Getting Started

Access Hermes SEG Administrator Console

Using a browser, access the Hermes SEG Administrator Console at <a href="https://<IP_ADDRESS>/admin/">https://<IP_ADDRESS>/admin/ where <IP_ADDRESS> is the IP address of your server.

If you have recently rebooted your system, you may get a **500 Internal Server Error** when attempting to access the **Hermes SEG Administrator Console**. This usually means that the Authentication Server has not initialized yet. This error usually goes away on its own. Wait a couple of minutes and try refreshing your browser again.

Login with the following default credentials

- Username: admin
- Password: ChangeMe2!

Set Network Settings

- Navigate to System --> Network Settings.
- Set the Network Mode drop-down to Static.
- Fill in the **Host Name** field. Ensure you enter only the name without the domain part. For example, if the FQDN of your Hermes SEG appliance is going to be **smtp.domain.tld**, then in the **Host Name** field you will simply enter **smtp** without the domain part.
- Fill in the **Primary Domain Name** field. For example, if the FQDN of your Hermes SEG appliance is going to be **smtp.domain.tld**, then in the **Primary Domain Name** field you will simply enter **domain.tld**.
- Fill in the Hermes SEG appliance **IP Address**, select the appropriate **Subnet Mask** for your network, fill in the **Gateway** and **DNS1**. If applicable, fill in **DNS2** and **DNS3** fields.
- Click on the **Submit** button. Once the settings are saved, they will not take effect until you click on the **Apply Settings** button.
- Click on the Apply Settings button (Figure 2).

Network Settings Home / Network Settings
▲ Success! ×
Changes Saved. You must click on the Apply Settings button below for the changes to take effect. If you have changed the system IP address and you access the system via the IP Address ensure you connect to the New IP Address . If you changed the system IP address and you access the system via the system via the system via Host Name, ensure the new IP address is updated in DNS. Apply Settings
Network Mode
Static
Hostname
smtp
Primary Domain Name
domain.tld
IP Address
192.168.1.200
Subnet Mask
/24 (255.255.255.0)
Gateway
192.168.1.1
DNS1
192.168.1.100
DNS2
192.168.1.120
DNS3
192.168.1.130
Submit

• If you changed Hermes SEG IP Address, your browser will most likely time out. Remember, to access the Hermes SEG Administrator Console Web GUI at

<u>https://<NEW_IP_ADDRESS/admin/</u> where is the **<NEW_IP_ADDRESS>** is the IP you set above.

Set System Certificates

• Navigate to System --> System Certificates.

Hermes SEG Community Version

Hermes SEG Community Version will allow you to create Certificate Signing Requests to submit to 3rd party CAs and import certificates from 3rd party CAs.

 Click the Import Certificate button, enter a friendly name for the certificate in the Certificate Name field, paste the contents of the certificate including the -----BEGIN CERTIFICATE----- & -----END CERTIFICATE----- lines in the Certificate field, paste the contents of the unencrypted key including the -----BEGIN PRIVATE KEY----- & -----END PRIVATE KEY----- lines in the Unencrypted Key field, paste the contents of the root and Intermediate CA certificates including the -----BEGIN CERTIFICATE----- & -----END CERTIFICATE----- lines in the Root and Intermediate CA Certificates field and click the Import button (Figure 3):



Hermes SEG Pro Version

Hermes SEG Pro Version will allow you to create Certificate Signing Requests to submit to 3rd party CAs, import certificates from 3rd party CAs as well as Request Lets Encrypt (Acme) Certificates.

If you wish to import a 3rd party CA certificate, please follow the Hermes SEG Community instructions above to import a certificate. If you wish to request a Lets Encrypt (Acme) certificate, follow the instructions below:

Before requesting **Acme Certificates** ensure that **BOTH** ports **TCP 80** and **TCP 443** are open to Hermes SEG from the Internet and the domain you are requesting the certificate is pointing to the Internet accessible IP address of your Hermes SEG machine. We recommend that you test using the **Acme Staging** server first to ensure the request works before attempting to use **Acme Production**. The reason we initially **Request Acme Certificate** utilizing the **Acme Staging** server is because Lets Encrypt is much more lenient with rate limits with failed requests in their staging environment than their production environment, click here for details.

