Release Notes

HySecure 5.2 SP2 Upgrade Patch build 5299

Last Updated: 28th November 2020

The information contained in this document represents the current view of Accops Systems Private Limited on the issues discussed as of the date of publication. Because Accops Systems Private Limited must respond to changing market conditions, it should not be interpreted as a commitment on the part of Accops Systems Private Limited. Accops Systems Private Limited cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. ACCOPS SYSTEM PRIVATE LIMITED MAKES NO WARRANTIES, EXPRESSED OR IMPLIED IN THIS DOCUMENT.

Contact Accops Systems Private Limited.
Email: info@accops.com
Call: +91 20 6719 0123

HySecure 5.2 Release Notes Document Revision History

Date	***Changes***
28-Nov-2020	5.2 SP2 (Version 5.2.5299)
5-Dec-2018	5.2 SP1 (Version 5.2.5230)
10-Sept-2018	5.2 (Version 5.2.5200)

CONTENTS

OVERVIEW

This document outlines the details of new features / bug fixes / features enhancement / known issues in the Accops HySecure gateway V5.2.5299 ISO and Upgrade Patch.

INSTALLATION MODES OF HYSECURE

HySecure 5.2.5299 can be installed using following methods:

1. Install on any x86 based hardware using HySecure 5.2.5299 ISO
2. Install on any virtual machine using HySecure 5.2.5299 ISO
3. Upgrade an existing deployment of HySecure using the upgrade patch

Please refer to the HySecure 5.0 install guide for detailed instructions on how to install HySecure 5.0.

HYSECURE ISO 5.2.5299 INSTALLATION

GETTING HYSECURE ISO 5.2.5299

Download link:
https://support.accops.com/a/solutions/articles/12000076159

INSTALLING HYSECURE ISO

Refer HySecure Installation document

UPGRADE PATCH INSTALLATION

UPGRADE COMPATIBILITY OF UPGRADE PATCH 5.2.5299

The upgrade 5.2.5299 is applicable on either the Service Pack OR one of the Hot Fixes mentioned in the table below.

Existing HySecure Type	Compatible Version
Service Pack	HySecure Gateway 5.2 SP1 (5.2.3.0)
Hot Fix	5232; 5235; 5236 6017; 6026; 6028; 6033; 6042; 6048; 6052; 6060; 6061; 6063

Note: Please note that if HySecure version is lower than 5.2.3.0 then first upgrade HySecure gateway to HySecure gateway 5.2.3.0 version. Then apply this 5.2 SP2 upgrade patch.

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

GETTING UPGRADE PATCH 5.2.5299

Download link:
https://support.accops.com/a/solutions/articles/12000076159

NEW FEATURES

ACCESS CONTROL

ADVANCE EMAIL ALERT FOR APPLICATION ACCESS ACL EXPIRY

Advance Email Alert configuration features provides the option to get Email alert before Access Control Policy expires for the users. In this feature, Users and Security Officer/Administrator will receive an Email alert regarding Access control policy on the defined day prior to expiry date of Access control.

Note: Advance Email Alert for Access control Expiry feature is only applicable to "Application Access" type Access Control.

Email Alert Recipients: Below mentioned users will get Email Alert for Access control expiry.

- Security Officer
- Administrator
- Active Directory/LDAP/Native Users: Advance Email Alert for Access control Expiry will be sent to end users only if they have logged into HySecure at least once after upgrade patch is applied.

Note: Monitoring User will not receive Advance Email Alert for Access control Expiry.

AUTHENTICATION & AUTHORIZATION

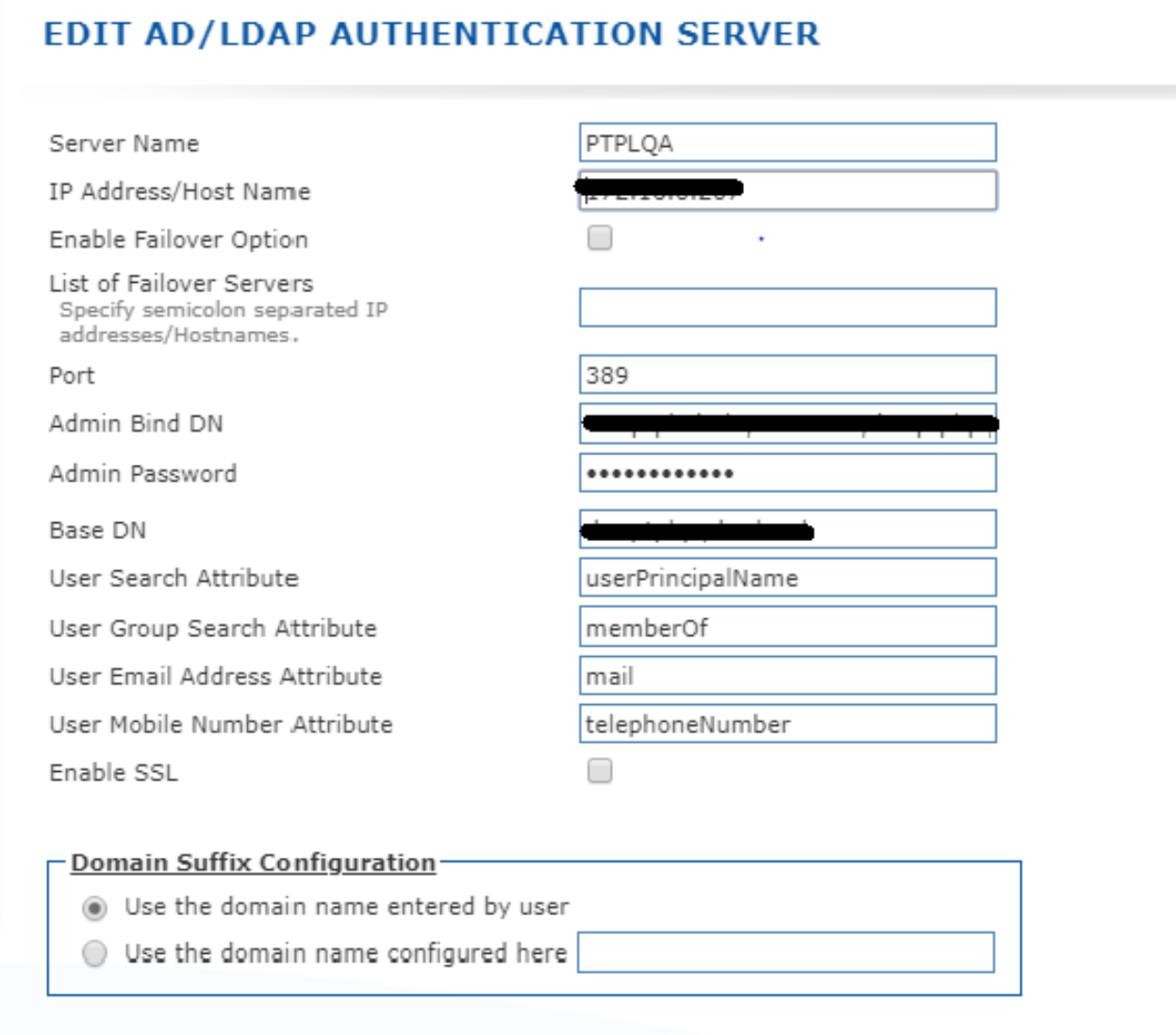
UPN BASED LOGIN SUPPORT

In this build, we have added support for UserPrincipalName based login. To configure UserPrincipalName based login administrator needs to do following changes in HySecure management console:

a) Access HySecure Management console using security officer account.

b) Go to Auth. Management → Authentication Server.
c) Change User search attribute from “SamAccountName” to “UserPrincipalName”.
d) Security Officer can configure UserPrincipalName by two methods:

    i. Use the domain name entered by user: In this method, domain name entered by user will be used for login. User need to enter his/her login name in UPN Format: username@domain name.
    ii. Use the domain name entered here: In this method, domain name entered here will be used for user login. User need to enter his/her login name in UPN Format: username. Domain name will be automatically added by HySecure gateway.



To enable UPN based login from HySecure client, additional settings is required apart from UPN configuration in authentication domain. Enable below option in client settings to enable UPN based login from HySecure client.

LOGGING OF ACTIVE USER SESSION

In this build, we have provided support to log the active session out of total user session.

This active user session will be calculated by subtracting idle timeout of the user from user's total session time.
Total session time of a user = User logout time – User login time
Active User session = Total session time of a user – Idle time of a user

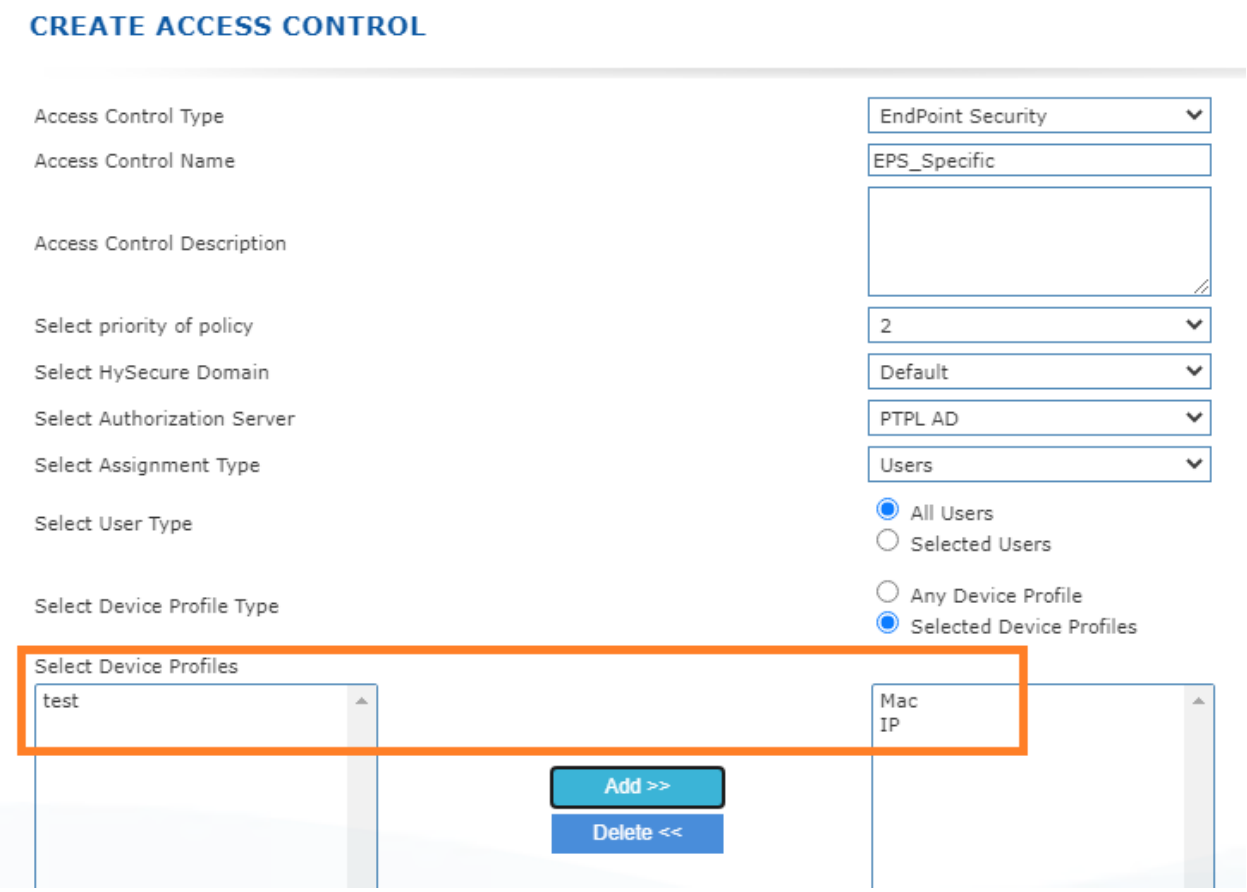
ACCOPS DIRECTORY SERVER SUPPORT

In this build we have provided Accops directory server support to authenticate application securely with two factor authentication. This method will be helpful to integrate two factor authentication for the application where two factor authentication is not supported by default.

