



Release Notes

HySecure ISO 5.2 build 5200

Last Updated: 10 Sept 2018

Copyright © 2017, 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 to be a commitment on the part of Accops Systems Private Limited., and 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, EXPRESS 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 express 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

CONTENTS

Overview	6
How to Install HySecure 5.2 build 5200	6
How to get HySecure 5.2 build 5200	6
new feature in 5.2.5200	7
New dash board.....	7
Access control UI enhancements	8
Access control expiry	9
Access control for notification	10
Account lockout	11
Password policy.....	12
geo-fencing based EPS policy.....	14
WAN IP based EPS policy.....	16
domain based EPS policy.....	17
enhancement in 5.2.5200	20
UPDATED ACCOPS LOGO	20
HYSECURE DOMAIN CHANGE TO DEFAULT	20
NEW HYSECURE CLIENT.....	20
IMPROVED PERFORMANCE OF REMOTE MEETING.....	20
UAC SUPPORT IN REMOTE MEETING	20
NEW PORTAL UI	20
application access log	21
Security issues Fixed in 5.2.5200.....	22
Issues Fixed in 5.2.5200.....	22
Known Issues in 5.2.5200	23
new feature in 5.1.5169.....	27
Bulk user upload from managemnt page.....	27
role base administration support	29
Accops RMS intregation.....	30
saml identity federation support	32

New HyLite mode	34
separate HyID policy for hysecure and HyID desktop agent	35
New HyID desktop agent policy configuration.....	36
Enable HyID Desktop Agent:	36
Offline OTP Configuration:	38
New control for upload/download file using hylite	38
new menu option on Hylite RDP page	39
Option to drag menu on hylite RDP page:.....	40
risk based OTP profile configuration.....	40
Hyid support for ldap user.....	41
enhancement in 5.1.5169.....	43
Updated accops logo.....	43
new HySecure client.....	43
Improved performance of remote meeting.....	43
UAC support in remote meeting	43
New portal UI	43
Security issues Fixed in 5.1.569	45
Issues Fixed in 5.0.5169	47
Known Issues in 5.1.5169	48
How to Install HySecure 5.0 build 5087	51
How to get HySecure 5.0 build 5087	51
feature enhancement in 5.0.5087.....	51
Issues Fixed in 5.0.5087.....	52
Known Issues in 5.0.5087	53
How to Install HySecure 5.0 build 5080	56
How to get HySecure 5.0 build 5080	56
How to migrate from HySecure 4.7.4080 to 5.0.5080.....	57
New feature in 5.0.5080.....	58
feature enhancement in 5.0.5080.....	59
Issues Fixed in 5.0.5080.....	60
Known Issues in 5.0.5080.....	63
How to Install HySecure 5.0 build 5057	66

How to get HySecure 5.0 build 5057	66
How to migrate from HySecure 4.7.4080 to 5.0.5057	67
New Features in HySecure 5.0.5.7	67
Issues Fixed in 5.0.5057	72
Known Issues in 5.0.5057	73
How to Install HySecure 5.0 build 5035	76
How to get HySecure 5.0 build 5035	76
How to migrate from HySecure 4.7.4080 to 5.0.5035.....	77
New Features in HySecure 5.0.3.5	77
SECURITY ISSUES Fixed in 5.0.5035.....	84
Issues Fixed in 5.0.5035.....	86
Known Issues in 5.0.5035	88
Known Security Issues in 5.0.5035	90
How to get HySecure 5.0 build 5016.....	92
New Features in HySecure 5.0.1.6.....	92
Known Issues IN 5.0.5016.....	106
New Features in 5005	108
Known Issues in 5005.....	114

OVERVIEW

This document outlines the new features / bug fixes/ features enhancement/ known issues in the Accops HySecure 5.0. 5200 GA release.

5.2.5200

Released on 10 Sept 2018

HOW TO INSTALL HYSECURE 5.2 BUILD 5200

HySecure 5.0 can be installed using following methods:

1. Install on any x86 based hardware using HySecure 5.0 ISO
2. Install on any virtual machine using HySecure 5.0 ISO

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

HOW TO GET HYSECURE 5.2 BUILD 5200

Download the HySecure ISO:

https://propalmsnetwork-my.sharepoint.com/:u:/g/personal/support_accops_com/EVVEuSCAF_5DpqqVOUMyODABHkK7yoVot8Bk5rPVZOc2jA?e=bZob4l

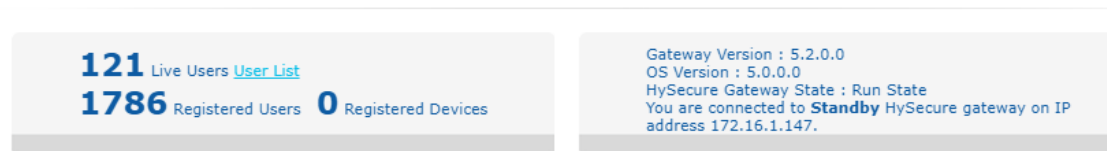
MD5 Checksum of HySecure upgrade patch: **0dc2c0e5bf51aec876e5a413f1f28d47**

NEW FEATURE IN 5.2.5200

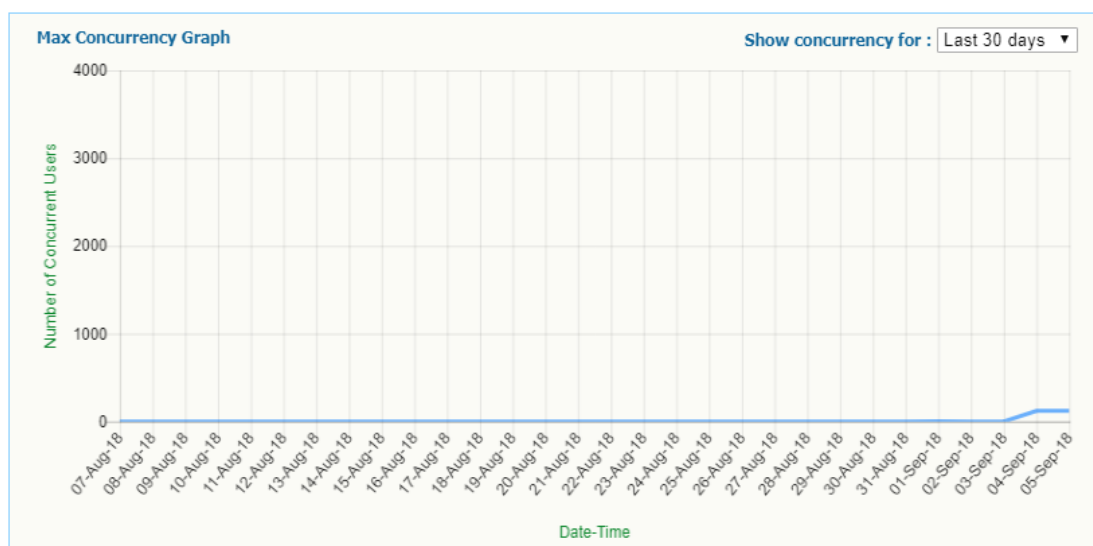
NEW DASH BOARD

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

If administrator wants to create access control for specific user or user group, then select radio button called "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

Select Authorization Server

Select Assignment Type

Select User Type

Select Users

demo

demo1

demo12

demo2

demo3

demo4

demo5

Add >>

Delete <<

Default

Primary AD

Users

☐ All Users

☒ Selected Users

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.

demo

demo1

demo12

demo2

demo3

demo4

demo5

Add >>

Delete <<

Select Application Group

Add >>

Delete <<

Access Filter

Access Control Valid Till :

Access Control State

Submit

Reset

September 2018

Mon	Tue	Wed	Thu	Fri	Sat	Sun
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

YYYY-MM-DD

☒ Enable ☐ Disable

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	<div></div>
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) *	<div></div>
Specify semicolon separated Email addresses.	
Access Control State	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<div>SubmitReset</div>	

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	<input type="text" value="Account Lockout"/>
Access Control Name	<input type="text" value="LockoutPolicy"/>
Access Control Description	<div></div>
Select HySecure Domain	<input type="text" value="Default"/>
Select Authorization Server	<input type="text" value="Primary AD"/>
Select Assignment Type	<input type="text" value="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 :	<input type="text" value="YYYY-MM-DD"/>
Access Control State	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

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 it does not match with 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.

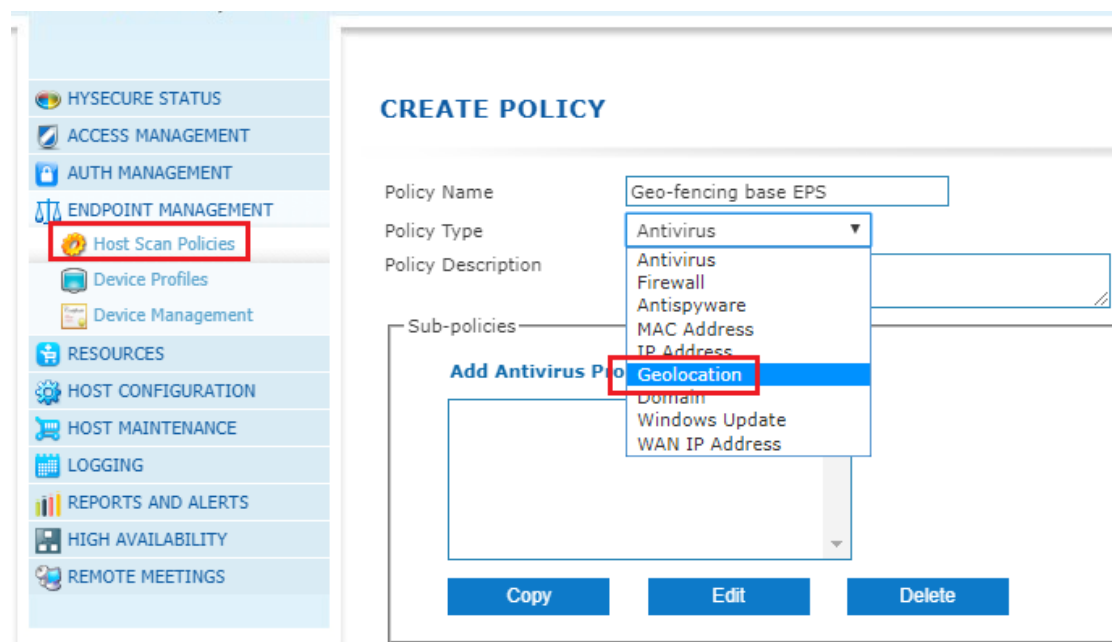
Maximum number of failed authentication attempts: No. of failed authentication attempts allowed for the user. After these attempts user account will be locked. Once the account is locked, the administrator will need to manually unlock the user from the management console.

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 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 below screenshot:

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
☐ Device Profile

Profile Description

Policies

The Policies which are added to this Device Profile will be applied to all devices in this profile.

Geolocation

Blocked Applications

ADD POLICIES TO PROFILE

Add ->

Remove <-

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, 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: Antivirus ▼

Policy Description:

Sub-policies:

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

Add Antivirus Pro

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.

step1

CREATE POLICY

Policy Name:

Policy Type: Domain

Policy Description:

Sub-policies:

Add Domain Policy

step2

ADD DOMAIN POLICY

Domain Policy Name:

☒ Allow ☐ Block

Domains:

step3

ADD DOMAINS

Domain:

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

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

Add ->
Remove <-

Allow_domain

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.

