

Release Notes

HySecure 5.2 SP1 Upgrade Patch build
5230

Last Updated: 5 Dec 2018

Copyright © 2018, Accops Systems Private Limited. All Rights Reserved.

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.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the explicit written permission of Accops Systems Private Limited.

Contact Accops Systems Private Limited.

Email: info@accops.com

Call: +91 9595 277 001

Release Notes Document Revision History

<i>Date</i>	<i>Changes</i>
15-Feb-2017	Version 5.0.5004 RC1 Release
06-May-2017	Version 5.0.5016 RC 4
16-June-2017	Version 5.0.5035 RC5 Release
14-Aug-2017	Version 5.0.5057 GA Release
03-Nov-2017	Version 5.0.5080 SP1 Release
15-Dec-2017	Version 5.0.5087 SP2 Release
01-June-2018	Version 5.1.5169 RC Release
10-Sept-2018	Version 5.2.5200 GA Release
5-Dec-2018	Version 5.2.5230 SP1 Release

CONTENTS

Overview	6
How to Install HySecure 5.2 build 5230.....	6
How to get HySecure 5.2 build 5230	7
new feature in 5.2.5230.....	7
hardware token support in hyID.....	7
LDAP user and user group support in ACL	11
enhancement in 5.2.5230	12
Hyid support for radius users.....	12
VIP support for LDAP and native user.....	12
VIP related log.....	12
new user profile on hysecure management console.....	12
new HySecure client	12
Issues Fixed in 5.2.5230	13
Known Issues in 5.2.5230.....	14
new feature in 5.2.5200.....	18
New dash board.....	18
Access control UI enhancements.....	19
Access control expiry	20
Access control for notification	21
Account logout	22
Password policy	23
geo-fencing based EPS policy	25
WAN IP based EPS policy.....	27
domain based EPS policy	28
enhancement in 5.2.5200	30
Updated accops logo	30
HySecure domain change to default.....	30
new HySecure client	31
Improved performance of remote meeting	31
UAC support in remote meeting.....	31
New portal UI.....	31
application access log	32

Security issues Fixed in 5.2.5200	32
Issues Fixed in 5.2.5200	33
Known Issues in 5.2.5200.....	33
new feature in 5.1.5169.....	37
Bulk user upload from managemnt page	37
role base administration support	40
Accops RMS intregation.....	41
saml identity federation support.....	43
New HyLite mode.....	44
separate HyID policy for hysecure and HyID desktop agent.....	45
New HyID desktop agent policy configuration	46
Enable HyID Desktop Agent:	46
Offline OTP Configuration:.....	48
New control for upload/download file using hylite.....	49
new menu option on Hylite RDP page.....	50
Option to drag menu on hylite RDP page:	50
risk based OTP profile configuration	51
Hyid support for ldap user	52
enhancement in 5.1.5169	53
Updated accops logo	53
new HySecure client	53
Improved performance of remote meeting	53
UAC support in remote meeting.....	53
New portal UI.....	53
Security issues Fixed in 5.1.569	55
Issues Fixed in 5.0.5169	57
Known Issues in 5.1.5169.....	58
Appendix A: Upgrading HySecure Cluster.....	61
Upgrading Standby HySecure Cluster Manager Node:	62
Upgrading Dedicated HySecure Gateway Node:	63
Bring the cluster up again	63
Upgrading Old (last) Active HySecure Cluster Manager Node:	65
appendix B: Upgrading HySecure standalone setup.....	66

OVERVIEW

This document outlines the new features / bug fixes / features enhancement / known issues in the Accops HySecure 5.2. 5230 SP1 release

5.2.5230

Released on 5 Dec 2018

HOW TO INSTALL HYSECURE 5.2 BUILD 5230

UPGRADE COMPATIBILITY OF V5.2.3.0

HySecure 5.2.3.0 SP1 upgrade patch is compatible with upgrades from the HySecure 5.2.0.0 versions only.

Note: Please note that if HySecure version is below than 5.2.0.0 then first need to upgrade this gateway into HySecure 5.2.0.0 version. Then apply this 5.2 SP1 upgrade patch.

Please refer section [Appendix A: Upgrading HySecure Cluster](#) for procedures to upgrade HySecure Cluster.

Please refer section [Appendix B: Upgrading HySecure standalone gateway](#) for procedures to upgrade HySecure gateway.

HOW TO GET HYSECURE 5.2 BUILD 5230

Download the HySecure upgrade patch:

<https://propalmsnetwork->

[my.sharepoint.com/:u:/g/personal/support_accops_com/EUv58L4ynTJDhV83UZdhnJ0BfNwiNLxEJi3lsz5y74zMA?e=scr08y](https://propalmsnetwork-my.sharepoint.com/:u:/g/personal/support_accops_com/EUv58L4ynTJDhV83UZdhnJ0BfNwiNLxEJi3lsz5y74zMA?e=scr08y)

MD5 Checksum of HySecure upgrade patch: **0c7ec3c2c265d01cd808afeb0a19ce80**

NEW FEATURE IN 5.2.5230

HARDWARE TOKEN SUPPORT IN HYID

In this release, we have added support for hardware token as a means to provide two factor authentication. Now, HySecure administrator can configure hardware tokens on HySecure server and individual tokens can be assigned to users to perform additional authentication. Hardware token can be assigned to local native, Active Directory, LDAP and radius user.

First administrator needs to import hardware tokens on HySecure gateway. For importing hardware tokens, go to RESOURCES->Hardware Token and import the XML file of any OAUTH compliant OTP Token file. The server will automatically recognize if the token is HOTP (event based) or TOTP (time based) token. If the HMAC secrets are encrypted, then you either need the password or the encryption key for which the appropriate PSKC file needs to be uploaded.



IMPORT HARDWARE TOKENS

Here you may upload the XML file of any OAUTH compliant OTP Token.
The server will automatically recognize if the token is HOTP(event based) or TOTP (time based) token.
If the HMAC secrets are encrypted you either need - depending on the encryption the password or the encryption key.

Select Authentication Domain	DefaultAuthDomain ▼
Select encryption type	Not Encrypted ▼
Key/Password value	Not Encrypted
Choose PSKC File*	Key protected
	Password protected
<div>Submit Cancel</div>	

If everything is valid then all hardware tokens will be imported automatically, and the administrator can see the list of hardware tokens on HySecure gateway. Please note that hardware tokens are imported for specific authentication domain. Hence, while importing hardware tokens please ensure that the proper authentication domain is selected.

Select Authentication Domain	DefaultAuthDomain ▼
Select encryption type	Key protected ▼
Key/Password value	FF178589972390F7AC06DAB97B51D!
Choose PSKC File*	<div>Choose File No file chosen</div>
<div>Submit Cancel</div>	

Successfully imported the hardware tokens.

Count of failed hardware tokens are : **0** Count of Passed hardware tokens are : **15**

[Download passed entries](#)

Please click [here](#) to view the list of hardware tokens

Once hardware tokens are successfully imported, the administrator needs to assign each hardware token to specific users. For assigning hardware tokens to users, go to AUTH MANAGEMENT->Users Profiles. Here, administrator needs to create a user profile if not done previously. In case user profile is already created, the administrator can proceed to assign a hardware token to that user.

#	Status	User Name	Authentication Domain	Authentication Server	Authentication failed attempts
<input type="checkbox"/>		qa1	LDAP	LDAP	0
<input type="checkbox"/>		qa3	LDAP	LDAP	0

☐ Check all

[Add User](#)
[Unlock](#)
[Lock](#)
[Delete](#)
[Profile Details](#)

For assigning hardware token to a user, select user and click on profiles details button or click on user name, then assign token.

Basic Info

User Name	qa1
Authentication Domain	LDAP
Authentication Server	LDAP
Authorization Server	NONE
Alternate Mobile	-
Alternate Email	-
First Login Time	2018-11-20 13:33:49
Last Login Time	2018-11-20 13:33:49

Tokens

Mobile Token	Not Activated Activate
Hardware Token	Not Assigned Assign

REGISTER HARDWARE TOKEN

User Name:

Authentication Domain:

Select a serial number for the user profile:

0200082580

0200082579

0200082578

0200082577

0200082576

0200082575

e.g. 0200082584

Submit

Cancel

Once hardware token is assigned to user, next step is creating HyID (OTP) policy for this user so that upon logging into HySecure, user is prompted to enter hardware token OTP. Go to AUTH MANAGEMENT->HyID Policy and create a HyID policy for that user with hardware token. Or if HyID policy is already created then modify this policy and enable newly added hardware token.

HySecure Authentication

☒ Enable Two factor authentication
 ☐ Disable Two factor authentication

Select 2FA tokens

☒ Enable in-line 2FA

Select tokens

Email Token	<input type="checkbox"/>
SMS Token	<input type="checkbox"/>
Email and SMS Token	<input type="checkbox"/>
Mobile Token	<input type="checkbox"/>
Hardware Token	<input checked="" type="checkbox"/>

Email and SMS OTP Configuration

Select OTP token length

06 digit

Select OTP token expiry time

05 min

☐ Enable OTP token use for multiple time

Select OTP token regenerate timeout

30 sec

At any time, administrator can unassign hardware token from user profile. Also, administrator can get complete information about total number of assigned and unassigned tokens from the hardware token page. To get complete token information as report click on export token link, it will generate a report in CSV format for download. From this report, administrator can get which token is assigned to which user.

HARDWARE TOKENS

Search Filter

Search tokens

Show

Enter comma separated Search String or (*) for all tokens

No of assigned tokens : 1

No of unassigned tokens : 14

List of hardware tokens

[Export Tokens](#)

Delete		Import Tokens						
#	Status	Serial No	User Name	Authentication Domain	Manufacturer	Algorithm	Token length	Token Interval
<input type="checkbox"/>		0200082570		LDAP	Entrust Datacard	TOTP	8	30

LDAP USER AND USER GROUP SUPPORT IN ACL

Till now for LDAP authentication server, user and user group were not fetched from LDAP server while creating access control on HySecure server. In this release, access control can be created for LDAP user or user group.

ENHANCEMENT IN 5.2.5230

HYID SUPPORT FOR RADIUS USERS

In this release, support of HyID policy for radius users has been added. Now hardware token can be assigned to radius user to login to the gateway.

VIP SUPPORT FOR LDAP AND NATIVE USER

Now, virtual IP address can be assigned to LDAP user group or native user group. So, when user login on HySecure gateway virtual IP address will be assigned automatically for that user from virtual IP address pool.

VIP RELATED LOG

Virtual IP related all log will be available on user activity log. The details of user activity is now documented in the activity log. When user logs out from HySecure, the Virtual IP will be automatically unassigned and documented in activity log.

TLS 1.2 SUPPORT FOR SMTP

In this release, TLS 1.2 support for SMTP has been added. HySecure can now send email to SMTP servers supporting TLS 1.2

NEW USER PROFILE ON HYSECURE MANAGEMENT CONSOLE

In this release, we have enhanced the user profile section. Administrator can now manage all two-factor authentication assigned to user and user details from a single webpage.

NEW HYSECURE CLIENT

This release contains new HySecure Windows client version 5.1.0.5. In this client some critical bugs related to HyWorks have been fixed. The client also improves and reduces the time taken for a user to login to the gateway.

ISSUES FIXED IN 5.2.5230

SECURITY FIXES

This release provides fixes for internally reported security issues.

HYLITE APPLICATION LAUNCHING ISSUE ON IE BROWSER

On Windows 8 OS HyLite application did not launch using IE browser. This issue has been fixed on this release.

EPS (END POINT SECURITY) NOT APPLICABLE FOR MOBILE DEVICES.

EPS rules did not apply for logins from mobile devices and allowed such login requests to go through. This issue has been fixed in this release. EPS scan is now compulsory for all the clients. This option is disabled by default. Administrator need to enable this option using backed. Take SSH and go to location "/home/fes" and edit file called "features.status". In this file EPSMANDATORY tag value should be 1 for scan EPS for all types of client. If this tag value is 0 then will works as before.

AUDIO NOT WORKING ON SAFARI BROWSER

On Safari browser audio did not work when using HyLite Pro. This issue has been fixed in this release.

GEOLOCATION AND WAN IP LOGIN ISSUE

Create a geolocation base EPS policy on HySecure. In that policy block US and allow india branch office WAN IP. Then from india branch office user will not be able to login. This issue has been fixed in this release.

HYLITE OTHER THAN DEFAULT PORT

In previous release, HyLite did not work with ports other than the default port. This issue has been fixed in this release.

USER LOGIN ISSUE IF ACTIVE GATEWAY IS DOWN.

If active gateway is down and user had a HyID policy assigned, then user was unable to login. This issue has been fixed in this release.

NETWORK INTERFACE DISPLAY ISSUE

If gateway has multiple network interfaces then on HySecure management page, the route entry add option only displayed one network interface. This issue is fixed in this release.

STATIC ROUTE ADD ISSUE

In previous release, if administrator tried to add static routes from management page then after rebooting the gateway the route entries were deleted automatically. This problem has been fixed in this release.

KNOWN ISSUES IN 5.2.5230

IOS CLIENT LOGIN ISSUE

Accops HyClient (iOS client) won't be able to connect to this build. Accops will release new iOS client to fix this issue.

PASSWORD POLICY CONFIGURATION GETTING BYPASSED FROM USER PROFILE

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

PRINTER REDIRECTION NOT SUPPORTED ON LINUX VDI USING HYLITE

Printer redirection not working on Linux VDI when using HyLite mode.

FORCEFUL UPGRADATION OF HYSECURE CLIENT NOT WORKING FROM HYBRID MODE.