ENFORCEMENT OF SPECIFIC DEVICE PROFILES AT USER/ USER GROUP LEVEL

In earlier build, Endpoint security was applied over HySecure domain level. Now we can apply device profile of endpoint security at user/ user group level. User/ user group will be able to login only if device fulfills one of the selected device profiles. To enforce specific device profiles at user/ user group level follow below mentioned steps:

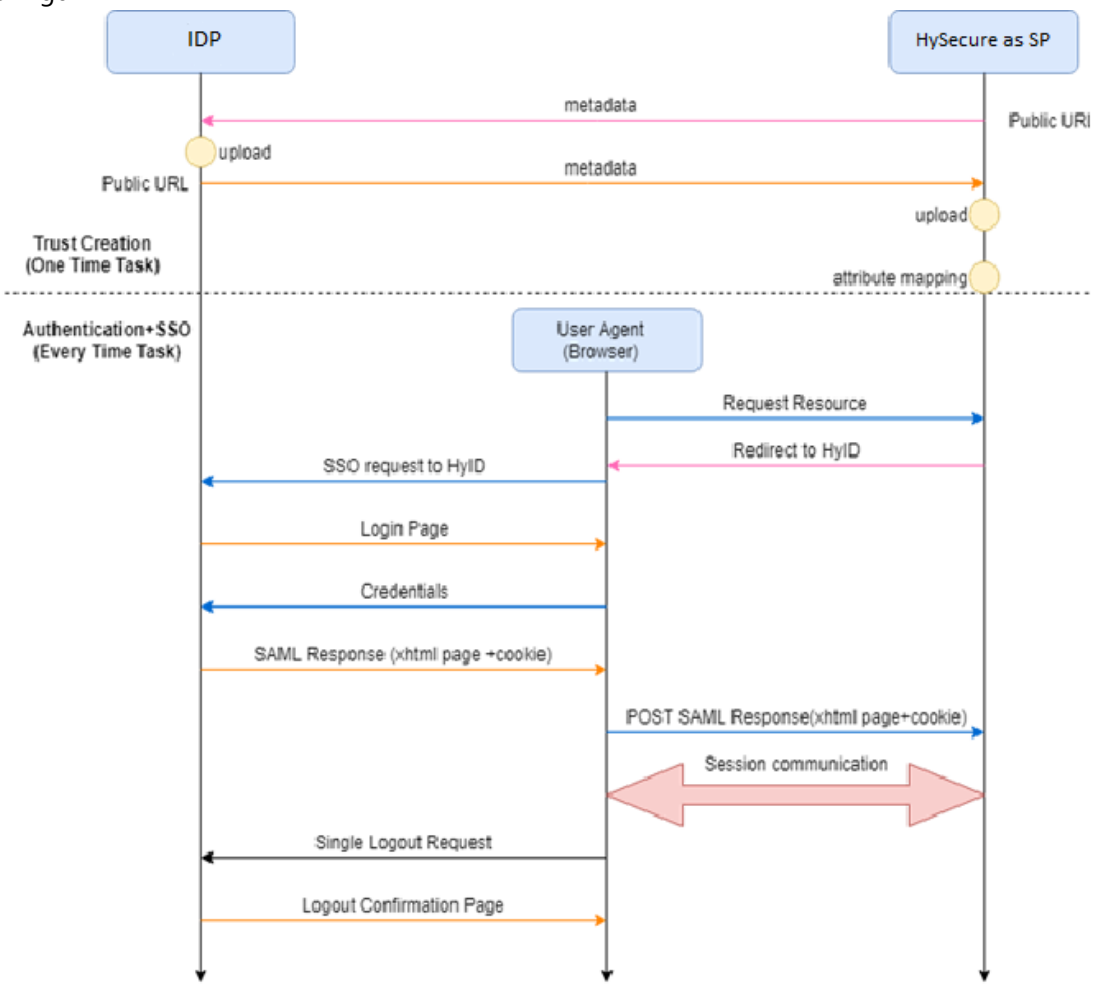
- Login into HySecure management console as Security Officer.
- Go to Access Management → Access controls.
- Click on Add and select "Endpoint Security" as Access control type.
- Select the HySecure domain and respective Authorization server.
- Select the user/ user group for whom access from Hylite/HySecure client will be authorized.
- Select the device profile to be applied on user profile.
- Click on submit.



SAML IDENTITY PROVIDER AUTHENTICATION IN HYSECURE GATEWAY

In this build, we have added support of SAML Identity provider with HySecure gateway. In this mode, HySecure gateway will act as Service provider.

Configu



CONFIGURING SAML IDP AUTHENTICATION IN HYSECURE GATEWAY

The process to enable SAML based external IDP server is as follows:

1. Add SAML IDP as authentication server in HySecure
    a. Using IDP Metadata file or manually configure the settings
2. Configure Accops HySecure as SAML SP in SAML IDP configuration
    a. Using Accops SP Metadata file or manually configure the settings.

Follow below steps to add SAML IDP in HySecure:

- Get the IDP metadata from the SAML IDP which needs to be integrated.
- Login to HySecure and access the management console.
- Go to Auth Management → Authentication servers → Add.
- Select the authentication server type as SAML IDP.
- Upload the IDP metadata.
- SAML response attributes need to be defined on the portal.

- Save the configuration form.
- Option to download Accops HySecure SP metadata will be enabled against the IDP.
- Download the metadata from the list of authentication servers and import the metadata file in IDP.

SR NO	SETTING NAME	DESCRIPTION
01	IdP Issuer URI	Unique identifier of the IDP server. This is a string value or a URI and must match the IDP identifier on the IDP server.
02	IdP Single Sign ON URL	Authentication URL of the IDP server. SAML SP will redirect unauthenticated users on this URL
03	IdP Signature Certificate	This is the public certificate of IDP which is shipped with IDP metadata. This is used to verify the signature of SAML response that comes from IDP
04	Request Binding	SAML 2.0 has the following binding • HTTP Redirect Binding • HTTP POST Binding • HTTP Artifact Binding HySecure supports HTTP Redirect and Post bindings. For SAML SP Initiated HTTP Redirect is used. It is recommended to set this value to *HTTP Redirect Binding*
05	Request Signature	Whether the SAML ***AuthNRequest*** Request send by SP needs to be signed or not, if it is enabled the signature is added in the SAML AuthnRequest. It is recommended to keep this checked
06	Response Signature Verification	This field or selection signifies on what parameters signature will be created It can be on one of the following parameters a. Response b. Assertion c. Response + Assertion

		It is recommended to keep the value as ***Response***
07	Response Signature Algorithm	Which signature algorithm needs to be used should be selected here. Following are supported a. SHA1 b. SHA256 SHA256 is recommended algorithm.

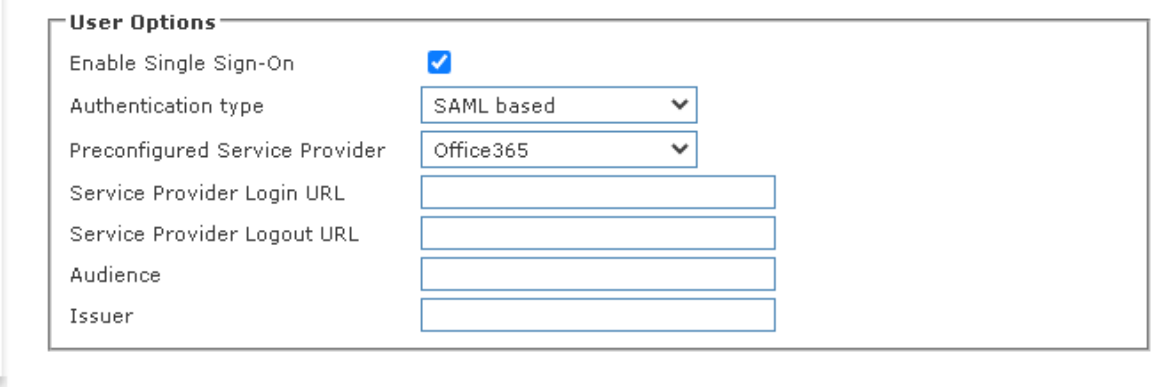
SAML SERVICE PROVIDER SUPPORT IN HYSECURE GATEWAY

In this build, we have added support of SAML based web application access like Office365, Salesforce through HySecure gateway.

CONFIGURING SAML WEB APPS IN HYSECURE GATEWAY

Follow below steps to configure SAML based Web apps in HySecure gateway:

- Login into HySecure management console.
- Go to Access management → Applications.
- Click on add application and select App type as HTTPS
- Enter Web application address, Application port and other details.
- In User options, select Authentication type as SAML based and Select preconfigured service provider appropriately.



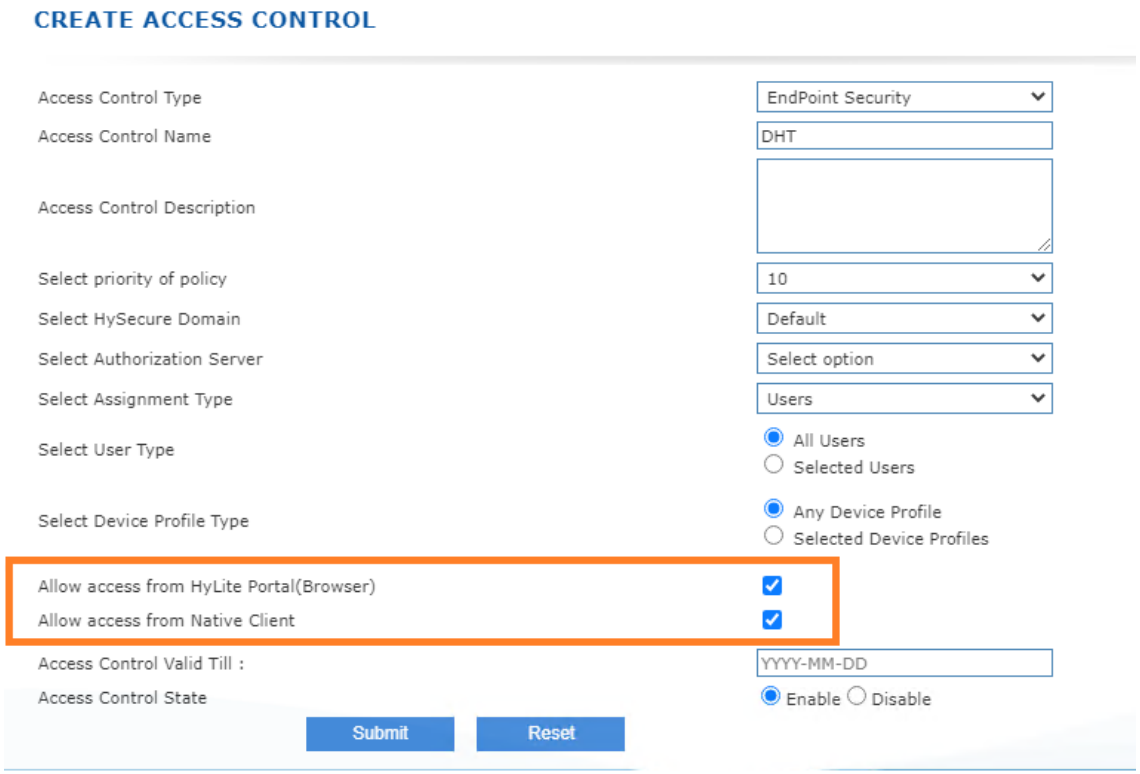
- Enter Service provider login URL: Login URL of the SAML based Web application which will be accessed through HySecure gateway.
- Enter Service provider logout URL: Logout URL of the SAML based Web application which will be accessed through HySecure gateway.

USER/USER GROUP LEVEL LOGIN AUTHORIZATION

In this build, we have added support to allow/block login through HyLite and HySecure Client for specific user/user group. Now Security officer can create an Endpoint Security access control to allow/block login. Please follow below mentioned steps:

- Login into HySecure management console as Security Officer.
- Go to Access Management → Access controls.

- Click on Add and select "Endpoint Security" as Access control type.
- Select the HySecure domain and respective Authorization server.
- Select the user/ user group for whom access from Hylite/HySecure client will be authorized.
- Mark the checkbox against "Allow access from HyLite Portal (Browser), if login access from browser is to be provided.
- Mark the checkbox against "Allow access from Native client, if login access from HySecure client is to be provided.
- Click on Submit.



END-POINT SECURITY

WEB LOGIN RESTRICTION FEATURE

HySecure gateway provides user application access through both HySecure client and HySecure Web portal which is HyLite portal. In this build, we have provided an option to restrict user login through HyLite Portal. After restricting HyLite portal, **only Mobile token registration will be allowed** through HyLite portal and user will not be able to access applications through HyLite portal.

