhTugtP07n9YygbmB7hGTPaFl
vozdu2k8zg8y5QeZNgIhAMZLNh42J7LVt4WzqXTsZ+Fu4QQTaP5Pbnjdo7PilnIq
AHYAzPsPaoVxCWX+lZtTzumyfCLphVwNl422qX5UwP5MDbAAAAGYmsxqjQAABAMA
RzBFAiEA7iaAWdafgSP131NorV6hWKrJzcgp6/nNiX10WGoC35wCIEQAypOeEokZ
46E7e8onDDgcd55V2w6Wm3pcAuBsV205MA0GCSqGSIb3DQEBCwUAA4IBAQAstbUU
YptgtGJ3rxA5MlSA4eZY8kUv4brIJbl90MIRugxZOoGz/J1M7UBz/ajRCTfs5GIV
9Ph1XsSkzQwlJDZjicwaSDzI16FeiSh3C8BK2SR57uG0CoFrPMwsMzT4xnp8/RZA
GrJg5zvfqwf+FyxXKtv3xrA5dF6lBPi6O0mloGWnO7Nd9fl3gimzpE8Aks9scoQ3
Pb6sKvsBXWrxBRFkLuemx/cQNXkY65QzinC7QEQge6OX26M82zjlFjgs5w6wpzfb
UsxYRoj4/YTWPxjyGu79Sv8cMjdvVZmp2iP3jJHSectMc7EavmGsX06m6lm0mirQ
He2ylQh/onoVdxpM
-----END CERTIFICATE-----
 1 s:C = US, O = Google Trust Services, CN = WR2
   i:C = US, O = Google Trust Services LLC, CN = GTS Root R1
-----BEGIN CERTIFICATE-----
MIIFCzCCAvOgAwIBAgIQf/AFoHxM3tEArZ1mpRB7mDANBgkqhkiG9w0BAQsFADBH
MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
QzEUMBIGA1UEAxMLR1RTIFJvb3QgUjEwHhcNMjMxMjEzMDkwMDAwWhcNMjkwMjIw
MTQwMDAwWjA7MQswCQYDVQQGEwJVUzEeMBwGA1UEChMVR29vZ2xlIFRydXN0IFNl
cnZpY2VzMQwwCgYDVQQDEwNXUjIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCp/5x/RR5wqFOfytnlDd5GV1d9vI+aWqxG8YSau5HbyfsvAfuSCQAWXqAc
+MGr+XgvSszYhaLYWTwO0xj7sfUkDSbutltkdnwUxy96zqhMt/TZCPzfhyM1IKji
aeKMTj+xWfpgoh6zySBTGYLKNlNtYE3pAJH8do1cCA8Kwtzxc2vFE24KT3rC8gIc
LrRjg9ox9i11MLL7q8Ju26nADrn5Z9TDJVd06wW06Y613ijNzHoU5HEDy01hLmFX
xRmpC5iEGuh5KdmyjS//V2pm4M6rlagplmNwEmceOuHbsCFx13ye/aoXbv4r+zgX
FNFmp6+atXDMyGOBOozAKql2N87jAgMBAAGjgf4wgfswDgYDVR0PAQH/BAQDAgGG
MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjASBgNVHRMBAf8ECDAGAQH/
AgEAMB0GA1UdDgQWBBTeGx7teRXUPjckwyG77DQ5bUKyMDAfBgNVHSMEGDAWgBTk
rysmcRorSCeFL1JmLO/wiRNxPjA0BggrBgEFBQcBAQQoMCYwJAYIKwYBBQUHMAKG
GGh0dHA6Ly9pLnBraS5nb29nL3IxLmNydDArBgNVHR8EJDAiMCCgHqAchhpodHRw
Oi8vYy5wa2kuZ29vZy9yL3IxLmNybDATBgNVHSAEDDAKMAgGBmeBDAECATANBgkq
hkiG9w0BAQsFAAOCAgEARXWL5R87RBOWGqtY8TXJbz3S0DNKhjO6V1FP7sQ02hYS
TL8Tnw3UVOlIecAwPJQl8hr0ujKUtjNyC4XuCRElNJThb0Lbgpt7fyqaqf9/qdLe
SiDLs/sDA7j4BwXaWZIvGEaYzq9yviQmsR4ATb0IrZNBRAq7x9UBhb+TV+PfdBJT
DhEl05vc3ssnbrPCuTNiOcLgNeFbpwkuGcuRKnZc8d/KI4RApW//mkHgte8y0YWu
ryUJ8GLFbsLIbjL9uNrizkqRSvOFVU6xddZIMy9vhNkSXJ/UcZhjJY1pXAprffJB
vei7j+Qi151lRehMCofa6WBmiA4fx+FOVsV2/7R6V2nyAiIJJkEd2nSi5SnzxJrl
Xdaqev3htytmOPvoKWa676ATL/hzfvDaQBEcXd2Ppvy+275W+DKcH0FBbX62xevG
iza3F4ydzxl6NJ8hk8R+dDXSqv1MbRT1ybB5W0k8878XSOjvmiYTDIfyc9acxVJr
Y/cykHipa+te1pOhv7wYPYtZ9orGBV5SGOJm4NrB3K1aJar0RfzxC3ikr7Dyc6Qw
qDTBU39CluVIQeuQRgwG3MuSxl7zRERDRilGoKb8uY45JzmxWuKxrfwT/478JuHU
/oTxUFqOl2stKnn7QGTq8z29W+GgBLCXSBxC9epaHM0myFH/FJlniXJfHeytWt0=
-----END CERTIFICATE-----
