Release Notes

AHS-HF-5427-GU0005

Last Updated: 13th January 2022

CONTENTS

1 OVERVIEW

This document outlines the fixes and enhancements provided in Hotfix **AHS-HF-5427-GU0005** and how to apply hotfix on HySecure gateway. It is recommended to apply this hotfix on gateway version 5.4.2.7.

Note: Down time is required while applying this hotfix.

AHS-HF-5427-GU0005

Released on 13th January 2022

2 HOW TO APPLY HOTFIX

2.1.1 Upgrade compatibility of Hotfix AHS-HF-5427-GU0005

HySecure Hotfix AHS-HF-5427-GU0005 is a cumulative hotfix and can be applied on any HySecure gateway based on V5427.

List of hotfixes included in AHS-HF-5427-GU0005:

1. AHS-HF-5427-GU0004

Please refer Appendix A: Upgrading HySecure Cluster for procedure to upgrade **HySecure cluster gateway**.

2.1.2 How to get HySecure Hotfix AHS-HF-5427-GU0005

Please login into support.accops.com using your registered account to download this hotfix.

Click here to get the link

Md5sum: **a5a1cbc2e515a47d7a276af6b8a87c22**

3 NEW FEATURES

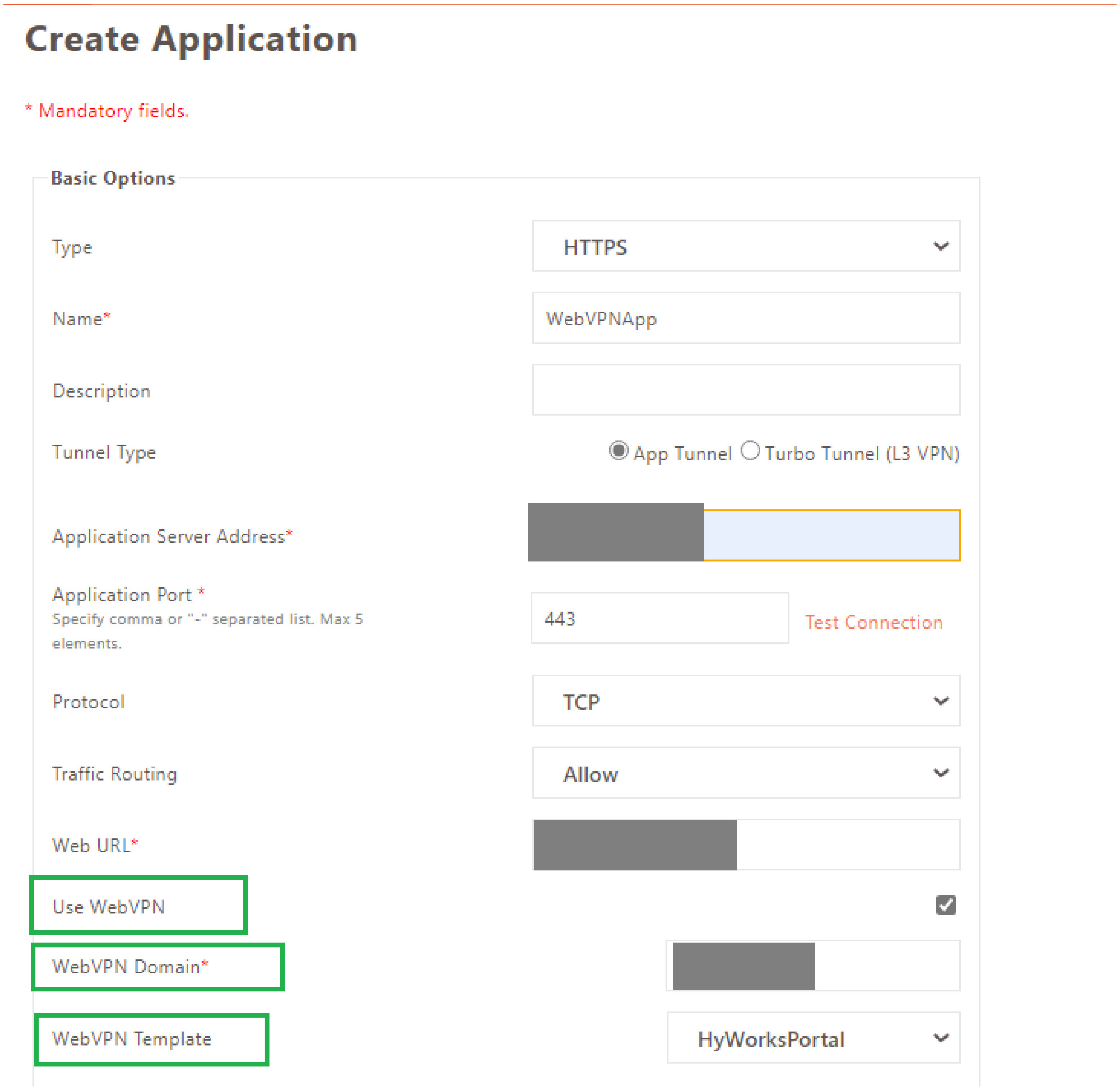
3.1.1 Web VPN (Reverse Proxy) support for HTTP/HTTPS app access through Web browser

In HySecure version 5.3, there was a support to publish HTTP/HTTPS based applications which could be accessed over a browser without the need for any Accops client installation. This feature, called Web VPN or alternatively as Reverse Proxy support, has been restored in the current HotFix.