Click the Request Acme Certificate button, enter a friendly name in the Certificate
 Name field, enter the FQDN (domain name) you wish to request a certificate, enter a valid e-mail address in the Notifications E-mail address field, leave the Acme Server drop-down field set to Acme Staging and click the Request button (Figure 4):



- If the Acme Certificate Request fails, double-check that the FQDN (domain name) points to the Internet accessible IP of your Hermes SEG machine and that BOTH ports TCP/80 (HTTP) and TCP/443 (HTTPS) are allowed through your firewall and try again.
- If the Acme Certificate Request succeeds, locate the newly created certificate in your certificate list, click the ______icon and on the resultant Delete Certificate confirmation click on Yes (Figure 5):



 Click the Request Acme Certificate button again, enter a friendly name in the Certificate Name field, enter the FQDN (domain name) you wish to request a certificate, enter a valid e-mail address in the Notifications E-mail address field, this time set the Acme Server drop-down field set to Acme Production and click the Request button (Figure 6):



Set Console Settings

The Hermes SEG **Console Settings** sets the method you wish to access Hermes SEG machine which includes the Admin Console, User Console and the Ciphermail Console. By default, the **Console Mode** is set to **IP Address**, however, an IP address is not contusive to using SSL certificates. Therefore, if you plan to use a SSL certificate to access the Hermes SEG machine without getting certificate errors, you must set the Console Mode to **Host Name**. The Host Name you set does **NOT** necessarily have to the the same **Host Name** you set in **Network Settings** above. The **Host Name** and **Primary Domain Name** you set in the Network settings is used for SMTP transactions such as **SMTP TLS** and it's not related to Hermes SEG console access.

- Navigate to System --> Console Settings.
- Set the **Console Mode** drop-down to **Host Name** and in the resultant **Host Name** field that appears, fill in the desired host name you wish to use (**Figure 7**):

Figure 7

Console Settings	Home / Console Settings
+ Generate DH Parameters File	
Console Mode	
▲ If you change the Console Mode to IP Address or Host Name ensure you change your browser's address to re Address or the Host Name you set. This setting also sets the Ciphermail Portal and the User Console addresses.	flect the new system IP
Host Name	~
Host Name	
smtp.domain.tld	

• The **Console Certificate** field is pre-populated with the **system-self-signed** certificate. If you wish to use a SSL certificate you previously set in the **Set System Certificates** section above, simply delete the **system-self-signed** entry and start typing the friendly name of the certificate you setup previously that matches the host name. The system will locate the certificate and display it in a drop-down list. Click on the certificate and the system will automatically populate all the rest of the Certificate fields such as the Subject, Issuer, Serial and Type (**Figure 8**):

Figure 8

Console Certificate			
myd			
mycertificate	.lu		

 We highly recommend that you enable HTTP Strict Transport Security (HSTS), Online Certificate Status Protocol (OCSP) Stapling, Online Certificate Status Protocol (OCSP) Stapling Verify and click the Submit button (Figure 9):

HTTP Strict Transport Se	ecurity (HSTS)	
Enable (Recommended)		•
Online Certificate Status	Protocol (OCSP) Stapling	
Enable (Recommended)		•
Online Certificate Status	Protocol (OCSP) Stapling Verify	
Enable (Recommended)	•	~
Cultural		
Submit		

After clicking the **Submit** button and you changed the Console Mode from IP Address to Host Name, your browser will **NOT** automatically redirect you to the new console address.

Ensure you enter the new address in your browser as <a href="https://endotedots/https://endotedots/lambda-is-is-is-head-completer-style="border: 1px style="border: 1px style="type: 1px style: 1px style="

 Additionally, we recommend that you generate a DH (Diffie-Hellman) Parameters file by clicking the Generate DH Parameters File button and on the resultant Generate Diffie-Hellman (DH) Parameters File confirmation window, click on Yes (Figure 10):

Old Web G

Generate Diffie-Hellman (DH) Parameters File

Generate DH

Console Se

Console Mode

Host Name

Console Certificat

mycertificate

Certificate Subject

Certificate Issuer

C = US, O = Let's

CN = c

Host Name

▲ If you chang Address or the F This process will take very long time to complete (~40 minutes on 1 CPU systems).

If this the first time you are generating a Diffie-Hellman (DH) file, when the process is complete there will be a new Diffie-Hellman (DH) key-exchange drop-down option on the Console Settings page. The option will only appear when the process is complete.