 2 s:C = US, O = Google Trust Services LLC, CN = GTS Root R1
   i:C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
-----BEGIN CERTIFICATE-----
MIIFYjCCBEqgAwIBAgIQd70NbNs2+RrqIQ/E8FjTDTANBgkqhkiG9w0BAQsFADBX
MQswCQYDVQQGEwJCRTEZMBcGA1UEChMQR2xvYmFsU2lnbiBudi1zYTEQMA4GA1UE
CxMHUm9vdCBDQTEbMBkGA1UEAxMSR2xvYmFsU2lnbiBSb290IENBMB4XDTIwMDYx
OTAwMDA0MloXDTI4MDEyODAwMDA0MlowRzELMAkGA1UEBhMCVVMxIjAgBgNVBAoT
GUdvb2dsZSBUcnVzdCBTZXJ2aWNlcyBMTEMxFDASBgNVBAMTC0dUUyBSb290IFIx
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAthECix7joXebO9y/lD63
ladAPKH9gvl9MgaCcfb2jH/76Nu8ai6Xl6OMS/kr9rH5zoQdsfnFl97vufKj6bwS
iV6nqlKr+CMny6SxnGPb15l+8Ape62im9MZaRw1NEDPjTrETo8gYbEvs/AmQ351k
KSUjB6G00j0uYODP0gmHu81I8E3CwnqIiru6z1kZ1q+PsAewnjHxgsHA3y6mbWwZ
DrXYfiYaRQM9sHmklCitD38m5agI/pboPGiUU+6DOogrFZYJsuB6jC511pzrp1Zk
j5ZPaK49l8KEj8C8QMALXL32h7M1bKwYUH+E4EzNktMg6TO8UpmvMrUpsyUqtEj5
cuHKZPfmghCN6J3Cioj6OGaK/GP5Afl4/Xtcd/p2h/rs37EOeZVXtL0m79YB0esW
CruOC7XFxYpVq9Os6pFLKcwZpDIlTirxZUTQAs6qzkm06p98g7BAe+dDq6dso499
iYH6TKX/1Y7DzkvgtdizjkXPdsDtQCv9Uw+wp9U7DbGKogPeMa3Md+pvez7W35Ei
Eua++tgy/BBjFFFy3l3WFpO9KWgz7zpm7AeKJt8T11dleCfeXkkUAKIAf5qoIbap
sZWwpbkNFhHax2xIPEDgfg1azVY80ZcFuctL7TlLnMQ/0lUTbiSw1nH69MG6zO0b
9f6BQdgAmD06yK56mDcYBZUCAwEAAaOCATgwggE0MA4GA1UdDwEB/wQEAwIBhjAP
BgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTkrysmcRorSCeFL1JmLO/wiRNxPjAf
BgNVHSMEGDAWgBRge2YaRQ2XyolQL30EzTSo//z9SzBgBggrBgEFBQcBAQRUMFIw
JQYIKwYBBQUHMAGGGWh0dHA6Ly9vY3NwLnBraS5nb29nL2dzcjEwKQYIKwYBBQUH
MAKGHWh0dHA6Ly9wa2kuZ29vZy9nc3IxL2dzcjEuY3J0MDIGA1UdHwQrMCkwJ6Al
oCOGIWh0dHA6Ly9jcmwucGtpLmdvb2cvZ3NyMS9nc3IxLmNybDA7BgNVHSAENDAy
MAgGBmeBDAECATAIBgZngQwBAgIwDQYLKwYBBAHWeQIFAwIwDQYLKwYBBAHWeQIF
AwMwDQYJKoZIhvcNAQELBQADggEBADSkHrEoo9C0dhemMXoh6dFSPsjbdBZBiLg9
```

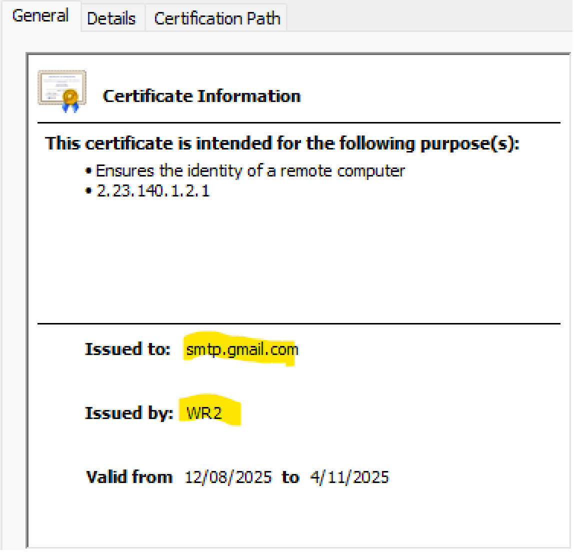
```
NR3t5P+T4Vxfq7vqfM/b5A3Ri1fyJm9bvhdGaJQ3b2t6yMAYN/olUazsaL+yyEn9
WprKASOshIArAoyZl+tJaox118fessmXn1hIVw41oeQa1v1vg4Fv74zPl6/AhSrw
9U5pCZEt4Wi4wStz6dTZ/CLANx8LZh1J7QJVj2fhMtfTJr9w4z30Z209fOU0iOMy
+qduBmpvvYuR7hZL6Dupszfnw0Skfths18dG9ZKb59UhvmaSGZRVbNQpsg3BZlvi
d0lIKO2d1xozclOzgjXPYovJJIultzkMu34qQb9Sz/yilrbCgj8=
-----END CERTIFICATE-----
---
Server certificate
subject=CN = smtp.gmail.com

issuer=C = US, O = Google Trust Services, CN = WR2

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 4383 bytes and written 419 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
250 SMTPUTF8
^C
$
```

Type in control-C to terminate the session. As shown above we have 3x certificates in PEM format. I'll copy them separately into a text file and then rename it with the extension of DER, so I can view them.