Web VPN offers browser based secure access with MFA, to HTTP/HTTPS applications without directly exposing them on the internet. It does not require installation of any client software or tool on the end user machine. Published application can be accessed over any web browser if the application supports it.

Steps to publish Web VPN supported HTTP/HTTPS:

- Login to management console.
- Go to Apps and click on Add.
- Select Application Type as **HTTP or HTTPS** as the case might be and fill the other application details.
- Check **Use Web VPN** checkbox.
- Enter **Web VPN Domain**. (Enter virtual IP of HySecure gateway).
- Select **Web VPN Template** as per requirement. (Choose default if you don’t have any app with similar Web VPN configuration).
- Click on Submit button present at bottom and application will be successfully created.



Create Application

* Mandatory fields.

Basic Options

Type	HTTPS
Name*	WebVPNApp
Description	
Tunnel Type	● App Tunnel ○ Turbo Tunnel (L3 VPN)
Application Server Address*	[redacted]
Application Port * Specify comma or "-" separated list. Max 5 elements.	443 Test Connection
Protocol	TCP
Traffic Routing	Allow
Web URL*	[redacted]
Use WebVPN	☑
WebVPN Domain*	[redacted]
WebVPN Template	HyWorksPortal

3.1.2 Default Templates for Web VPN (Reverse Proxy)

There are typically similar HTTP/HTTPS based applications which need to be published in Web VPN. To facilitate a quick and error free mechanism of creating such applications, templates support has been introduced in this Hotfix.

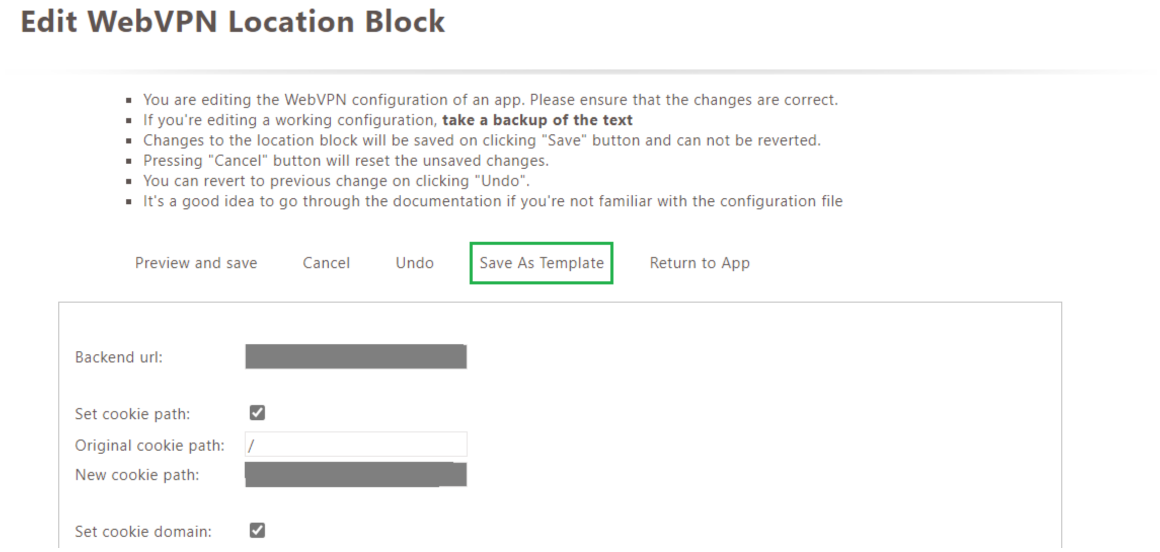
Any application can be saved as a template in HySecure gateway. These saved templates can be later used to create similar types of HTTP/HTTPS application with Web VPN enabled thus avoiding keying in similar configuration again.

Besides the ability to save templates, there are default templates available for HTTP and HTTPS based applications as well as for “HyWorksPortal” and “ARS”.

To save template of any Web VPN based application, follow below steps:

- Login into HySecure Management console.
- Go to Apps and modify the application whose template is to be saved.

- Click on *Save as template*.



Edit WebVPN Location Block

- You are editing the WebVPN configuration of an app. Please ensure that the changes are correct.
- If you're editing a working configuration, **take a backup of the text**
- Changes to the location block will be saved on clicking "Save" button and can not be reverted.
- Pressing "Cancel" button will reset the unsaved changes.
- You can revert to previous change on clicking "Undo".
- It's a good idea to go through the documentation if you're not familiar with the configuration file

Backend url: [redacted]

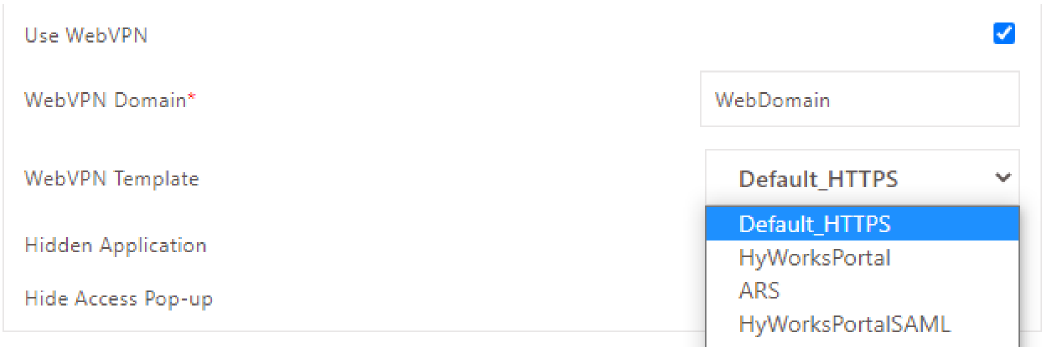
Set cookie path: ☑

Original cookie path: /

New cookie path: [redacted]

Set cookie domain: ☑

To use saved templates while creating application, select the saved templates from Web VPN template list.