/our l Jser (

If this is not the first time you are generating a Diffie-Hellman (DH) file, generating a new file will automatically Disable the Diffie-Hellman key-exchange for your system, replace the existing Diffie-Hellman (DH) file and remove the Diffie-Hellman (DH) key-exchange drop-down option from the Console Settings page. You must manually re-enable the Diffie-Hellman (DH) key-exchange option when the process is complete.

Are you sure you want to Generate a Diffie-Hellman (DH) Parameters File?



Generating a DH Parameters file can take a very long time to complete (~40 minutes on 1-CPU systems). You can proceed to configure the rest of your system (DO NOT reboot the system while it's generate a DH Parameters file) and check back under System
 --> Console Settings to see if a new Diffie-Hellman (DH) key-exchange drop-down appears set it to Enable and click the Submit button below (Figure 11).

Figure 11

Ξ

Diffie-Hellman (DH) key-exchange	
Enable (Recommended)	~
HTTP Strict Transport Security (HSTS)	
Enable (Recommended)	~
Online Certificate Status Protocol (OCSP) Stapling	
Enable (Recommended)	~
Online Certificate Status Protocol (OCSP) Stapling Verify	
Enable (Recommended)	*
Submit	\triangleright

If you follow the above recommendations, you should be able to achieve an **A+ rating** on the Qualys SSL Labs SSL Server Test (Figure 12):

Figure 12



Set SMTP TLS Settings

It's important to set SMTP TLS in order to transmit e-mail messages between your Hermes SEG machine and other e-mail servers using TLS encryption.

Before you can set **SMTP TLS**, you must first have either imported or requested a SSL Certificate in the **Set System Certificates** section above for the **Hostname** and **Primary Domain Name** you set in the **Set Network Settings** above.

- Navigate to Gateway --> SMTP TLS Settings.
- Set the SMTP TLS Mode drop-down to Opportunistic TLS.
- The SMTP TLS Certificate field is pre-populated with the system-self-signed certificate. If you wish to use a SSL certificate you set in the Set System Certificates section above, simply delete the system-self-signed entry and start typing the friendly name of the certificate you setup previously that matches the Hostname and Primary Domain Name you set in the Set Network Settings above. The system will locate the certificate and display it in a drop-down list. Click on the certificate and the system will automatically populate all the rest of the Certificate fields such as the Subject, Issuer, Serial and Type (Figure 13):

SMTP TLS Certificate	
myce	
mycertificate	6
=== DO NOT DELETE ===	40

• Click the **Submit** button (Figure 14):

SMTP TLS Settings

.

F Add Domain
SMTP TLS Mode
Opportunistic TLS (Recommended)
Do NOT select the system-self- signed Certificate
SMTP TLS Certificate
mycertificate
Certificate Subject
CN = U. in iteration in the
Certificate Issuer
C = US, O = Let's Encrypt, CN = R3
Certificate Serial
140451000004000000000000000000000000000
Certificate Type
Acme
Submit

Change admin System Account Password

- Navigate to System --> System Users.
 In the System Users screen, click the click in the connext to the admin Username (Figure 15).

System	Users					Home	e / System Users
+ Create	System User						
Copy CS Show 25 rows	SV Excel PDF	Print					
						Search:	
Edit 11	Username 🌐	E-Mail 1	First Name	Last Name	Access Control	†↓ Built-In †↓	Active îl
ľ	admin	someone@domain.tld	System	User	ONE FACTOR	YES	YES
Edit	Username	E-Mail	First Name	Last Name	Access Control	Built-In	Active
Showing 1 to	0 1 of 1 entries						
		\searrow				Previo	us 1 Next

In the Edit System User screen, set the Set User Password drop-down to YES, enter a new password in the User Password field that appears and click the Submit button (Figure 16).

Figure 16

Edit System User	Home / Edit System User
り Back to System Users	
Username	
admin	
E-Mail Address	
someone@domain.tld	
First Name	
System	
Last Name	
User	
Access Control Policy	
Warning! Before setting Access Control Policy to Two Factor ensure you first read the Access Control Policy Documentation , ensure e-mail delivery works as expected, the e-mail addresses for this System Use an authenticator app such as FreeOTP, Google Authenticator, Authy etc installed on your mobile device	r is correct and you have
One Factor	~
Set User Password	
YES	~
Check Password Against haveibeenpwned.com	
YES	~
User Password	6
Submit	

We highly recommend that you also set **Two Factor** authentication (2FA) for the **System** User account by following the instructions on the **System Users** <u>documentation</u>.