Here are the three certificates in der format which you can double click to see.



Certificate Information

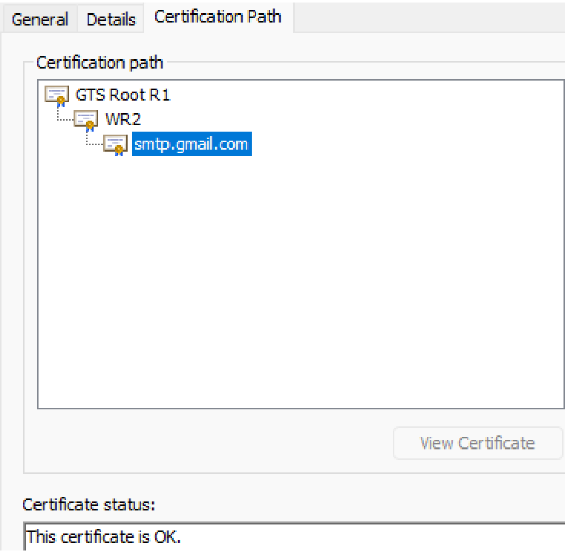
This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- 2.23.140.1.2.1

Issued to: smtp.gmail.com

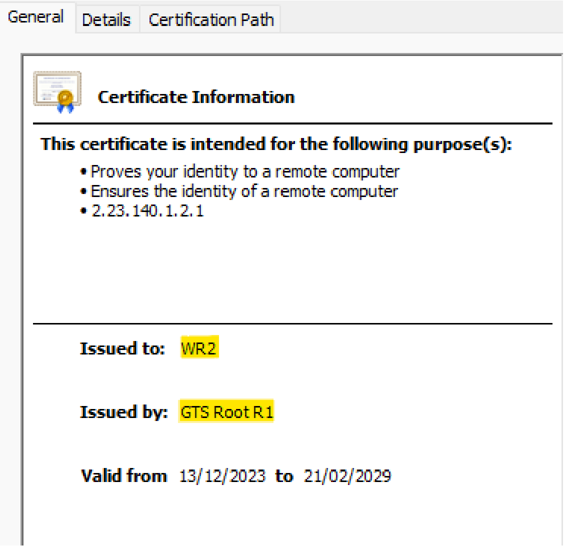
Issued by: WR2

Valid from 12/08/2025 **to** 4/11/2025



Certificate status:

This certificate is OK.



Certificate Information

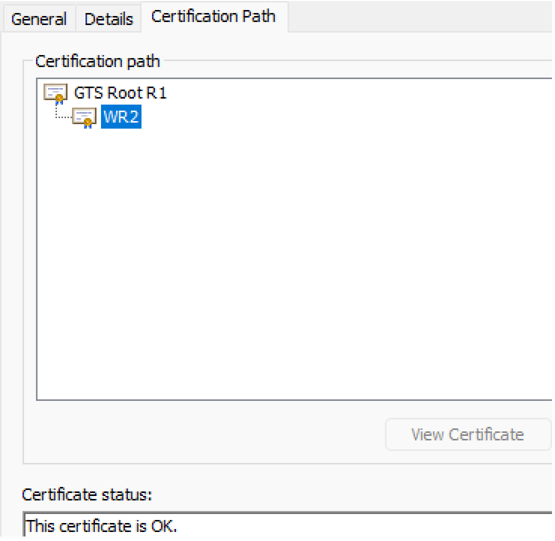
This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1

Issued to: WR2

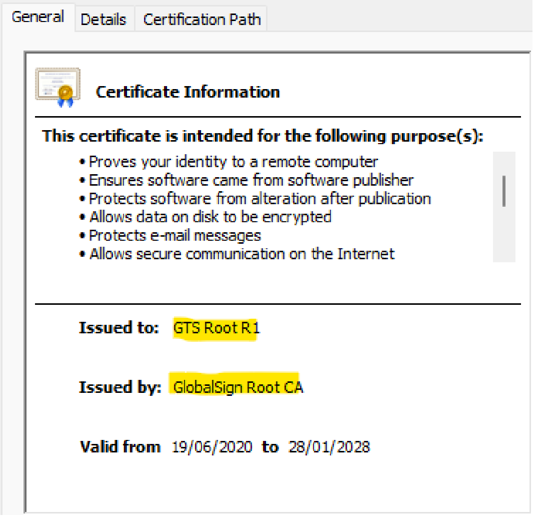
Issued by: GTS Root R1

Valid from 13/12/2023 **to** 21/02/2029



Certificate status:

This certificate is OK.