Use WebVPN ☑

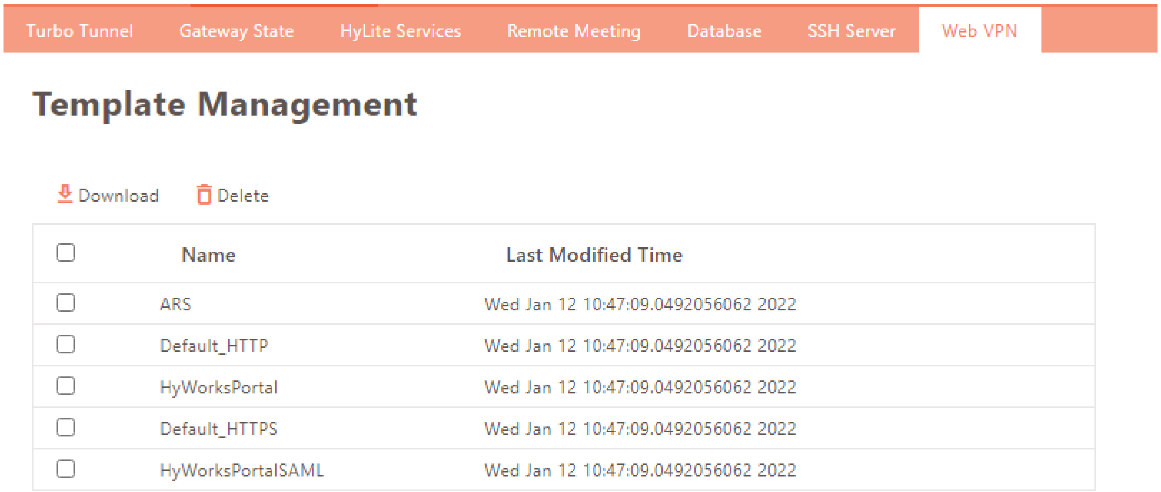
WebVPN Domain* WebDomain

WebVPN Template Default_HTTPS

Hidden Application

Hide Access Pop-up

These saved templates can be managed under *Settings →Services Config → Web VPN.*



Template Management

□	Name	Last Modified Time
□	ARS	Wed Jan 12 10:47:09.0492056062 2022
□	Default_HTTP	Wed Jan 12 10:47:09.0492056062 2022
□	HyWorksPortal	Wed Jan 12 10:47:09.0492056062 2022
□	Default_HTTPS	Wed Jan 12 10:47:09.0492056062 2022
□	HyWorksPortalSAML	Wed Jan 12 10:47:09.0492056062 2022

3.1.3 Decoupling Virtual IP and Database IP to avoid Virtual IP being a Single Point of Failure

Till the previous versions, the HySecure Virtual IP was tightly coupled with the Database IP address. So, any failure of the Virtual IP used to result in the Database connection issues which in-turn resulted in the user requests not getting served.

In this version, the two IP addresses are de-coupled resulting in the normal functioning of the gateway even if the Virtual IP goes down for any reason. However, this change will help serve the user requests, only if the real IP address of the HySecure Gateway node is being used for connections, rather than the virtual IP.

Note: If Public IP address is mapped to HySecure gateway's Virtual IP then all users connecting to Public IP address will be disconnected in case of Virtual IP going down.

3.1.4 HA Failover in case of DB service going down

All database transactions are done on the active node. If for some reasons, the database service on the active node goes down, then the inability of the Gateway to perform database transactions will lead to the Gateway failure. This issue is addressed from this version. From now on, in such situations, the database transactions are switched to the standby node, provided the standby node is healthy.

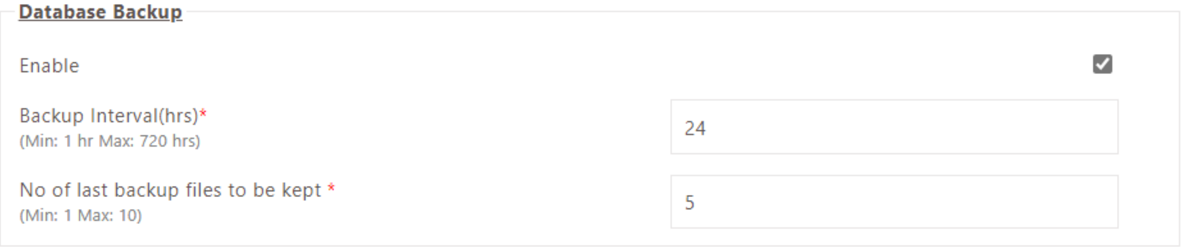
Note: This functionality is disabled by default and needs to be enabled from backend

3.1.5 HySecure Database Auto Backup

Till the previous version, the responsibility of keeping backups used to lie with the HySecure administrator. However, in case of absence of any backup, an un-towards failure used to lead to a total re-configuration of the gateway which becomes a painful process.

To avoid such situations, database backup is enabled by default with 5 last backups being kept and which are taken at an interval of 24 hours.