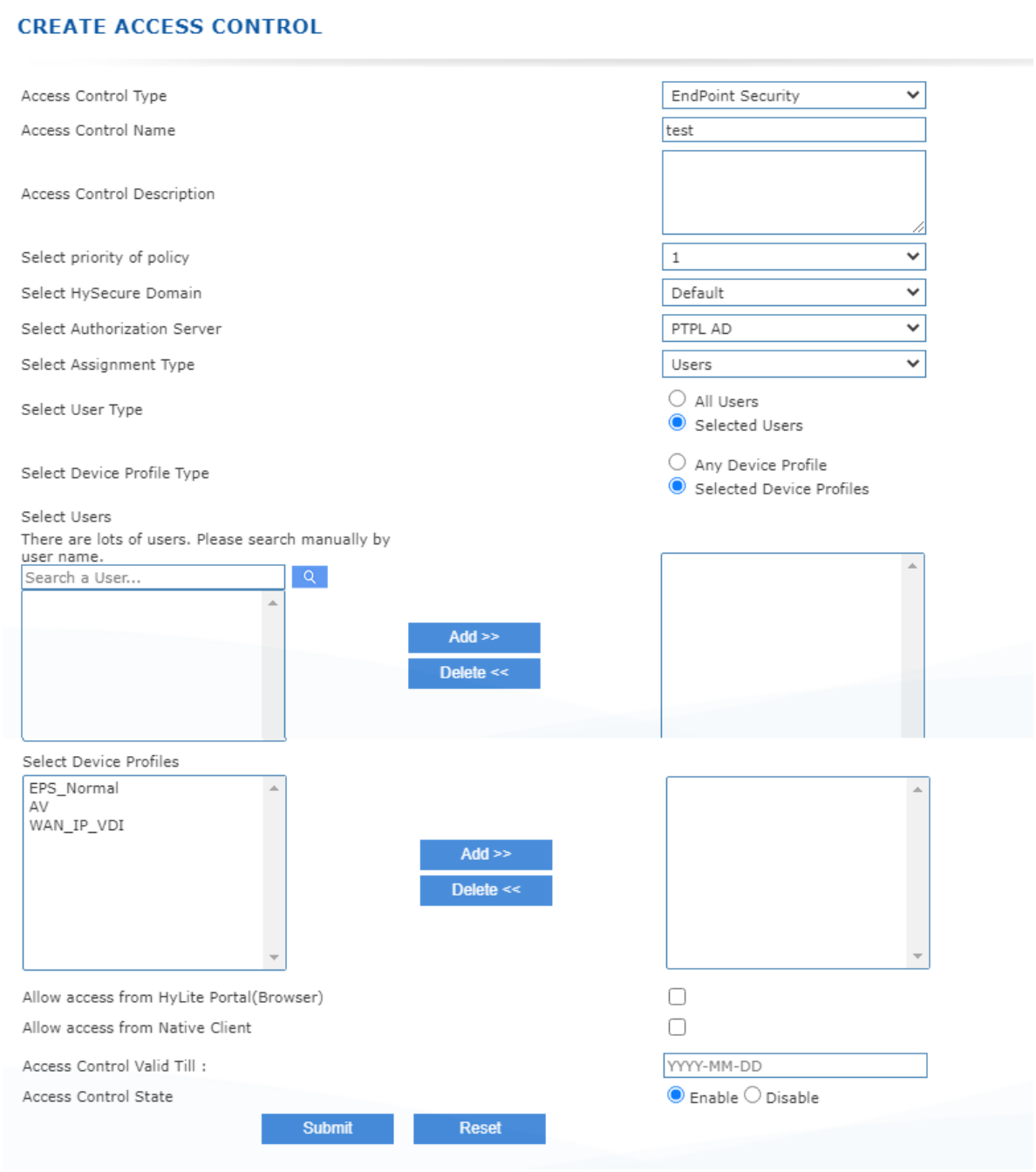
HOW TO CONFIGURE WEB LOGIN RESTRICTION:

To configure web login restriction, administrator user needs to follow below steps:

- Login as Security officer in HySecure Management console.
- Go to Host Configuration → Client Settings.
- Scroll down to Web portal logon mode selection.
- Select “Restrict Web login and allow mobile token registration” and click on submit.

USER/USER GROUP BASED EPS SUPPORT

In this build, we have added support to apply Endpoint security to specific user/user group in HySecure domain. Now security officer/administrator user can create EPS based access control for specific user /user group to enforce EPS. Also, security officer/administrator can choose whether to enable/disable login from either HySecure client or HyLite portal or both for specific user/user group.



PRIORITY IN EPS AND DEVICE ID BASED ACCESS CONTROL

In this build, we have added support for prioritizing the access control to be applied on end users. Currently this support is provided for device Id and EPS based Access control. Lesser the priority number means higher the priority of access control. For e.g. if there are two device ID access control for a user, then access control having lesser priority number will be applied.
Also, if two access control have same priority number then access control appearing higher in the list will be on priority.

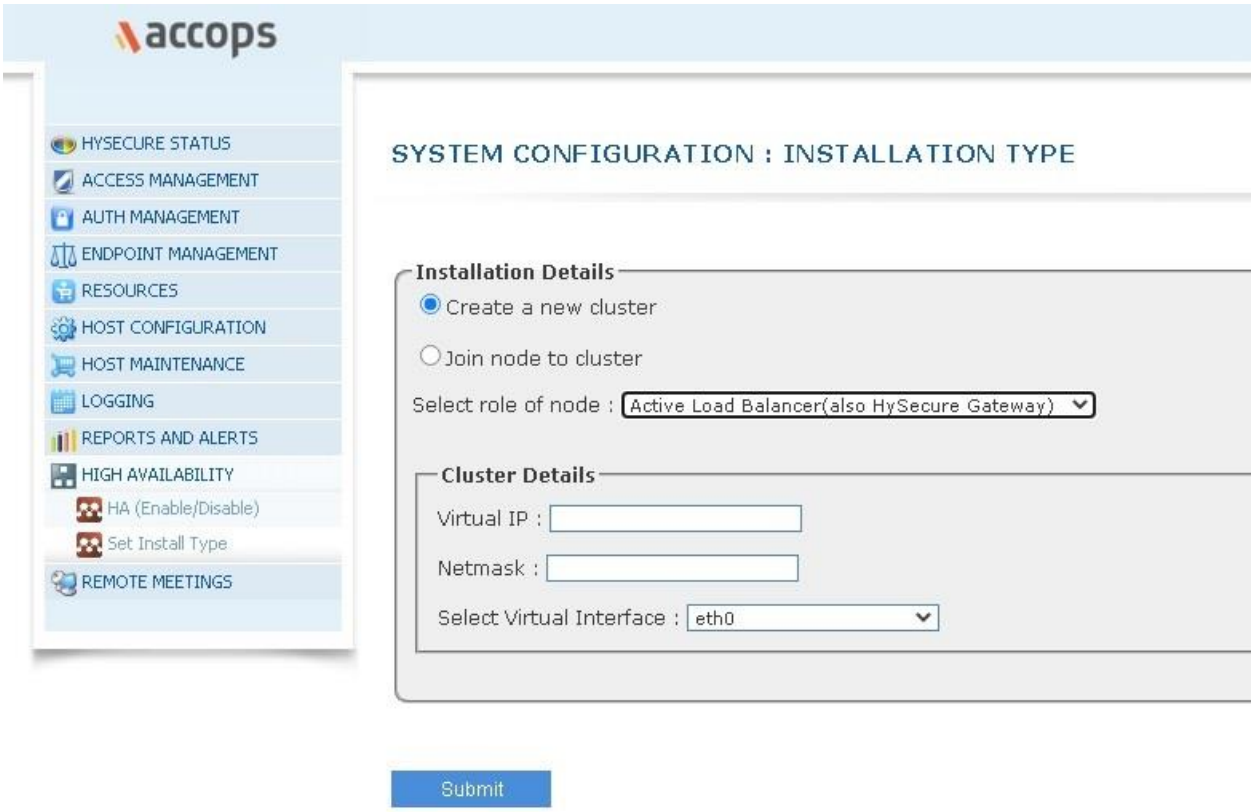
HA

SET INSTALL TYPE FOR HYSECURE HA CLUSTER

In this build, we have changed the option to set the installation type such as Active Load balancer, Backup Load Balancer and HySecure Gateway. While doing preboot, there will be no option to select Active load balancer, Backup load balancer or Real HySecure gateway. To set installation type follow below steps:

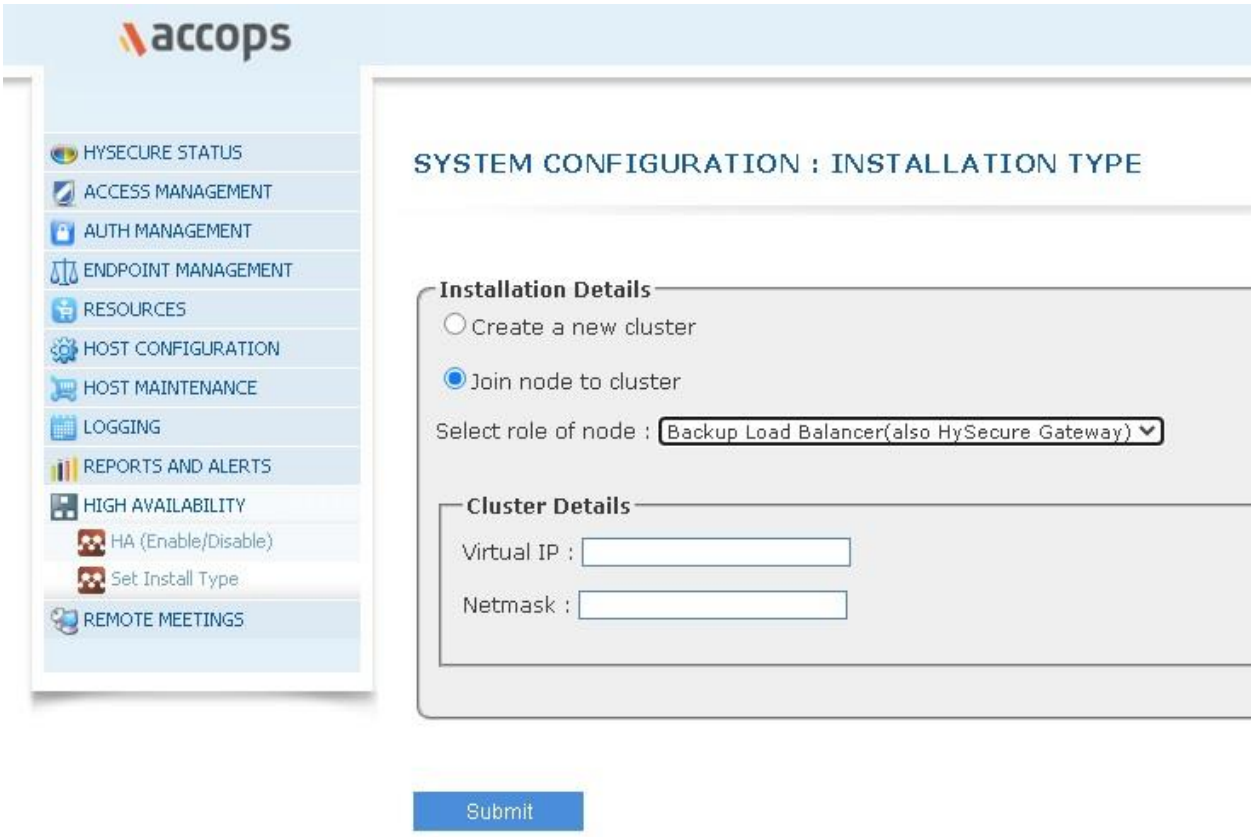
STEPS TO INSTALL ACTIVE LOAD BALANCER

- Complete the preboot of HySecure gateway.
- Login as Security officer.
- In HySecure management console, go to High Availability → Set Install type.
- Select "Create a new cluster" in Installation details.
- Select "Active load balancer (also HySecure gateway)" option in select role of node dropdown.
- Enter virtual IP, netmask for virtual IP and click on submit.
- Msg will appear "successfully converted to HA Active node."