Force upgradation of HySecure client not working.

RMS CONFIGURATION NEED TO DO MANUALLY AFTER 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 ON STANDALONE GATEWAY

On HySecure standalone gateway RMS will not work. RMS mode is supported only on HA setup.

SOMETIMES HYSECURE MANAGEMENT PAGE IS SHOWING ACCESS DENIED

While logging as security office and accessing HySecure management page, an Access Denied page may be displayed.

Workaround: Refresh the page or close the page and login again as Security Officer.

ON ACTIVE USER PAGE, IP ADDRESS IS SHOWING 0.0.0.0 WHEN USER LOGIN USING HYLITE ON IE BROWSER.

IP address is showing 0.0.0.0 value on HySecure Active user page, if user is login using IE browser.

DEVICE ID ISSUE

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.

CLIENT USER LOGIN EXITED WHEN MORE THAN 160 APPLICATIONS ASSIGNED TO USER

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

UNABLE TO CONNECT TO GATEWAY AFTER STATE CHANGE

On HySecure gateway if administrator wants to change the gateway state then sometimes HySecure services may not be accessible.

IMPORT USER FROM CSV TAKES TIME

CSV import for users on the Management console takes time.

MESSAGE ON LICENSE GOT EXPIRED

If HySecure license has expired, then HyLite portal will not show appropriate message.

NOT ABLE TO MODIFY LOW SECURITY USER DETAILS

On HySecure gateway if user backup is restored from 5087 then after restoration, mobile number of that user is not updated. Workaround is creating with the mobile number.

USERS AVAILABLE IN LOCAL USER GROUP ONLY

While restore user backup if email ID already exists on new gateway then user will not be imported but will be displayed on the local user group.

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.

CGI DOWNLOADS SOMETIMES WHILE SAVING POLICIES IN HYSECURE MANAGEMENT CONSOLE

On HySecure Management page sometimes CGI download automatically while click on any option.

MULTIPLE VDI POWER ON OPTION NOT WORKING USING HYLITE

If one user has more than one VDI machines and user try to power on all VDI machines from HyLite portal at a time, then only one VDI machine will power on. So, if user wants to power on multiple VDI machines, first power on one machine first, once it is up then proceed to power on another machine.

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.

WHITE SPACE ON FULL SCREEN ON APP 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.

HYLITE LOG FILE DOWNLOAD OPTION NOT AVAILABLE FROM MANAGEMENT PAGE.

In this release, there is no option to download HyLite logs from the management page. Administrator can download HyLite logs from backend using WINSCP tool.

COPY-PASTE FROM REMOTE M/C TO LOCAL MACHINE: CTRL+C, CTRL+V SUPPORTED. RIGHT CLICK COPY-PASTE OPTION NOT SUPPORTED

Copy-paste option from RMS VM to local machine using right click option is not supported.

INCORRECT IDLE TIME ON ACTIVE USERS PAGE

On HySecure Active user page, idle time is showing wrong time. Although user is using RMS VM still on HySecure active user page idle time keeps on increasing.

ON SAFARI BROWSER, ACCOPS HYPRINT DOES NOT WORKING

On MAC OS, Safari browser does not support HyPrint using HyLite.

IF PDF IS NOT INSTALLED ON LOCAL MACHINE, THEN USING IE 11 BROWSER PDF FILE WILL DOWNLOAD WHILE GIVING PRINT USING ACCOPS PRINTER

If PDF 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.

IF PDF IS NOT INSTALLED ON LOCAL MACHINE, THEN USING EDGE BROWSER, PRINT OPTION NOT SHOWING WHILE GIVE PRINT USING ACCOPS PRINTER/ACCOPS HYPRINT

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

NO RESOLUTION ADJUSTMENT FOR REMOTE SESSION, IF BROWSER WINDOW IS RESIZED.

After launching RDP using HyLite, if user resizes the browser then RDP screen will not adjust the screen size accordingly.

HYID ACCOUNT LOCK OUT TIME DOES NOT WORKING.

HyID account lock out time is not supported in this version. It will be fixed in next version.

HYLITE SHARED DRIVE TAKES TIMES TO MAP

While launching RMS VM using HyLite, HyLite shared drive takes time to display on the screen.

IN UPLOAD ONLY MODE: ON DRAGGING FILES INTO DOWNLOAD FOLDER, FILES DISAPPEAR AND THEN REAPPEAR ON REFRESHING.

If upload only is configured on HyLite configuration page, then while dragging file into download folder on HyLite shared drive, file will have disappeared. The file is displayed upon refresh.

IN UPLOAD ONLY MODE: ACCOPS HYLITE PRINTER OR ACCOPS HYPRINT WILL NOT WORK

If upload only is configured on HyLite configuration page, user will not be able to execute print jobs using Accops printer or Accops HyPrint. Download option should be enabled on HyLite configuration page for printing.

RMS VM LAUNCHING ISSUE

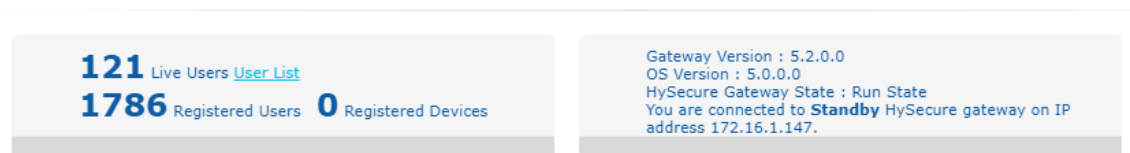
When launching RMS VM using HyLite, sometimes it will show message like "Please wait while connecting" and not able to connect to VM. But if user refresh or relaunch RMS VM then it will connect to VM.

NEW FEATURE IN 5.2.5200

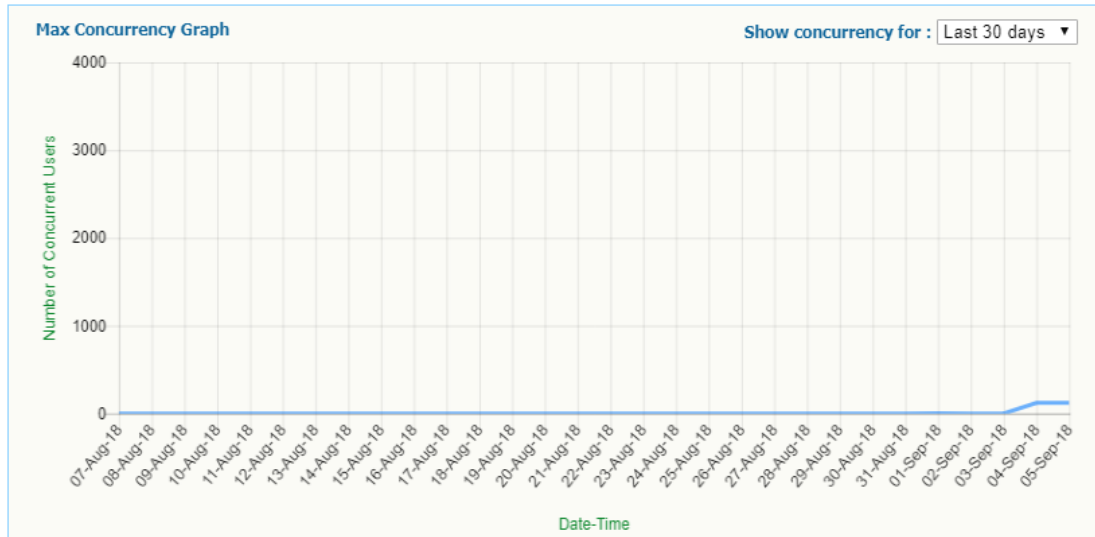
NEW DASH BOARD

The Dashboard now displays the count of registered users and registered devices on HySecure gateway. *Registered users* are the unique users that have logged in, in the past, on HySecure gateway and *Registered devices* are the devices from which users have logged in, in the past. To view the list of registered users, go to AUTH MANAGEMENT→User Profiles. Similarly, to view the list of registered devices, go to ENDPOINT MANAGEMENT→Device Management. Note that *Live Users* is the total number of users that are currently logged in on a gateway.

DASHBOARD



Administrator also can get the information about the maximum concurrent users for 3 different timeframes viz. last 30 days, last 7 days and last 24 hours. If the administrator selects "Last 30 days", then the graph shows maximum concurrent users for all 30 days from the current day. If "Last 24 hours" is selected then the graph will show the maximum concurrent users for every hour, for the last 24 hours. In a nutshell, day wise peak is plotted for the last 30 days, hour wise peak is plotted for last 7 days, and minute wise peak is plotted for last 7 days.



ACCESS CONTROL UI ENHANCEMENTS

Access control UI has been modified. In the previous release, Access Control Name was the first option. This has now been modified to Access Control Type. While creating any ACL, administrator needs to select 'Access Control Type' first.

CREATE ACCESS CONTROL

Access Control Type	<div>Application Access ▼</div>
Access Control Name	<input type="text"/>
Access Control Description	<div><input type="text"/></div>
Select HySecure Domain	<div>Select option ▼</div>
Select Authorization Server	<div>Select option ▼</div>
Select Assignment Type	<div>Select option ▼</div>

For 'All user' or 'All User Group' related access control, administrator needs to select the appropriate radio button for "All user" or "All User Group" respectively after selecting Authorization Server and Assignment Type. In previous release, administrator was required to search all user / all group for creating ACL for all.

CREATE ACCESS CONTROL

Access Control Type	Application Access ▼
Access Control Name	TestACL
Access Control Description	This is test <u>ACL</u>
Select HySecure Domain	Default ▼
Select Authorization Server	Primary AD ▼
Select Assignment Type	Users ▼
Select User Type	<input checked="" type="radio"/> All Users <input type="radio"/> Selected Users

If administrator wants to create access control for specific user or user group, then select radio button labelled “*Selected Users*”. After selecting this button, search windows will appear on the page automatically. Here, type and search the user or user group to proceed adding them to ACL.

Select HySecure Domain	Default ▼
Select Authorization Server	Primary AD ▼
Select Assignment Type	Users ▼
Select User Type	<input type="radio"/> All Users <input checked="" type="radio"/> Selected Users
Select Users	

- demo
- demo1
- demo12
- demo2
- demo3
- demo4
- demo5

ACCESS CONTROL EXPIRY

Access control expiry option has been added in this release. Administrator can now set the expiry date for all access control policies except “Notification” policy. The applicable ACL shall be put in disabled state upon reaching the expiry date and users shall not be permitted to login to the gateway thereafter. While creating access controls, administrator needs to set the required expiry date on “Access Control Valid Till” field.

The screenshot displays the ACL configuration interface. On the left, there is a search bar with 'demo' entered and a list of application groups: demo1, demo12, demo2, demo3, demo4, and demo5. Below this is a 'Select Application Group' section with an empty list. In the center, there are 'Add >>' and 'Delete <<' buttons. On the right, there is another empty list for application groups. Below the lists, there is a calendar for 'September 2018' with the date '5' selected. Below the calendar is a date input field with the placeholder 'YYYY-MM-DD' and radio buttons for 'Enable' and 'Disable'. At the bottom, there is an 'Access Filter' section with a red-bordered field labeled 'Access Control Valid Till :', an 'Access Control State' section, and 'Submit' and 'Reset' buttons.

Once the access control has expired, an email notification will be sent to the email Id that was specified while creating the notification policy (Note: To get email on acl expiry, another access control of the type 'notification' needs to be created). After ACL expiry, administrator can enable and change the ACL expiry date if required. Administrator can set ACL expiry date any time and set expiry date to never expire by deleting the date from "Access Control Valid Till" field.

ACCESS CONTROL FOR NOTIFICATION

New access control type called "Notification" has been added in this release. Using this type of ACL, administrator can receive notifications on HySecure for following events:

- User Login
- User First Login
- Access Control Policy Expiry
- Account Lockout
- New Device Registration

Note: Email is sent to all email IDs that were specified in *Email Recipients* field creating the notification ACL.

Email notification can be set for users of following authorization servers:

- Active Directory
- LDAP
- Radius
- Native.

CREATE ACCESS CONTROL

Access Control Type	Notifications
Access Control Name	Notification
Access Control Description	
Select HySecure Domain	Default
Select Authorization Server	Primary AD
Select Assignment Type	Users
Select User Type	<input checked="" type="radio"/> All Users <input type="radio"/> Selected Users
Events	Enable Email Notifications
User First Login	<input type="checkbox"/>
User Login	<input type="checkbox"/>
User Logout	<input type="checkbox"/>
Access Control Policy Expiry	<input type="checkbox"/>
Account Lockout	<input type="checkbox"/>
Application Access	<input type="checkbox"/>
New Device Registration	<input type="checkbox"/>
Recipient Email(s) *	
Specify semicolon separated Email addresses.	
Access Control State	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

In an Email notification policy, for the events **Access Control Policy Expiry** and **Account Lockout**, "User Type" should be *All users or All groups*. These events cannot be configured for *Selected users or user groups*.

For other notification events namely **User Login, User First Login and New Device Registration**, User Type field can be set as *All users/ All groups* or *Selected User/ user group*.

Example: If notification policy has been configured for the event User Login with User Type as All Users, then email will be sent to the administrator (If email Id is specified) when any user logs in to HySecure gateway from the specified domain. If notification policy is created for specific user/ specific user group, then notification shall be triggered when that specific user will login to HySecure gateway.