It can be configured from HySecure Management console under *Auto Backup* in *General Settings*.



Database Backup

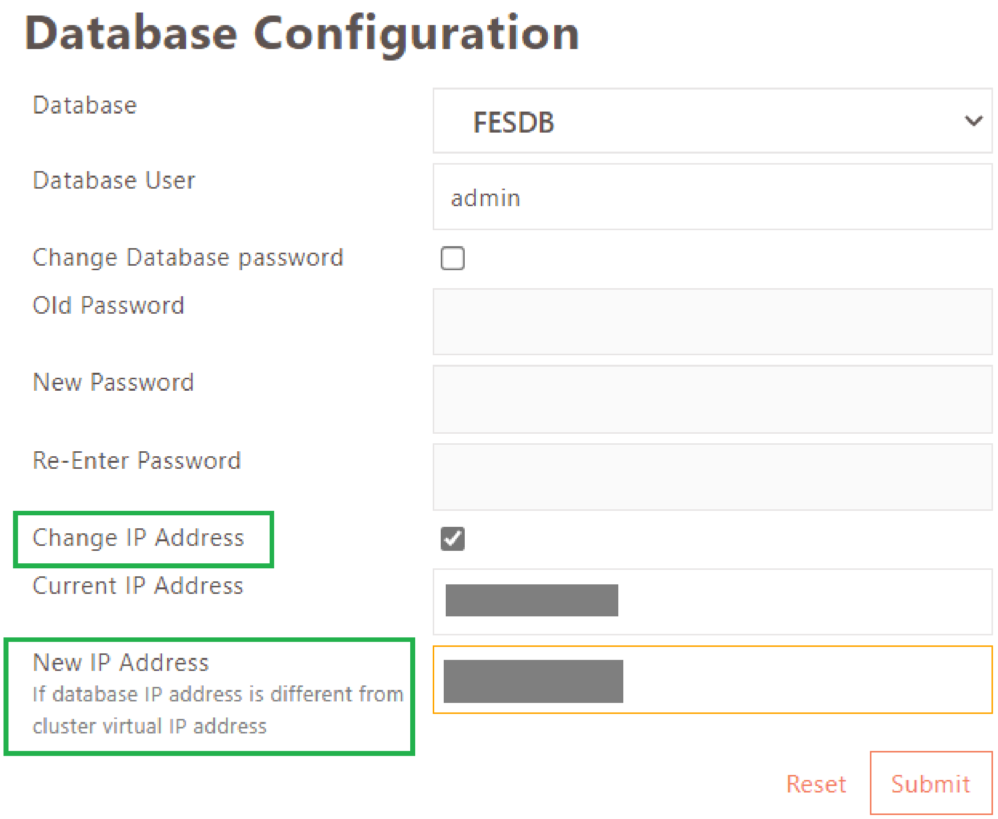
Enable	☑
Backup Interval(hrs)* (Min: 1 hr Max: 720 hrs)	24
No of last backup files to be kept * (Min: 1 Max: 10)	5

3.1.6 Database IP configuration through management console

In cloud-based deployments (for e.g., AWS, Microsoft Azure) of HySecure gateway, external load balancers are configured instead of HySecure internal load balancer. Till previous version, this configuration could only be done from backend via ssh, but from this version it is available through HySecure management console. Administrator must enable “Allow access for public IP” from global settings.

Steps:

- Put gateway in configuration state and access database configuration
- Select the database as FESDB.
- Enable change IP address.
- Add cloud computing-based load balancer IP address in new IP address and then submit.



Database Configuration

Database	FESDB
Database User	admin
Change Database password	□
Old Password	
New Password	
Re-Enter Password	
Change IP Address	☑
Current IP Address	[redacted]
New IP Address If database IP address is different from cluster virtual IP address	[redacted]

3.1.7 Auto archival and purge of User reporting data

Till the previous version, there was no check on the size of user reporting database having logs related to user login and application access. This used to affect the gateway operations when the size used to increase significantly.

To address this issue, periodic archival is performed from this version and old records are purged. The default configuration is to run the archiving at 2300 hrs daily and truncate records older than 30 days. This can be customized.

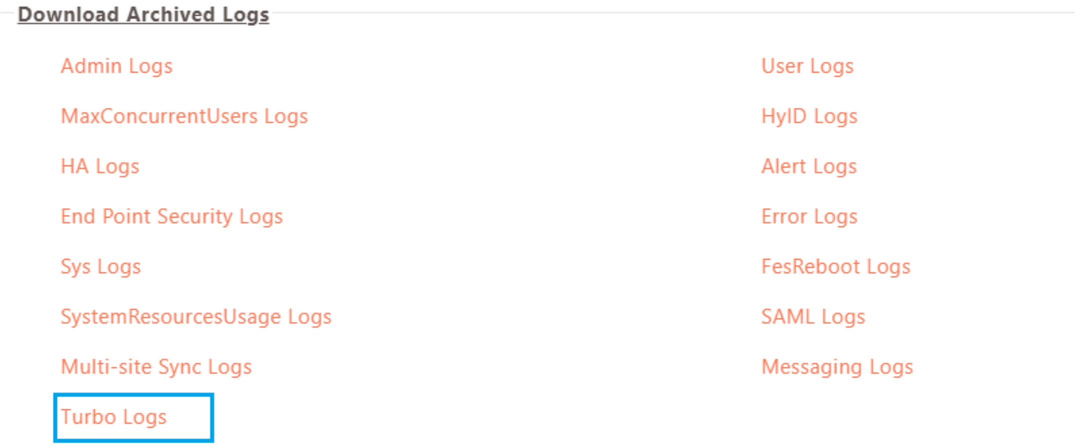
Note: Reporting data older than a month will be removed immediately after applying this Hotfix.