Setup Domains

In order for Hermes SEG to deliver email, you must first set the domain(s) that Hermes SEG will process email for along with their corresponding destination email server(s). You can add as many domains and destination email servers as required. An email server can be configured as an IP address or a Host Name as long as the Hermes SEG can reach it over the TCP port you set. Multiple domains can be pointed to the same email server if necessary.

- Navigate to **Gateway --> Domains**.
- Click the Create Domain button (Figure 17):

Domains	Hom	e / Domains
Create Domain		
Copy CSV Excel PDF Print Show 25 rows • entries	Ç,	

- The system will generate a temporary Domain Name, Destination Address and redirect you to the **Edit Domain** page.
- Adjust the pre-populated Domain Name field to the actual domain name you are using.
- Set the **Delivery Method** field to **SMTP** if you wish to have Hermes SEG relay e-mail for that domain or set it to **NONE** if you wish Hermes SEG to discard and silently drop any received e-mail for that domain. Note that setting the **Delivery Method** to **NONE** will disable all other fields.
- Set the Recipient Delivery field to ANY if you wish to have Hermes SEG relay e-mail for any recipients regardless if those recipients are added in Gateway --> Internal Recipients or Gateway --> Virtual Recipients. This method relies on the destination e-mail server to reject e-mail for non-existent recipients. Note that this method has the potential of adding extra load on the destination e-mail server but offers more flexibility because it doesn't require you to add Internal or Virtual recipients before hand.
 Alternatively, set the Recipient Delivery to SPECIFIED if you wish to have Hermes SEG relay e-mail only for recipients that have been added in Gateway --> Internal
 Recipients or Gateway --> Virtual Recipients. This method will reject any e-mail for non-existent Internal or Virtual recipients by Hermes SEG thus reducing the load on the destination server.
- Set the **Destination Address** field to the IP Address or the FQDN of the destination email server you wish to have Hermes SEG relay e-mail.
- Set the **Destination Port** field to the TCP port of the destination e-mail server you wish to have Hermes SEG relay e-mail.
- Set the Destination Requires Authentication field to NO if the destination e-mail server does not require authentication or set to YES if the destination e-mail server requires authentication. Setting to YES will add a Destination Username field and a Destination Password field which will have to be filled with a destination e-mail server username and password. Note that if Gateway --> Relay Host is Enabled, Hermes SEG will not allow you to save a domain with Destination Requires Authentication field set to YES. You must first set Gateway --> Relay Host to Disabled.

- Set the Destination Use MX Lookup to NO if you do not wish to have Hermes SEG perform MX lookups to relay e-mail for the domain you are adding. This will prevent e-mail loops if Hermes SEG is the primary MX host for the domain and it's usually the most common configuration. Set the Destination MX Lookup to YES if you wish to have Hermes SEG perform MX lookups to relay e-mail for the domain are adding. Please note that the Destination Use MX Lookup field is not available if the Destination Requires Authentication field is set to YES (Figure 18).
- Click the **Submit** button to save your changes.

Edit Domain	Home / Edit Domain
b Back to Domains	
Domain Name	
473_domain.tld	
Delivery Method	
SMTP (Recommended)	~
Recipient Delivery	
ANY	~
Destination Address	
smtp.473_domain.tld	
Destination Port	
25	
Destination Requires Authentication	
A You will not be allowed to set the Destination Requires Authentication field below to YES if Gateway> Relay Host is set to Enabled	
NO	~
Destination Use MX Lookup	
NO	~
Submit	

Add Internal Recipients

If you have setup any domains in the **Setup Domains** section above with the **Recipient Delivery** field set to **SPECIFIED**, then you **MUST** add either **Internal Recipients** or **Virtual Recipients** in order to process incoming e-mail and relay that email to the correct recipient mailboxes which are located on the destination email server(s) for the domain(s) you setup in the **Setup Domains** section above. This section will guide you with adding **Internal Recipients**.