Also, while creating notification policy please enter Recipient Email ID. To send notifications to multiple email addresses, please enter the required email addresses in this field separated by a semicolon (;). Example: [user1@company.com;admin@company.com;so@company.com](#)

Note: While creating notification type access control, please ensure that SMTP is configured on HySecure gateway.

ACCOUNT LOCKOUT

Account lockout feature is available on this release. Account lockout is new type of access control. Using this type of ACL administrator can lock user accounts on HySecure gateway if they haven't logged into the gateway for a specified amount of time after first/most recent login. Account lockout policy is

applicable for the authorization servers: Native, Active Directory, LDAP and Radius. This type of policy is applicable for *All user or All User Group*. The lockout policy cannot be applied to a *Selected User / User Group*.

CREATE ACCESS CONTROL

Access Control Type	Account Lockout ▼
Access Control Name	LockoutPolicy
Access Control Description	<div></div>
Select HySecure Domain	Default ▼
Select Authorization Server	Primary AD ▼
Select Assignment Type	Users ▼
Select User Type	<input checked="" type="radio"/> All Users
User should not be able to login after Valid range is from 01 to 999 days	<input type="text"/> days of first login
User should not be able to login after Valid range is from 01 to 999 days	<input type="text"/> days of last login
Access Control Valid Till :	YYYY-MM-DD
Access Control State	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Submit
Reset

The following scenarios can be implemented:

User should not be able to login after a certain period from first login: If administrator wants that after specific number of days of first login, user account will be locked on HySecure gateway.

User should not be able to login after a certain period from the most recent / last login: If administrator wants that after specific number of days of last login, user account will be locked on HySecure gateway

If any user account is locked due to account lockout policy, then account lockout notification will be sent to the specific email account, given that an email notification policy exists for Account Lockout event.

PASSWORD POLICY

For native users, a new password policy setting has been added in this release. This password policy will be applicable for all native users including Low Security User and all type of certificate users. Once the administrator configures the password policy on gateway, the newly set passwords for all Native Users will be verified against the configured policy. If the password doesn't meet the requirements specified by the password policy, an appropriate error message shall be displayed.

PASSWORD POLICY

PASSWORD POLICY SETTINGS

Minimum length of password (min 6 , max 20) :	<input type="text" value="6"/>
Minimum number of special characters in password :	<input type="text" value="0"/>
Minimum number of digits in password :	<input type="text" value="0"/>
Minimum number of uppercase characters in password :	<input type="text" value="0"/>
Minimum number of lowercase characters in password :	<input type="text" value="0"/>
Keywords that password should not include (Comma separated, case insensitive list of keywords , maximum 2048 characters allowed):	<input type="text"/>
Check against dictionary :	<input type="checkbox"/>
Do not allow user id(or parts of user id) in password :	<input type="checkbox"/>
Do not allow username (or parts of username) in password :	<input type="checkbox"/>
Number of previous passwords current password should not be same as (min 0, max 10):	<input type="text" value="0"/>
Password expiry time(days) (0 means never, max 365) :	<input type="text" value="0"/>
Maximum number of failed authentication attempts :	<input type="text" value="3"/>

Submit

Minimum length of password (min 6, max 20): Specify the minimum length of password.

Minimum number of special characters in password: Specify the minimum number of special characters in password

Minimum number of digits in password: Specify the minimum number of digits in password

Minimum number of uppercase characters in password: Specify the minimum number of uppercase characters in password

Minimum number of lowercase characters in password: Specify the minimum number of lowercase characters in password

Keywords that password should not include: Specify the keywords that should not be in password. User can enter multiples keywords with comma separated values.

Check against dictionary: Mark the checkbox to check the strength of password. Common English words will be rejected.

Do not allow user id (or parts of user id) in password: Mark the checkbox to reject the password which contains more than 2 characters from User ID. For e.g. if User ID is Accops then password Acc@123 or cop@123 or Accops will be rejected.

Do not allow username (or parts of username) in password: Mark the checkbox to reject the password which contains more than 2 characters from Username. For e.g. if Username is Accops then password Acc@123 or cop@123 or Accops will be rejected

Number of previous passwords current password should not be same as (min 0, max 10): Enter the no. of previous passwords to check while setting new password for any user. Password matching with these users will be rejected.

Password expiry time(days): Enter the time after which user's password will expire. Here 0 means never expire and maximum value which can be set is 365 days.

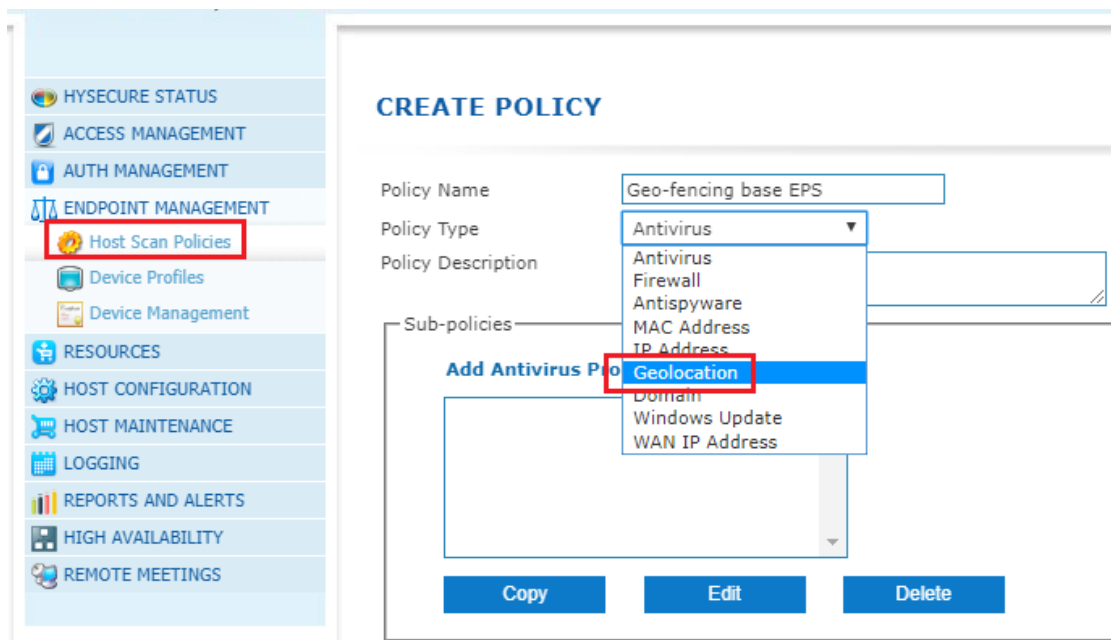
Maximum number of failed authentication attempts: No. of failed authentication attempts allowed for the user. After these attempts user account will be locked. Once the account is locked, the administrator will need to manually unlock the user from the management console.

GEO-FENCING BASED EPS POLICY

Geo-Fencing based EPS (End Point Security) policy support has been added in HySecure. Using this EPS policy, administrator can set up a virtual boundary around a geographical location, known as a geofence. This policy is applied at a domain level and once applied, any user who is a part of this domain shall be governed by the applicable policy for this domain. For e.g. if the administrator has applied a policy on a domain named 'Mumbai' to allow logins, the gateway will permit access only if the user's IP address belongs to Mumbai. Access to users attempting to login to the gateway from anywhere else will not be permitted. The geo-fencing policy on the domain to allow or restrict access can be set at a granular level of Country, State or City name.

Note: Geo-Fencing based EPS policy requires an Endpoint Protection Security License to be applied on the gateway.

To configure, please go to ENDPOINT MANAGEMENT → Host Scan Policies. Add host scan policy of the type "Geolocation".



Click on *Add Geolocation Policy* to configure a policy to Allow or Block access. Further, select the appropriate geo-fencing level (Country/State/City) to be applied for this policy as given in the screenshot below:

ADD GEOLOCATION POLICY

Geolocation Policy Name

☒ Allow
☐ Block

Select Country ▼

Select State ▼

Select City ▼

Once the level of access has been selected, click Submit. Next go to **ENDPOINT MANAGEMENT** → **Device Profiles** and create a new profile. Click on '*Add policies to profile*' and select add the Geo-Fencing policy created previously and click on submit to apply.

CREATE PROFILE

Profile Name Security Level

☐ Mandatory Profile

Profile Description

Policies

The Policies which are added to fall in this Device Profile

Geolocation

Blocked Applications

ADD POLICIES TO PROFILE

Geolocation

WAN IP BASED EPS POLICY

Extending the Geo-fencing capabilities, HySecure also supports allowing or denying access to the gateway based on the user's WAN IP address. For e.g. if the administrator wishes to allow access to the gateway from a specific WAN IP address (belonging to a branch office) and deny access from other IP addresses, this can be achieved by setting up a WAN IP based EPS policy.

To configure, please go to **ENDPOINT MANAGEMENT** → **Host Scan Policies**. Add host scan policy of the type "WAN IP Address".

CREATE POLICY

Policy Name: WAN IP

Policy Type: Antivirus

Policy Description:

Sub-policies:

- Antivirus
- Firewall
- Antispyware
- MAC Address
- IP Address
- Geolocation
- Domain
- Windows Update
- WAN IP Address

Buttons: Copy, Edit, Delete

Buttons: Submit, Cancel

Click on Add WAN IP Address to configure a policy to Allow or Block access. Next, select Allow/Block and specify the WAN IP Address on which the policy should be applied. Multiple WAN IP addresses can be specified by separating the IP addresses with a pipe (|).

step1

CREATE POLICY

Policy Name: WAN IP

Policy Type: WAN IP Address

Policy Description:

Sub-policies:

Add WAN IP Address Policy

Copy Edit

Submit

step2

ADD WAN IP ADDRESS POLICY

WAN IP Address Policy Name: Allow_WAN_IP

☒ Allow

☐ Block

WAN IP Addresses:

Add Delete

Submit Reset

step3

ADD WAN IP ADDRESS

☒ Add WAN IP Addresses

☐ Add WAN IP Range

WAN IP Address:

(WAN IP Address format : IP1[IP2][IP3...])

Submit Reset

Once the level of access has been selected, click Submit. Next go to **ENDPOINT MANAGEMENT** → **Device Profiles** and create a new profile. Click on 'Add policies to profile' and select to add the WAN IP Address policy created previously and click on submit to apply.

CREATE PROFILE

CREATE PROFILE

Profile Name: Device Profile

Security Level: 1

☒ Mandatory Profile

☐ Quarantine Profile

Profile Description:

Policies:

The Policies which are added below must be satisfied by the End Point Devices to fall in this Device Profile.

Add Policies to Profile

ADD POLICIES TO PROFILE

Geolocation

WAN_IP

Add ->

Remove <-

Submit Cancel

DOMAIN BASED EPS POLICY

It is now possible to allow or disable access to the gateway based on whether the user's device is part of a pre-configured domain. For e.g. if the administrator wishes to only allow access to the users whose devices are part of a domain named accops.com and deny access to all other devices, it can be implemented using this feature.

To configure, please go to **ENDPOINT MANAGEMENT** → **Host Scan Policies**. Add host scan policy of the type "Domain"

CREATE POLICY

Policy Name:

Policy Type:

Policy Description:

Sub-policies:

Add Antivirus Pro

Copy **Edit** **Delete**

Domain

Windows Update

WAN IP Address

Click on Add Domain to configure a policy to Allow or Block access. Next, select Allow/Block and specify the domain name(s) on which the policy should be applied. Multiple domain names can be specified by separating them with a comma.

CREATE POLICY

Policy Name:

Policy Type:

Policy Description:

Sub-policies:

Add Domain Policy

Copy **Edit**

ADD DOMAIN POLICY

Domain Policy Name:

☒ Allow ☐ Block

Domains:

Add **Delete**

Submit **Reset**

ADD DOMAINS

Domain:

(Domain List Format - Domain1,Domain2,Domain3...)

Submit **Reset**

Once the level of access has been selected, click Submit. Next go to ENDPOINT MANAGEMENT→Device Profiles and create a new profile. Click on 'Add policies to profile' and select to add the Domain policy created previously and click on submit to apply.

CREATE PROFILE

Profile Name Security Level

☐ Mandatory Profile
☐ Quarantine Profile

Profile Description

Policies

The Policies which are added below must be satisfied by the End Point Devices to fall in this Device Profile.

Add Policies to Profile

172.16.1.145/fes-bin/zoneManager.cgi?type=2&Poli... — □ ×

Not secure | 172.16.1.145/fes-bin/zoneManager.cgi?type=2&Poli...

ADD POLICIES TO PROFILE

Geolocation
WAN_IP

Allow_domain

Add ->
Remove <-

Submit Cancel

ENHANCEMENT IN 5.2.5200

UPDATED ACCOPS LOGO

New Accops logo has been updated in this upgrade patch. After applying this upgrade patch HySecure web portal logo will change to the latest logo.

HYSECURE DOMAIN CHANGE TO DEFAULT

In this release HySecure domain name has been changed from DefaultDomain to Default. If HyWorks is configured on HySecure then in previous release HySecure domain name need to change first to default. Now by default, HySecure domain name will be default only.

NEW HYSECURE CLIENT

This release contains new HySecure windows client version 5.0.9.0. In this client some critical bugs related to HyWorks has been fixed. Also, login time has been reduced in this client.

IMPROVED PERFORMANCE OF REMOTE MEETING

In this release performance of remote meeting has been improved. In previous release, access to remote meeting was slower. In this Windows client release, access to remote meeting has become faster.