4 ENHANCEMENTS

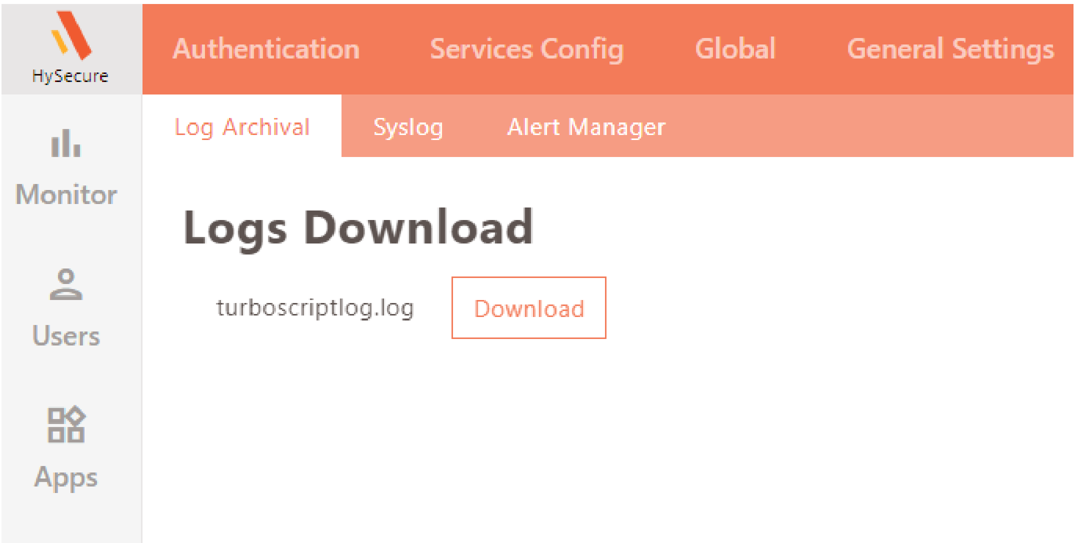
4.1.1 Addition of Turbo logs

To improve turbo troubleshooting and thus optimizing on the turbo configuration, multiple activity logs & admin logs are added along with error messages and warnings. Separate log file for Turbo based transaction occurring among HySecure clients and HySecure gateway are also created from this version. To download these logs, follow below steps:

- Login into HySecure management console.
- Go to *Settings* → *Logs* → *Log Archival* and click on *Turbo Logs.*

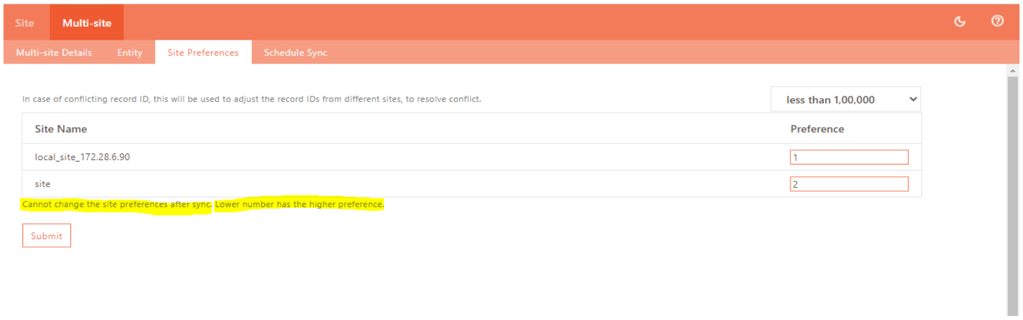


- Download desired log file by clicking on download button.



4.1.2 Multisite sync enhancements

- The highest presence on the site preference page is mentioned on site page. Information about it is added above *Submit* button. The lowest number set in preference has the highest priority for data synchronization. First preference of data synchronization is given to the site which has the least in preference set.



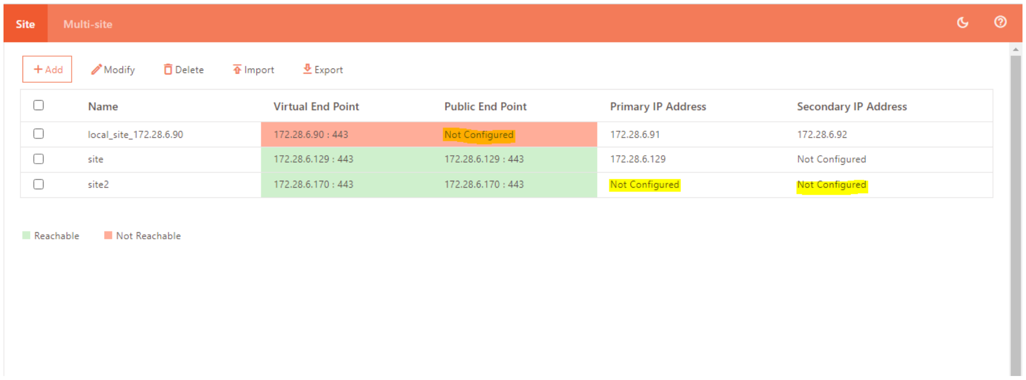
In case of conflicting record ID, this will be used to adjust the record IDs from different sites, to resolve conflict.

less than 1,00,000

Site Name	Preference
local_site_172.28.6.90	1
site	2

Cannot change the site preferences after sync. Lower number has the higher preference.