- Navigate to Gateway --> Internal Recipients.
- Click the Create Recipient(s) button (Figure 19):

Internal Recipients	Home / Internal Recipients
Create Recipient(s)	
Copy CSV Excel PDF Print Show 25 rows \$ entries	

In the Add Internal Recipient(s) page, in the Recipient(s) field, enter an e-mail address each in each own line, select the appropriate options in the SVF Policy to Assign, Quarantine Reports, Quarantine Report Frequency, Train Bayes Filter from User Portal, Download Messages from User Portal, PDF encryption, S/MIME Encryption, S/MIME SIGNATURE, PGP Encryption drop-downs and click the Submit button (Figure 20):

Figure 20

Add Internal Recipient(s)	e / Add Internal Recipient(s)
b Back to Internal Recipients	
Recipient(s)	
user1@domain.tdd user2@domain.tdd user3@domain.tdd	
SVE Policy to Acian	10
Default 34-tics	~
Quarantine Reports	
Enable Report Only if Quarantined Messages Exist	~
Quarantine Report Frequency	
Daily (Previous Day's Quarantine Report)	~
Train Bayes Filter from User Portal	
A Warning!	
Ensure you do NOT enable for inexperienced recipients. Improperly training Bayes Filter will affect ALL excipients.	
Citable	~
Download Messages from User Portal	
A Warring!	
Enabling can expose recipients to mehane	
	_
Disable	~
Please Note!	
Setting POF, SyMME or POP Encryption below to Enable will significantly increase the amount of time it takes to add new recipient(s)	
PDF Encryption	
Daable	~
\$/MIME Encryption	
Drable	~
SyMMing SickATURE (Fictive only when SVMMC Certificate present Fictive only when SVMMC Certificate present	
San Economic Messanes Only	~
PGP Encryption	
Disable	~
Schen Lander Sch	

Set Postmaster, Admin E-mail Address and TimeZone

- Navigate to System --> System Settings.
- Fill in **Postmaster E-mail Address** field with an email belonging to a **Relay Domain** you setup above.

- Fill in the Admin E-mail Address field with an email of domain outside of the system (i.e. a domain that the system does not relay email Ex: someone@hotmail.com).
- Delete the **America/New_York** default **TimeZone** entry and start typing your continent and a drop-down with the available **TimeZones** for that continent will appear where you can select the appropriate one for your location (**Figure 21**).

System Settings		Home / System Settings
Add Serial Number	L ₂	
Postmaster E-mail Address		
postmaster@domain.tld		
Admin E-mail Address		
someone@domain.tld		
TimeZone		
America/		
America/Adak		
America/Anchorage		
America/Anguilla		
America/Antigua		
America/Araguaina		
America/Argentina/Buenos_Aires		
America/Argentina/Catamarca		
America/Argentina/Cordoba		
America/Argentina/Jujuy		
America/Argentina/La_Rioja		
America/Argentina/Mendoza		
America/Argentina/Rio_Gallegos		

• Click the **Submit** button.

Set Relay Networks

In addition to inbound email, if the email server(s) you added will also be sending outbound email through the Hermes SEG (recommended), you must allow their IP address(es) to send (relay) email through the Hermes SEG.

- Navigate to Gateway --> Relay Networks.
- Ensure IP Address is selected and the under the IP Address field enter the IP Address of the email server that you want to allow to send email through the Hermes SEG, under the Note field, enter a short description identifying the email server (ensure that you don't use any spaces or special characters in the Note field) and click the Add button (Figure 22)

Relay IPs/Networks

Add Relay IPs/Networks

Select the type of entry (IP Address or Network) you wish to add below and proceed adding your entry into the Permitted Relay IPs/Networks.

192.168.0.100		Exchange_Server	Add
IP Address		Note	
\bigcirc	Network Address		
\bullet	IP Address		

- Repeat as necessary for every email server that you want to allow to send outbound email through the Hermes SEG.
- As you add entries, you will notice that each entry shows up under the **Permitted Relay IPs/Networks to be added** section (**Figure 23**)

Figure 23

Permitted Relay IPs/Networks to be added	
192.168.0.100> Exchange_Server> TO BE ADDED	
Ψ	
	Cancel All Add

🖋 IP Address ready to be added. Please click the Apply Settings to add the IP Address to the system and apply your changes

 After you are finished adding all your permitted email servers, you must apply the settings in order for the changes to take effect. On the bottom of the page, click on the **Apply Settings** button (**Figure 24**)

Figure 24

Apply Settings

Initialize Pyzor

Pyzor is a collaborative, networked system to detect and block spam using digests of messages. Vipul's Razor is a distributed, collaborative, spam detection and filtering network.