Certificate Information

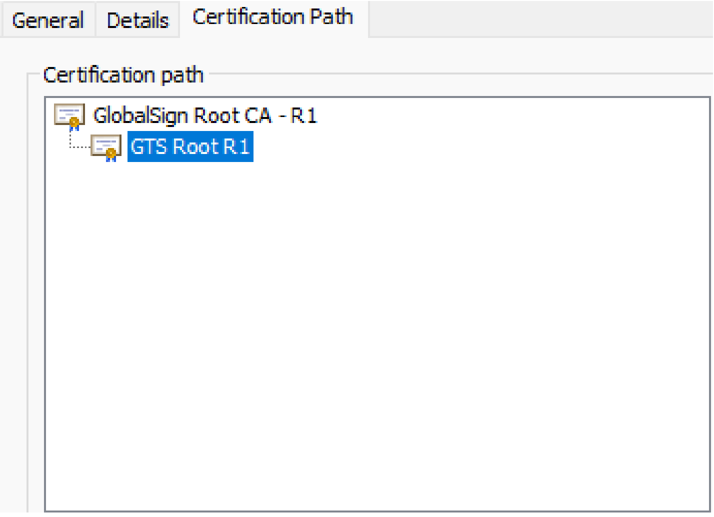
This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data on disk to be encrypted
- Protects e-mail messages
- Allows secure communication on the Internet

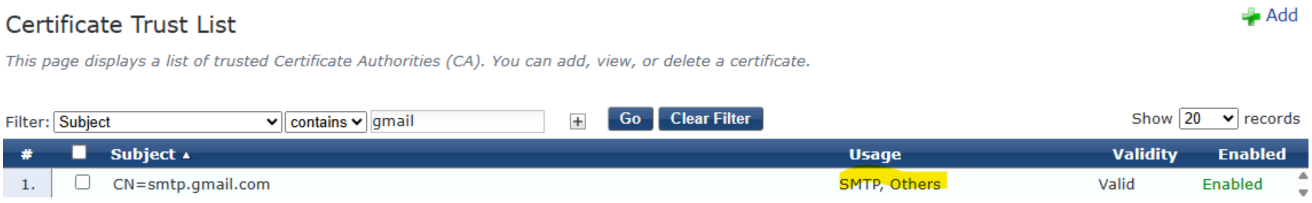
Issued to: GTS Root R1

Issued by: GlobalSign Root CA

Valid from 19/06/2020 **to** 28/01/2028



Next, you need to import them to certificate trust list in ClearPass by navigating to Administration » Certificates » Trust List and then adding the certificate. Here you need to ensure that the usage is for SMTP.

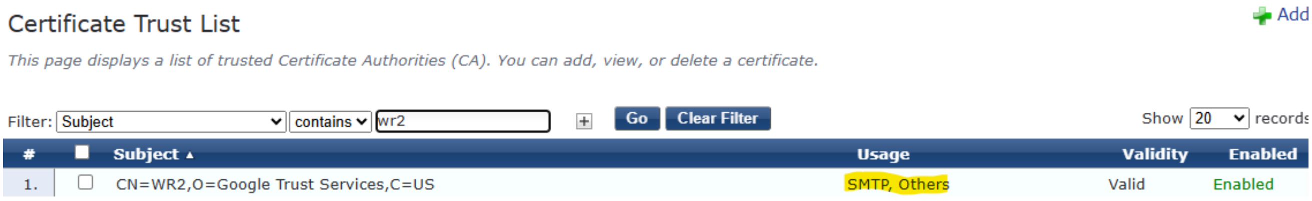


Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains gmail Show 20 records

#	□	Subject ▴	Usage	Validity	Enabled
1.	□	CN=smtp.gmail.com	SMTP, Others	Valid	Enabled

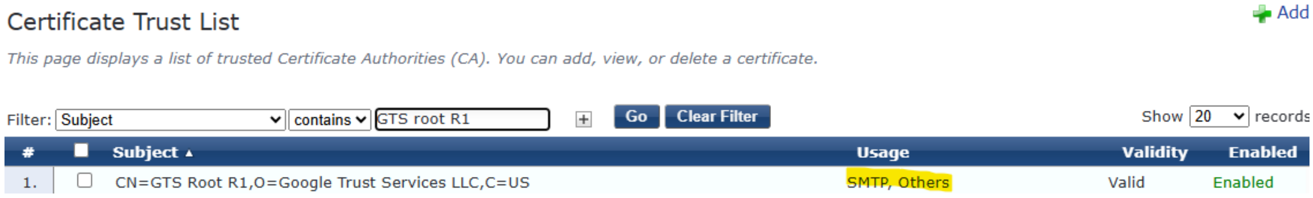


Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains wr2 Show 20 records

#	□	Subject ▴	Usage	Validity	Enabled
1.	□	CN=WR2,O=Google Trust Services,C=US	SMTP, Others	Valid	Enabled



Certificate Trust List

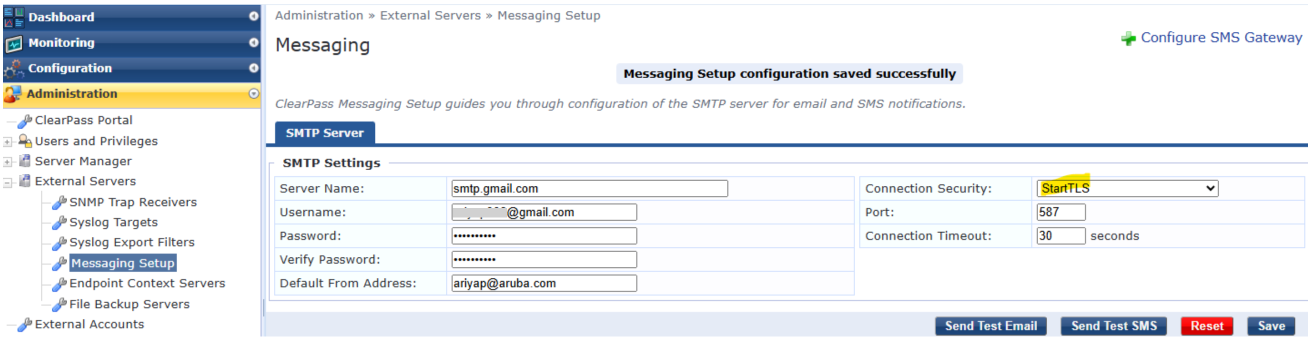
This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains GTS root R1

Show 20 records