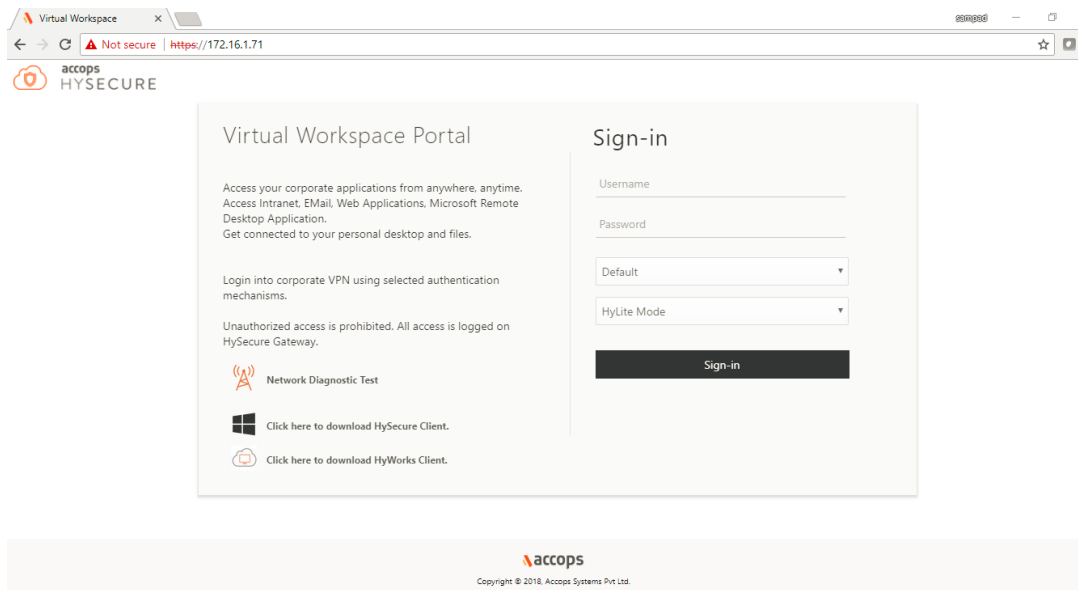
User needs to install HySecure windows client version 5.0.9.0 for faster access and better performance of Remote meeting.

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

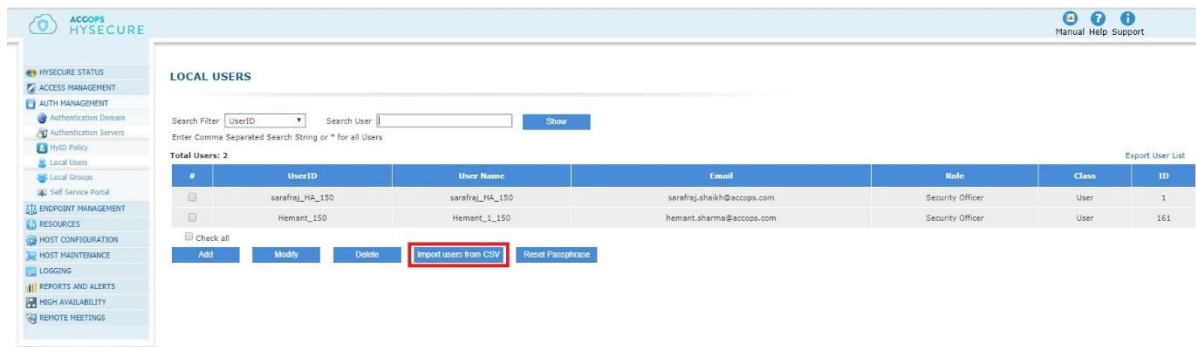
While launching RMS VM using HyLite, sometimes it will show message like "Please wait while connecting" and not able to connect to VM. But if user refresh or relaunch RMS VM then it will connect to VM.

NEW FEATURE IN 5.1.5169

BULK USER UPLOAD FROM MANAGEMENT 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.

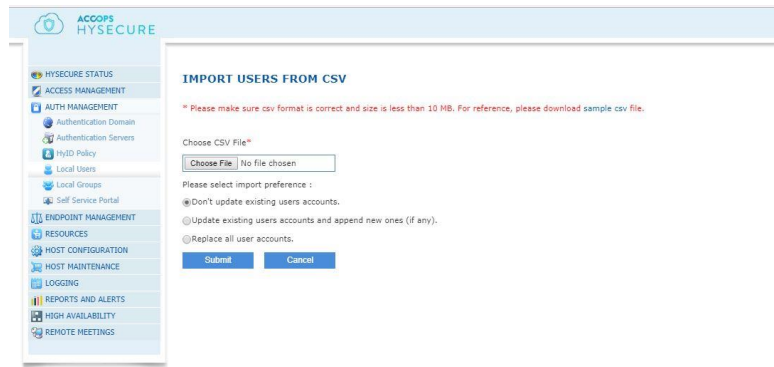


Administrator can upload only Low Security User (without certificate user) using this import user option. One CSV file can upload up to 1000 users onto HySecure gateway at a time.

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

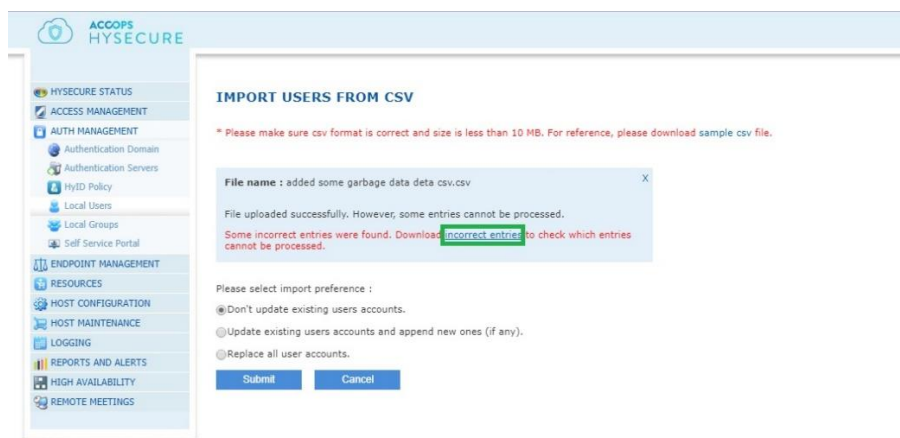
After adding users into CSV file, follow below steps:

- 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.

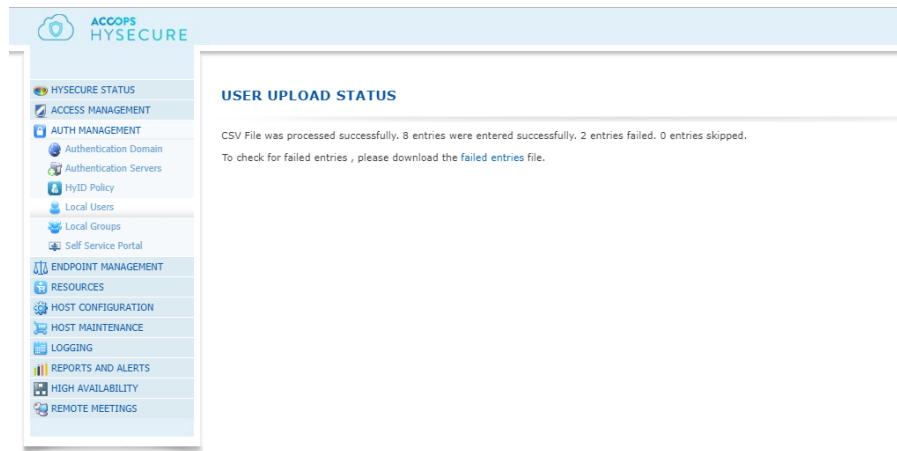


- If "don't update existing user accounts" is selected, then existing user accounts will remain as they were, no changes will be made to existing user accounts. If already existing users in gateway also exists in CSV file, then already existing users will be unchanged and remaining user will be added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

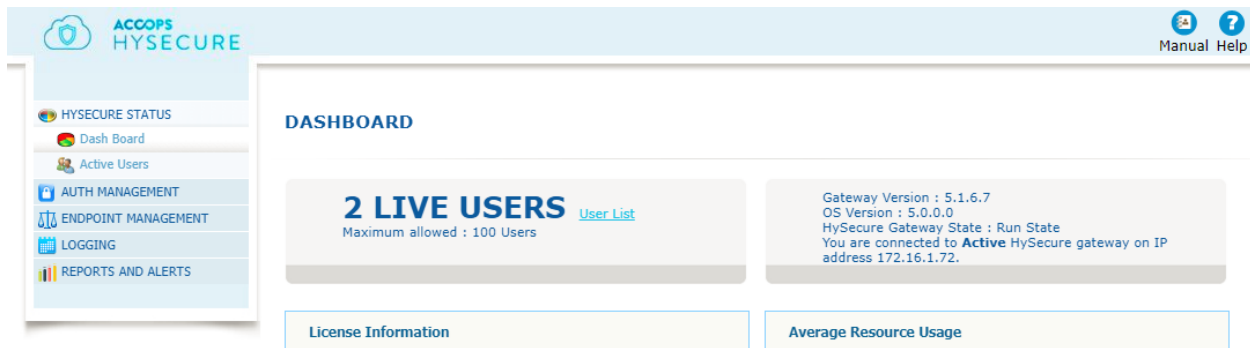


ROLE BASE ADMINISTRATION SUPPORT

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*	<input type="text" value="Monitor"/>
User E-mail Address*	<input type="text" value="info@accops.com"/>
Administrator E-mail Address*	<input type="text" value="support@accops.com"/>
Mobile number	<input type="text"/>
Class	<input type="text" value="User"/>
Role	<input type="text" value="Low Security User"/>
Hostname	<input type="text"/>
User must change password at next logon	<input type="checkbox"/>
Password never expires	<input type="checkbox"/>
Send details via email	<input type="checkbox"/>
Send details on mobile	<input type="checkbox"/>
Account is disabled	<input type="checkbox"/>
Account expires on	<input type="text" value="DD"/> <input type="text" value="MM"/> <input type="text" value="YY"/>
Login details	
User ID*	<input type="text"/>
Password*	<input type="password"/>
Confirm Password*	<input type="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.

The screenshot shows the 'HySecure Configuration' web interface. On the left is a sidebar menu with options: 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, and HyLite Configuration. The main content area is titled 'Web Portal logon mode selection'. It contains several settings: 'Force install TSE Client. Do not ask user for install/upgrade confirmation' (checkbox), 'Version of the Propalms TSE Client in format a.b.c.d, like 6.5.3.0' (text input with '7.0.3.0'), and 'TSE Client MSI Installer download URL. (Recommended: Point this URL to local TSE server path).' (text input with 'http://bit.ly/TSEClientv7MSINE'). Below these are three checkboxes: 'Enable RMS mode.' (checked), 'Enable HyLite mode.' (checked), and 'Enable Hybrid mode.' (checked). At the bottom, there is a 'Select Default logon mode.' dropdown menu set to 'HyLite Mode'. A 'Submit' button is at the bottom right.

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.

ACCOPS HYSECURE

ADD IDENTITY PROVIDER

SAML CONFIGURATIONS

GENERAL SETTINGS

Upload IdP Metadata : Choose File | Federation.ta (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 :

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.