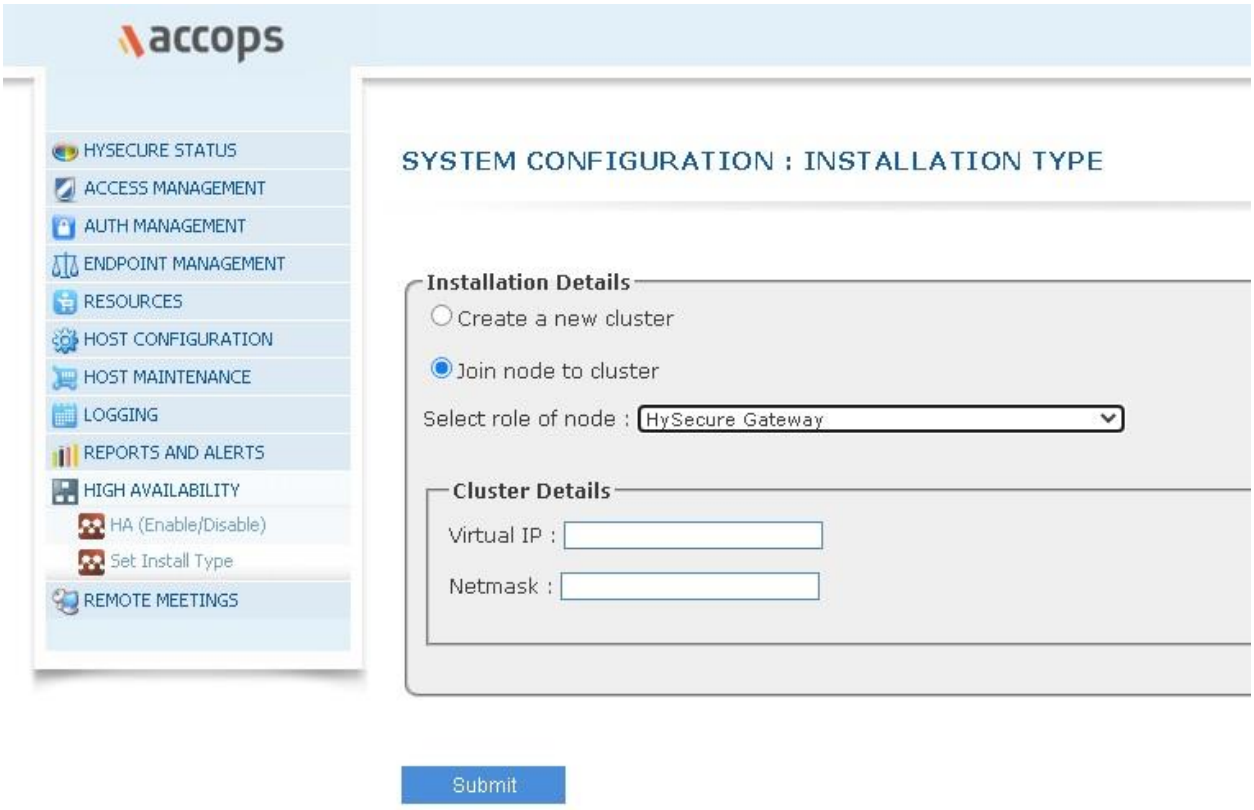
STEPS TO INSTALL BACKUP LOAD BALANCER

- Complete the preboot of HySecure gateway.
- Login as Security officer.
- In HySecure management console, go to High Availability → Set Install type.
- Select "Join node to cluster" in Installation details.
- Select "Backup load balancer (also HySecure gateway)" option in select role of node dropdown.
- Enter virtual IP, netmask for virtual IP and click on submit.



STEPS TO INSTALL HYSECURE GATEWAY(REAL NODE)

- Complete the preboot of HySecure gateway.
- Login as Security officer.
- In HySecure management console, go to High Availability → Set Install type.
- Select "Join node to cluster" in Installation details.
- Select "Backup load balancer (also HySecure gateway)" option in select role of node dropdown.
- Enter virtual IP, netmask for virtual IP and click on submit.



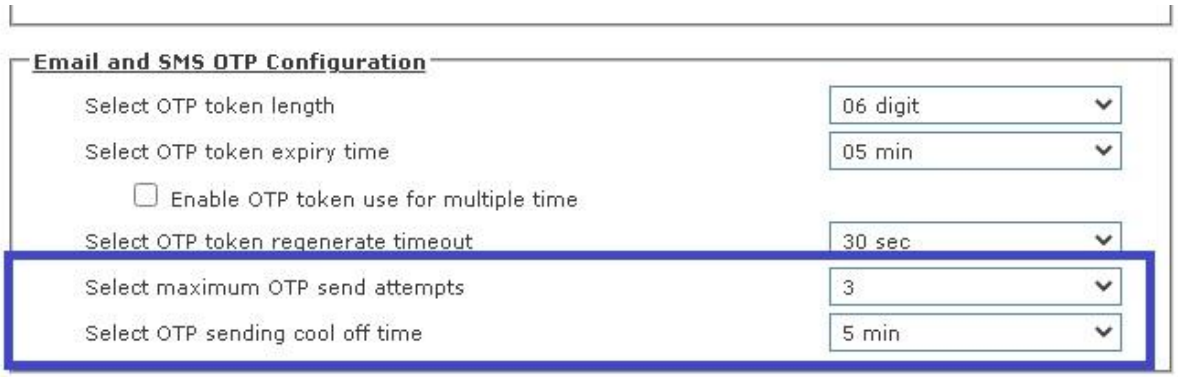
HYID

PREVENT OTP FLOODING ON HYSECURE GATEWAY

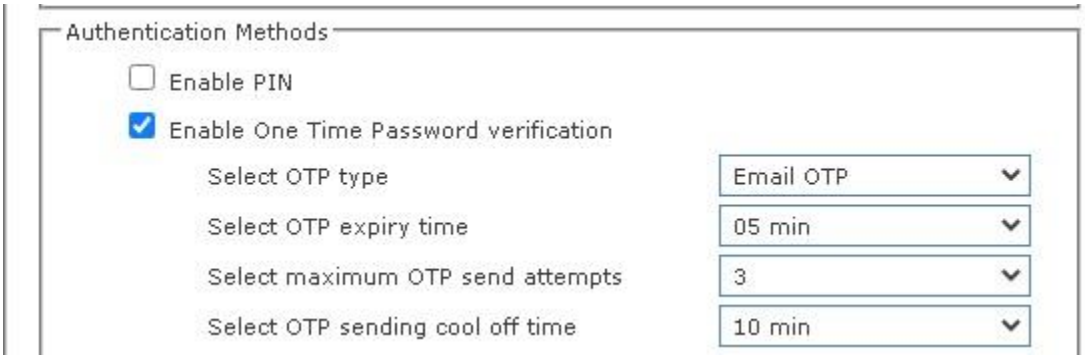
In earlier versions of HySecure gateway, there was no restriction for OTP request for following events:

- User login
- Mobile token registration
- Forgot password

In this build, we have provided an option to limit number of OTPs a user can request for a specific time of interval. By default, user can request OTP for 3 times in 5 minutes. If a user requests OTP 3 times and unable to login, user needs to wait for OTP cool off period which is 5 minutes by default. Administrator/Security officer user can prevent OTP flooding by selecting number of OTP send attempt requests and cool off time while creating HyID policy. . Refer below screenshot.



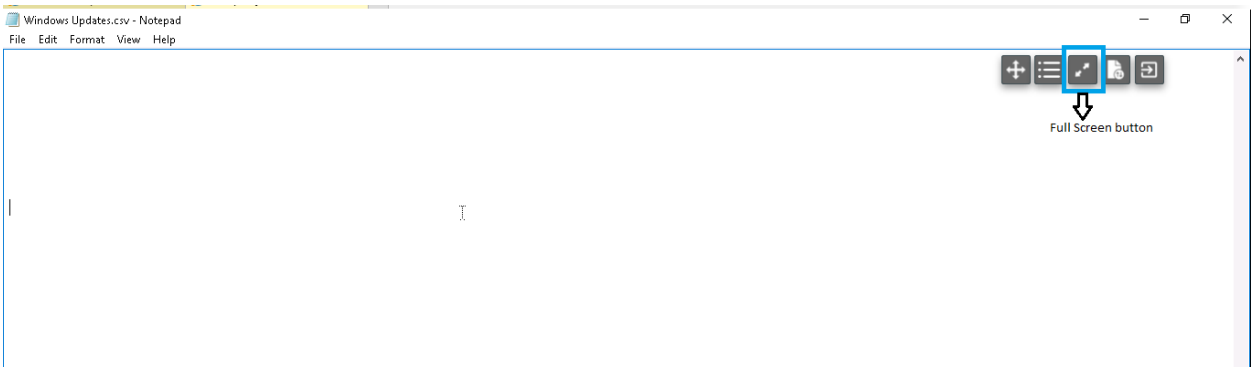
For preventing OTP flooding while resetting forgot password, security officer/administrator can select number of OTP attempt requests and cool off time by editing self-service portal in Authentication domain. Refer below screenshot.



HYLITE

FULL SCREEN MODE IN HYLITE PORTAL

In this build, we have provided support to user applications in full screen mode through HyLite Portal. On HyLite mode when user launch any application, end user can see the full screen option on the top right edge of the page. If user clicks on this option, application will launch in full screen mode.

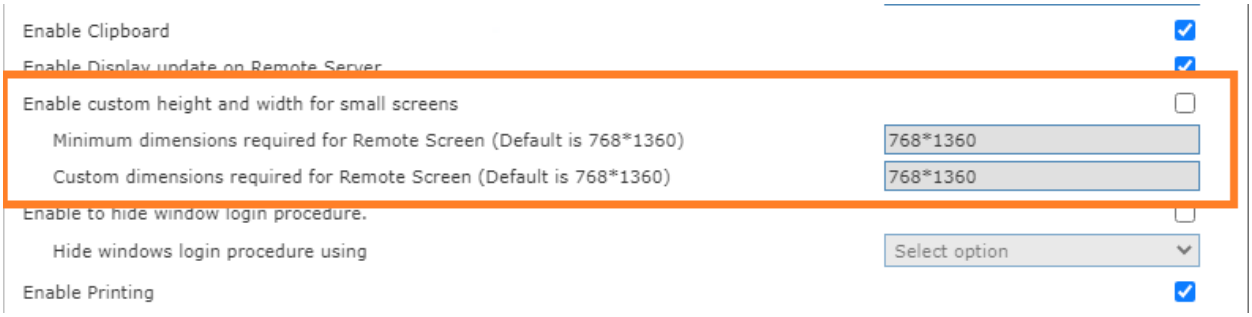


When user wants to exit from full screen mode then user can click on full screen button or press “Esc” key to exit from full screen mode.

CUSTOM HEIGHT AND WIDTH SUPPORT

In a specific scenario, if the resolution of client machine’s monitor is less than the RDP application resolution then in that case user gets to see cropped image of RDP application. To resolve this, we have added custom height and width support. In this feature, administrator/security officer can customize height and width for RDP application and when RDP application resolution is more than specified than user will get scroll bar to browse content near edges. To enable Display update follow below steps:

- Login as security officer.
- Go to Host configuration → HyLite configuration
- Select the checkbox against “enable custom height and width for small screen”.
- Set appropriate resolution and click on submit.



DISPLAY UPDATE ON REMOTE SERVER

In earlier build when user enable full screen for any application in HyLite portal then user got to see black stripes on upper and lower edge. In this build, we have added support to update remote

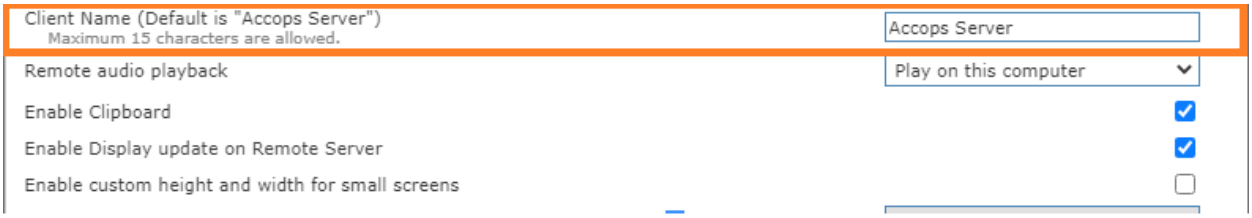
display resolution as per the browser window. Now if browser window is being resized then remote application resolution will update accordingly. To enable Display update follow below steps:

- Login as security officer.
- Go to Host configuration → HyLite configuration
- Select the checkbox against "enable display update on remote server" and click on submit.