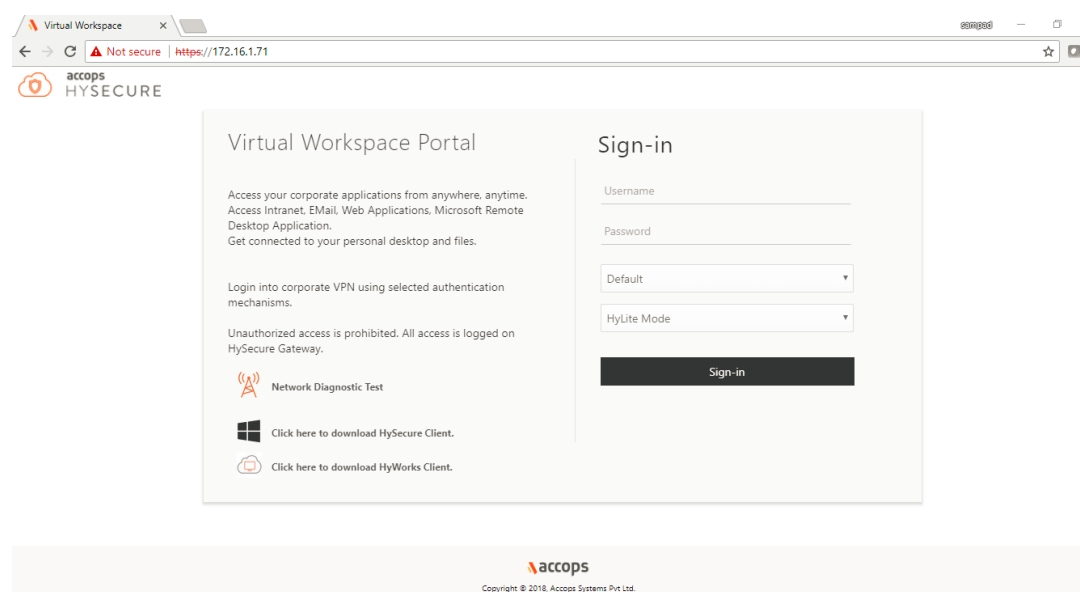
User needs to install HySecure windows client version 5.0.9.0 for faster access and better performance of Remote meeting.

UAC SUPPORT IN REMOTE MEETING

In previous release, during remote session if UAC pop up shows on remote machine, then meeting got disconnected. This issue has been fixed in this release.

NEW PORTAL UI

HyLite and Hybrid portal UI has been changed in this release. After applying upgrade patch portal UI will change. Now HySecure domain name will be display below password field.



APPLICATION ACCESS LOG

Now on activity log administrator can get details application access log. If for any reason HySecure gateway is not able to reach the application server, then while end user tries to access that application, on activity log this reachability fail will be logged.

SECURITY ISSUES FIXED IN 5.2.5200

Multiples vulnerabilities are fixed in this release. Please find the CVE details which are fixed in this upgrade patch.

CVE-2018-2938 (<https://nvd.nist.gov/vuln/detail/CVE-2018-2938>)

CVE-2018-2941 (<https://nvd.nist.gov/vuln/detail/CVE-2018-2941>)

CVE-2018-2973 (<https://nvd.nist.gov/vuln/detail/CVE-2018-2973>)

CVE-2018-2940 (<https://nvd.nist.gov/vuln/detail/CVE-2018-2940>)

CVE-2018-2952 (<https://nvd.nist.gov/vuln/detail/CVE-2018-2952>)

CVE-2018-2964 (<https://nvd.nist.gov/vuln/detail/CVE-2018-2964>)

ISSUES FIXED IN 5.2.5200

HYLITE PORTAL LOGIN ISSUE

If user has more than 200 application, then user not able to login using HyLite portal. This issue has been fixed in this release.

RENAME ONEGATE DOMAIN TO HYSECURE DOMAIN

Create an IP address pool in resources. Go to IP Address pool and look on the list. Error: Onegate domain is written in list instead of Hysecure domain. This is fixed in this release.

COULD NOT GET EMAIL OTP IF SMS OTP FAILS

Create HyID Policy with "*Email and SMS Token*". Login using HyLite/Client >> Get OTP. User should get OTP on Email and SMS. Actual: User failed to get SMS OTP. This issue is fixed on this release.

NOT ABLE TO LOGIN USING REGISTERED DEVICE IF DEVICE HAVING MULTIPLE LAN CARDS

Enable domain-based device id policy for 2 devices, one of the devices having 15 LAN cards. User was unable to login from device with 15 LAN cards to device ID policy. This issue has been fixed on this release.

KNOWN ISSUES IN 5.2.5200

RMS CONFIGURATION NEED TO DO MANUALLY AFTER UPGRADE PATCH

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

RMS NOT WORKING ON STANDALONE GATEWAY

On HySecure standalone gateway RMS will not work.

SOMETIMES HYSECURE MANAGEMENT PAGE IS SHOWING ACCESS DENIED

While logging as security office and access HySecure management page sometimes it is showing access denied error message.

Workaround: Need to refresh page or close the page and login again as security officer.

ON ACTIVE USER PAGE, IP ADDRESS IS SHOWING 0.0.0.0 WHEN USER LOGIN USING HYLITE ON IE BROWSER.

IP address is showing 0.0.0.0 value on HySecure Active user page, if user is login using IE browser.

DEVICE ID ISSUE

On HySecure gateway if device id is configured only for browser. And if user first time login using client, then user can login from any browser.

CLIENT USER LOGIN EXITED WHEN MORE THAN 160 APPLICATIONS ASSIGNED TO USER

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

UNABLE TO CONNECT TO GATEWAY AFTER STATE CHANGE

On HySecure gateway if administrator wants to change the gateway state then sometimes HySecure services

IMPORT USER FROM CSV TAKES TIME

If administrator wants to import user from CSV on HySecure then it will take time for import user.

MESSAGE ON LICENSE GOT EXPIRED

If HySecure license is expired, then HyLite portal will not show appropriate message.

NOT ABLE TO MODIFY LOW SECURITY USER DETAILS

On HySecure gateway if user backup is restored from 5087 then after restoring mobile number of that user not able to update. Workaround is creating same with mobile number.

USERS AVAILABLE IN LOCAL USER GROUP ONLY

While restore user backup if email id already exists on new gateway then user will not be import but on the imported local user group that user will show.

USER SESSION REMAINED ACTIVE ON HYWORKS IF IDLE TIMEOUT IS DIFFERENT

Idle timeout at Hyworks controller must be greater than Idle timeout at HySecure gateway. Login into HySecure as AD user. 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.

CGI DOWNLOADS SOMETIMES WHILE SAVING POLICIES IN HYSECURE MANAGEMENT CONSOLE

On HySecure management page sometimes CGI download automatically while click on any option.

MULTIPLE VDI POWER ON OPTION NOT WORKING USING HYLITE

If one user has more than one VDI machines and user try to power on all VDI machines from HyLite portal at a time, then only one VDI machine will power on. So, if user wants to power on multiple VDI machine. Then first power on one machine first, once it is up then trying to power on another machine.

APPLICATION RECONNECT DOES NOT WORK WITH SHELL MODE.

On HyWorks in connection profile shell mode is enabled. Then HyLite does not support application reconnect in shell mode.

WHITE SPACE ON FULL SCREEN ON APP MODE

On HyWorks if application published as remote app mode. Then login and launch application using HyLite portal. After launching click on full screen button. While launching application on full screen mode there will be white space on below of the page.

OLDER OS VERSION ISSUE IN OS CONSOLE

In previous release, after applying upgrade patch HySecure OS version was not upgraded in OS console. This issue has been fixed in this release.

HYLITE LOG FILE DOWNLOAD OPTION NOT AVAILABLE FROM MANAGEMENT PAGE.

In this release, there is no option to download HyLite logs from management page. Administrator can download HyLite log from backend using WINSCP tool.

COPY-PASTE FROM REMOTE M/C TO LOCAL MACHINE: CTRL+C, CTRL+V SUPPORTED. RIGHT CLICK COPY-PASTE OPTION NOT SUPPORTED

Copy-paste option from RMS VM to local machine using right click option is not supported.

INCORRECT IDLE TIME ON ACTIVE USERS PAGE

On HySecure Active user page, idle time is showing wrong time. Although user is using RMS VM still on HySecure active user page idle time keeps on increasing.

ON SAFARI BROWSER, ACCOPS HYPRINT DOES NOT WORKING

On MAC OS, safari browser does not support HyPrint using HyLite.

IF PDF IS NOT INSTALLED ON LOCAL MACHINE, THEN USING IE 11 BROWSER PDF FILE WILL DOWNLOAD WHILE GIVING PRINT USING ACCOPS PRINTER

If PDF 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.

IF PDF IS NOT INSTALLED ON LOCAL MACHINE, THEN USING EDGE BROWSER, PRINT OPTION NOT SHOWING WHILE GIVE PRINT USING ACCOPS PRINTER/ACCOPS HYPRINT

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

NO RESOLUTION ADJUSTMENT FOR REMOTE SESSION, IF BROWSER WINDOW IS RESIZED.

After launching RDP using HyLite, if user do browser resize then RDP screen will not adjust the screen size accordingly.

HYID ACCOUNT LOCK OUT TIME DOES NOT WORKING.

HyID account lock out time is not supported in this version. It will be fixed in next version.

HYLITE SHARED DRIVE TAKES TIMES TO MAP

While launch RMS VM using HyLite, HyLite shared drive called takes time to display on the screen.

IN UPLOAD ONLY MODE: ON DRAGGING FILES INTO DOWNLOAD FOLDER, FILES DISAPPEAR AND THEN REAPPEAR ON REFRESHING.

If upload only is configured on HyLite configuration page. Then while dragging file into download folder on HyLite shared drive, file will have disappeared. And then re-appear on refresh option.

IN UPLOAD ONLY MODE: ACCOPS HYLITE PRINTER OR ACCOPS HYPRINT WILL NOT WORK

If upload only is configured on HyLite configuration page. Then user will not be able to give print using Accops printer or Accops HyPrint. Download option should be enabled on HyLite configuration page for printing.

SOMETIMES RMS VM LAUNCHING ISSUE

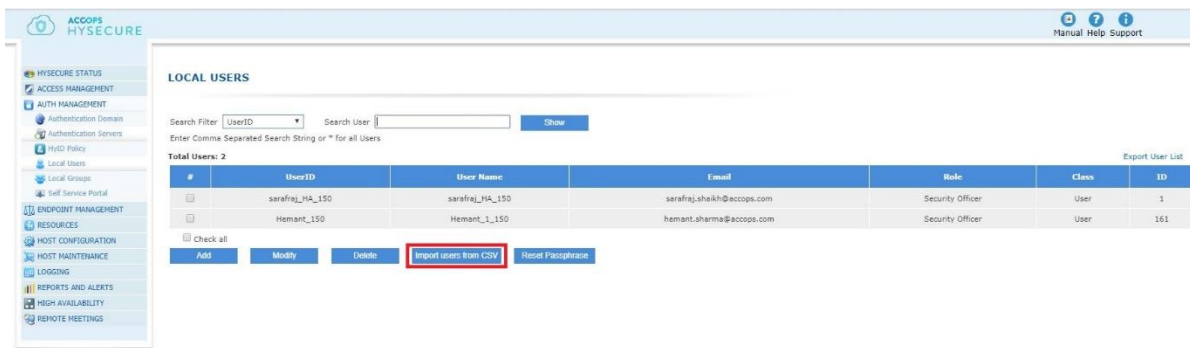
While launching RMS VM using HyLite, sometimes it will show message like "Please wait while connecting" and not able to connect to VM. But if user refresh or relaunch RMS VM then it will connect to VM.

NEW FEATURE IN 5.1.5169

BULK USER UPLOAD FROM MANAGEMNT PAGE

Administrator can upload bulk user from HySecure management page. The administrator needs to create HySecure local user list in CSV format. CSV format should be same as sample format which is available on bulk user import page.

After applying this upgrade patch, Security officer will need to clear cache of the browser and login again. Now go to option AUTH MANAGEMENT → Local User. Here administrator needs to click on "Import User From CSV" button to upload users into HySecure local database from CSV file.

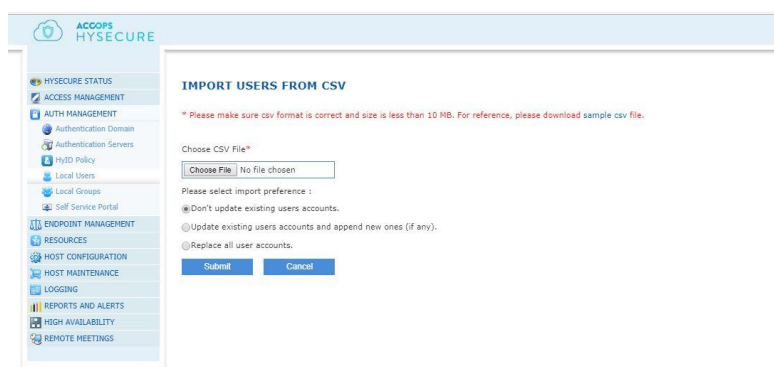


Administrator can upload only Low Security User (without certificate user) using this import user option. One CSV file can upload up to 1000 users onto HySecure gateway at a time.

Download sample CSV file from import user from CSV page. Add users according to sample CSV file format.