ADD IDENTITY PROVIDER

SAML CONFIGURATIONS

GENERAL SETTINGS

Upload IdP Metadata : Federation.ta (3).xml

Identity Provider Name * :

Identity Provider Protocol : SAML 2.0

SAML PROTOCOL SETTINGS

IdP Issuer URL * :

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 URL * :

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:

HyID Policy Description:

HyID Policy Type:

User Database

Select Authentication Domain:

Select Authorization Server:

Select Policy assignment Type:

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 ☒

SMS Token ☒

Email and SMS Token ☐

Mobile Token ☒

Email and SMS OTP Configuration

Select OTP token length:

Select OTP token expiry time:

☐ Enable OTP token use for multiple time

Select OTP token regenerate timeout:

Mobile token configuration

Select OTP token length:

Select OTP token expiry time:

☒ Enable OTP token use for multiple time

Select OTP token regenerate timeout:

☒ Enable self-service mobile token registration for users.

☒ Allow re-activation of same device.

Allow multiple mobile devices per User:

Common OTP Configuration

☐ Account lockout on number of failed attempts

Account Lockout Time:

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

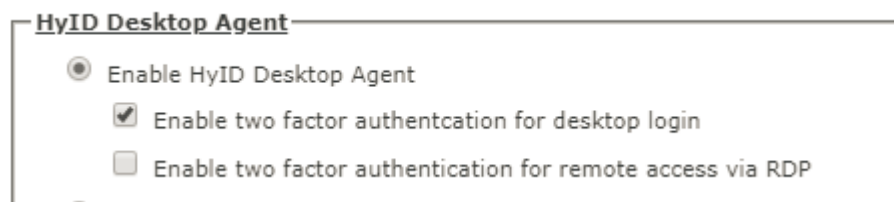
Enabled two factor authentications for windows login, HyID desktop agent need to install on windows machine. And on HySecure server HyID policy need to create for desktop agent. This HyID desktop agent setting will be push to all windows machine at the time of login.

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.

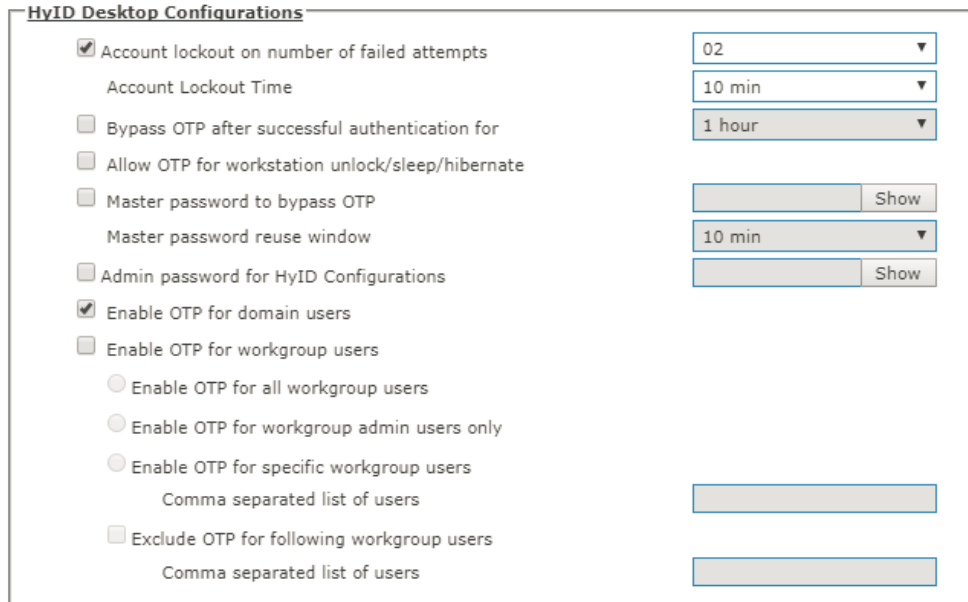
Enable two factor authentications for desktop login: If enabled, users will have to provide OTP to login into the desktop/server console.

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 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: [Text Field] Show
- Master password reuse window: 10 min
- ☐ Admin password for HyID Configurations: [Text Field] 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: [Text Field]
- ☐ Exclude OTP for following workgroup users: [Text Field]

- **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.

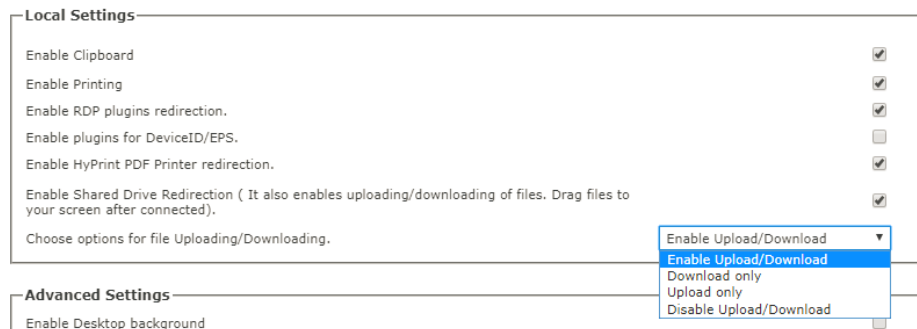
- Enable upload/download
- Upload only
- Download only
- Disable upload/download

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.

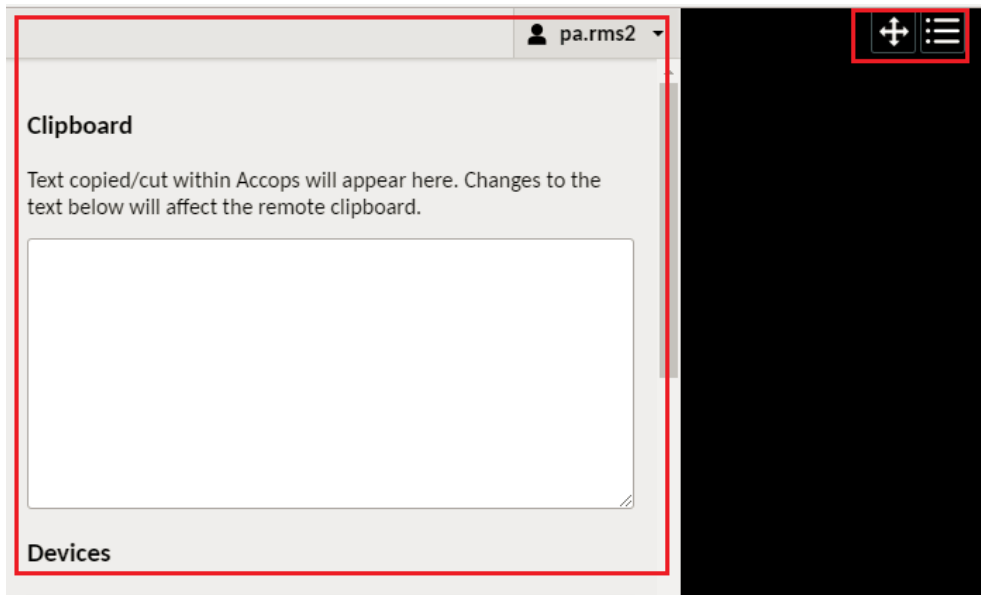
Download only: This option will allow end user only download file using HyLite. File upload feature will be disabled.

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



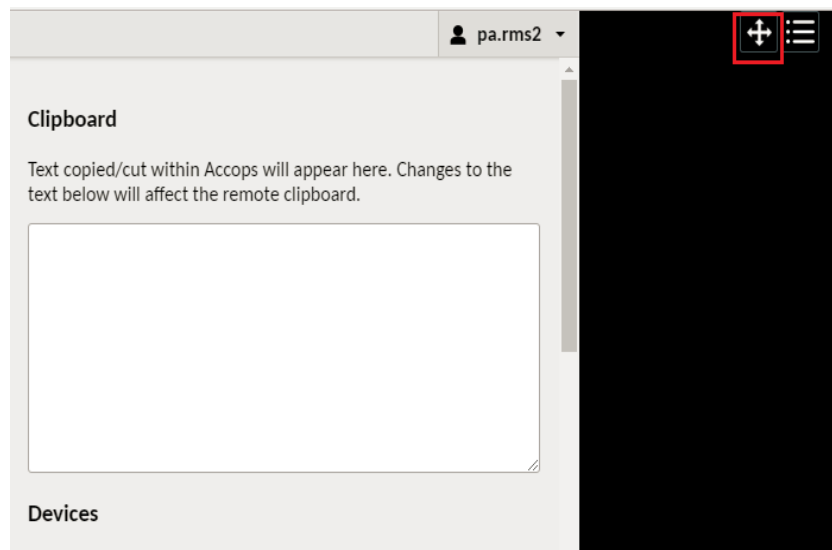
NEW MENU OPTION ON HYLITE RDP PAGE

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:

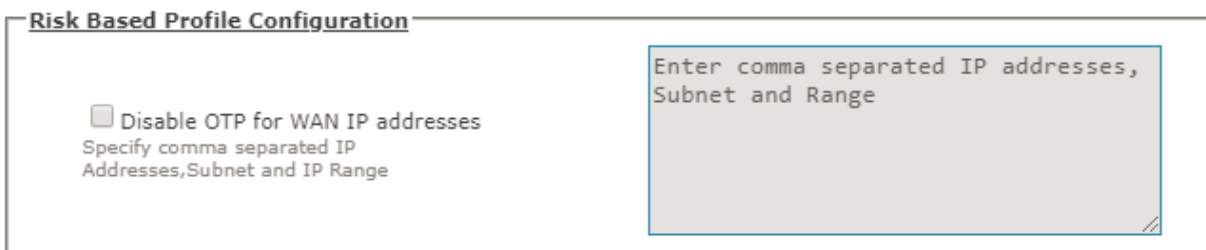
IP Address: A.B.C.D (e.g. 10.2.234.23)

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=com
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	<div> <input type="text" value="Search a Group..."/> <div> <div>Add >></div> <div>Delete <<</div> </div> </div> <div> <div>Select option</div> <div>Users</div> <div>User Groups</div> <div>Organizational Unit</div> </div>

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.

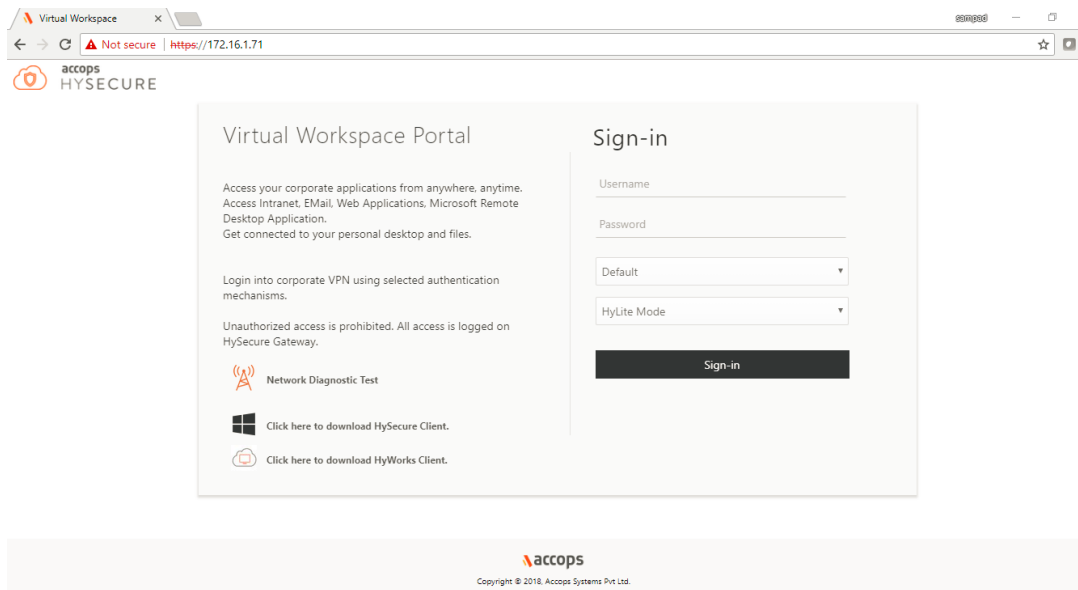
UAC SUPPORT IN REMOTE MEETING

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.