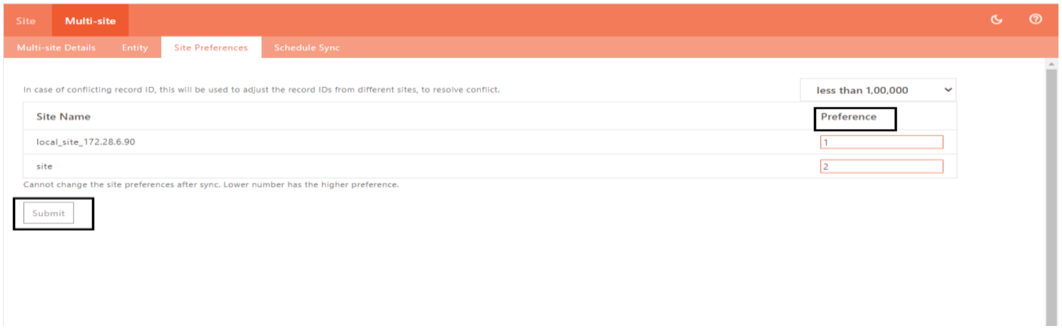
- Not configured tag added instead of NA:0 for public IP address endpoint is added. It is a cosmetic fix, in blank data field of Public End point, Primary IP Address and Secondary IP Address earlier its NA:0 tag was present which is replaced by *Not Configured*.



□	Name	Virtual End Point	Public End Point	Primary IP Address	Secondary IP Address
□	local_site_172.28.6.90	172.28.6.90 : 443	Not Configured	172.28.6.91	172.28.6.92
□	site	172.28.6.129 : 443	172.28.6.129 : 443	172.28.6.129	Not Configured
□	site2	172.28.6.170 : 443	172.28.6.170 : 443	Not Configured	Not Configured

🟩 Reachable 🟥 Not Reachable

- Once the preference set in site preferences it cannot be edited the submit button gets greyed-out after the schedule sync is set. The newly added sites after the first sync gets preference set automatically.



In case of conflicting record ID, this will be used to adjust the record IDs from different sites, to resolve conflict.

less than 1,00,000

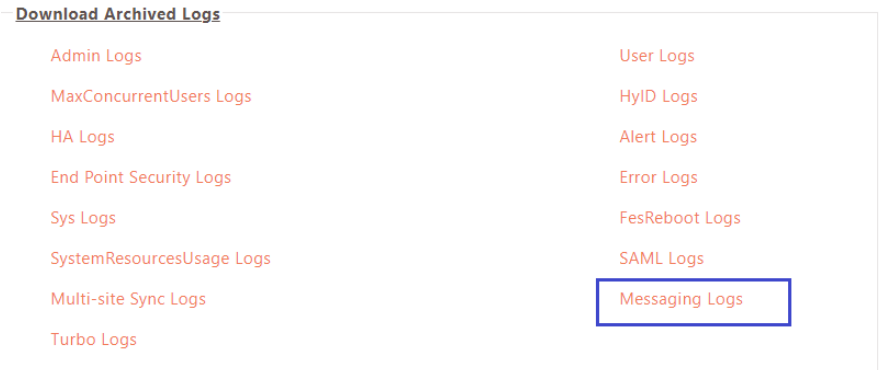
Site Name	Preference
local_site_172.28.6.90	1
site	2

Cannot change the site preferences after sync. Lower number has the higher preference.

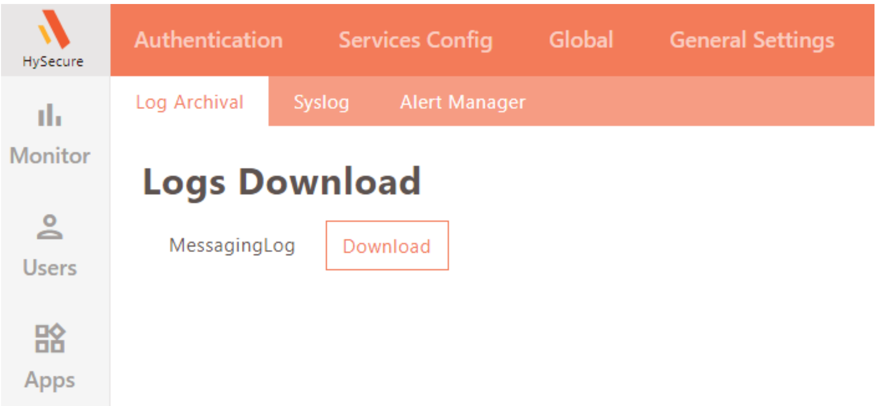
4.1.3 SMTP and SMS logs

If any Email or SMS is sent to Administrator/End user then the logs of that event will be logged in a log file. This enhancement will help in troubleshooting the issues such as OTP not being received by the end user, or any Email alert not being received. To download these logs, follow below steps:

- Login into HySecure management console.
- Go to *Settings* → *Logs* → *Log Archival* and click on *Messaging Logs.*



- Download desired log file by clicking on download button.