#	□	Subject ▲	Usage	Validity	Enabled
1.	□	CN=GTS Root R1,O=Google Trust Services LLC,C=US	SMTP, Others	Valid	Enabled

And finally, I’ll configure the messaging server.



Administration » External Servers » Messaging Setup

Messaging

Messaging Setup configuration saved successfully

ClearPass Messaging Setup guides you through configuration of the SMTP server for email and SMS notifications.

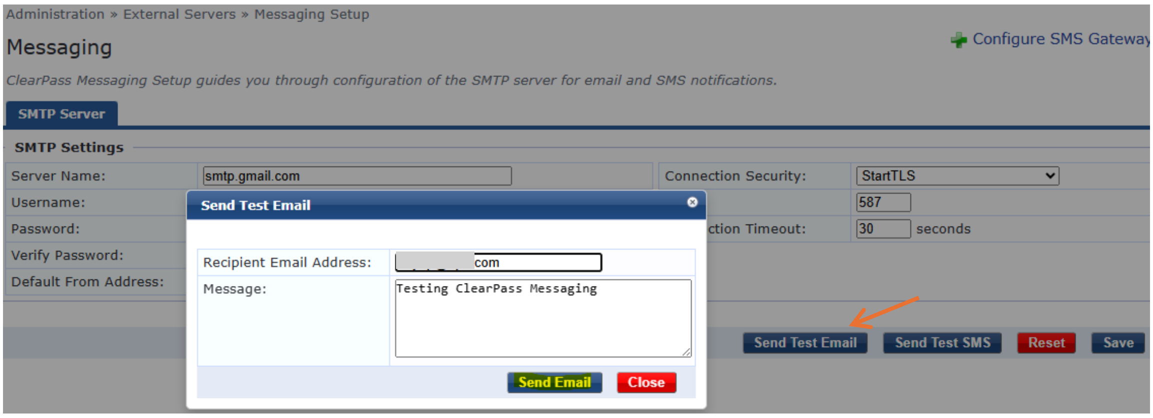
SMTP Settings

Server Name:	smtp.gmail.com	Connection Security:	StartTLS
Username:	[redacted]@gmail.com	Port:	587
Password:	••••••••••	Connection Timeout:	30 seconds
Verify Password:	••••••••••		
Default From Address:	ariyap@aruba.com		

Note that the username should be the Gmail email address and the password should be the App password that we created after we enabled the two-factor authentication for the Gmail account. Lastly, the default from address, is the from email address and in my case it is fictious email address.

2.4 Testing

You can send a quick test email directly from the messaging setup.



Administration » External Servers » Messaging Setup

Messaging

ClearPass Messaging Setup guides you through configuration of the SMTP server for email and SMS notifications.