Accops HySecure Release Note – v 5.0



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.

5.0.5087

Released on 15 Dec 2017

HOW TO INSTALL HYSECURE 5.0 BUILD 5087

HySecure 5.0 can be installed using following methods:

3. Install on any x86 based hardware using HySecure 5.0 ISO
4. Install on any virtual machine using HySecure 5.0 ISO
5. Upgrade any existing HySecure installation based on previous 5.0 release candidates
6. Upgrade existing installations based on HySecure (previously OneGate) 4.7.4080

Please refer to the HySecure 5.0 install guide for detailed instructions on how to install HySecure 5.0. For upgrading HySecure (OneGate) 4.7 4080, refer to the instructions in this document. For upgrading any other older installation, refer to the release notes of 4.7.4080.

HOW TO GET HYSECURE 5.0 BUILD 5087

Download the HySecure ISO from this location:

https://propalmsnetwork-my.sharepoint.com/personal/support_accops_com/_layouts/15/guestaccess.aspx?docid=073b350e966e64e7cb554be2100e0a9ae&authkey=AfEY3OkdcfBRtGNLO0-GbU0&e=61234052c3c0422b89141329bd431695

MD5 Checksum of HySecure ISO: **d36ef7a1606c48121c2df43c6fa4b0b5**

FEATURE ENHANCEMENT IN 5.0.5087

COOKIES HAVE BEEN REMOVED WHILE LOGIN USING HYSECURE PORTAL.

For security reason HySecure web portal cookies have been removed.

ISSUES FIXED IN 5.0.5087

SOMETIMES HYLITE TEMPORARY DRIVE WAS NOT ABLE TO BE MAPPED

Sometime while login using HyLite mode, HyLite temporary drive was not able to be mapped. This issue is fixed in this release.

KEYBOARD SELECTION ISSUE ON HYLITE LOGIN PAGE.

While login using HyLite mode, user need to select keyboard language. If user select Japanese language, then after logout from portal keyboard language is set to default English. This issue has been fixed in this release.

FD LEAK FOR HYSECURE SERVICES.

There were some FD leaks due to HySecure services in SP1 release. This FD leaks have been fixed in this release.

KNOWN ISSUES IN 5.0.5087

HYSECURE SERVICES TAKES TIME TO RESTART WHILE DO HYSECURE STATE CHANGE

Sometimes HySecure services takes time to restart while do HySecure gateway state change. It may take up to 1 min.

SOMETIMES HYPRINT FAILS TO PRINT FILE USING HYSECURE

Sometimes using HyPrint module, not able to print file because print spooler service stopped unexpectedly.

Workaround: Use new HyPrint version 3.0.5.6 (released with HyWorks v3.0-SP1.1 patch). Release details and download links are available at following location

<http://support.accops.com/solution/articles/12000038817-patch-hyworks-v3-0-sp1-1>

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.

SEARCH FILTER DOES NOT WORK PROPERLY ON ACTIVE USER PAGE.

In HySecure management page, go to Active users. Here admin can apply search filter and search data. This search option does not work properly.

Workaround: Need to enter complete user name in search bar.

HYLITE PORTAL IS SHOWING NULL AT SELECT ORGANIZATION

If there are multiple organizations on HySecure gateway. Then on HySecure web portal login page NULL value is showing where organization name is displaying. This issue occurs only when user login first time at web portal.

Workaround: Select organization and submit it.

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 BROWSER PARAMETER IS SHOWING WRONG BROWSER DETAILS

After device id is enabled then login with HyLite using browser Edge-40 but in gateway device profile it is showing browser parameter as Chrome-52 instead of Edge 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.

TEST CONNECTION FAIL IF PASSWORD CONTAIN “#”

Open HySecure management page, go to Authentication server and configure AD server. While configuring AD, if user password contains special char “#” then AD test connection will fail.

WEB PORTAL LOG ON MODE SOMETIMES NOT SHOWING

If HyLite and Hybrid both mode options are enabled on HySecure gateway. Then sometimes on IE 11 browser, portal logon mode dropdown list option does not show on portal login page.

Workaround: Refresh the browser, then logon mode will be visible on HySecure portal.

NEED TO CLICK TWO TIMES ON HYLITE SIGN-OUT BUTTON

After login on HyLite portal, launch HyWorks application. Then on top of HyLite screen there is one button to sign-out from this application session. Sometimes if user click on this sign-out button, this application session will not sign-out.

Workaround: Click again on this sign out button for signing-out.

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.

VDI DOES NOT WORK ON CHROME VERSION 61 USING HYLITE MODE.

Dedicated and share hosted VDI does not launch on chrome browser (version 61) using HyLite mode, if HySecure SSL certificate does not sign by valid trusted CA. So, upload valid SSL sign certificate signed by trusted CA or use upgraded version of chrome or IE browser.

HYLITE TEMPORARY MAP DRIVE OPTION DOES NOT WORK AFTER RESIZING PORTAL BROWSER

If dedicated VDI OS is windows 7 or windows server 2008, then drive redirection will not work after browser resized.

FULL SCREEN OPTION DOES NOT WORK ON HYLITE FOR IE 10

Full screen option does not work for Internet explorer 10 on Windows 8.

HYID DOES NOT WORK FOR LDAP USER.

HyID two factor authentication does not work when LDAP server is configured for authentication. The issue will be fixed in the next hotfix.

PASSWORD CHANGE ISSUE FOR CERTIFICATE USER

Security officer, administrator and certificate-based users cannot change the password. The issue will be fixed in the next hotfix.

BOOTSTRAP PAGE GOES TO NOT RESPONDING STATE

While configuring the HySecure gateway, on bootstrap page, the browser may hang and not show the pass phrase of the first security officer. In such case, there are two options:

1. Reinstall HySecure: Choose reset firmware option from HySecure OS console.
2. Do SSH to HySecure gateway and get the passphrase from this file: `/home/fes/firstso.passphrase`

VIRTUAL IP ADDRESS FEATURE IS BROKEN

Virtual IP address assignment feature does not work in this release.

HA VIRTUAL IP ADDRESS CHANGE

In HySecure cluster, it is not possible to change the virtual IP address from HySecure management page. Using command line, it is possible to change HA VIP. Please go to Accops support portal for more details.

SOMETIMES COPY-PASTE FUNCTION HANGS FOR MS EXCEL APPLICATION IN HYLITE MODE

Sometimes copy -paste operation hangs for Microsoft excel application in HyLite mode.

Workaround: Double click on excel row and try to paste contains.

HYSECURE INSTALLATION ON HYPER-V TAKES TIME

When installing HySecure ISO on Hyper-V, it can take quite long to install the ISO. This issue happens on some Hyper-V installations.

SPECIFY DOMAIN NAME FOR ENDPOINT DETECTION FEATURE NOT WORKING

If domain name is configured on HySecure gateway. Then try to login from non-domain machine, HySecure client can login. But it should not login from non-domain machine.

SPECIFY SPECIFIC FILE PATH FOR ENDPOINT DETECTION FEATURE NOT WORKING

Verify Specify specific file path for endpoint detection not working.

USING IE BROWSER NOT ABLE TO ADD MULTIPLES MAC ID AT A TIME.

If try to configure MAC base EPS policy on IE browser. Then at a time more than 50 MAC id can't be added using IE browser. But using chrome browser administrator can add.

5.0.5080

Released on 03 Nov 2017

HOW TO INSTALL HYSECURE 5.0 BUILD 5080

HySecure 5.0 can be installed using following methods:

7. Install on any x86 based hardware using HySecure 5.0 ISO
8. Install on any virtual machine using HySecure 5.0 ISO
9. Upgrade any existing HySecure installation based on previous 5.0 release candidates
10. Upgrade existing installations based on HySecure (previously OneGate) 4.7.4080

Please refer to the HySecure 5.0 install guide for detailed instructions on how to install HySecure 5.0. For upgrading HySecure (OneGate) 4.7 4080, refer to the instructions in this document. For upgrading any other older installation, refer to the release notes of 4.7.4080.

HOW TO GET HYSECURE 5.0 BUILD 5080

Download the HySecure ISO from this location:

https://propalmsnetwork-my.sharepoint.com/personal/support_accops_com/_layouts/15/guestaccess.aspx?docid=007c39ba02d

[e3421e83d4dc1d24cf9e7c&authkey=AdMy-nzXPQ35J44eQse2LPc&e=e62983467eb04d0ab8eb694274ce8923](https://propalmsnetwork-my.sharepoint.com/personal/support_accops_com/_layouts/15/guestaccess.aspx?docid=0612d948ff34748a8b50a1a5807d2f092&authkey=Aa399w_g5GSGICPQustNI9Q&e=d8512f50830f4dd981a583f85d5e41d9)

MD5 Checksum of HySecure ISO: **1ce86b1ff74cad2d2415c8bccf40865**

Download the HySecure upgrade patch:

https://propalmsnetwork-my.sharepoint.com/personal/support_accops_com/_layouts/15/guestaccess.aspx?docid=0612d948ff34748a8b50a1a5807d2f092&authkey=Aa399w_g5GSGICPQustNI9Q&e=d8512f50830f4dd981a583f85d5e41d9

MD5 Checksum of HySecure upgrade patch: **e3007b9d9d42468f0566c0fda495ab7a**

HOW TO MIGRATE FROM HYSECURE 4.7.4080 TO 5.0.5080

HySecure 5.0 release is based on the new HySecure OS version 5.0. Previous released versions were based on CentOS 5.6 based OS and hence it's not possible to upgrade older 4.8 based deployments to new 5.0 releases.

This release supports migration of HySecure 4.7.4080 to HySecure 5.0.5080 by way of configuration restore. It is advised to user setting backup from HySecure version 4.7.4080 and then import it to HySecure 5.0. User setting backup includes all user settings, access policies, application configuration etc. The User setting backup does not include SSL certificates, licenses and system network settings.

It is required to reapply the license to the 5.0 gateway. Request support@accops.com to reset the already activated license to reapply the same serial key on the new gateway.

Note: Migration to 5.0 version is supported only from HySecure 4.0.8.0 (previously OneGate) to HySecure 5.0.8.0. So, if there is any customer who is using lower version of 4.0.8.0. they need to upgrade their gateway to 4.0.8.0 first.