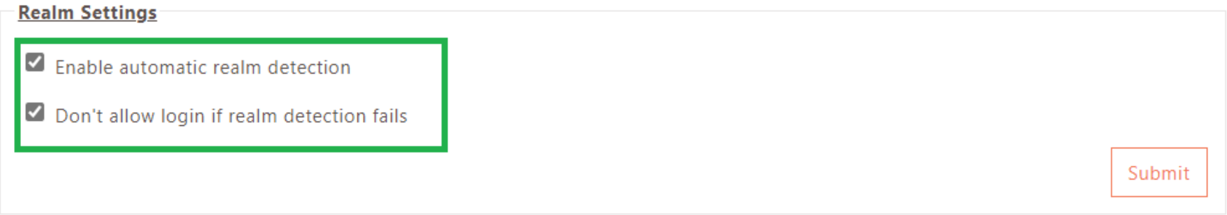
5 FIXED ISSUES

5.1.1 All Realms were visible if user access HyLite Portal without URI (Multitenancy Environment)

In previous build, if multitenancy environment is set up and user access HySecure gateway through IP address or hostname instead of URI then user was able to see all the configured realms. In this build, we have fixed this issue, now user won't be able to see the list of realms and will be provided error message as "Please enter correct URL provided by your organization"

To ensure that user is not able to see any realms, administrator need to enable below configurations in Settings → Global → Server.

- Enable automatic realm detection.
- Don't allow login if realm detection fails.



Realm Settings

☑ Enable automatic realm detection

☑ Don't allow login if realm detection fails

5.1.2 Minimum length for database admin's password

In earlier build, there was no minimum length for database admin's password while changing it from management console or OS console. Now, database admin's password must be at least 16 characters while changing from management console/OS console.

5.1.3 Desktop Agent type HyID policy is not working for LINUXPROID agent.

In this build, we have added support for LINUXPROID agent which will work with Desktop Agents and Desktop agent type HyID policy.

5.1.4 Multiple app icons for same applications are visible on HyLite Portal

In this build, we have fixed an intermittent issue where same hosted application is visible with multiple app icons in HyLite Portal.

5.1.5 Special character support in SMTP server and SMS gateway password field

In this build, we have added support for mentioned special characters in SMS gateway password field and SMTP server field.

Character	Name	Character	Name	Character	Name
!	Exclamation	,	Comma	[	Left bracket
”	Double quote	-	Minus	\	Backslash
#	Number sign (hash)	.	Full stop	]	Right bracket

Character	Name	Character	Name	Character	Name
$	Dollar sign	/	Slash	^	Caret
%	Percent	:	Colon	_	Underscore
&	Ampersand	;	Semicolon	`	Grave accent (backtick)
’	Single quote	<	Less than	{	Left brace
(	Left parenthesis	=	Equal sign	|	Vertical bar
)	Right parenthesis	>	Greater than	}	Right brace
*	Asterisk	?	Question mark	~	Tilde
+	Plus	@	At sign		

5.1.6 Blank device profile name in Endpoint Security Access Control

On some setups which were upgraded from HySecure gateway V5230 to HySecure gateway V5427 using upgrade Patch, device profile was appearing with blank name while creating endpoint security access control. In this build, we have fixed that issue.

5.1.7 Unable to modify IP Address in case of Network type application

In this build, we have fixed an issue where administrator/security officer was facing incorrect error while modifying IP address in Network type application which restrict administrator/security officer from modifying the same.

5.1.8 Login failure in application using Accops Directory Server

In this build we have fixed an issue where users were not able to login into applications which were using Accops Directory server as authentication method.

5.1.9 HyLite Plugin based login failure into chromium-based browsers

In earlier build, HyLite plugin for device ID/EPS was not working. So, if administrator had configured HyLite plugin for device ID/EPS then user from Chromium based browsers i.e., Google chrome and new Microsoft Edge were not able to login. In this build we have fixed that issue.

5.1.10 HyLabs not working

In earlier build, users were not able to access HyLabs based desktops. This issue has been fixed in this build.

5.1.11 Incorrect Parsing of user log in case of device approval through external API

In earlier build, if device was getting approved by external API, then username column used to have log detail instead of username for that log entry. In this build, we have fixed the same.

5.1.12 HyID Policy bypass if authorization server is different than authentication server

If authentication had authorization server different than authorization server then user was not being asked OTP even if HyID policy was present for the user. In this build, we have fixed the same.

5.1.13 Application published with hostname containing hyphen not being accessible

In this build, we have fixed an issue where user was getting error “Server refused connection” while accessing application which was published with hyphen in hostname.

5.1.14 Unable to rename Anonymous authentication domain name

In previous build, Security officer/Administrator was not being able to modify name of Anonymous authentication domain and was shown incorrect error message “Domain creation failed because another Authentication Domain configured with Anonymous Authentication server already exists.” This issue has been fixed in this build.

5.1.15 Registered users search with authentication server was not working

Search of registered users was not working with search filter as “Authentication Server”. Security officer/Administrator was getting incorrect error “No user found”. In this build, we have fixed the same.

5.1.16 Removed non-working entities in Multi Site Sync

In this build, we have removed non-working entities in multi-site sync.

5.1.17 Internal Server Error while configuring Site preferences in Multi Site sync

In earlier build, Security officer/Administrator was facing internal server error while configuring site preferences for enabling multi site sync. This issue has been fixed in this build.

5.1.18 Removed traffic routing option “block the traffic”

In previous build, when a turbo tunnel type application was created then traffic routing was being set to “*block the traffic*” by default which resulted into application not being accessible. For this application to work, user had to manually select “Route traffic to HySecure gateway”. In this build, we have removed traffic routing option which was blocking application from working.