CUSTOMIZABLE CLIENT NAME

In this build, we have added support to customize the client name. To customize client name, follow below mentioned steps:

- Login as security officer.
- Go to Host configuration → HyLite configuration
- Enter desired client name and click on submit.



HIDE WINDOWS LOGIN PROCEDURE

Whenever a user login into Windows PC then during login process multiple channels are being created. In this build, we have added support to hide Windows login procedure while these channels are being created. To enable "Hide windows login procedure" follow below mentioned steps:

- Login as security officer.
- Go to Host configuration → HyLite configuration
- Select the checkbox against "enable to hide window login procedure" and select desired channels.
- Click on submit.

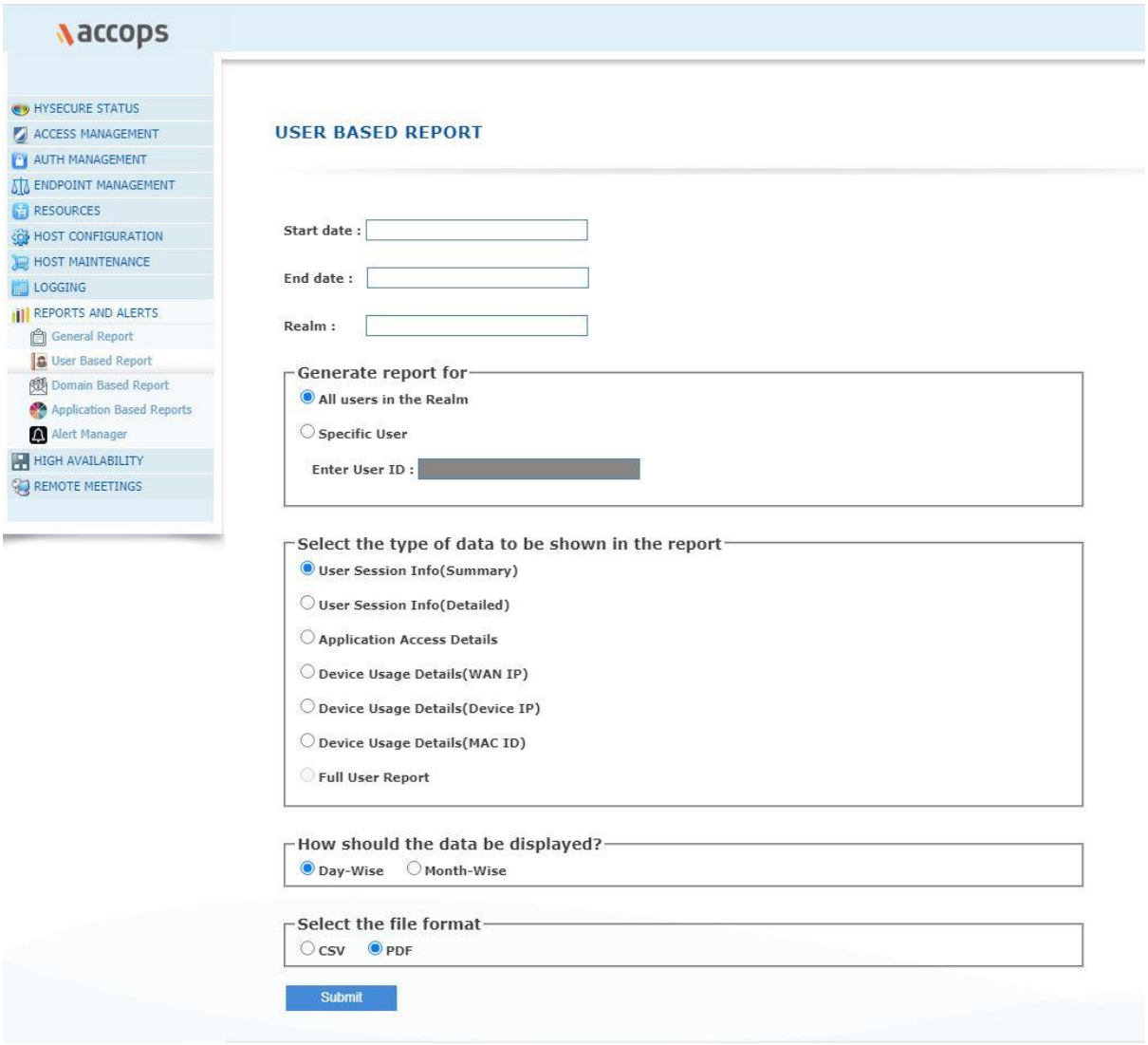
WINDOWS KEY AND ALT KEY COMBINATION IN HYLITE FULL SCREEN MODE

In this build, we have added support of key combination of Alt keys and Windows key in full screen mode only. This feature is limited to IE 11 and Chrome browser. For e.g. now Windows + R key will open run in remote application itself and also Alt + Tab will switch tab inside remote application.

LOGGING & REPORTING

NEW USER BASED REPORTS

In this build, we have redesigned **user-based report** section. Now Security Officer/Administrator/Monitor user will be able to create user report which is more categorized and contains a lot more information.
Below screenshot will give a glance on how to **generate user-based report** according to redesigned format:



Keywords required to understand various user reports are as follows:

- **Session**: If a user logs in and logs out after some time then this whole incident is called as session.
- **Session coun**t: Numbers of distinct sessions
- **Active time**: Time period during which user was accessing some application and working.
- **Total session duration**: Logout time – Login time. In other words, summation of active time and time when user was sitting idle and not accessing any application.
- **Total Active time**: Summation of active time for a user for the report duration
- **Total Session time**: Summation of total session duration for a user for the report duration
- **Last Access time**: Time stamp when user accessed an application for the last time
- **Access count**: No. of times a user has accessed any application.

Types of user reports are as follows:

User session info (summary) report

This report contains the details of session count, active time, total active time and total session time for a user/all user. This report can be generated both month wise and day wise in CSV and PDF format.

User session info (detailed) report
Apart from all the details provided in User session info (summary) report, this report will also provide information about user's login time and logout time. This report can't be generated in month wise format. It can be generated in both CSV and PDF format.

Application Access details report
This report provides the information about application access count for any application and last access time for all the application user/all users has accessed for the interval. This report can be generated both month wise and day wise in CSV and PDF format.

Device usage details report (WAN IP)
This report provides the information about the device WAN IP from which user has logged in and provide the number of times user has logged in from a WAN IP. This report can be generated both month wise and day wise in CSV and PDF format.

Device usage details report (Device IP)
This report provides the information about the device local IP address from which user has logged in and provide the number of times user has logged in from a local IP address. This report can be generated both month wise and day wise in CSV and PDF format.

Device usage details report (Mac ID)
This report provides the information about the device Mac address from which user has logged in and provide the number of times user has logged in from a Mac address. This report can be generated both month wise and day wise in CSV and PDF format.

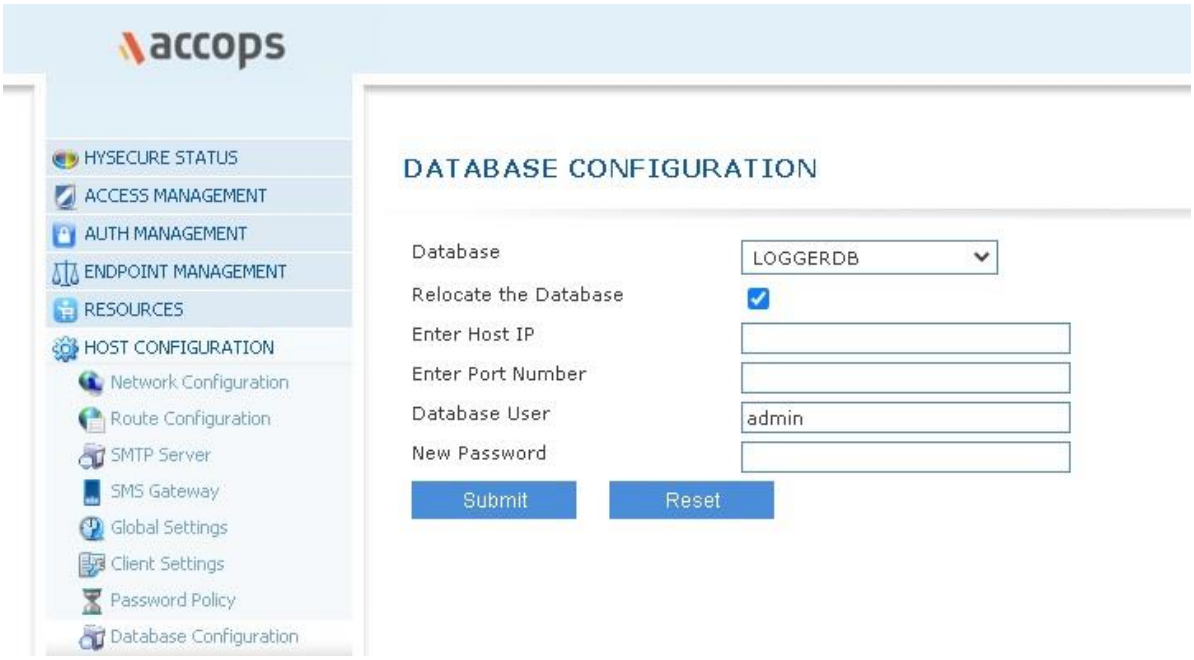
Full user report
This report type provides the details provided in all other report types in a single report. This report can't be generated in CSV format and only applicable for specific user.

HYSECURE LOGGERDB DATABASE RELOCATION THROUGH HYSECURE MANAGEMENT CONSOLE

LoggerDB database is responsible for storing data for User based report. By default, loggerDB is hosted on the HySecure gateway. We can also host the LoggerDB on a different HySecure Server or Centos server. If relocated on another HySecure gateway, then it is recommended that another HySecure gateway is solely used for LoggerDB only. Steps to relocate HySecure loggerDB database:

- Login as Security officer into Active node's management console (Do not login using Virtual IP)
- Put HySecure gateway in configuration state.

- Go to Host configuration → Database configuration.
- Select database as LoggerDB
- Mark the checkbox “Relocate the Database.”
- Enter the IP of Server where HySecure LoggerDB is going to be relocated.
- Enter Database port: 3306
- Enter current Database password of the new HySecure LoggerDB.
- Click on submit.
- HySecure gateway database LoggerDB has been relocated successfully. Put HySecure gateway in Run state.



HYSECURE DATABASE PASSWORD CHANGE THROUGH HYSECURE MANAGEMENT CONSOLE

In this build, we have provided feature to change HySecure gateway database password through HySecure management console. HySecure gateway database password can be changed from HySecure’s active node’s in configuration mode. Steps to change database password:

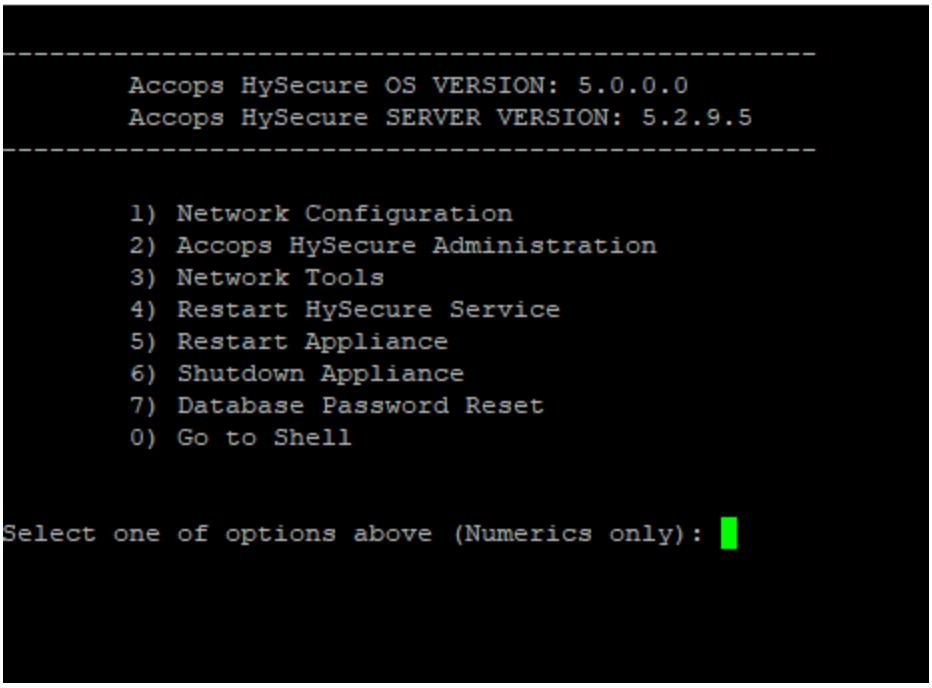
- Login as Security officer into Active node’s management console (Do not login using Virtual IP)
- Put HySecure gateway in configuration state.
- Go to Host configuration → Database configuration.
- Select database as FESDB
- Enter old password.
- Enter and confirm new password.
- Click on submit.