After adding users into CSV file, follow below steps:

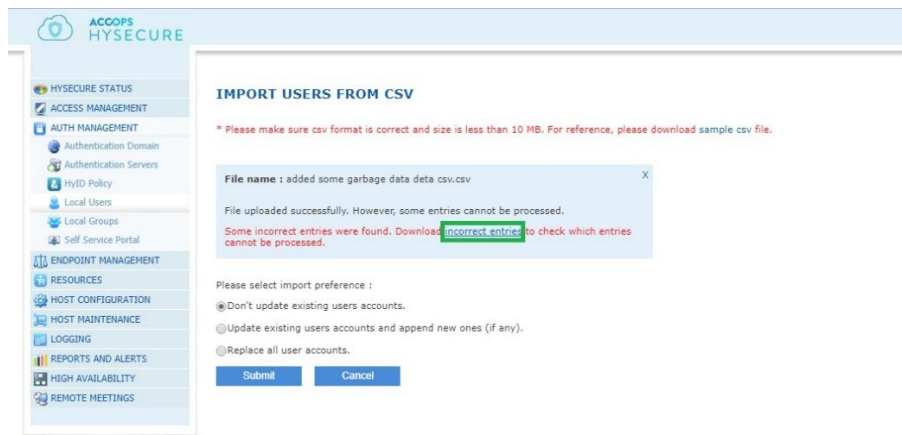
- Login to HySecure management console.
- Go to AUTH management >> Local users.
- Click on "Import users from CSV".
- Upload CSV file and select one of the three options accordingly.



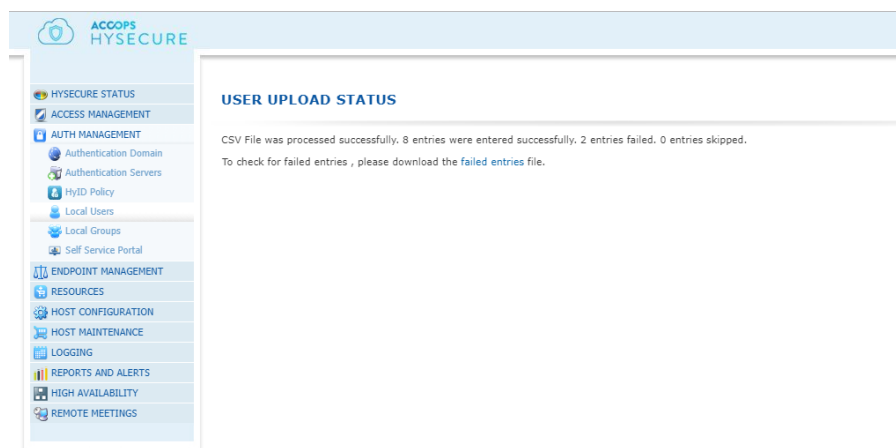
- If "don't update existing user accounts" is selected, then existing user accounts will remain as they were, no changes will be made to existing user accounts. If already existing users in gateway also exists in CSV file, then already existing users will be unchanged and remaining user will be added in gateway.

- If “update existing user accounts and append new ones (if any)” is selected, then already existing users in gateway will get updated and remaining users of CSV will be added in gateway.
- If “Replace all user accounts” is selected, then existing users in gateway will be removed from gateway and all the users existing in CSV will be added in gateway.

Once CSV is uploaded, administrator can download the list of incorrect entries so that administrator can correct those entries.



After importing the users by CSV, administrator can see the number of successful entries, skipped entries and failed entries. The Administrator can also download the list of failed entries from the same page.

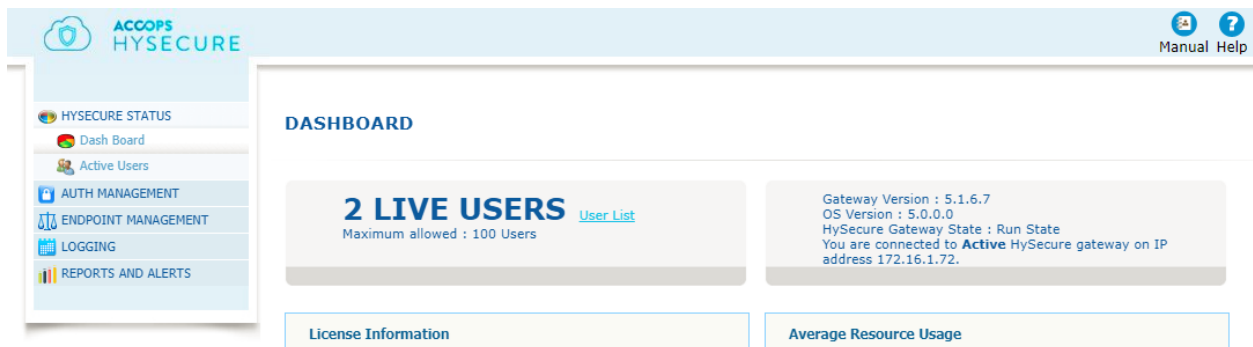


ROLE BASE ADMINISTRATION SUPPORT

Now security officer can create monitor user on HySecure gateway for log monitor purpose. This monitor user has read only access and this user has access of following options.

- Dash Board
- Active Users
- User Profiles
- Device Management
- Activity Log.
- User log
- Admin Log
- HyID Log
- EndPoint Security Log
- Log Download
- Syslog Configuration
- General Reports
- User Base report
- Domain Base Report
- Application Base Report

Monitor user can view the log and download the log files from HySecure. But not able to modify any setting on HySecure.



For creating monitoring user, login as security officer and open management page. Go to Auth Management→Local Users. Here creates user with role as monitoring. Monitor user is certificate user, so after user is created on HySecure passphrase will be created. And user will need to enroll this passphrase like certificate user.

CREATE USER

* Mandatory fields.

User Name*	Monitor
User E-mail Address*	info@accops.com
Administrator E-mail Address*	support@accops.com
Mobile number	
Class	User
Role	Low Security User
Hostname	Low Security User
User must change password at next logon	High Security User
Password never expires	Administrator
Send details via email	Security Officer
Send details on mobile	Monitoring User
Account is disabled	
Account expires on	DD MM YY
Login details	
User ID*	
Password*	
Confirm Password*	

ACCOPS RMS INTREGATION

In this release Accops RMS has been integrated with HySecure. Administrator can configure RMS as application on HySecure and then user can access RMS VDI using HyLite only.

After successfully applying the patch on HySecure gateway please follow below steps for RMS configuration.

RMS mode is a special mode of HySecure web portal for users. RMS must be configured in shell so that users can access the RMS portal via HySecure web portal.

To configure RMS on HySecure, follow these steps:

1. Take SSH access to Primary gateway of HySecure HA cluster.
2. Edit web server configuration file "/etc/httpd/conf/httpd.conf" using vi editor.
#sudo vi /etc/httpd/conf/httpd.conf
3. Enter Primary RMS server and secondary RMS server IP address in case of RMS HA setup as shown below in snapshot. If RMS setup is standalone, then edit primary RMS Server IP address and comment the line to edit the secondary RMS Server IP address.
4. Save this file using below command;
5. Press Esc key and then: x!

```
Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e; path=/" env=BALANCER_ROUTE_CHANGED
<Proxy "Balancer://rmscluster">
  BalancerMember "https://10.0.2.105" route=pri
  BalancerMember "https://10.0.2.106" route=sec
  ProxySet stickySession=ROUTEID
</Proxy>
<Location /RMS/>
  Order allow,deny
  Allow from all
  SetEnv proxy-nokeepalive 1
  SetEnv proxy-initial-not-pooled 1
  ProxyPass balancer://rmscluster/RMS/
  ProxyPassReverse balancer://rmscluster/RMS/
</Location>
```

Enter Primary RMS server IP address

Enter Secondary RMS Server IP address

6. Restart httpd service on primary gateway using below command
"systemctl restart httpd"
7. Changes will sync to all other nodes in HA cluster. No need to do this step on other gateways in HA cluster.
8. Login as security officer, go to Access management→Applications
9. Add new application with application type as HyWorks controller (Primary) and HyWorks controller (Secondary) in case of HyWorks HA Setup. If HyWorks setup is standalone, then add only HyWorks controller (Primary).
10. Add a Network type application and Publish VDI range for RMS VDIs.
11. Go to Host configuration→Client Settings, enable RMS mode under Web portal logon mode selection.

HOST CONFIGURATION

- Network Configuration
- Route Configuration
- Proxy Server
- SMTP Server
- SMS Gateway
- Global Settings
- Client Settings
- Password Expiry Time
- Database Password
- SSH Configuration
- Virtual Server
- HyLite Configuration

Force install TSE Client. Do not ask user for install/upgrade confirmation

Version of the Proprietary TSE Client in format a.b.c.d, like 6.5.3.0

TSE Client MSI Installer download URL. (Recommended: Point this URL to local TSE server path).

7.0.3.0

http://bit.ly/TSEClientv7MSINE

Submit

Web Portal logon mode selection

Enable RMS mode. ☒

Enable HyLite mode. ☒

Enable Hybrid mode. ☒

Select Default logon mode.

HyLite Mode

Submit

SAML IDENTITY FEDERATION SUPPORT

SAML service provider support has been added on HySecure in this release. After integrating SAML identity provider as authentication server, HySecure will authenticate user from SAML IDP and HySecure gateway will act as service provider.

Also, SAML as identify provider can be configured on HySecure using console access.

Please follow below steps for configure SAML IDP as authentication server on HySecure

1. Go to "Authentication Servers" and click on add → "SAML IDENTITY PROVIDER".

CREATE AUTHENTICATION SERVER

Select server type

- ☒ AD/LDAP
- ☐ RADIUS
- ☐ ProID
- ☐ SAML IDENTITY PROVIDER

2. In General Settings → "Upload Idp Metadata" tab, choose the metatdata.xml file and upload. This metadata xml file will be provided by SMAL IDP.

The screenshot displays the 'ADD IDENTITY PROVIDER' configuration page in the HySecure console. The left sidebar shows the navigation menu with 'AUTHENTICATION' selected. The main content area is titled 'ADD IDENTITY PROVIDER' and contains a 'SAML CONFIGURATIONS' section. Within this section, the 'GENERAL SETTINGS' tab is active. The 'Upload Idp Metadata' button is highlighted with a red box. Below it, the 'Identity Provider Name' is set to 'SAML 2.0'. The 'SAML PROTOCOL SETTINGS' section includes fields for 'IdP Issuer URI', 'IdP Single Sign-On URL', and 'IdP Signature Certificate'. The 'SERVICE PROVIDER SETTINGS' section includes fields for 'SP Issuer URI', 'Assertion Consumer Service URL', 'SP Initiated URL', and 'Name ID Format'. The 'AUTHENTICATION SETTINGS' section includes fields for 'IdP Username', 'SAML Email Attribute', and 'SAML Mobile No. Attribute'. The 'Submit' and 'Reset' buttons are at the bottom.

3. Give the Identity Provider Name which administrator want to give.
4. After uploading the Metadata.xml file the rest of the data fields will be populated automatically.
5. In "SERVICE PROVIDER SETTINGS" → "SP Issuer URI" → Give the IP address of the gateway where you are configuring ADFS.
 - a. Take similar steps for "Assertion Consumer Service URL" and "SP Initiated URL". Replace the hostname with IP of the gateway.

ACCOPS HYSECURE

ADD IDENTITY PROVIDER

SAML CONFIGURATIONS

GENERAL SETTINGS

Upload IdP Metadata : Federation_1a (3).xml

Identity Provider Name * :

Identity Provider Protocol : SAML 2.0

SAML PROTOCOL SETTINGS

IdP Issuer URI * :

IdP Single Sign-On URL * :

IdP Signature Certificate * :

Issuer : CN=ADFS Signing - adfs.accops.com
Expiration : Nov 6 11:00:25 2018 GMT

Request Binding :

Request Signature : ☐ Sign SAML Authentication Requests

Response Signature Verification :

Response Signature Algorithm :

SERVICE PROVIDER SETTINGS

SP Issuer URI * :

Assertion Consumer Service URL * :

SP Initiated URL * :

Name ID Format * :

AUTHENTICATION SETTINGS

IdP Username :

SAML Email Attribute :

SAML Mobile No. Attribute :

6. Click on Submit.
7. Add ADFS in the Authentication Domain and HySecure Domain.

NEW HYLITE MODE

In this release new HyLite version has been added. So now there are two clientless versions HyLite and HyLite Pro (older one). By default, HyLite Pro is selected. If administrator want to change the HyLite then go to Host Configuration → HyLite Configuration and select Default RDP client from drop down list.

HyLite Pro is yearly subscription base license. So, after completing one year, HySecure client less access mode will automatically use HyLite mode.

HyLite Settings

RDP client

Default RDP client

HyLite Pro
HyLite
HyLite Pro

SEPARATE HYID POLICY FOR HYSECURE AND HYID DESKTOP AGENT

In this release HyID policy configuration options have been changed. Now separate HyID policy need to be created for HySecure login and HyID desktop agent login. If administrator wants to apply HyID for HySecure login then HyID policy type should be HySecure.

CREATE HYID POLICY

HyID Policy Name

TestHyIDPolicy

HyID Policy Description

HyID Policy Type

HySecure

User Database

Select Authentication Domain

DefaultAuthDomain

Select Authorization Server

PTPL AD

Select Policy assignment Type

User Groups

Select User Group

Search a Group...