Hermes SEG uses both of these components for better spam detection. Both of these components must be initialized before Hermes SEG can use them.

• Navigate to **Content Checks** --> **Initialize Pyzor** and click on the **Initialize Pyzor** button. Wait for successful completion before proceeding further (**Figure 25**).



Initialize Vipul's Razor

Before attempting to initialize Vipul's Razor, ensure the Hermes SEG has outbound Internet access. Initialization can take a few minutes to complete, so please be patient.

• Navigate to **Content Checks --> Initialize Vipul's Razor** and click on the **Initialize Razor** button. Wait for successful completion before proceeding further (**Figure 26**).

Figure 26



Clear Bayes Database

The Bayes Database tries to identify spam by looking at what are called *tokens*; words or short character sequences that are commonly found in spam or ham.

On a new Hermes SEG installation, it's always best to ensure a clean Bayes Database before you start processing email.

Navigate to Content Checks --> Clear Bayes Database and click on the Clear
 Database button. Wait for successful completion before proceeding further (Figure 27).

Figure 27



Set Encryption Settings

- Navigate to Encryption --> Encryption Settings.
- Fill in Encryption by e-mail subject keyword field or leave it set to default [encrypt].
- Select whether you wish to **Remove the e-mail subject keyword after encryption** or leave it to default **Yes**.

- Fill in the **PDF Reply Sender E-mail** field. This must be an email address with a domain that Hermes SEG relays email. Ex: **postmaster@domain.tld**
- Click the button for the **Server**, **Client** and **Mail Secret Keyword** fields to generate random keywords, or set your own 10-character minimum uppler/lower case letter/number keywords.
- Click on the **Save Settings** button and after the settings are saved, click the **Apply Settings** button(**Figure 28**).

?

Figure 28

Encryption Settings	
Trigger encryption by e-mail subject***	
Enabled	
O Disabled (Not recommended)	
Encryption by e-mail subject keyword****	
[encrypt]	
Remove e-mail subject keyword after encryption	
Yes (Recommended)	
O No	
Secure Portal Address (Default: https://hermes.domain.tld/web/portal)	
https://https://hermes.domain.tld/web/portal/	
	_
PDF Reply Sender E-mail	_
postmaster@domain.tld	
Click Button to Generate Server Secret Keyword Server Secret Keyword (Minimum 10 characters, Upper/Lower Case Le	etters and numbers ONLY)
yzki8pmdziicv3zosgi715wewparknbolidubx9aq ijnqjgciusmvyen4	HT I
Click Button to Generate Client Secret Keyword	
Client Secret Keyword (Minimum 10 characters, Upper/Lower Case Let	tters and numbers ONLY)
jq3axsgyv4tnpwuteu2kvrkgezs8zdbl1c5h9w6am7byomnrjhdcfpq	fil
Click Button to Cenerate Mail Secret Keyword	
Mail Secret Keyword /Minimum 10 charactere Upper/Lower Case Lette	are and numbers ONLY
han secret Reyword (winning in to characters, opper/Lower Case Lette	
proceedozgraw rodikawenizieninipilepilogetikodxvstiej94/1pyryzv	13
	Save Settings
	oave oeunys

Change the Ciphermail admin Account Password

Navigate to <u>https://<IP_ADDRESS>/ciphermail/</u> where <IP_ADDRESS> is the IP Address of your machine and login with the Username of admin and password of admin (Figure 29):

Figure 29



• Once logged in, click on the **Admin** entry on the top menu and on the Administrators page, click on the admin username (**Figure 30**).



• In the Edit Administrator: admin page, enter a new password in the first Password field and then verify it in the second Password field and then click on the Apply button at the bottom of the page (Figure 31). Passwords must be at least 8 characters long, they must contain letters, numbers and special characters.

Figure 31



Recommendations

Register for Barracuda Central Account

Hermes SEG comes pre-configured to use the Barracuda RBL (Realtime Block List), however you must first register for an account and provide your DNS Server IPs at <u>Barracuda Central</u> before you will be allowed to use it.

Revision #39 Created 17 November 2020 12:23:49 by Dino Edwards Updated 5 June 2022 19:02:13 by Dino Edwards