- HySecure gateway database password has been changed successfully. Put HySecure gateway in Run state.

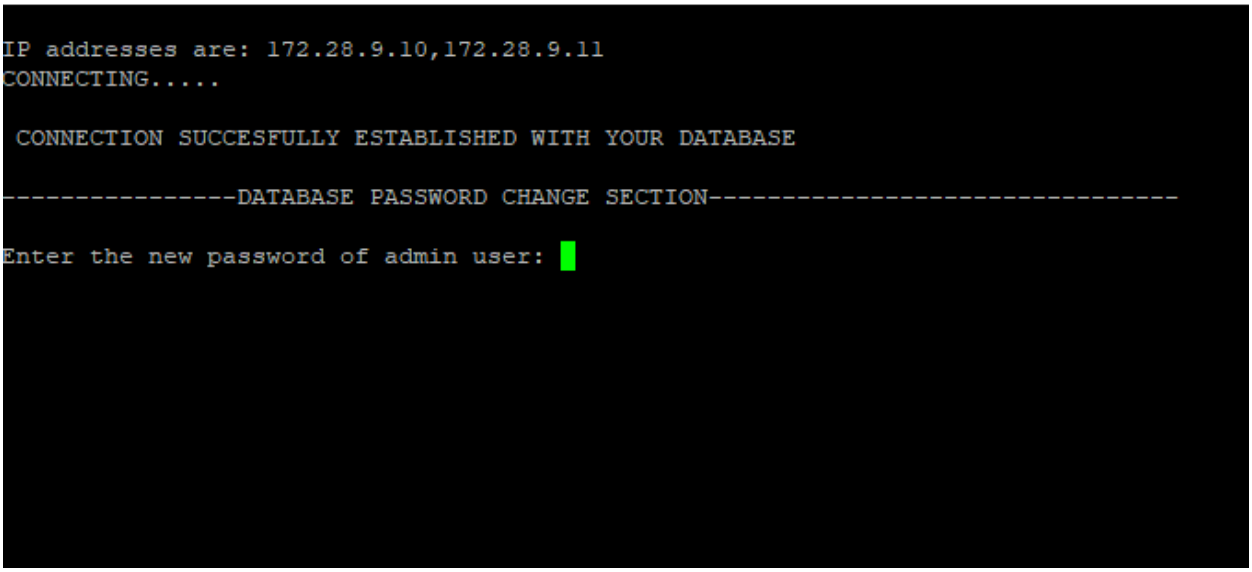
HYSECURE DATABASE PASSWORD CHANGE THROUGH HYSECURE OS CONSOLE

In this build, we have provided feature to change HySecure gateway database password through HySecure OS console. HySecure gateway database password can be changed only **from HySecure's active node's in configuration mode**. Steps to change database password:

- Login into HySecure OS console.
- Select option 7 Database password reset by entering 7.



- Enter the new database password.



- Click on submit.
- HySecure gateway database password has been reset successfully. Put HySecure gateway in Run state.

LICENSING

SUBSCRIPTION BASED LICENSE FEATURE SUPPORT

In this build, we have added support of HySecure gateway license based on subscription period for specific days.

ENHANCEMENTS

ACCESS CONTROL

DEVICE APPROVAL STATUS IN DEVICE MANAGEMENY CSV

In this build we have added support to filter out devices in Device management CSV based on their approval status.

ENHANCED ACCESS FILTER

In this build, we have enhanced access filter for application access control. Now the logged in users will also be logged out and application will be closed once access filter duration expires.

ADDITIONAL DEVICE PARAMETERS

In this build, we have added a new device parameter "Device ID". This device parameter will fetch a device ID which is unique to every machine and will not change. This device parameter will be more helpful in distinguishing when a user login through Accops Nano OS.

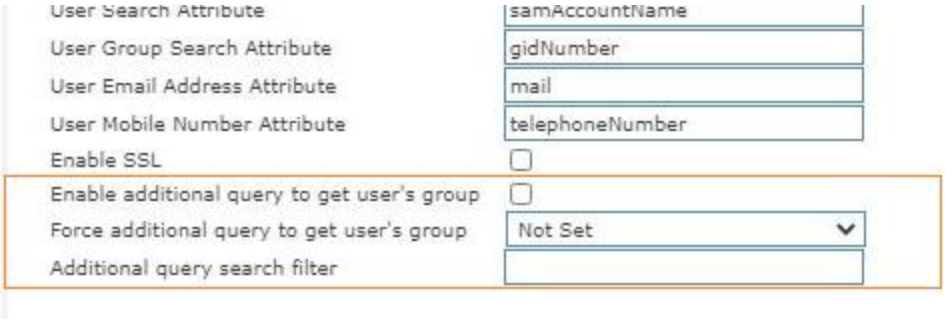
AUTHENTICATION & AUTHORIZATION

ADDED SUPPORT OF TLS 1.2 WITH AD/LDAP SERVER

In earlier build, HySecure gateway was able to communicate with AD/LDAP server using TLS 1.1, TLS 1.0 only. In this build we have added support of TLS 1.2 with AD/LDAP server.

ADDITIONAL USER GROUP SEARCH QUERY FOR AD/LDAP AUTHENTICATION SERVER

In this build, we have added support for additional user group search query for AD and LDAP authentication server.



CLIENT

LATEST HYSECURE CLIENT RELEASE

In this build, we have also bundled latest HySecure client which is V5.2.2.7.

END-POINT SECURITY

LAST UPDATED SUPPORT FOR SYMANTEC ANTIVIRUS IN EPS HOST SCAN POLICY

In this build, we have added support of verifying last database update time for Symantec Antivirus.

HYBRID MODE

HYBRID MODE SUPPORT FOR SERVICE PROVIDER-INITIATED LOGIN

In this build, we have added support of login through Hybrid mode in service provider-initiated login for SAML based apps.

HYLITE

HYLITE PORTAL OPTIMIZATION

In this build, we have optimized HyLite portal for smoother performance and scalability.

SEAMLESS CLIPBOARD SUPPORT FOR IE 11 AND GOOGLE CHROME BROWSER

In earlier build, if user wants to copy some text from remote machine to local machine or vice versa then user was needed to first copy text in clipboard menu in HyLite portal. With this build, we have

added feature to copy paste text seamlessly from remote machine to local machine and vice versa through IE 11 and Google Chrome browser in HyLite portal.

LICENSING

INCREASED CONCURRENT USERS LICENSE COUNT FOR HYSECURE GATEWAY

In this version, we have increased concurrent users license count to 65000 users.

LOGGING & REPORTING

ADDED DESKTOP HOSTNAME IN USER LOGS

In this build, we have added hostname of the device from which user is logged in user logs in case of Idle timeout and Force logout.
Note: Hostname will only be visible in user logs from backend only.

LOGGING OF ACTIVE USER SESSION

In this build, we have provided support to log the active session out of total user session.

This active user session will be calculated by subtracting idle timeout of the user from user's total session time.
Total session time of a user = User logout time – User login time
Active User session = Total session time of a user – Idle time of a user

ADDED HYSECURE CLIENT VERSION IN USER LOGS

In this build, we have added version of HySecure client from which user has logged in user logs.
Note: Hostname will only be visible in user logs from backend only.

ADDED SOURCE HYSECURE NODE COLUMN IN USER LOGS

In user logs from HySecure management console, we have added a column named "**Source Node**". Details under this column shows HySecure node hostname where user session is hosted.

ADDED ADMIN LOGS FOR MULTIPLE ADMINISTRATIVE ACTIVITIES

In this build, we have added logs for multiple activities done by Security officer and administrator user.

ADDED ACTIVITY LOGS FOR MULTIPLE USER ACTIVITIES

In this build, we have added logs for multiple end user activities.

HOURLY LOG ARCHIVAL IN LOG SETTINGS

In this build, we have added support of log files archival on hourly basis.

MISCELLANEOUS

ADDED HARDWARE TOKEN ASSIGNMENT STATUS IN EXPORTED USER PROFILE CSV

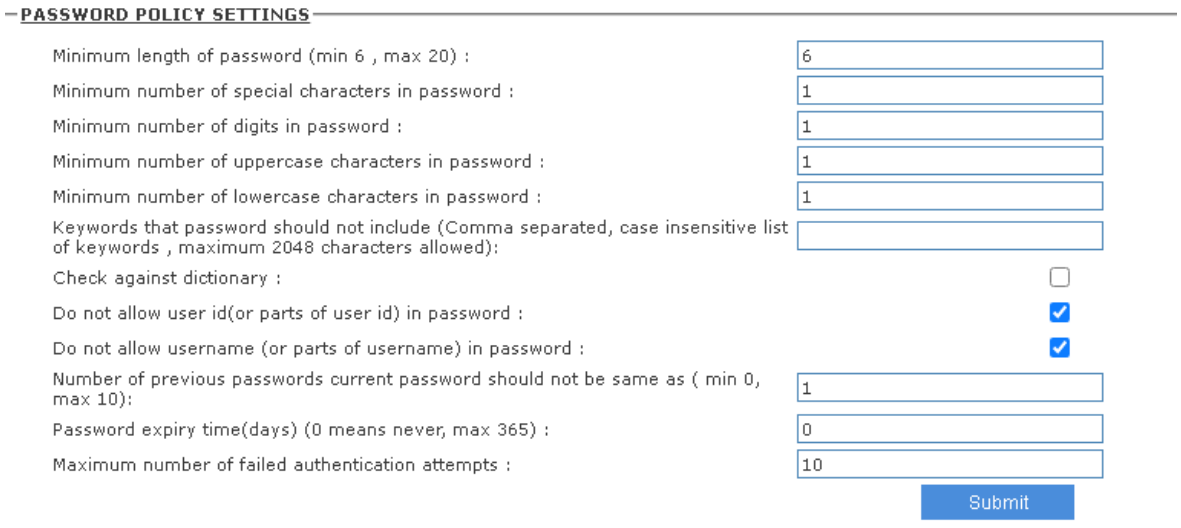
In this build, we have added details to show whether hardware token is assigned to user in the exported user profile CSV.

ADDED MULTIPLE OPTIONS TO CLIENT SETTINGS

In this build, we have put multiple options from backend to be configurable from client settings in HySecure management console.

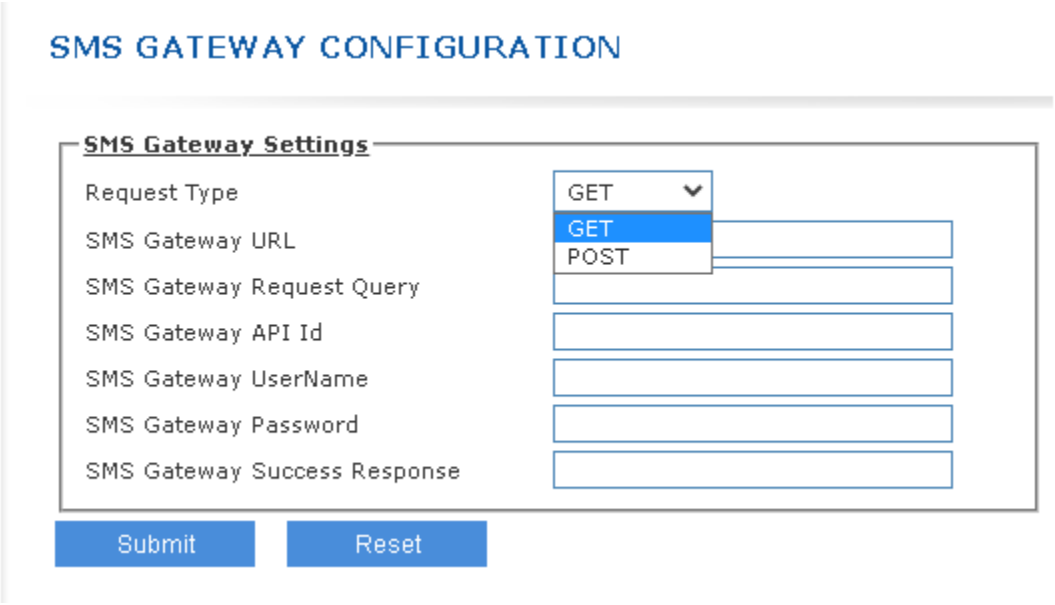
UPDATED DEFAULT PASSWORD POLICY FOR LOCAL USER

In this build, we have changed the default password policies to enforce strong passwords for new local users. Below is the current default password policy for local users:



POST REQUEST SUPPORT FOR SMS GATEWAY

In this build, we have added support for sending SMS OTP using POST request. Earlier, HySecure gateway was only supporting GET request for sending SMS OTP. Now HySecure gateway supports both GET and Post request for sending SMS OTP.