SMTP Settings

Server Name: smtp.gmail.com

Connection Security: StartTLS

Username:

Port: 587

Password:

Connection Timeout: 30 seconds

Verify Password:

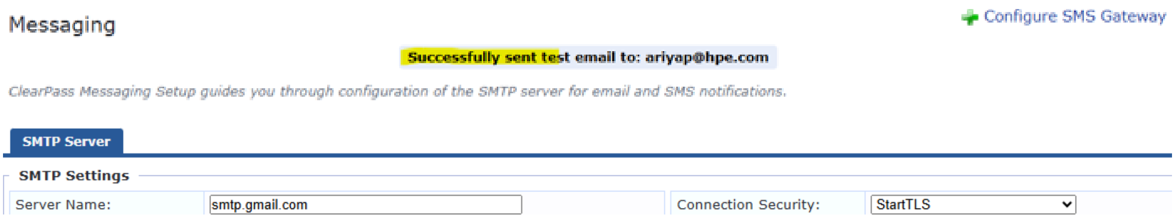
Default From Address:

Send Test Email

Recipient Email Address: [redacted]com

Message: Testing ClearPass Messaging

This is what I get after I click the “Send Email” button.



Messaging

Successfully sent test email to: ariyap@hpe.com

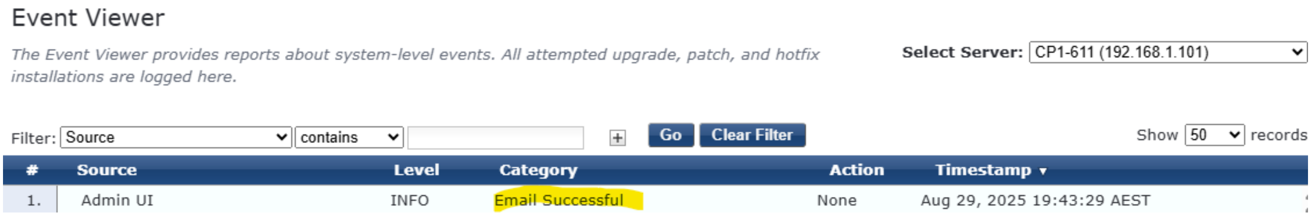
ClearPass Messaging Setup guides you through configuration of the SMTP server for email and SMS notifications.

SMTP Settings

Server Name: smtp.gmail.com

Connection Security: StartTLS

You can then go to Monitoring » Event Viewer and have a look at the logs.



Event Viewer

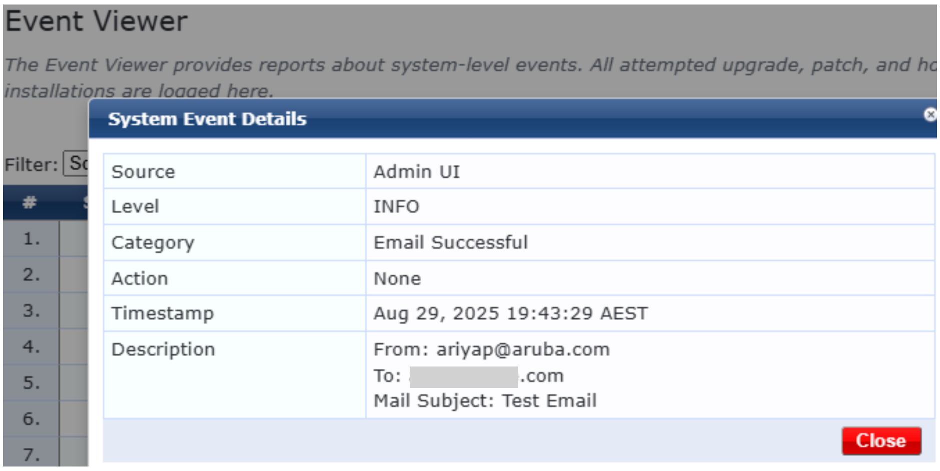
The Event Viewer provides reports about system-level events. All attempted upgrade, patch, and hotfix installations are logged here.

Select Server: CP1-611 (192.168.1.101)

Filter: Source contains

Show 50 records

#	Source	Level	Category	Action	Timestamp ▾
1.	Admin UI	INFO	Email Successful	None	Aug 29, 2025 19:43:29 AEST



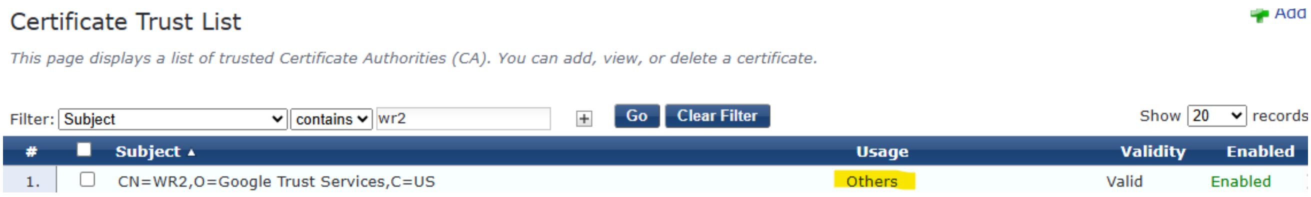
Event Viewer

The Event Viewer provides reports about system-level events. All attempted upgrade, patch, and hc installations are logged here.