NEW FEATURE IN 5.0.5080

PASSWORD CHANGE FOR LDAP USER

LDAP user can change password using HySecure client. If LDAP user wants to change password using HySecure client SSL must be configured on LDAP server. Without SSL configuration user will not be able to change password.

SYSLOG SUPPORT

SYSLOG support has been added on this version. This syslog setting option is under LOGGING on HySecure management page. By default, syslog will be disabled. If administrator wants to enable syslog on HySecure gateway, then enable syslog option and enter syslog server IP address and port. Then submit this syslog setting. Once syslog configuration setting has been submitted, HySecure log will send to syslog server automatically.

For HySecure HA setup, administrator need to enable syslog on Active node only.

The screenshot displays the Accops HySecure management interface. On the left is a sidebar menu with the following items: HYSECURE STATUS, ACCESS MANAGEMENT, AUTH MANAGEMENT, ENDPOINT MANAGEMENT, RESOURCES, HOST CONFIGURATION, HOST MAINTENANCE, LOGGING, Activity Logs, User Logs, Admin Logs, HyID Logs, End Point Security Logs, Log Settings, and Syslog Settings. The main content area is titled 'SYSLOG CONFIGURATIONS'. It contains two sections: 'SYSLOG STATUS' and 'CONFIGURATIONS'. The 'SYSLOG STATUS' section shows 'State : Syslog is enabled.' with a 'Disable' button. The 'CONFIGURATIONS' section contains a form with the following fields: 'Hostname/IP Address' (text input with value '172.16.1.180'), 'Port' (text input with value '514'), and 'Level' (dropdown menu with value 'INFO'). A 'Submit' button is located at the bottom right of the configuration form.

FEATURE ENHANCEMENT IN 5.0.5080

SMTP SERVER CONFIGURATION STATUS MESSAGE

While configure SMTP server on HySecure gateway, SMTP server status message will display on SMTP configuration page. If SMTP server not reachable from HySecure server then proper error message will be display.

SMTP Server Settings

SMTP Mail Server *

smtp.1and1.com

SMTP Server Port *

25

☒ Enable TLS

☒ Enable SMTP Authentication

SMTP Username

sampad.sarkar@propalmsnetwork.

SMTP Password

.....

Confirm Password

.....

SMTP Email Sender

otp@accops.com

SMTP Client Hostname

ha1.local

Specify the email id which should be used to send all emails.
If no email ID is specified, the email ID of the logged in HySecure administrator will be used.

This hostname will be sent to SMTP server as the identity for the SMTP client.

Submit

Reset

Please wait while saving SMTP server configuration.

ISSUES FIXED IN 5.0.5080

SECURE DESKTOP IS CRASHING ON WIN 7 64 BIT MACHINE

If network profile detection is enabled and user try to login on windows 7 64-bit OS, then secure desktop is crashing. This issue is fixed on client version 5066.

SPECIAL SYMBOL "" SUPPORT IN DOMAIN USER GROUP

If domain user belongs to user group, and user group contain special symbol "", then user was not able to login. In this release this issue has been resolved.

HYSECURE ON-DEMAND CLIENT >>NAME RESOLUTION ISSUE

If two applications having same IP address, Then On-Demand client, will resolved name for only one application. So only one application will be assessable using name. This issue is fixed on client version 5066

WHEN LAUNCHING THE HYSECURE CLIENT, IDM DOWNLOAD MANAGER WEB PORTAL IS ALSO OPENING

This issue is fixed on client version 5066.

NOT ABLE TO SCROLL DOWN ISSUE ON HYSECURE CLIENT LAUNCHPAD

This issue is fixed on client version 5066

NOT ABLE TO LAUNCH RDP PROGRAM FILE PATH APPLICATION USING HYWORKS LAUNCHER

If RDP application is configured with program file path. Then HyWorks launcher not able to lunch RDP application. This issue is fixed on client version 5066

DISK UTILIZATION SHOWING WRONG VALUE ON STANDALONE GATEWAY

On HySecure dash board, Disk utilization showing wrong value on standalone gateway. This is fixed on this release.

NETWORK DIAGNOSTICS TEST SHOWING SPEED 0 KB/S

Network Diagnostics Test showing speed 0 KB/S. This is fixed on this release.

UNWANTED OPTION AT THE TIME CREATION ACL FOR NATIVE USERS

After HySecure gateway installation when administrator try to create access control for native user, unwanted value is display on authentication server dropdown list. This is fixed on this release. Now only native server will be display.

CREATE ACCESS CONTROL

Access Control Name	ACLforNativeusers
Access Control Description	
Select HySecure Domain	DefaultDomain
Select Authorization Server	Native
Select Assignment Type	Select option
Select Native Group Type	Native
Access Control Type	-1
Select User Group	-1

WHILE ADD STANDBY NODE IN HYSECURE HA CLUSTER, STATUS MESSAGE NOT DISPLAY ON BROWSER

While add secondary node into HySecure HA cluster, proper status message will not display on browser. In this release, this issue is fixed.

IN WHOLE SYSTEM BACKUP CUSTOMIZED UPLOADED APPLICATION ICON NOT SHOWING

While restore whole system backup uploaded customized application icons not able to restore. In this release, this issue is fixed.

KNOWN ISSUES IN 5.0.5080

WEB PORTAL LOG ON MODE SOMETIMES NOT SHOWING

If HyLite and Hybrid both mode options are enabled on HySecure gateway. Then sometimes on IE 11 browser portal logon mode dropdown list option does not showing on portal login page. But if refresh the browser, then logon mode will be visible on HySecure portal.

NEED TO CLICK TWO TIMES ON HYLITE SIGN-OUT BUTTON

After login on HyLite portal, launch HyWorks application. Then on top of HyLite screen there is one button to sign-out from this application session. Sometimes if user click on this button sign-out button, this application session will not sign-out, again click on this sign out button for signing-out.

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.

VDI DOES NOT WORK ON CHROME VERSION 61 USING HYLITE MODE.

Dedicated and share hosted VDI does not launching on chrome browser (version 61) using HyLite mode, if HySecure SSL certificate does not sign by valid trusted CA. So, upload valid SSL sign certificate sign by trusted CA. Or use lower version of chrome or IE browser.

HYLITE TEMPORARY MAP DRIVE OPTION NOT WORK AFTER RESIZING PORTAL BROWSER

If dedicated VDI OS is windows 7 or windows server 2008, then drive redirection will not work after browser resized.

FULL SCREEN OPTION DOES NOT WORK ON HYLITE FOR IE 10

Full screen option does not work for Internet explorer 10 on Windows 8.

HYID DOES NOT WORK FOR LDAP USER.

HyID two factor authentication does not work when LDAP server is configured for authentication. The issue will be fixed in the next hotfix.

PASSWORD CHANGE ISSUE FOR CERTIFICATE USER

Security officer, administrator and certificate-based users cannot change the password. The issue will be fixed in the next hotfix.

BOOTSTRAP PAGE GOES TO NOT RESPONDING STATE

While configuring the HySecure gateway, on bootstrap page, the browser may hang and not show the pass phrase of the first security officer. In such case, there are two options:

3. Reinstall HySecure: Chose reset firmware option from HySecure OS console.
4. Do SSH to HySecure gateway and get the passphrase from this file: `/home/fes/firstso.passphrase`

VIRTUAL IP ADDRESS FEATURE IS BROKEN

Virtual IP address assignment feature does not work on this release.

HA VIRTUAL IP ADDRESS CHANGE

In HySecure cluster, it's not possible to change the virtual IP address from HySecure management page. Using command line, it is possible to change HA VIP. Please go to accops support portal for more details.

SOMETIMES COPY-PASTE FUNCTION HANG FOR MS EXCEL APPLICATION ON HYLITE MODE

Sometimes copy -paste operation hangs for Microsoft excel application on HyLite mode.

Workaround: Double click on excel row and try to paste contains.

HYSECURE INSTALLATION ON HYPER-V TAKES TIME

When installing HySecure ISO on Hyper-V, it can take quite long to install the ISO. This issue happens on some Hyper-V installations.

SPECIFY DOMAIN NAME FOR ENDPOINT DETECTION FEATURE NOT WORKING

If domain name is configured on HySecure gateway. Then try to login from non-domain machine, HySecure client can login. But it should not login from non-domain machine.

SPECIFY SPECIFIC FILE PATH FOR ENDPOINT DETECTION FEATURE NOT WORKING

Verify Specify specific file path for endpoint detection not working.

USING IE BROWSER NOT ABLE TO ADD MULTIPLES MAC ID AT A TIME.

If try to configure MAC base EPS policy on IE browser. Then at a time more than 50 MAC id not able to add using IE browser. But using chrome browser administrator can add.

5.0.5057

Released on 14 June 2017

HOW TO INSTALL HYSECURE 5.0 BUILD 5057

HySecure 5.0 can be installed using following methods:

11. Install on any x86 based hardware using HySecure 5.0 ISO
12. Install on any virtual machine using HySecure 5.0 ISO
13. Upgrade any existing HySecure installation based on previous 5.0 release candidates
14. Upgrade existing installations based on HySecure (previously OneGate) 4.7.4080

Please refer to the HySecure 5.0 install guide for detailed instructions on how to install HySecure 5.0. For upgrading HySecure (OneGate) 4.7 4080, refer to the instructions in this document. For upgrading any other older installation, refer to the release notes of 4.7.4080.

HOW TO GET HYSECURE 5.0 BUILD 5057

Download the HySecure ISO from this location:

https://propalmsnetwork-my.sharepoint.com/personal/support_accops_com/_layouts/15/guestaccess.aspx?docid=03a14bf5201a84e37bdd5ce813d3269b0&authkey=ASQcG_lygGYEC7oAQVvxsLY

MD5 Checksum of HySecure ISO: **bcc9a2c9f7a7c86da2f64c99013ba412**

Download the HySecure upgrade patch:

https://propalmsnetwork-my.sharepoint.com/personal/support_accops_com/_layouts/15/guestaccess.aspx?docid=01d2e8c0c22b54dc091885fc367a1c445&authkey=AZRZUXp7QjfDI9yT6AxlRs

MD5 Checksum of HySecure upgrade patch: **d6e9c4497ffb2bca1fe3c46b831db04d**

HOW TO MIGRATE FROM HYSECURE 4.7.4080 TO 5.0.5057

HySecure 5.0 release is based on the new HySecure OS version 5.0. Previous released versions were based on CentOS 5.6 based OS and hence it's not possible to upgrade older 4.8 based deployments to new 5.0 releases.

This release supports migration of HySecure 4.7.4080 to HySecure 5.0.5057 by way of configuration restore. It is advised to user setting backup from HySecure version 4.7.4080 and then import it to HySecure 5.0. User setting backup includes all user settings, access policies, application configuration etc. The User setting backup does not include SSL certificates, licenses and system network settings.

It is required to reapply the license to the 5.0 gateway. Request support@accops.com to reset the already activated license to reapply the same serial key on the new gateway.

Note: Migration to 5.0 version is supported only from HySecure 4.0.8.0 (previously OneGate) to HySecure 5.0.5.7. So, if there is any customer who is using lower version of 4.0.8.0. they need to upgrade their gateway to 4.0.8.0 first.

NEW FEATURES IN HYSECURE 5.0.5.7

MORE SECURE HYSECURE GATEWAY

HySecure 5057 is more secure than previous version. Security improvement done as per OWASP (Open Web Application Security Project) international guide line. Also, vulnerability which was found last release is fixed in this release.