SECURE PORT 465 SUPPORT FOR SMTP SERVER

In earlier build, HySecure gateway was only supporting port 25 and secure port 587 for communicating with SMTP server. In this build, we have added support of secure port 465 for SMTP server configuration.

UPDATED ACCOUNT LOCKOUT POLICY FOR SECURITY OFFICER

In earlier build, if security officer authentication was failed for 3 consecutive times while logging then Security officer account used to get locked. In this build, we have changed limit from 3 to 10.

PERFORMANCE IMPROVEMENTS

Many performance improvements have happened as part of this release. This will be evident from the Performance Results section. The improvements are focussed from the perspective of supporting a higher number of users, improvising on the memory utilisation and Database optimizations.

SECURITY FIXES AND ENHANCEMENTS

DISABLE TLS 1.0 & TLS 1.1 BY DEFAULT

This release modifies the default behavior of gateway's TLS 1.0 & 1.1 configuration and disables the applicable ciphers as they have been deprecated and reached End of Life (EoL) status.

SPRING CLEANING - PUBLIC DIRECTORIES

All the unwanted files from public directory have been removed to reduce the attack vector.

XML PARSING ERROR

XML parsing error is handled properly reducing the XML related attacks.

ENHANCED THE SECURITY POSTURE OF CLIENT CONFIGURATION FILE

Potential exposed data has been removed from the client configuration file in this release.

UPDATED JQUERY VERSION

jQuery has been updated in this release.

VERIFY THAT HTTP RESPONSE HEADERS INCLUDE SECURITY HEADERS FOR API CALLS

Various security headers have been added in this release to enhance the security posture.

OPENSSL, OPENSSH AND KERNEL VERSION UPDATE

All the components have been updated to the latest secure versions.

SECURITY OF API CALLS HAS BEEN ENHANCED

Strong Input validation and sanitization has been implemented

REMOVAL OF SERVER HEADERS

Details of server has been removed from the server headers.

TOMCAT UPGRADE

Tomcat has been upgraded to the latest secure version.

UPGRADE INTERNAL COMPONENTS OF SERVER

All the components have been upgraded to latest secure version

USAGE OF SELF-SIGNED CERTIFICATE WITH COMMON NAME ACCOPS.COM DURING PREBOOT

“accops.com” has been replaced with “XX” in certificate common name during preboot.

PERFORMANCE RESULTS

Setup Details	Gateway Configurations	Load Applied	Observations
Active Node: CPUs: 8 ,Memory: 16 GB Standby: No physical server Real Node 1: CPUs: 8 ,Memory: 16 GB Real Node 2: CPUs: 8 ,Memory: 16 GB	25 Applications 5 Application Groups AD users used for the test Each user belongs to 50 AD User Groups	**Load:** 10000 users in ramp-up period of 2 mins **Load Script:** User Login + Web Application Access + User Logout Load ran continuously for 3 days.	**Resource Utilization** DB Node: Average CPU Usage: 37% Memory Usage: 39% Real Node1: Average CPU Usage: 43% Memory Usage: 53% Real Node2: Average CPU Usage: 35% Memory Usage: 54% **Latencies:** Average latency for **User Login is 4636 ms** Average latency for **App Access is 4400 ms**

MAX SUPPORTED VALUES FOR POLICIES/APPS

Access management --> Applications				
	MyDesktop and files	User mapping information	257 per desktop	1000 desktops
	Network Application	Application Server addresses	255 per application	255 characters
Endpoint Management--> Host scan policies				
	Domain based host scan policy	Domains	65,535 characters.	753 characters, 85 Domains
	Local IP bases host scan policy	IP addresses	65,535 characters.	8000 characters, 500 IP addresses
	Mac address-based host scan policy	MAC addresses	65,535 characters.	2000 Mac addresses
	WAN IP address-based host scan policy	WAN IP addresses	65,535 characters.	8000 characters, 500 IP addresses

ISSUES FIXED

ACCESS CONTROL

FIXED DEVICE ID ISSUE

In earlier version, on HySecure gateway if device ID is configured only for browser and if user logs in using client for the first time then the user can login from any browser.

FIXED NON-PERSISTENT FILTER ISSUE IN DEVICE MANAGEMENT

In earlier version, if search filter was applied, then that search filter was getting reset to default view when Security officer user switched to next page for viewing more search results.
In this build, we have fixed this issue. Now search filter will not reset if security officer user clicked on next page button.

AUTHENTICATION & AUTHORIZATION

FIXED ACCOUNT AUTO UNLOCK ISSUE IN SELF SERVICE PORTAL

In Self Service Portal, if account lockout is enabled on incorrect OTP attempts while resetting password through forgot password option, hen account was not unlocking automatically after defined time period. In this build, we have fixed this issue. If any account is locked due to incorrect OTP attempts, then account will unlock automatically at the time of resetting password if defined time period has been passed.

RDP SESSION REMAIN CONNECTED IN CASE OF FORCE LOGOUT FIX

In earlier build, if a user has connected RDP application and then administrator force logout user from management console. In that scenario, RDP session remain connected. We have fixed this issue in this version, now after force logout connected RDP will also be disconnected.

FIXED RDP BASED APPLICATIONS LEFT OPEN AFTER FORCE LOGOUT

In earlier version, when HySecure Security officer/administrator user removes user session by doing force logout then opened RDP application remained working until users closes them or try to connect next time. In this build, we have fixed this issue. Now open RDP based application will be closed after security officer/administrator user force logout the user.

BACKUP / RESTORE

FIXED AUTO BACKUP ON FTP SERVER

In this build, we have fixed an issue where Auto Backup of whole system backup and user backup was not being sent on FTP server.
Note: **HySecure gateway only supports Passive FTP.**

END-POINT SECURITY

FIXED REMOTE MACHINE TO LOCAL MACHINE RIGHT CLICK COPY PASTE OPTION NOT SUPPORTED

In earlier version, from remote machine to local machine copy paste is supported only through Ctrl + C, Ctrl + V option. In this build we have added support of copy paste using right click.

FIXED MAC ADDRESS CASE SENSITIVITY ISSUE FOR DEVICE ID VERIFICATION

In earlier build, Mac address validation for any client device was case sensitive. In this build, we have fixed this issue.

FIXED SYMANTEC FIREWALL DETECTION ISSUE

In this build, we have fixed an issue where HySecure gateway was unable to detect Symantec firewall while scanning host for EPS.

HYBRID MODE

FIXED MAC ADDRESS ISSUE WITH HYBRID MODE

In earlier version, when user logged in through HyBrid mode then user device's Mac addresses were not detected by HySecure gateway. In this build, we have fixed this issue.

HYID

FIXED ACCOUNT AUTO UNLOCK ISSUE IN HYID POLICY

In HyId policy, if account lockout is enabled on incorrect OTP attempts then account was not unlocking automatically after defined time period. In this build, we have fixed this issue. If any

account is locked due to incorrect OTP attempts, then account will unlock automatically at the time of login if defined time period has been passed.

FIXED LOCAL USER CASE SENSITIVITY ISSUE FOR OTP

In earlier version, when HyID policy was created for user group and local user entered username in uppercase then local user was able to login without entering OTP. In this build, we have fixed this issue.

HYLITE

CACHE CONTROL ENHANCEMENT

This build, adds the necessary configuration to prevent caching of responses from the gateway via APIs.

FIXED INCORRECT MESSAGE ON HYLITE PORTAL WHEN HYSECURE LICENSE GOT EXPIRED

In earlier version, if HySecure license has been expired, then on logging into HyLite portal it shows incorrect error message as "Authentication failed". In this build, we have fixed this issue. Now user will be shown correct message as "HySecure Gateway license has expired. Please report this incidence to your Administrator."

FIXED NO RESOLUTION ADJUSTMENT FOR RDP WINDOWS, IF BROWSER IS RESIZED

In earlier versions, after launching RDP using HyLite, if user resizes the browser then RDP screen will not adjust the screen size accordingly. In this build, we have added support to update RDP window resolution as per browser size change.

FIXED WHITE SPACE ON APP SCREEN IN FULL SCREEN MODE

On HyWorks if application is published as a remote app, attempts to login and launch application using HyLite portal in full screen mode will show white spaces on the bottom of the page. This issue has been fixed in this build, now if user enable full screen mode then application will fit to screen, and no white spaces will be shown to user.

FIXED FILE TRANSFER ISSUE FOR PORT OTHER THAN 443

In previous build, if HySecure gateway's SSL port was other than 443 then file upload and download through HyLite would not work. In this build, we have fixed this issue. Now user can upload and download files also when HySecure gateway's SSL port is other than 443.

FIXED APPLICATION TAB TITLE ISSUE IN HYLITE PORTAL

In earlier version, tab title for applications page was “Accops HyLite”. In this build, we have fixed this issue to show application name in tab title.

FIXED CTRL KEYMAPPING ISSUE WITH HYLITE FULL SCREEN MODE

In earlier version, ctrl key mapping was not working when user enable full screen mode. In this build, we have fixed this issue.

LOGGING & REPORTING

INCORRECT USER COUNT IN GENERAL REPORT IF EPS IS NOT FULFILLED

In earlier version, if user was logged in through quarantine profile, then user was not included in logged in user count in general report. In this version, we have fixed this issue.

ADDED LOGS FOR CLOSURE OF APPLICATION IN CASE OF FORCE LOGOUT

In this build, we have added activity logs for force closure of application in case of force logout.

FIXED PASSPHRASE RESET ADMIN LOG ISSUE

In earlier version, when a high security user’s passphrase was reset then admin log did not have details of user whose passphrase was reset. In this build, we have fixed this issue.

FIXED DISPLAY OF REGISTRATION ID IN ACTIVITY LOGS

In this build, we have fixed an issue where Registration ID was shown instead of username for security officer in Activity logs in case of auto logout due to idle time out.

MISCELLANEOUS

FIXING ERROR MESSAGE DISCLOSURE

The build includes fixes to prevent disclosure of information through error messages when gateway is sent a specially crafted request.

FIXED EMAIL ISSUE WITH SOME EMAIL ADDRESSES

In earlier versions, with some longer email addresses users faced an issue of email OTP not being received. In this version, we have fixed this issue.

FIXED IDLE TIMEOUT ISSUE

In earlier version, if Idle timeout is configured as 30 minutes then in some cases, user session may not logout and remain idle for more than 30 minutes. In this build, we have fixed this issue.

MISSING LOGOUT TIME FOR SESSION REUSE FIX

In earlier build, if any user session gets disconnected due to network connectivity or device getting shut down then user logout log was missing in user logs. In this version, we have fixed this issue.

FIRST USER LOGGED IN AFTER HYSECURE REBOOT SESSION LOGOUT FIX

In earlier build, first user logged in after HySecure gateway reboot session logged out because of idle timeout even if user was accessing application. In this version, we have fixed this issue.

FIXED FAIL TO CHANGE PASSWORD IF PASSWORD LENGTH WAS MORE THAN 16 CHARACTERS

In this build, we have fixed an issue where active directory users were not able to change password through HyLite Portal if password length was exceeding 16 characters. Now users can change password of length up to 40 characters through HyLite portal.

FIXED TCPDUMP SYNTAX ERROR THROUGH OS CONSOLE

In this build, we have fixed an issue where administrator user was unable to take TCPdump through HySecure gateway OS console.