System Event Details

Source	Admin UI
Level	INFO
Category	Email Successful
Action	None
Timestamp	Aug 29, 2025 19:43:29 AEST
Description	From: ariyap@aruba.com To: [redacted].com Mail Subject: Test Email

Now to generate email failures, I am going to remove SMTP as the certificate usage of WR2 intermediate certificate.



Certificate Trust List

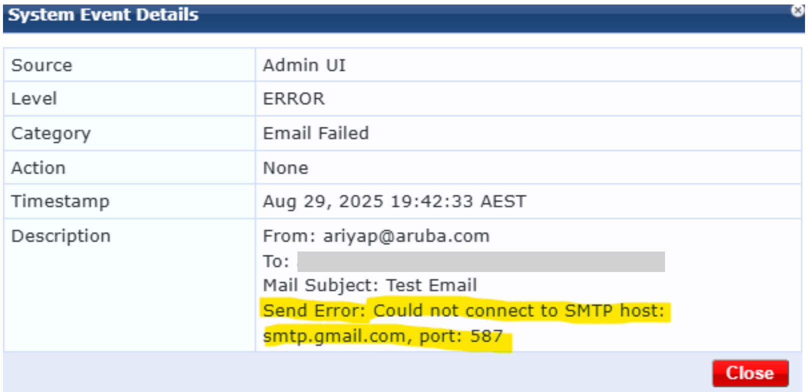
This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains wr2

Show 20 records

#	☐	Subject ▴	Usage	Validity	Enabled
1.	☐	CN=WR2,O=Google Trust Services,C=US	Others	Valid	Enabled

Let us go to the messaging setup and send test email. And this time I get a failed message shown below.

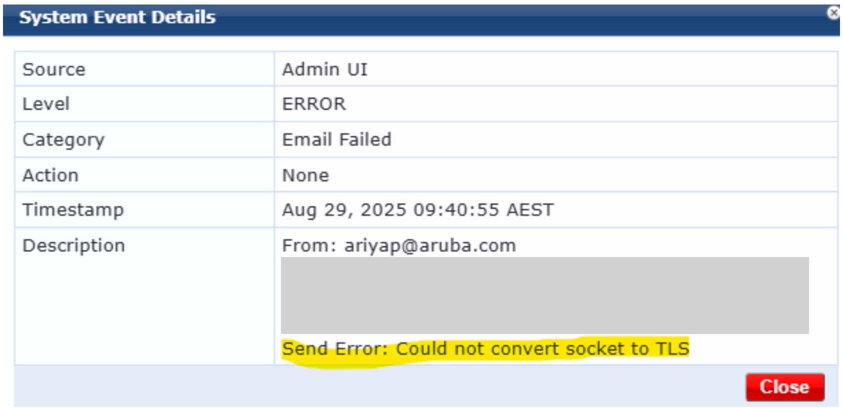


System Event Details

Source	Admin UI
Level	ERROR
Category	Email Failed
Action	None
Timestamp	Aug 29, 2025 19:42:33 AEST
Description	From: ariyap@aruba.com To: [redacted] Mail Subject: Test Email Send Error: Could not connect to SMTP host: smtp.gmail.com, port: 587

These failed messages could be because of something is blocking the outgoing traffic or have a mismatch with the certificate chain like the certificate usage is not SMTP.

If you are missing a certificate chain that Is not in the Trust list of ClearPass then most likely you get the following error that points to certificate that is not trusted.



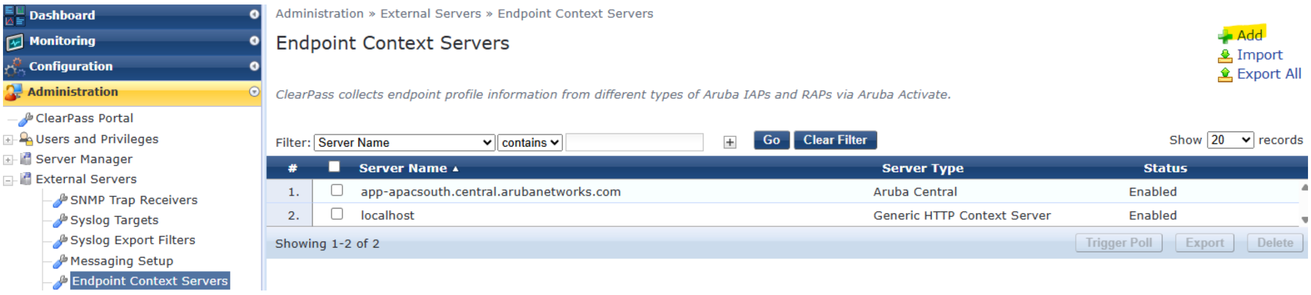
System Event Details

Source	Admin UI
Level	ERROR
Category	Email Failed
Action	None
Timestamp	Aug 29, 2025 09:40:55 AEST
Description	From: ariyap@aruba.com [redacted] Send Error: Could not convert socket to TLS

2.5 ClearPass Endpoint Context Server Configuration

In this section, I'll demonstrate how to add an endpoint context server to enable the use of an SMTP messaging gateway within post-authentication enforcement profiles. While not mandatory, this setup adds significant flexibility to solutions that require email notifications

Navigating to Administration » External Servers » Endpoint Context Servers, I am adding a new context server of type Generic HTTP server.