Security point of view this version is more secure and stable. Using this release HySecure can get rating A or A+ for SSL test lab.

NEW CLIENT SETTING

Following new options are added as client settings:

Broadcast message warning.	<input type="text"/>
Broadcast pre login message	<input type="text"/>
Broadcast post login message.	<input type="text"/>

Broadcast message warning: This is message broadcasting option in HySecure. So that if administrator wants to broadcast message to end HySecure user. This message will be display before login.

Broadcast pre-login message: This is message broadcasting option in HySecure. So that if administrator wants to broadcast message to end HySecure user. This message will be display before login.

Broadcast post login message: This is message broadcasting option in HySecure. So that if administrator wants to broadcast message to end HySecure user. This message will be display after login into HySecure gateway.

Uninstall LSP on logout	<input type="checkbox"/>
Uninstall NSP on logout	<input type="checkbox"/>

Uninstall LSP on logout: If this option is enabled then at the time of logout from HySecure gateway, client LSP module will be uninstalled from end user machine.

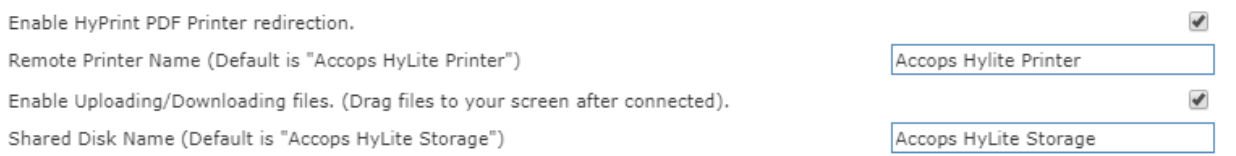
Uninstall NSP on logout: If this option is enabled then at the time of logout from HySecure gateway, client NSP module will be uninstalled from end user machine.

Upgrade Settings	
Enable HySecure Client upgrade notification to users.	<input checked="" type="checkbox"/>
Forcefully update HySecure client if the user's client version is equal to or below this version (format a.b.c.d, like 3.7.1.5). To forcefully update all the HySecure client enter "*" and leave blank to disable forcefully update.	<input type="text"/>

Forcefully update HySecure client: This option will be used for HySecure client upgradation. To forcefully update all the HySecure client enter "*" and leave blank to disable forcefully update. Also, HySecure administrator can specify specific client version to upgrade forcefully.

HYPRINT PDF PRINTER SUPPORT ON HYLITE

In this release HyPrint pdf printer support has been added in HyLite configuration option. By default, HyPrint pdf printer redirection option is enabled. If this option is enabled then when user try to give print using HyLite, user can select HyPrint pdf printer and it will be created pdf file on user's local machine. Then user can print using that pdf file. For working this option "Enable uploading/downloading file" check box should be enabled.



NON-ADMIN CLIENT RENAME TO ON-DEMAND CLIENT

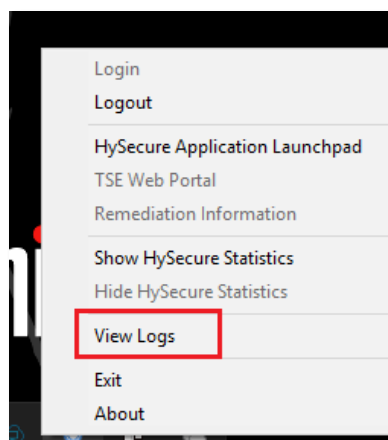
In previous release there is option to upload non-admin client. This non-admin client has been renamed to On-Demand client in this release.

NEW HYSECURE WINDOWS CLIENT SIGN BY MICROSOFT.

In this release, new HySecure windows client 5063 has been bundle. This client contains driver which is sign by Microsoft. This new windows client logo has been changed. Also removed some crashes. Accops HySecure windows client driver has some issue on windows 10. Which is resolved by this sign driver.

HYSECURE WINDOWS CLIENT LOG FROM CLIENT UI.

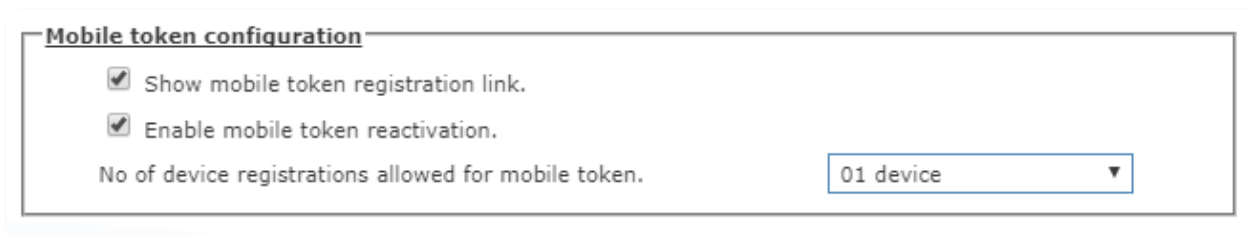
Now there is option to see HySecure windows client log from client UI.



HYID MOBILE TOKEN CONFIGURATION

New options have been added in HyID configuration option in this release. When user select mobile token check box, mobile token configuration option automatically will be visible. Here there are two configurable links. One is "Show mobile token registration link" and another is "Enable mobile token reactivation". If administrator want to hide mobile token registration or reactivation link, just uncheck the check box and save the setting.

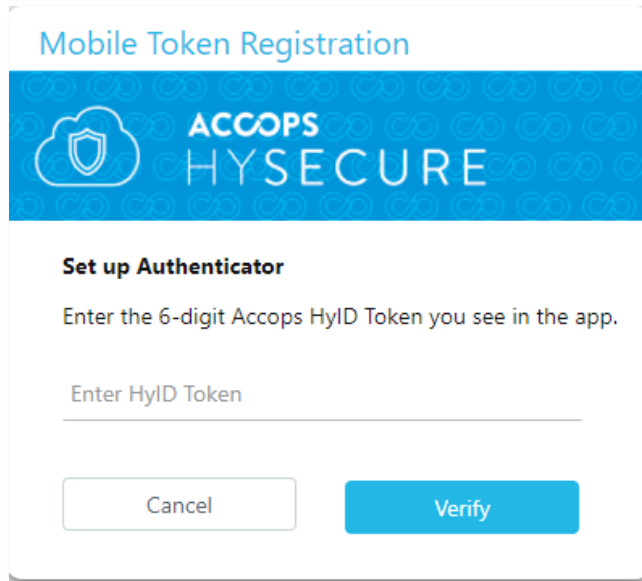
There is another option called "No of device registrations allowed for mobile token". Here administrator can specify the number of HyID token registered devices per user. So that same user can register HyID token from how many mobile devices. By default, one user can register HyID mobile token from only one mobile device.



The screenshot shows a configuration window titled "Mobile token configuration". Inside the window, there are two checked checkboxes: "Show mobile token registration link." and "Enable mobile token reactivation.". Below these checkboxes is a label "No of device registrations allowed for mobile token." followed by a dropdown menu. The dropdown menu currently displays "01 device" with a downward arrow icon.

HYID MOBILE TOKEN REGISTRATION

HyID mobile token registration process has been changed in this release. Now after HyID token configuration on end user mobile devices user need to set up authenticator the token number for completed the mobile token registration. After this process, mobile token can be used for login. Without token set up authenticator, mobile token registration process can't be completed.

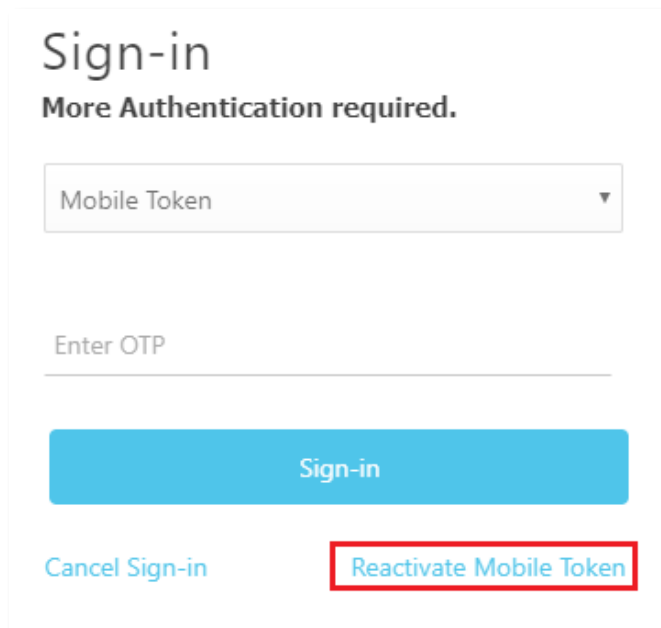


The dialog box is titled "Mobile Token Registration" in blue text. Below the title is a blue header bar with the "ACCOPS HYSECURE" logo, which consists of a cloud with a shield icon and the text "ACCOPS HYSECURE". The main content area is white and contains the heading "Set up Authenticator" in bold. Below this heading is the instruction "Enter the 6-digit Accops HyID Token you see in the app." followed by a text input field with the placeholder "Enter HyID Token". At the bottom of the dialog are two buttons: a white "Cancel" button and a blue "Verify" button.

REACTIVATE MOBILE TOKEN

When user select mobile token on web portal user will get option for reactivate mobile token. If user want to reactivate mobile token, then user need to click on this link "Reactivate mobile token" and get select OTP token type to get OTP.


Then scan this QR code using Accops HyID app. If QR code is not working, then click on CAN'T SCAN IT? link to get registration key for manual registration. Now HyID is configured on user mobile device. Enter HyID mobile token number on set up authenticator window for completed the mobile token reactivation process. Once it is set up successfully, now it is ready for use.



The dialog box is titled "Sign-in" in large black text, with the subtitle "More Authentication required." below it. It features a dropdown menu with "Mobile Token" selected. Below the dropdown is a text input field with the placeholder "Enter OTP". At the bottom of the dialog are three buttons: a blue "Sign-in" button, a blue "Cancel Sign-in" button, and a blue "Reactivate Mobile Token" button which is highlighted with a red rectangular border.

ACCESS RDP APPLICATION USING EDC LAUNCHER

When user try to access RDP application using HySecure windows client, by default it will launch RDP application using EDC launcher. But if administrator wants to launch RDP application using MSTSC, go to client setting and enabled setting "Use Default Windows app for RDP app launch"

A screenshot of a user interface element, likely a settings window. It shows a single line with the text "Use Default Windows app for RDP app launch" followed by a small, empty square checkbox on the right side. The entire element is enclosed in a light gray border with a subtle drop shadow.

Use Default Windows app for RDP app launch

ISSUES FIXED IN 5.0.5057

CLIENT CRASH

Sometimes windows client crashes while access application. It is fixed in this version.

CLIENT NOT RESPONDING MODE

Sometimes windows client goes to not responding mode. It is fixed in this version.

ON WINDOWS 10, HYSECURE WINDOWS CLIENT DRIVER NOT WORKING

HySecure client driver does not load on windows 10 anniversary update edition. It is fixed this in this release.

CLIENT UPGRADE ISSUE USING HYBRID MODE.

There was issue while upgrade client using HyBrid mode. This is fixed in this release.

IDLE TIME OUT FEATURE STOPS WORKING

In HySecure cluster, once failover to standby gateway is completed, the idle timeout function stops working. This issue is fixed in this version.