5.1.19 Incorrect active session time and total session time for some users in user report

In specific case where two user profiles were created for a user, active session time and total session time might appear incorrect in user report. We have fixed this issue in this build.

5.1.20 Multiple User Profile creation in some setups

On some specific setups duplicate user profile might get created because of ‘None’ value in authorization server. This issue has been fixed in this build.

5.1.21 Enter button not working while submitting OTP

In this build, we have fixed an issue where on pressing enter button won’t submit OTP entered in HyLite portal for login.

6 KNOWN ISSUES

6.1.1 Database Auto Backup failure in absence of Standby Node

HySecure gateway store database backup file in Standby node, if a cluster does not have Standby node, then Database will not be backed up.

6.1.2 Web VPN based application's rule file not restored by User Backup on Standby/Real node

In case of user backup restoration, rule files for Web VPN based Web application will only be restored on Active node. Rule files must be transferred to Standby and Real node from Active node to get Web VPN based Web application work correctly.

6.1.3 No Admin logs in case of Database Auto Backup events

In this hotfix, we have added feature to periodically backing up HySecure database. Below are the known issues related to same:

- No admin log in case of successful database backup generation.
- No admin log/Error log in case of database backup generation failure.
- No admin log when earliest database backup file gets deleted because of new database backup file generation.

6.1.4 Return to App button on edit Web VPN rules page not working.

After clicking on Return to App button present on Edit Web VPN Location Block page it shows blank page with error.

6.1.5 Reporting database file reserving storage after purge

Even after reporting database is purged, some amount of storage is being reserved by reporting database file.

6.1.6 Sometimes connection to Sites from Management cluster may fail due to timeout

As there is no timeout for connection with site sometimes management cluster wait for long time and connection is not established due to which other activities starts failing in this situation multi-site may stop working.

6.1.7 URI is not supported with clients. (Multitenancy)

While login into HySecure Gateway URI is not supported with client in server address if Multitenancy is enabled on gateway.

7 APPENDIX A: UPGRADING HYSECURE CLUSTER

The section describes the detailed process to apply hotfix on HySecure Cluster having three nodes (Active, Standby and Real Gateway server):

To upgrade HySecure cluster, follow these main steps:

- Upgrade the HySecure real Node
- Upgrade the HySecure standby Cluster Manger Node
- Upgrade the HySecure active Cluster Manger Node

7.1.1 Upgrading real HySecure Cluster Node:

- Connect to Real HySecure Cluster node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Real node**.**

- Login as security officer.
- Now go to "HA enable/disable" page under "High Availability" section and enable maintenance mode.
- Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option ***Hotfix or service pack*** and upload the HySecure hotfix file.
- It may take 1 minutes or more to upload the hotfix based on network bandwidth between your PC and Gateway.
- Once the hotfix file is uploaded and upgrade is started, the message will be displayed on the browser. In some cases, the message may not come on the management console. Refresh the browser and see if the upgrade has completed.
- After hotfix is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the hotfix installation logs.

7.1.2 Upgrading standby HySecure Cluster Manager Node:

- Connect to Standby HySecure Cluster Manager node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Standby node**.**

- Login as security officer.
- Now go to "HA enable/disable" page under "High Availability" section and enable maintenance mode.
- Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option ***Hotfix or service pack*** and upload the HySecure hotfix file.
- It may take 1 minutes or more to upload the hotfix based on network bandwidth between your PC and Gateway.

- Once the hotfix file is uploaded and upgrade is started, the message will be displayed on the browser. In some cases, the message may not come on the management console. Refresh the browser and see if the upgrade has completed.
- After hotfix is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the hotfix installation logs.

7.1.3 Upgrading active HySecure Cluster Manager Node:

- Connect to Active HySecure Cluster Manager node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Active node**.**

- Login as security officer.
- Now go to "HA enable/disable" page under "High Availability" section and enable maintenance mode.
- Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option ***Hotfix or service pack*** and upload the HySecure hotfix file.
- It may take 1 minutes or more to upload the hotfix based on network bandwidth between your PC and Gateway.
- Once the hotfix file is uploaded and upgrade is started, the message will be displayed on the browser. In some cases, the message may not come on the management console. Refresh the browser and see if the upgrade has completed.
- After hotfix is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the hotfix installation logs.

7.1.4 Disabling Maintenance mode in Active Node

- Connect to Active HySecure Cluster Manager node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Standby node**.**

- Login as security officer.
- Now go to "HA enable/disable" page under "High Availability" section and disable maintenance mode.

7.1.5 Disabling Maintenance mode in Standby Node

- Connect to Standby HySecure Cluster Manager node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Standby node**.**

- Login as security officer.
- Now go to "HA enable/disable" page under "High Availability" section and disable maintenance mode.

7.1.6 Disabling Maintenance mode in Real Node

- Connect to Real HySecure node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of real node**.**

- Login as security officer.
- Now go to “HA enable/disable” page under “High Availability” section and disable maintenance mode.

About Accops

Accops Systems Private Limited. under “Accops” brand is a globally leading developer and provider of Enterprise Mobility solutions involving Application and Desktop Virtualization, Secure Remote Access and Privilege Access Management solutions.

Accops’ software and hardware products enable businesses to efficiently virtualize, secure and deliver business applications, corporate workspace and network services to their employees, partners, vendors, home users and mobile users, enabling instance access from anywhere using any device.

Tel: India +91 9595 277 001 | Europe +49 341 3315 78 30
Email: sales@accops.com | Web: www.accops.com