All Groups
WseAllowShareAccess
WseAllowComputerAccess
WseAllowMediaAccess
WseAllowAddInAccess
WseAllowDashboardAccess
WseAllowHomePageLinks
Allowed RODC Password Replic
allusers
outall

Add >>
Delete <<

HySecure Authentication

☒ Enable Two factor authentication
☐ Disable Two factor authentication

Select tokens

Email Token	<input checked="" type="checkbox"/>
SMS Token	<input checked="" type="checkbox"/>
Email and SMS Token	<input type="checkbox"/>
Mobile Token	<input checked="" type="checkbox"/>

Email and SMS OTP Configuration

Select OTP token length: 06 digit
 Select OTP token expiry time: 05 min
☐ Enable OTP token use for multiple time
 Select OTP token regenerate timeout: 30 sec

Mobile token configuration

Select OTP token length: 06 digit
 Select OTP token expiry time: 05 min
☒ Enable OTP token use for multiple time
 Select OTP token regenerate timeout: 30 sec
☒ Enable self-service mobile token registration for users.
☒ Allow re-activation of same device.
 Allow multiple mobile devices per User: 01 devices

Common OTP Configuration

☐ Account lockout on number of failed attempts: 02
 Account Lockout Time: 10 min

Risk Based Profile Configuration

☐ Disable OTP for WAN IP addresses
 Specify comma separated IP Addresses, Subnet and IP Range

Enter comma separated IP addresses, Subnet and Range

NEW HYID DESKTOP AGENT POLICY CONFIGURATION

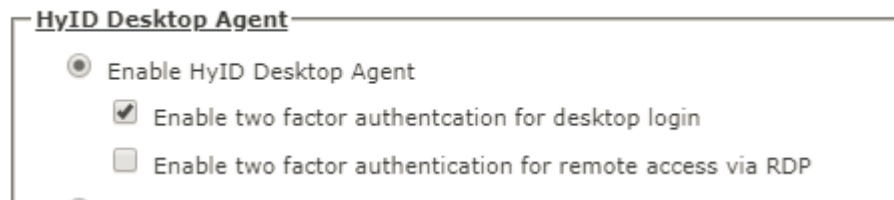
Enabled two factor authentications for windows login, HyID desktop agent need to install on windows machine. And on HySecure server HyID policy need to create for desktop agent. This HyID desktop agent setting will be push to all windows machine at the time of login.

ENABLE HYID DESKTOP AGENT:

If this option is enabled, then only HyID desktop agent policy will be applied for specified user/user group/OU. After enabling this option, administrator needs to select at least one of the options mentioned below.

Enable two factor authentications for desktop login: If enabled, users will have to provide OTP to login into the desktop/server console.

Enable two factor authentications for remote access via RDP: If enabled, user will have to provide OTP when he/she attempts to initiate RDP to the target machine which has HYID desktop agent. If disabled, users will be able to RDP to the target machine without specifying OTP.

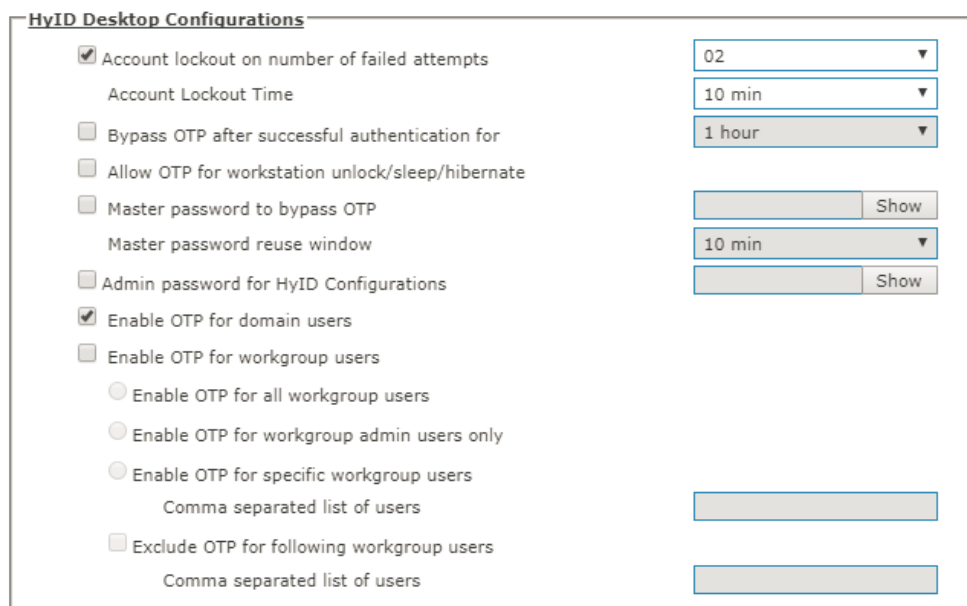


HyID Desktop Agent

- ☒ Enable HyID Desktop Agent
 - ☒ Enable two factor authentication for desktop login
 - ☐ Enable two factor authentication for remote access via RDP

HYID DESKTOP CONFIGURATIONS

This is HyID desktop agent advance configuration setting. These HyID agent configuration settings will be pushed from HyID server to all HyID agents. HyID desktop configuration setting will be pushed whenever HyID agent communicates with the HyID server.



HyID Desktop Configurations

- ☒ Account lockout on number of failed attempts: 02
 - Account Lockout Time: 10 min
- ☐ Bypass OTP after successful authentication for: 1 hour
- ☐ Allow OTP for workstation unlock/sleep/hibernate
- ☐ Master password to bypass OTP: [] Show
 - Master password reuse window: 10 min
- ☐ Admin password for HyID Configurations: [] Show
- ☒ Enable OTP for domain users
- ☐ Enable OTP for workgroup users
 - ☐ Enable OTP for all workgroup users
 - ☐ Enable OTP for workgroup admin users only
 - ☐ Enable OTP for specific workgroup users
 - Comma separated list of users: []
- ☐ Exclude OTP for following workgroup users
 - Comma separated list of users: []

- **Account lockout on number of failed attempts:** User account will be locked after the specified number of failed login attempts.
- **Account Lockout Time:** Once the user is locked after failed attempts, this configuration would indicate the duration for which the user account will be locked.
- **Bypass OTP after successful authentication for:** This configuration indicates the time for which OTP will not be requested after a successful authentication. After that time duration automatically, OTP will be asked again.
- **Allow OTP for workstation unlock/sleep/hibernate:** If this option is enabled then the user will need to provide OTP when he/she tries to unlock the system OR recover from the system which has gone into sleep or hibernate mode.
- **Master password to bypass OTP:** Admin can configure the master password, which can be used on the end user's machine, to bypass OTP. The duration for which this password will be valid is indicated by the configurable field indicated next.

- **Master password reuse window:** This is the period for which the above-mentioned master password can be used.
- **Admin password for HyID Configurations:** Specifies the admin password needed to change HyID agent configuration settings on end user's machine.
Without the admin password, HyID configuration setting on end user's machine will not be editable.
- **Enable OTP for domain users:** If this option is enabled then all domain users will need to enter OTP at the time of login onto windows machine. Otherwise HyID agent will bypass OTP for domain users.
- **Enable OTP for workgroup users:** If this option is enabled then workgroup users as per the subsequent configurations will need to enter OTP at the time of login into windows machine. Otherwise HyID agent will bypass OTP for workgroup users.
- **Enable OTP for all workgroup users:** If this option is enabled then all workgroup user will need to enter OTP at the time of login onto windows machine
- **Enable OTP for workgroup admin users only:** If this option is enabled then local machine's admin user needs to enter OTP at the time of login into windows machine.
- **Enable OTP for specific workgroup users:** If this option is enabled then only specified workgroup users (local machine users) need to enter OTP at the time of login onto windows machine. Rest of the local machine users can login without OTP. Here admin can specify multiple users list in a comma separated form.
- **Exclude OTP for following workgroup users:** If this option is selected then the specified users (local machine users) can login onto windows machine without OTP. Here admin can specify multiple users list in a comma separated form.

OFFLINE OTP CONFIGURATION:

Here administrator can configure offline mobile token configuration settings. These configuration settings will be configurable when mobile token option is enabled.

- **Enable Offline OTP token:** If this option is enabled, then offline mobile token option will be available for end user. Otherwise end user will not be able to login if HyID agent is not reachable from HyID server.
 - **Select Offline OTP token expiry time:** After enabling offline OTP token, administrator needs to select Offline token expiry time so that after the specified time interval, offline token will get expired.
 - **Maximum login attempts using Offline OTP:** Here administrator can specify the number of times end user can login using offline token. If max limit is reached, end user will not be able to login using offline token.

Offline OTP Configuration

☒ Enable Offline OTP token

Select Offline OTP token expiry time 01 min ▼

Maximum login attempts using Offline OTP 01 ▼

NEW CONTROL FOR UPLOAD/DOWNLOAD FILE USING HYLITE

Administrator can control end user file upload/download using this option. There are four options which administrator can configure on HyLite configuration page.

- Enable upload/download
- Upload only
- Download only
- Disable upload/download

Enable upload/download: This option will allow end user to upload and download file using HyLite.

Upload only: This option will allow end user to only upload file using HyLite. File download feature will be disabled.

Download only: This option will allow end user only download file using HyLite. File upload feature will be disabled.

Disable upload/download: This option will disable end user for upload and download file using HyLite. Both File upload and download will be disabled.

Local Settings

Enable Clipboard ☒

Enable Printing ☒

Enable RDP plugins redirection. ☒

Enable plugins for DeviceID/EPS. ☐

Enable HyPrint PDF Printer redirection. ☒

Enable Shared Drive Redirection (It also enables uploading/downloading of files. Drag files to your screen after connected). ☒

Choose options for file Uploading/Downloading. Enable Upload/Download ▼

Advanced Settings

Enable Desktop background ☐

Enable Upload/Download

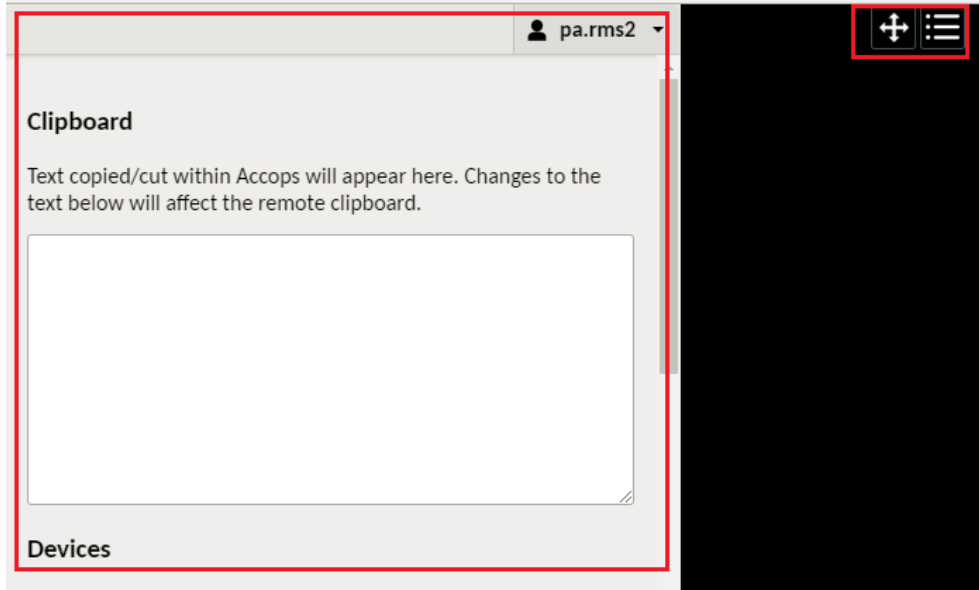
Download only

Upload only

Disable Upload/Download

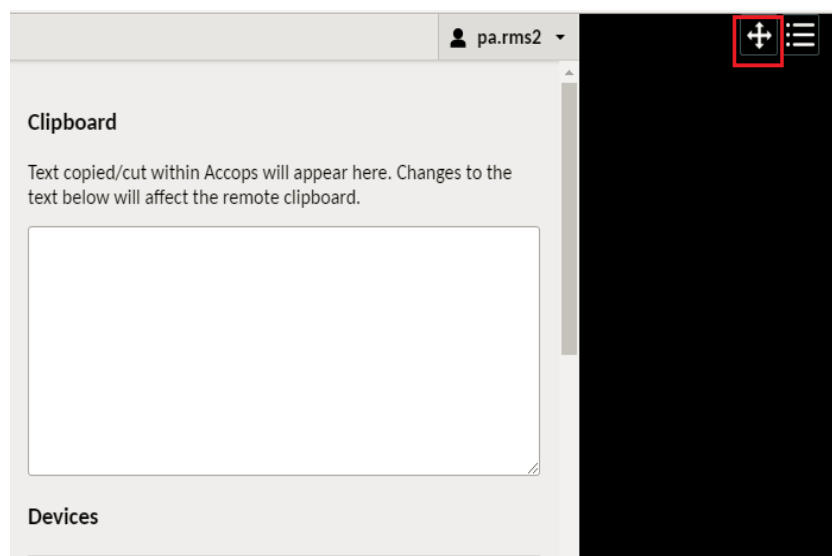
NEW MENU OPTION ON HYLITE RDP PAGE

In this release new HyLite menu option is available on RDP access page. If user click on menu option, HyLite menu will be available on left side the screen. Using this menu option user can do copy-paste, file upload -download etc.



OPTION TO DRAG MENU ON HYLITE RDP PAGE:

After login into RMS VDI, User can drag the menu option anywhere on the screen using this option. It will give end user better usability.



RISK BASED OTP PROFILE CONFIGURATION

If there is a need to bypass OTP for a specific IP or a network, then single/multiple IP address, IP Range or a subnet can be configured for which OTP will be disabled. The IP address considered is the WAN IP address of the user visible to HyID server. If the user is behind a proxy server or a NAT server, the WAN IP address of the user is considered as the proxy server IP or NAT server IP address. Administrator can specify comma separated multiple IP address, subnet or IP address range.