HYSECURE NON-ADMIN CLIENT DOES NOT SUPPORT HYWORKS APP

HySecure non-admin client does not support HyWorks application. This issue is fixed in this release.

DOWNLOAD LOG FILE ISSUE

Log file not able to download from log setting. This issue is fixed. Now if administrator try to download log file need to click on download button and log file will download as CSV format.

KNOWN ISSUES IN 5.0.5057

FULL SCREEN OPTION DOES NOT WORK ON HYLITE FOR IE 10

Full screen option does not work for Internet explorer 10 on Windows 8.

JOINING STANDBY GATEWAY REQUIRES REFRESH

When joining standby gateway to cluster, the browser needs to be refreshed to get status of cluster joining.

HYID DOES NOT WORK FOR LDAP USER.

HyID two factor authentication does not work when LDAP server is configured for authentication. The issue will be fixed in the next hotfix.

PASSWORD CHANGE ISSUE FOR CERTIFICATE USER

Security officer, administrator and certificate-based users cannot change the password. The issue will be fixed in the next hotfix.

VPN SERVICES RESTART WHILE ADMIN CHANGE IDLE TIME OUT

The issue is fixed now. VPN service will not be started when idle timeout is changed

BOOTSTRAP PAGE GOES TO NOT RESPONDING STATE

While configuring the HySecure gateway, on bootstrap page, the browser may hang and not show the pass phrase of the first security officer. In such case, there are two options:

5. Reinstall HySecure: Chose reset firmware option from HySecure OS console.
6. Do SSH to HySecure gateway and get the passphrase from this file: `/home/fes/firstso.passphrase`

VIRTUAL IP ADDRESS FEATURE IS BROKEN

Virtual IP address assignment feature does not work on this release.

ISP LOAD BALANCING

ISP load balancing feature does not work in this release. If admin enable this option user will not be able to login.

HA VIRTUAL IP ADDRESS CHANGE

In HySecure cluster, it's not possible to change the virtual IP address from HySecure management page. Using command line, it is possible to change HA VIP. Please go to accops support portal for more details.

SOMETIMES COPY-PASTE FUNCTION HANG FOR MS EXCEL APPLICATION ON HYLITE MODE

Sometimes copy -paste operation hangs for Microsoft excel application on HyLite mode.

Workaround: Double click on excel row and try to paste contains.

HYSECURE INSTALLATION ON HYPER-V TAKES TIME

When installing HySecure ISO on Hyper-V, it can take quite long to install the ISO. This issue happens on some Hyper-V installations.

SPECIFY DOMAIN NAME FOR ENDPOINT DETECTION FEATURE NOT WORKING

If domain name is configured on HySecure gateway. Then try to login from non-domain machine, HySecure client can login. But it should not login from non-domain machine.

SPECIFY SPECIFIC FILE PATH FOR ENDPOINT DETECTION FEATURE NOT WORKING

Verify Specify specific file path for endpoint detection not working.

CUSTOM APPLICATION ICONS NOT ABLE TO RESTORE WHILE RESTORE FROM WHOLE SYSTEM BACKUP

While restore whole system backup, custom application icons not able to restore.

5.0.5035

Released on 14 June 2017

HOW TO INSTALL HYSECURE 5.0 BUILD 5035

HySecure 5.0 can be installed using following methods:

15. Install on any x86 based hardware using HySecure 5.0 ISO
16. Install on any virtual machine using HySecure 5.0 ISO
17. Upgrade any existing HySecure installation based on previous 5.0 release candidates
18. Upgrade existing installations based on HySecure (previously OneGate) 4.7.4080

Please refer to the HySecure 5.0 install guide for detailed instructions on how to install HySecure 5.0. For upgrading HySecure (OneGate) 4.7 4080, refer to the instructions in this document. For upgrading any other older installation, refer to the release notes of 4.7.4080.

HOW TO GET HYSECURE 5.0 BUILD 5035

Download the HySecure ISO from this location:

https://propalmsnetwork-my.sharepoint.com/personal/support_accops_com/_layouts/15/guestaccess.aspx?docid=0d0091cf936694f0791292447117f3237&authkey=ARbR_Z_EjRTmZYEqZEOD7OU

MD5 Checksum of HySecure ISO: **b981f626fb999b4bf297631b9aa734df**

Download the HySecure upgrade patch:

https://propalmsnetwork-my.sharepoint.com/personal/support_accops_com/_layouts/15/guestaccess.aspx?docid=07dfd9261b3b44f77b3a4eea8ac8710dd&authkey=AZM8WM2d5AuEKVYGsADKm_E

MD5 Checksum of HySecure upgrade patch: **09d15b2cd1f0df40eb3065df7cf4cdbc**

HOW TO MIGRATE FROM HYSECURE 4.7.4080 TO 5.0.5035

HySecure 5.0 release is based on the new HySecure OS version 5.0. Previous released versions were based on CentOS 5.6 based OS and hence it's not possible to upgrade older 4.8 based deployments to new 5.0 releases.

This release supports migration of HySecure 4.7.4080 to HySecure 5.0.5035 by way of configuration restore. It is advised to user setting backup from HySecure version 4.7.4080 and then import it to HySecure 5.0. User setting backup includes all user settings, access policies, application configuration etc. The User setting backup does not include SSL certificates, licenses and system network settings.

It is required to reapply the license to the 5.0 gateway. Request support@accops.com to reset the already activated license to reapply the same serial key on the new gateway.

Note: Migration to 5.0 version is supported only from HySecure 4.0.8.0 (previously OneGate) to HySecure 5.0.3.5. So, if there is any customer who is using lower version of 4.0.8.0. they need to upgrade their gateway to 4.0.8.0 first.

NEW FEATURES IN HYSECURE 5.0.3.5

PORT 80 IS BLOCKED AND ALL CONFIGURATION IS HTTPS ENABLED

From 5.0.5035 release, all pre-boot configuration starting from first configuration page is moved to HTTPS based page. There is no server on port 80 anymore.

HYWORKS APPLICATION SUPPORT ON HYSECURE HYBRID PORTAL

With the new HySecure hybrid portal, support for HyWorks is added. User can login into HySecure with hybrid mode ON. After login, user can see all HyWorks published applications, virtual desktops, web applications, RDP applications, TSE Applications and user can also access local client-server applications.

This feature enables users to have easy access to HyWorks published applications along with other corporate applications like Intranet portal and client-server applications already installed on user PC. IT teams can use this feature to deliver the necessary agents on end user PC, avoiding sending client installers to users or training them.

When user logs into HySecure portal, the portal detects if the user PC has the HySecure client already installed or no. If not found, portal will prompt the user to download the HySecure client and install it. User must install the HySecure client. After installation, portal can move forward and log the user in. If the user has access to HyWorks published applications, portal will show the HyWorks apps along with

other applications (like Web and RDP which are accessible via HySecure) on the portal. When user clicks on any application, the respective application is launched.

HyWorks client is also required on end user machine for user to launch the application. If the user PC does not have HyWorks client installed, HySecure client downloads and install the HyWorks client automatically. When HySecure client is started by the portal, HySecure client checks for presence of HyWorks client. If not found, it downloads the HyWorks client from the URL configured on HySecure gateway and installs it on end user PC.

HyWorks portals uses the URL scheme to start the HySecure client.

The finer details of the feature are:

OS Supports: Windows Desktop OS, Windows 7 and above

Browser support: Internet explorer 10, Internet explorer 11, latest chrome, latest Firefox

Clients Required: HySecure Windows Client and HyWorks Windows Client

Admin Rights: Non-admin version of HySecure client and HyWorks client are configurable to avoid administrative rights on end user PC. The non-admin clients can be configured from management console, which is a default setting.

Application Support: HyWorks Apps, VDI, TSE, Web Applications, RDP, Locally installed client-server applications

Client Upgrade: The HySecure portal can update the clients on the end user PC on next login

Client download URL: Admin can upload new client installers on HySecure and alternatively set URL from where clients can be downloaded and installed.

HYWORKS CLIENT DOWNLOAD SETTINGS

Under **Client Settings** section, HyWorks Client Settings are added. These settings are used by HySecure Hybrid Portal and HySecure client to download and install/upgrade HyWorks client on user PC.

The screenshot shows the 'Hyworks Client Settings' configuration page. On the left is a sidebar with various system settings like Proxy Server, SAML Global Configuration, SMTP Server, SMS Gateway, Global Settings, Client Settings (highlighted), Password Expiry Time, Database Password, SSH Configuration, ISP Management, Virtual Server, and HyLite Configuration. The main panel is titled 'Hyworks Client Settings' and contains the following fields and checkboxes:

- Hyworks Client Version: 3.0.0.868
- Enable Hyworks full client download: ☒
- Enable Hyworks Client Upgrade: ☒
- Enable Hyworks Client Force Upgrade: ☐
- Enable SEP installation with HyWorks Client: ☐
- Enable Eltima installation with HyWorks Client: ☐
- Hyworks Full Client Installer Download URL: ccops_HyWorksSetupEssential.exe
- Hyworks Lite Client Installer Download URL: >lic/Accops_HyWorksLiteSetup.exe

A 'Submit' button is located at the bottom right of the settings panel.

Details of different options:

HyWorks Client Version: Version of the HyWorks client

Enable HyWorks full client download: When disabled, HyWorks Lite client is used. HyWorks Lite client do not require admin rights to install. When enabled, HyWorks client installer which require admin rights is used.

The HyWorks Lite client installer installs all the files in user's application data folder and does not make any changes to user PC that requires admin rights.

HyWorks full client installer install the HyWorks binaries in %PROGRAM FILES% folder and hence require admin rights to install.

Important Note: Some Anti-viruses policies restricts browsers from downloading software when coming from non-trusted SSL certificate-based websites. Anti-viruses may also block HyWorks installer when it tries to install the files in user's application data folders.

Enable HyWorks client upgrade: When enabled, HySecure client will upgrade the HyWorks client if any new upgrades are available. If disabled, HyWorks client will upgrade itself on its own, based on new version available on HyWorks server.

Enable HyWorks client Force upgrade: The option can be used to forcefully upgrade the HyWorks client and not give a choice to user to skip the upgrade.

Enable SEP Installation with HyWorks client: If enabled, SEP client for USB redirection is also installed along with HyWorks client. Admin must upload HyWorks client installer which has SEP client installer also built-in. The installer available on HySecure server by default do not include SEP client due to high size reasons. Admin can change the HyWorks client download URL to point it to Accops website to the latest integrated HyWorks client installer with SEP client.

Enable Eltima Installation with HyWorks client: If enabled, Eltima client, which is the free USB redirection module with HyWorks is also installed on user PC. Eltima client is included in all HyWorks client installers

HyWorks Full Client Installer Download URL: URL from where HyWorks Full Client (requires administrative rights) can be downloaded. By default, the URL is a relative URL, pointing to the installer already placed on HySecure gateway. This URL value is used when "**Enable HyWorks full client download**" is enabled.