Administration » External Servers » Endpoint Context Servers

Endpoint Context Servers

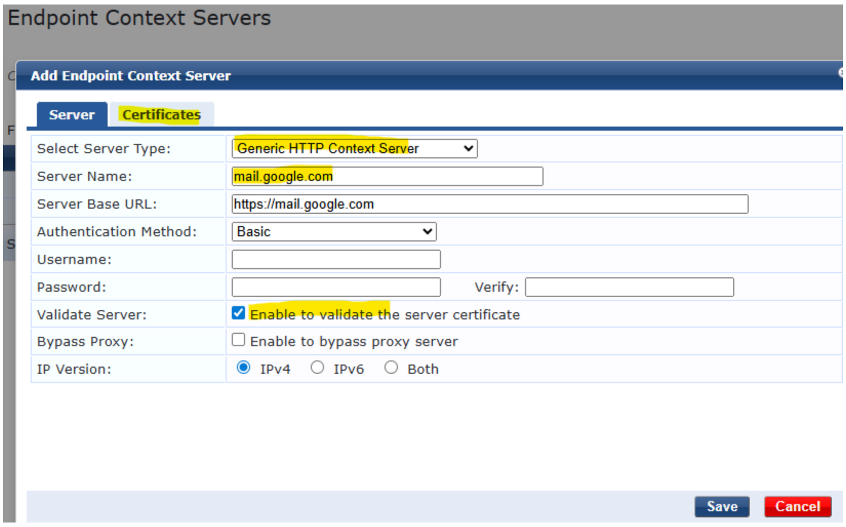
ClearPass collects endpoint profile information from different types of Aruba IAPs and RAPs via Aruba Activate.

Filter: Server Name contains

#	□	Server Name ▲	Server Type	Status
1.	□	app-apacsouth.central.arubanetworks.com	Aruba Central	Enabled
2.	□	localhost	Generic HTTP Context Server	Enabled

Showing 1-2 of 2

Make you enable the "validate server certificate" and that will add a new certificate tab.

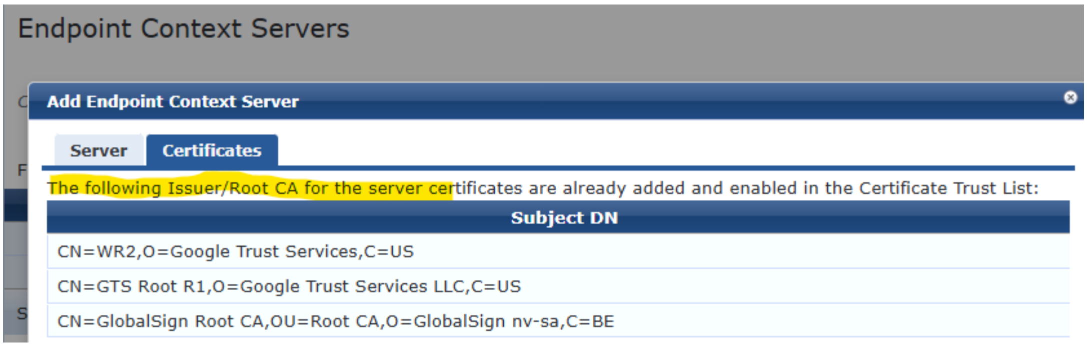


Endpoint Context Servers

Add Endpoint Context Server

Select Server Type:	Generic HTTP Context Server
Server Name:	mail.google.com
Server Base URL:	https://mail.google.com
Authentication Method:	Basic
Username:	
Password:	Verify:
Validate Server:	☑ Enable to validate the server certificate
Bypass Proxy:	□ Enable to bypass proxy server
IP Version:	● IPv4 ○ IPv6 ○ Both

Note that when you enable validating the server certificate check box, it will automatically pull the certificate chain to the trust list and enables them.



The following Issuer/Root CA for the server certificates are already added and enabled in the Certificate Trust List:

Subject DN
CN=WR2,O=Google Trust Services,C=US
CN=GTS Root R1,O=Google Trust Services LLC,C=US
CN=GlobalSign Root CA,OU=Root CA,O=GlobalSign nv-sa,C=BE

So, we could have used this method first instead of using OpenSSL. Then all we had to do was to edit the certificates and add SMTP certificate usage to them. However, it beneficial to be aware and know how to use OpenSSL as it is a primary tool for certificate manipulation and troubleshooting. As shown above you see that it is telling us that the certificates are already in the trust list of ClearPass. Now just save it.

In the next technote I will cover the enforcement profiles that can send email notifications.