One use case for this feature is when OTP is to be disabled for LAN users, but it must be enabled for users coming in from outside the corporate network. This option is available Auth Management->HyID Policy

Text field disabling OTP for WAN IP address intake capacity to 2048. Now administrator can input 2048 characters in this field. (Commas included)

The format for entering the details are:

IP Address: A.B.C.D (e.g. 10.2.234.23)

Subnet number: A.B.C.D/XX (e.g. 10.2.234.0/24)

IP address range: A.B.C.D – W.X.Y.Z. (e.g. 10.2.234.10-10.2.234.30)

E.g. data:

10.2.234.23,10.2.234.0/24,10.2.234.10-10.2.234.30

Risk Based Profile Configuration

☐ Disable OTP for WAN IP addresses
Specify comma separated IP
Addresses, Subnet and IP Range

Enter comma separated IP addresses,
Subnet and Range

HYID SUPPORT FOR LDAP USER

In this build, HySecure administrator can create HyID policy for LDAP user also. And then the user can login using OTP into HySecure gateway. While configuring LDAP as authentication server on HySecure, please verify LDAP attribute name for email and mobile number. Otherwise HySecure gateway may not be able to fetch user's email and mobile number from LDAP server.

EDIT AD/LDAP AUTHENTICATION SERVER

Server Name	LDAP
IP Address/Host Name	172.███.███.███
Port	389
Admin Bind DN	cn=admin,dc=labs,dc=accops,dc=...
Admin Password	*****
Base DN	dc=labs,dc=accops,dc=com
User Search Attribute	cn
User Group Search Attribute	memberOf
User Email Address Attribute	mail
User Mobile Number Attribute	telephoneNumber
Enable SSL	<input type="checkbox"/>

LDAP HyID policy can be created for the following

- All users
- Specific user
- All groups

Policy assignment type should be user or user group while creating HyID policy. HyID Policy for LDAP Organization unit is not supported.

CREATE HYID POLICY

HyID Policy Name	HyIDForLDAP
HyID Policy Description	
HyID Policy Type	HySecure
User Database	
Select Authentication Domain	LDAP
Select Authorization Server	LDAP
Select Policy assignment Type	Select option
Select User Group	Select option Users User Groups Organizational Unit
<input type="text" value="Search a Group..."/>	
<input type="button" value="Add >>"/>	<input type="button" value="Delete <<"/>

Also, HySecure administrator can disable OTP for specific LDAP user by creating HyID policy for the specific user and select disable OTP option.

Administrator can see the HyID log for LDAP user.

ENHANCEMENT IN 5.1.5169

UPDATED ACCOPS LOGO

New Accops logo has been updated in this upgrade patch. After applying this upgrade patch HySecure web portal logo will change into latest logo.

NEW HYSECURE CLIENT

This release contains new HySecure windows client version 5.0.9.0. In this client some critical bugs related to HyWorks has been fixed. Also, login time has been reduced in this client.

IMPROVED PERFORMANCE OF REMOTE MEETING

In this release performance of remote meeting has been improved. In previous release, access to remote meeting was slower. In this Windows client release, access to remote meeting has become faster.

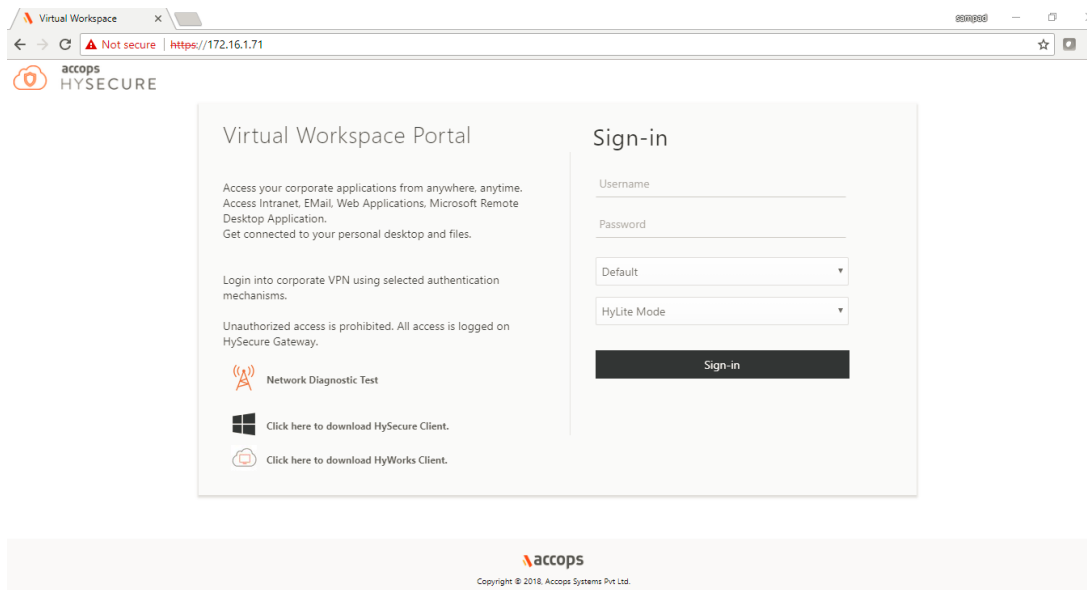
User needs to install HySecure windows client version 5.0.9.0 for faster access and better performance of Remote meeting.

UAC SUPPORT IN REMOTE MEETING

In previous release, during remote session if UAC pop up shows on remote machine, then meeting got disconnected. This issue has been fixed in this release.

NEW PORTAL UI

HyLite and Hybrid portal UI has been changed in this release. After applying upgrade patch portal UI will change. Now HySecure domain name will be display below password field.



SECURITY ISSUES FIXED IN 5.1.569

Multiples vulnerabilities are fixed in this release. Please find the CVE details which are fixed in this upgrade patch.

CVE-2016-10707 (<https://nvd.nist.gov/vuln/detail/CVE-2016-10707>)
CVE-2015-9251 (<https://nvd.nist.gov/vuln/detail/CVE-2015-9251>)
CVE 2018-5712 (<https://nvd.nist.gov/vuln/detail/CVE 2018-5712>)
CVE 2017-16642 (<https://nvd.nist.gov/vuln/detail/CVE 2017-16642>)
CVE 2017-11362 (<https://nvd.nist.gov/vuln/detail/CVE 2017-11362>)
CVE-2018-7584 (<https://nvd.nist.gov/vuln/detail/CVE-2018-7584>)
CVE-2018-5711 (<https://nvd.nist.gov/vuln/detail/CVE-2018-5711>)
CVE-2017-12934 (<https://nvd.nist.gov/vuln/detail/CVE-2017-12934>)
CVE-2017-12933 (<https://nvd.nist.gov/vuln/detail/CVE-2017-12933>)
CVE-2017-12932 (<https://nvd.nist.gov/vuln/detail/CVE-2017-12932>)
CVE-2017-11628 (<https://nvd.nist.gov/vuln/detail/CVE-2017-11628>)
CVE-2017-11145 (<https://nvd.nist.gov/vuln/detail/CVE-2017-11145>)
CVE-2017-11144 (<https://nvd.nist.gov/vuln/detail/CVE-2017-11144>)
CVE-2017-7890 (<https://nvd.nist.gov/vuln/detail/CVE-2017-7890>)
CVE 2016-6662 (<https://nvd.nist.gov/vuln/detail/CVE 2016-6662>)
CVE-2017-15365 (<https://nvd.nist.gov/vuln/detail/CVE-2017-15365>)
CVE-2017-3302 (<https://nvd.nist.gov/vuln/detail/CVE-2017-3302>)
CVE-2016-2047 (<https://nvd.nist.gov/vuln/detail/CVE-2016-2047>)
CVE-2016-6664 (<https://nvd.nist.gov/vuln/detail/CVE-2016-6664>)
CVE-2016-6663 (<https://nvd.nist.gov/vuln/detail/CVE-2016-6663>)
CVE-2016-5629 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5629>)
CVE-2016-5626 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5626>)
CVE-2016-5612 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5612>)
CVE-2016-5584 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5584>)
CVE-2016-5444 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5444>)
CVE-2016-5440 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5440>)
CVE-2016-3615 (<https://nvd.nist.gov/vuln/detail/CVE-2016-3615>)
CVE-2016-3521 (<https://nvd.nist.gov/vuln/detail/CVE-2016-3521>)
CVE-2016-3477 (<https://nvd.nist.gov/vuln/detail/CVE-2016-3477>)
CVE-2016-3452 (<https://nvd.nist.gov/vuln/detail/CVE-2016-3452>)
CVE-2016-0666 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0666>)
CVE-2016-0650 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0650>)
CVE-2016-0649 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0649>)
CVE-2016-0648 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0648>)
CVE-2016-0647 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0647>)
CVE-2016-0646 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0646>)
CVE-2016-0644 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0644>)

CVE-2016-0643 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0643>)
CVE-2016-0641 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0641>)
CVE-2016-0640 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0640>)
CVE-2016-0616 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0616>)
CVE-2016-0609 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0609>)
CVE-2016-0608 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0608>)
CVE-2016-0606 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0606>)
CVE-2016-0600 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0600>)
CVE-2016-0598 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0598>)
CVE-2016-0597 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0597>)
CVE-2016-0596 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0596>)
CVE-2016-0546 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0546>)
CVE-2016-0505 (<https://nvd.nist.gov/vuln/detail/CVE-2016-0505>)
CVE-2015-3152 (<https://nvd.nist.gov/vuln/detail/CVE-2015-3152>)
CVE-2018-2582 (<https://nvd.nist.gov/vuln/detail/CVE-2018-2582>)
CVE-2017-3231 (<https://nvd.nist.gov/vuln/detail/CVE-2017-3231>)
CVE-2016-5597 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5597>)
CVE-2016-5582 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5582>)
CVE-2016-5573 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5573>)
CVE-2016-5568 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5568>)
CVE-2016-5556 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5556>)
CVE-2016-5554 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5554>)
CVE-2016-5542 (<https://nvd.nist.gov/vuln/detail/CVE-2016-5542>)
CVE-2018-2639 (<https://nvd.nist.gov/vuln/detail/CVE-2018-2639>)
CVE-2018-2638 (<https://nvd.nist.gov/vuln/detail/CVE-2018-2638>)
CVE-2018-2627 (<https://nvd.nist.gov/vuln/detail/CVE-2018-2627>)
CVE-2017-10309 (<https://nvd.nist.gov/vuln/detail/CVE-2017-10309>)

ISSUES FIXED IN 5.0.5169

CA CERTIFICATE VALIDITY 1 YEAR.

In previous release HySecure CA certificate validity was 1 year. After applying this patch HySecure gateway CA certificate validity will change to 10 years.

RADIUS USER LOGIN ISSUE.

Radius authentication server module was broken in previous release. And radius user not able to login onto HySecure. This issue is resolved in this release.

ADMIN LOG AND USER ACTIVITY LOG SHOWING NA.

In previous release HySecure NA is showing in some field on admin log as well as user activity log. Now this NA display issue has been resolved. It will display proper data.

EMAIL AND SMS NOTIFICATION WHILE CREATING LOCAL USER

In previous release of HySecure while creating local user email and SMS not sending to created user. This issue has been fixed in this release. Please make sure that for SMTP and for SMS gateway is configured on HySecure server.

JAPANESE KEYBOARD SUPPORT IMPROVED

Using HyLite, Japanese keyboard has been improved. Lots of Japanese special key was not working in previous release. This issue has been fixed in this release.

JAPANESE LANGUAGE SUPPORT IN RMS PORTAL

Earlier, on accessing RMS portal all messages were available in English on Japanese OS. In this build, all the messages will be available in Japanese language on Japanese OS and Japanese browser.

NETWORK TYPE APPLICATION ISSUE

In previous release, some RMS VDI were inaccessible even if the network range was published in HySecure. In this release this issue has been fixed.

KNOWN ISSUES IN 5.1.5169

RMS CONFIGURATION NEED TO DO MANUALLY AFTER UPGRADE PATCH

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

RMS NOT WORKING ON STANDALONE GATEWAY

On HySecure standalone gateway RMS will not work.

SOMETIMES HYSECURE MANAGEMENT PAGE IS SHOWING ACCESS DENIED

While logging as security office and access HySecure management page sometimes it is showing access denied error message.

Workaround: Need to refresh page or close the page and login again as security officer.

ON ACTIVE USER PAGE, IP ADDRESS IS SHOWING 0.0.0.0 WHEN USER LOGIN USING HYLITE ON IE BROWSER.

IP address is showing 0.0.0.0 value on HySecure Active user page, if user is login using IE browser.

DEVICE ID ISSUE

On HySecure gateway if device id is configured only for browser. And if user first time login using client, then user can login from any browser.

MULTIPLE VDI POWER ON OPTION NOT WORKING USING HYLITE

If one user has more than one VDI machines and user try to power on all VDI machines from HyLite portal at a time, then only one VDI machine will power on. So, if user wants to power on multiple VDI machine. Then first power on one machine first, once it is up then trying to power on another machine.

APPLICATION RECONNECT DOES NOT WORK WITH SHELL MODE.

On HyWorks in connection profile shell mode is enabled. Then HyLite does not support application reconnect in shell mode.

WHITE SPACE ON FULL SCREEN ON APP MODE

On HyWorks if application published as remote app mode. Then login and launch application using HyLite portal. After launching click on full screen button. While launching application on full screen mode there will be white space on below of the page.