FIXED LEFT CLICK LONG PRESS ISSUE

In earlier version, while being on application screen if user pressed left click for some time, then it was behaving like right click. In this build. We have fixed this issue.

FIXED SYSTEM RESOURCE USAGE LOG FILE DOWNLOADING ISSUE

In this build, we have fixed an issue where security officer was unable to download system resource log file from HySecure management console.

FIXED LOCAL USER PASSWORD EXPIRE AFTER DAYS FEATURE

In this build, we have fixed an issue where password of local user was not expiring after days specified in HySecure Management console.

MONITORING

FIXED IP ADDRESS SHOWN AS 0.0.0.0 IN ACTIVE USERS PAGE WHEN USER LOGIN THROUGH IE BROWSER

In earlier version, when user login into HySecure gateway using Internet explorer, then user's IP address was incorrectly shown as 0.0.0.0 in Active users page. In this build, we have fixed this issue, now it will show correct IP address.

KNOWN ISSUES

ACCESS CONTROL

ACCESS CONTROL EXPIRY WORKS FOR ONLY APPLICATION ACCESS ACL

Access control expiry feature provided while creating/modifying any access control only works for Application access type access control. Feature is visible while creating other access control also, it will be removed later.

ACCESS CONTROL PRIORITY ONLY WORKS FOR EPS AND DEVICE ID TYPE ACL

Access control priority feature provided in this release, only works for device ID and EPS ACL. Feature is visible while creating other access control also, it will be removed later.

LOCAL USER GROUP VISIBLE WHILE CREATING ANONYMOUS GROUP APPLICATION ACCESS CONTROL

While creating application access-based access control for anonymous user group, Local user group created in HySecure will be visible along with DEFAULT_ANONYMOUS_USER_GROUP.

AUTHENTICATION & AUTHORIZATION

SAML APPLICATION SESSION NOT LOGGING OUT ON USER LOGOUT

User session from SAML application will not be logged out even if user logout from Hysecure gateway in below cases:

1. HySecure as Identity provider for SAML apps: e.g. Office365, Salesforce published as SAML web apps through HyLite.
2. HySecure as Service Provider: User gets access to application by logging into SAML Identity provider such as Azure AD.

END-POINT SECURITY

DEVICE ID POLICY RESTRICTION IF RELATED PARAMETERS ARE NOT SELECTED

If related parameters are not selected in device ID access control, then users may get message 'Login denied due to device restriction policy.' For e.g. if user is logging through browser and browser type & browser ID are not selected as device parameters then users may get above message while trying to login from approved browser.

MAC ADDRESSES LIST REMOVAL DUE TO SEARCH FILTER

In Mac address-based host scan policy, if Administrator/Security officer user searches Mac addresses from host scan sub policy and click on submit without removing search keyword, then search results only will be saved in host scan policy. Rest all Mac addresses will be deleted.

EPS REMEDIATION MSG MAY NOT APPEAR

In case of EPS failure, if a remediation message is configured for a host scan policy, then that remediation message may not appear to end user in case of EPS failure.

HA

UNABLE TO SWITCH USER VIP IF HYSECURE GATEWAY IS SWITCHED

If virtual IP address pool is configured for the user and HySecure gateway handling user session shuts down then in that case user session will be switched to another node but user's virtual IP would not be switched resulting into app access failure and user may have to login again.

HYBRID MODE

FORCEFUL UPGRADATION OF HYSECURE CLIENT NOT WORKING THROUGH HYBRID MODE

Force upgradation of HySecure client not working through Hybrid mode.

USER MAY NOT BE ABLE TO LOGIN IN HYBRID MODE IF EPS/DEVICE ID IS ENABLED FROM WINDOWS 8 DEVICES

If EPS/Device Id is enabled, then user may not be able to login into Hybrid mode from some Windows 8 devices.

HYID

INCORRECT ERROR MESSAGE WHEN OTP TOKEN IS ENTERED WITHOUT REQUESTING OTP TOKEN

In this build, if user enters OTP token without requesting any OTP token then user will get incorrect error message 'Authentication failed.' Instead of 'Invalid OTP. Please try again.

HYID DESKTOP AGENT(WINDOWS) NOT WORKING

In this version, HyID Desktop agent Windows will not work. However, Linux credential provider will be working fine.

INCORRECT CLIENT TYPE IN HYID LOG FOR LINUX CREDENTIAL PROVIDER

If a user has logged into Linux credential provider, then in HyID log client type will be shown as "HyLite Portal".

HYLITE

ON MAC OS, ACCOPS HYPRINT PDF DOES NOT WORK

On MAC OS, HyPrint Pdf printer using HyLite will not work. Since this feature is only supported on Windows OS.

INCORRECT ERROR MSG. ON HYLITE PORTAL IN CASE OF ALLOWED DEVICES EXHAUSTION

If device Id policy has been applied on user and user has already logged in from allowed number of devices and user tries to login from new device using HyLite portal, then user will get incorrect error message.
Incorrect msg: You are denied to login due to DEVICE Identification policy. Please contact your VPN administrator.

GENERIC ERROR MESSAGE ON HYLITE PORTAL WHEN LOGIN DENIED DUE TO EPS FAILURE

If user tries to login from a device which does not fulfill EPS host scan policies, then a generic error msg would be shown to user.
Error msg: "You are not allowed to login from this IP address".

USERNAME MORE THAN 25 CHARACTERS WILL NOT WRAP IN APPLICATION PAGE IN HYLITE PORTAL

Username with more than 25 characters will not wrap and due to which will not be completely visible in applications page (Left edge of screen) in HyLite portal.

INTERNATIONALIZATION

SESSION EXPIRY MESSAGE DUE TO IDLE TIMEOUT AND FORCE LOGOUT APPEARS IN ENGLISH LANGUAGE ON JAPANESE CLIENT MACHINE

If a user is logged out of HyLite portal due to idle timeout or Force logout on Japanese desktop, then also user get session expiry message in English language.

JAPANESE CHARACTERS NOT SUPPORTED IN HYSECURE MANAGEMENT CONSOLE

In HySecure gateway, Japanese characters will not be supported in following fields: Application name, Application group, Local user, Local user group, Authentication server Admin bind.

LOGGING & REPORTING

HYLITE LOG FILE DOWNLOAD OPTION NOT WORKING FROM HYSECURE MANAGEMENT CONSOLE

In this release, option to download HyLite logs from the management page is not working. Administrator can download HyLite logs from backend using WINSCP tool.

ACTIVITY LOG AND HYID LOG MAY NOT GENERATE FOR ADS MODULE IN CASE OF AUTH FAILURE

While logging through ADS module, if a user either incorrect username or incorrect OTP or incorrect password then Activity log and HyID log may not generate.

MISCELLANEOUS

PASSWORD POLICY GETTING BYPASSED WHEN ADMINISTRATOR USER RESET PASSWORD FROM USER PROFILE

Password policy does not apply while administrator tries to set password from user profile.

PDF FILE DOWNLOADS INSTEAD OF PRINT IF PDF READER IS NOT INSTALLED ON LOCAL MACHINE

If PDF reader is not installed on local machine, then using IE 11 browser PDF file will be downloaded instead of printing while giving print using HyLite Accops printer.

PRINT OPTION NOT VISIBLE THROUGH EDGE BROWSER IF PDF READER NOT INSTALLED ON LOCAL MACHINE

If PDF reader is not installed on local machine, then using Edge browser (v41), print option will not display while give print using Accops printer/Accops HyPrint.

MANUAL RMS CONFIGURATION AFTER APPLYING UPGRADE PATCH

After applying upgrade patch, administrator needs to configure RMS file again. Administrator also needs to restart httpd service after configuring.

RMS NOT WORKING IN HYSECURE VERSION 5.2 SP2

In this build, RMS feature will not be working. To use RMS feature, it is recommended to use HySecure V5.3 .

USER LOGGED OUT FROM HYSECURE CLIENT WHEN MORE THAN 160 APPLICATIONS ARE ASSIGNED

If user has more than 160 applications, HySecure windows client will automatically exit after login.

USER SESSION REMAINS ACTIVE ON HYWORKS IF IDLE TIMEOUT IS DIFFERENT

Idle timeout in Hyworks controller must be greater than Idle timeout at HySecure gateway. Login into HySecure as AD user and keep user idle for the defined time so that user session ends after idle timeout.

Expected Result: User session should end in both Hyworks and Hysecure and User machine.
Actual Result: User session ended on user machine and HySecure gateway but remained active on Hyworks controller.

APPLICATION RECONNECT DOES NOT WORK WITH SHELL MODE

If shell mode is enabled in connection profile page on HyWorks, HyLite does not support application reconnect in shell mode.

USER UNABLE TO LOGIN IF EXISTS IN 250 OR MORE USER GROUPS

If an Active directory user exists in 250 or more than 250 user groups, then user will not be able to login into HySecure gateway.

SSO WITH HYWORKS FAILS IF USER EXIST IN 110 OR MORE USER GROUPS

If an Active directory user exists in 110 or more than 110 user groups, then user will not be able to access Hyworks applications/VDI/SHD.

UNABLE TO DELETE ALL IP ADDRESS POOL

If administrator selects all IP address pools, then only oldest one will be deleted. To delete all the pool, security officer has to repeat this process until all the pools are deleted.

MAC ID VALIDATION USING EXTERNAL API NOT WORKING

In this version, Mac ID validation for auto approval of device will not work.

CUSTOM RDP RESOLUTION NOT BEING SET

In RDP application published through HySecure gateway, custom resolution will not be set by the option provided while publishing RDP application. RDP application will work in maximum resolution in all cases.

OPEN PROGRAM IN RDP APPLICATION NOT WORKING

Open Program option provided to open an application inside the RDP application published through HySecure gateway is not working in this version.

APP IP ADDRESS SHOWN AS NULL IN CASE OF MY DESKTOP FILESHARE TYPE APPLICATION

If user accessed My Desktop file share type application, then in Activity logs App IP address will be shown as null.

INTERNAL SERVER ERROR EXPIRED LOCAL USER ACCOUNT MODIFICATION

Administrator/Security officer may get internal server error if tried to modify expired local user account.

LOCAL USER SEARCH BASED ON USERID WILL NOT WORK

In this version, local user search by User ID filter will not be working.

SECURITY OFFICER USER CREATION EVEN IF CONFIRM PASSWORD FIELD IS LEFT BLANK

In this version, security officer user account will be created successfully even if confirm password field is left blank.

SINGLE IP ADDRESS AND PORT RANGE TCP APPLICATION MAY NOT WORK

If an application published with single IP address and port range, it may not work in this build.

APPENDIX A: UPGRADING HYSECURE CLUSTER

The section describes the detailed process to apply upgrade patch 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

UPGRADING REAL HYSECURE CLUSTER NODE:

1. 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 ***Firmware upgrade*** and upload the HySecure upgrade patch file.
- It may take 1 minutes or more to upload the upgrade patch based on network bandwidth between your PC and Gateway.
- Once the upgrade patch 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 upgrade patch is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the upgrade patch installation logs.

UPGRADING STANDBY HYSECURE CLUSTER MANAGER NODE:

2. 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 ***Firmware upgrade*** and upload the HySecure upgrade patch file.

- It may take 1 minutes or more to upload the upgrade patch based on network bandwidth between your PC and Gateway.
- Once the upgrade patch 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 upgrade patch is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the upgrade patch installation logs.

UPGRADING ACTIVE HYSECURE CLUSTER MANAGER NODE:

3. 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 "Upgrade Firmware" page under "Host Maintenance" Section => Select option ***Firmware upgrade*** and upload the HySecure upgrade patch file.
- It may take 1 minutes or more to upload the upgrade patch based on network bandwidth between your PC and Gateway.
- Once the upgrade patch 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 upgrade patch is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the upgrade patch installation logs.

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.

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 enables secure and instant access to business applications from any device and network, ensuring compliant enterprise mobility for business users while keeping governance with the organization.

Accops' workspace virtualization, access gateway and identity management solution suite help organizations to consolidate the distributed end user application infrastructure and bring endpoint management to the datacentre, improving the overall network security and reducing IT operational costs.

Accops is a single stop shop to build an integrated workspace for business users, providing seamless access to modern web applications, SaaS applications, client-server applications, legacy applications, virtual applications and virtual desktops. Accops was established in October 2012 and is headquartered in Pune, India.

Tel: India +91 20 6719 0123
Email: sales@accops.com | Web: www.accops.com