OLDER OS VERSION ISSUE IN OS CONSOLE

In previous release, after applying upgrade patch HySecure OS version was not upgraded in OS console. This issue has been fixed in this release.

HYLITE LOG FILE DOWNLOAD OPTION NOT AVAILABLE FROM MANAGEMENT PAGE.

In this release, there is no option to download HyLite logs from management page. Administrator can download HyLite log from backend using WINSCP tool.

COPY-PASTE FROM REMOTE M/C TO LOCAL MACHINE: CTRL+C, CTRL+V SUPPORTED. RIGHT CLICK COPY-PASTE OPTION NOT SUPPORTED

Copy-paste option from RMS VM to local machine using right click option is not supported.

INCORRECT IDLE TIME ON ACTIVE USERS PAGE

On HySecure Active user page, idle time is showing wrong time. Although user is using RMS VM still on HySecure active user page idle time keeps on increasing.

ON SAFARI BROWSER, ACCOPS HYPRINT DOES NOT WORKING

On MAC OS, safari browser does not support HyPrint using HyLite.

IF PDF IS NOT INSTALLED ON LOCAL MACHINE, THEN USING IE 11 BROWSER PDF FILE WILL DOWNLOAD WHILE GIVING PRINT USING ACCOPS PRINTER

If PDF 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.

IF PDF IS NOT INSTALLED ON LOCAL MACHINE, THEN USING EDGE BROWSER, PRINT OPTION NOT SHOWING WHILE GIVE PRINT USING ACCOPS PRINTER/ACCOPS HYPRINT

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

NO RESOLUTION ADJUSTMENT FOR REMOTE SESSION, IF BROWSER WINDOW IS RESIZED.

After launching RDP using HyLite, if user do browser resize then RDP screen will not adjust the screen size accordingly.

HYID ACCOUNT LOCK OUT TIME DOES NOT WORKING.

HyID account lock out time is not supported in this version. It will be fixed in next version.

HYLITE SHARED DRIVE TAKES TIMES TO MAP

While launch RMS VM using HyLite, HyLite shared drive called takes time to display on the screen.

IN UPLOAD ONLY MODE: ON DRAGGING FILES INTO DOWNLOAD FOLDER, FILES DISAPPEAR AND THEN REAPPEAR ON REFRESHING.

If upload only is configured on HyLite configuration page. Then while dragging file into download folder on HyLite shared drive, file will have disappeared. And then re-appear on refresh option.

IN UPLOAD ONLY MODE: ACCOPS HYLITE PRINTER OR ACCOPS HYPRINT WILL NOT WORK

If upload only is configured on HyLite configuration page. Then user will not be able to give print using Accops printer or Accops HyPrint. Download option should be enabled on HyLite configuration page for printing.

SOMETIMES RMS VM LAUNCHING ISSUE

While launching RMS VM using HyLite, sometimes it will show message like "Please wait while connecting" and not able to connect to VM. But if user refresh or relaunch RMS VM then it will connect to VM.

APPENDIX A: UPGRADING HYSECURE CLUSTER

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

To upgrade HySecure cluster, follow these main steps:

- Upgrade the HySecure Standby Cluster Manager Node
- Upgrade the Dedicated HySecure Gateway Node First
- Upgrade the HySecure Active Cluster Manager Node

Here are the downtime scenarios to consider

Upgrade HySecure Standby Node	Cluster status is unaffected. If HySecure gateway is active on this node, this load will be disrupted. Load is shared by other gateway nodes in the cluster	Users' active connection to this HySecure Gateway node will be disconnected. Users do not have to re-authenticate.
Upgrading Dedicated HySecure Gateway Node	Load on HySecure Gateway node is disrupted. Load is shared by other Gateway nodes in the cluster. Cluster status is unaffected	Users' active connection to this HySecure Gateway node will be disconnected. Users do not have to re-authenticate.
Upgrade HySecure Active Node	Cluster failover will happen. Temporary delay in routing connection from current active to standby. Standby node will become Active. If HySecure gateway is active on this node, this load will be disrupted. Load is shared by other gateway nodes in the cluster.	Users' active connection to this HySecure Gateway node will be disconnected. New user sessions while standby was being upgraded, will be become invalid and such users must re-login. Any configuration changes done on HySecure Active node will not be preserved and will be lost.

It is recommended to keep a downtime of 30 minutes per gateway node in the cluster. If there are 3 nodes, it is recommended to take 1.5 hours of downtime.

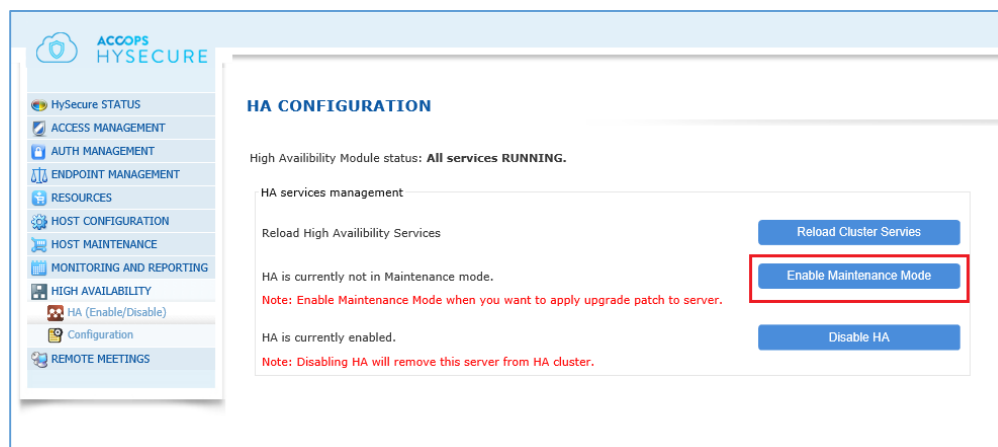
UPGRADING STANDBY HYSECURE CLUSTER MANAGER NODE:

1. 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.

2. Open management console and make sure you are connected to the Standby HySecure Cluster Manager node that you intend to upgrade.
3. Go to "HA Configuration" page and put the HySecure node in maintenance mode by clicking on "Enable Maintenance Mode"

Note: After this step, this gateway node will stop being part of the cluster and it will not show any cluster related status.



4. Please make the status for "High Availability Module Status" changes from "All services RUNNING" to "HA is in maintenance mode. All syncing services stopped properly. Maintenance/Upgrade activity can be performed now.". Please refresh the web page and wait till this message appear on screen.
5. Go to "HySecure Gateway State" page under "HySecure STATUS" section and put the HySecure gateway in "Configuration Mode".

Note: after this step, all active user connections to this gateway node will be disconnected.

6. Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option **Firmware Upgrade** and upload the HySecure Upgrade patch file.
7. It may take 10 minutes or more to upload the upgrade patch based on network bandwidth between your PC and Gateway.
8. Once the upgrade file is uploaded and upgrade patch 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.

9. Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on **View Logs** button to check the patch installation logs. In the last it should mention "successfully applied."
10. Keep the gateway in configuration and maintenance mode.
11. This node will be made active after upgrading the dedicated HySecure Gateway nodes as well.

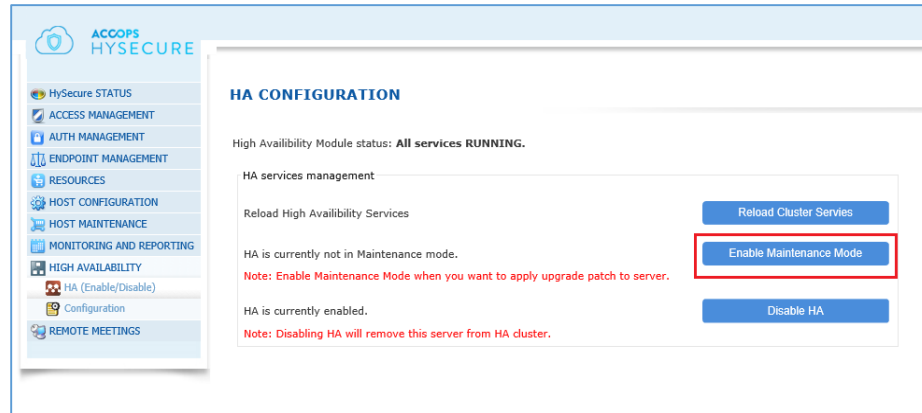
UPGRADING DEDICATED HYSECURE GATEWAY NODE:

1. Connect to Dedicated HySecure gateway as Security Officer.
Note: Do not connect using Virtual IP Address
2. Open management console and make sure you are connected to the dedicated HySecure Gateway node that you intend to upgrade.
3. Go to "HA Configuration" page and put the HySecure node in maintenance mode by clicking on "Enable Maintenance Mode"
Note: After this step, this gateway node will become inactive cluster node.
4. Go to "HySecure Gateway State" page under "HySecure STATUS" section and put the HySecure gateway in "Configuration Mode".
Note: after this step, all active user connections to this gateway node will be disconnected.
5. Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option **Firmware Upgrade** and upload the HySecure Upgrade patch file.
6. It may take 10 minutes or more to upload the upgrade patch based on network bandwidth between your PC and Gateway.
7. Once the upgrade file is uploaded and upgrade patch 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.
8. Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on **View Logs** button to check the patch installation logs. In the last it should mention "successfully applied."
9. Keep the gateway in configuration and maintenance mode.
10. Repeat above steps for all Dedicated HySecure Gateway nodes, if there are multiple dedicated HySecure Gateway nodes added to cluster.

BRING THE CLUSTER UP AGAIN

1. Do the HA Failover
 - a. Connect to **Active** HySecure Cluster Manager node as Security Officer.
Note: Do not connect using Virtual IP Address
 - b. Open management console and make sure you are connected to the Active HySecure Cluster Manager node.
 - c. Go to "HA Configuration" page and put the HySecure node in "Maintenance Mode"

- d. Note: After this step, this gateway node will stop being part of the cluster and none of the nodes in the cluster will show the status of cluster.
 - e. Go to "HySecure Gateway State" page under "HySecure STATUS" section and put the HySecure gateway in "Configuration Mode".
 - f. Logout from HySecure client
2. Make New Active Node ready
- a. Connect to Standby HySecure Cluster Manager node as Security Officer.
- Note: Do not connect using Virtual IP Address**
- b. Open management console and make sure you are connected to the Standby HySecure Cluster Manager node.
 - c. Go to "HySecure Gateway State" page under "HySecure STATUS" section and put the HySecure gateway in "Run Mode".
 - d. HySecure client will log out, re-login into HySecure client as Security Officer.
 - e. Go to "HA Configuration" page and disable the Maintenance mode.



- f. On the same page, confirm that all services status is shown as OK.
 - g. Now disconnect Active HySecure node from the network or shutdown the Active HySecure node by connecting to HySecure Management console from HySecure OS Shell of Active.
 - h. After 10 seconds, confirm that the Standby HySecure node has become "Active"
3. Make Dedicated Gateways join cluster again and ready to accept connections
- a. Now login into each Dedicated HySecure Gateway Node as Security Officer
 - b. Go to "HA Configuration" page and disable the Maintenance mode.
 - c. On the same page, confirm that all services status is shown as OK.
 - d. Repeat above steps for each HySecure gateway nodes.
 - e. The cluster should be up now.

UPGRADING OLD (LAST) ACTIVE HYSECURE CLUSTER MANAGER NODE:

1. Connect to last Active HySecure Cluster Manager node as Security Officer.

Note: Do not connect using Virtual IP Address

2. This node is already out of cluster and must be in maintenance mode (on HA page) and Configuration state (on HySecure Status page).
3. Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option **Firmware Upgrade** and upload the HySecure Upgrade patch file.
4. It may take 10 minutes or more to upload the upgrade patch based on network bandwidth between your PC and Gateway.
5. Once the upgrade file is uploaded and upgrade patch 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.
6. Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on **View Logs** button to check the patch installation logs. In the last it should mention "successfully applied."
7. Go to "HA Configuration" page and disable the Maintenance mode.
8. On the same page, confirm that all services status is shown as OK.

Note: After above step, this node should become the standby node in the cluster and status of full cluster should be visible on the dashboard.

9. Ensure that the node has joined the cluster as standby

APPENDIX B: UPGRADING HYSECURE STANDALONE SETUP

The section describes the detailed process to upgrade HySecure standalone setup.

To upgrade HySecure standalone gateway, follow these main steps:

- Login as security officer.
- Go to "HySecure Gateway State" page under "HySecure STATUS" section and put the HySecure gateway in "Configuration Mode".
Note: after this step, all active user connections to this gateway node will be disconnected.
- Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option **Firmware Upgrade** and upload the HySecure Upgrade patch file.
- It may take 15 minutes or more to upload the upgrade patch based on network bandwidth between your PC and Gateway.
- Once the upgrade file is uploaded and upgrade patch 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 patch is applied successfully, gateway will reboot automatically.
- Again, Login as Security Officer and verify new version from HySecure dash board.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on **View Logs** button to check the patch installation logs.
- If everything is ok, then change HySecure state to **RUN** state.

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.



Accops, HyWorks, HyDesk, HyID, HyLite, HySecure and HyAssist are registered trademarks of Accops Systems Private Limited. Other names may be trademarks of their respective owners. Accops System has the right to change, modify, transfer or otherwise revise the publication without notice.

Tel: India +91 9595 277 001 | Europe +49 341 3315 78 30

Email: sales@accops.com | Web: www.accops.com

Copyright © 2018, Accops Systems Private Limited. All Rights Reserved.