HyWorks Lite Client Installer Download URL: URL from where HyWorks Lite Client (Does not require administrative rights) can be downloaded. By default, the URL is a relative URL, pointing to

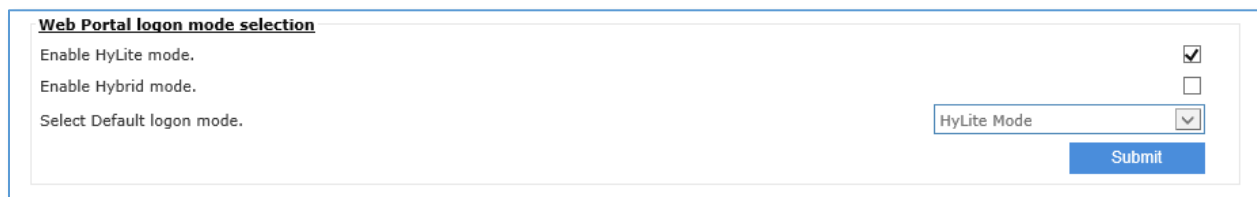
the installer already placed on HySecure gateway. This URL value is used when “**Enable HyWorks full client download**” is not enabled.

PORTAL MODE SELECTION OPTION

It is possible to set the portal mode to Hybrid or HyLite based on access requirements.

In Hybrid mode, portal will download HySecure client (and optionally HyWorks client), which enables user to access all type of applications.

In HyLite mode, only HyWorks published applications, TSE Apps and RDP based applications can be accessed. HyLite mode does not require installation of any agent on end user machine.



The image shows a web form titled "Web Portal logon mode selection". It contains three rows of settings:

- "Enable HyLite mode." with a checked checkbox.
- "Enable Hybrid mode." with an unchecked checkbox.
- "Select Default logon mode." with a dropdown menu currently showing "HyLite Mode".

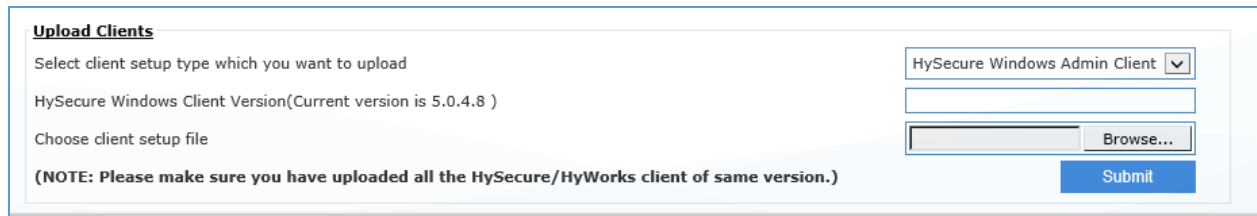
A blue "Submit" button is located at the bottom right of the form.

HYSECURE CLIENT MODE: ON-DEMAND CLIENT

It is now possible to install and use HySecure client on a machine without requiring administrative rights. HySecure client on-demand mode does not install files in %PROGRAMFILES% and do not perform tasks that require administrative rights. The new on-demand client mode uses a different technology than the full client mode. On-demand client is useful for access from unmanaged PC where the IT team as well as the user do not have administrative rights, for e.g. Contractor PC of a vendor.

UPLOAD NEW CLIENTS

It is possible to upload latest HySecure client installers from management console. It is possible to upload both type of clients, HySecure client and HySecure On-Demand client. When the new installers are uploaded, the version must be updated. Auto upgrade of client must be enabled from client settings to push the new client versions to end users.



Upload Clients

Select client setup type which you want to upload

HySecure Windows Client Version(Current version is 5.0.4.8)

Choose client setup file

(NOTE: Please make sure you have uploaded all the HySecure/HyWorks client of same version.)

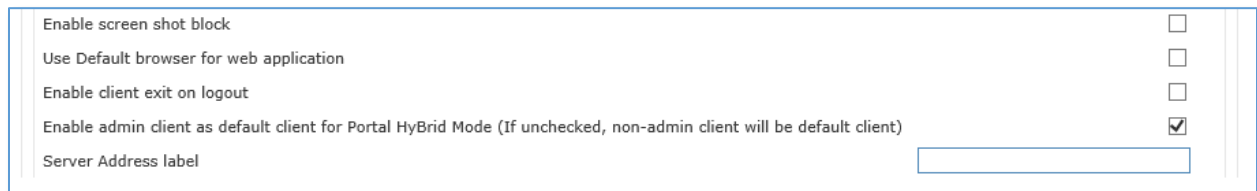
HySecure Windows Admin Client

Browse...

Submit

NEW CLIENT SETTING

Following new options are added as client settings:



Enable screen shot block ☐

Use Default browser for web application ☐

Enable client exit on logout ☐

Enable admin client as default client for Portal Hybrid Mode (If unchecked, non-admin client will be default client) ☒

Server Address label

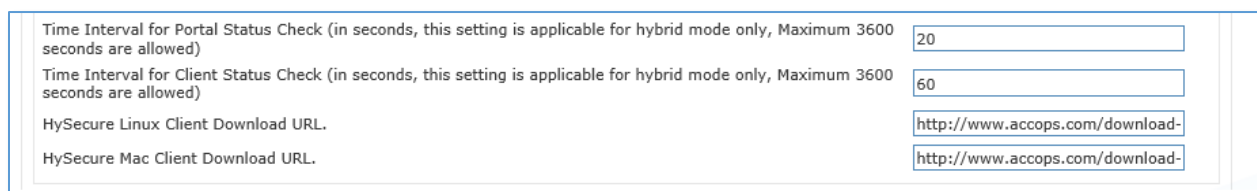
Enable screen shot block: If this option is enabling then after login into HySecure, screen capture function will be disable.

Use Default browser for web application: If this option is enabled then after login into HySecure, published web application will be launching in user's machine default browser.

Enable client exit on logout: While log out from HySecure client, client will be exit if this option is enabled.

Enable admin client as default client for Portal Hybrid Mode (If unchecked, non-admin client will be default client): By default, non-admin client will be used in case of Hybrid mode. But if this option is enabled then HySecure full client (admin client) will be used.

Server address label: HySecure admin can change the label of server address of HySecure windows client.



Time Interval for Portal Status Check (in seconds, this setting is applicable for hybrid mode only, Maximum 3600 seconds are allowed)

Time Interval for Client Status Check (in seconds, this setting is applicable for hybrid mode only, Maximum 3600 seconds are allowed)

HySecure Linux Client Download URL.

HySecure Mac Client Download URL.

Time Interval for Portal Status Check: HySecure admin can specify time interval for portal status check.

Time Interval for Client Status Check: HySecure admin can specify time interval for client status check.

HySecure Linux Client Download URL: URL to download Linux client

HySecure Mac Client Download URL: URL to download MAC OSX client

Following setting added in HyWorks client setting.

Enable Hyworks exit with HySecure Logout.	<input type="checkbox"/>
Enable HySecure logout on Hyworks license error.	<input checked="" type="checkbox"/>
Enable full width (Double-byte) characters check in username and password.	<input checked="" type="checkbox"/>
HyLite Keep Alive Time Interval (in minutes, this setting is applicable for HyWorks only, Maximum 60 minutes are allowed)	<input type="text" value="5"/>

Enable Hyworks exit with HySecure Logout: If this option is enabled then HyWorks client will be exit when log out from HySecure client.

Enable HySecure logout on Hyworks license error: If there is any HyWorks license related issue then HySecure client log out automatically.

Enable full width (Double-byte) characters check in username and password:

HyLite Keep Alive Time Interval (in minutes, this setting is applicable for HyWorks only, Maximum 60 minutes are allowed): Admin can specify HyLite keep alive time for HyWorks application only.

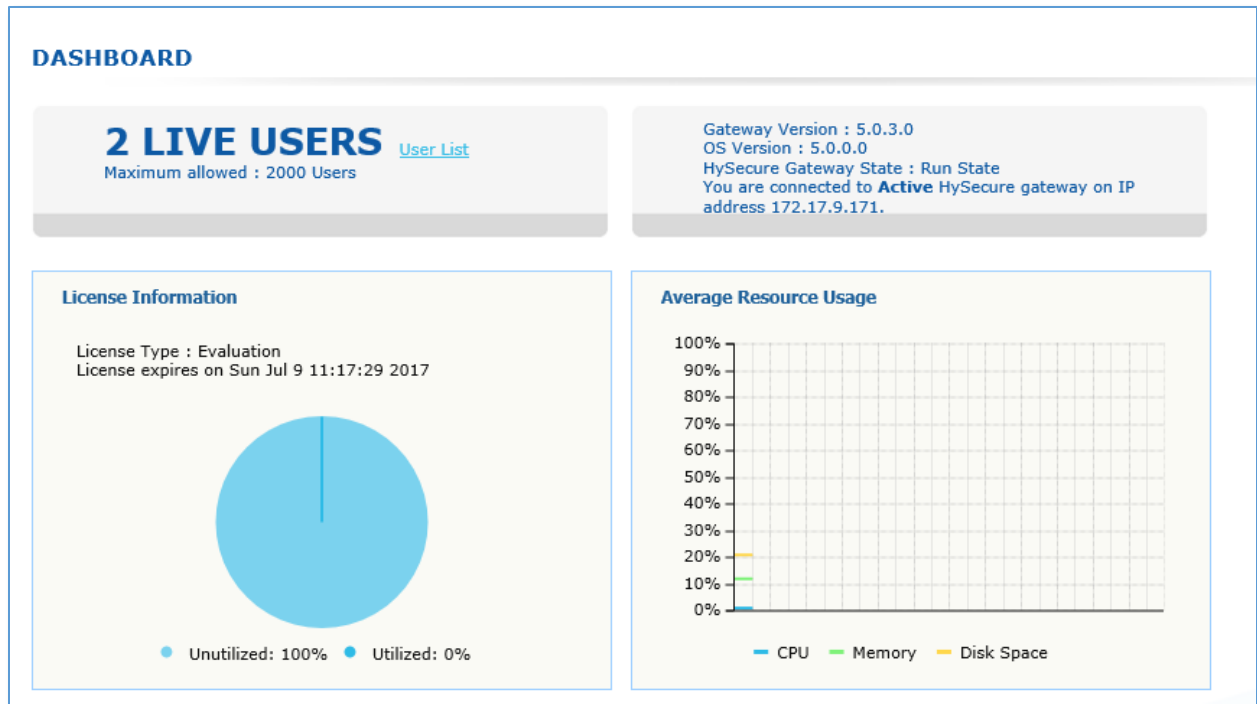
NON-WINDOWS CLIENT DOWNLOAD LINK

Download link for Linux and MAC OSX client are now linked to Accops website www.accops.com

The URLs can be updated from management console.

ADOBE FLASH REQUIREMENT ON DASHBOARD REMOVED

The charts on HySecure dashboard do not require Adobe flash any more. The charts are now developed in java script only.



UNLIMITED LOG ARCHIEVING FILES POSSIBLE

It is now possible to set any number of log archiving files. The total size of logs stored on gateway is limited by the total hard disk size available.

SUPPORT FOR NAME RESOLUTION FOR 64BIT APPLICATIONS

Till last release, for supporting name resolution in 64bit applications, hosts file-based name resolution is to be used, which required additional setting on end user PC (enable option "Use hosts file for name resolution" from client preferences).

From 5.0.5035 version, 64bit applications will have same capability support as with 32bit applications.

SECURITY ISSUES FIXED IN 5.0.5035

SSL / TLS VERSION UPGRADE

SSL / TLS version is upgraded to support TLS 1.2.

It is possible to disable vulnerable protocols like SSL 3.0, even TLS 1.0 and TLS 1.1.

SECURE CIPHER SUPPORT

All the latest and secure TLS 1.2 based ciphers are supported and enabled by default.

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)	FS
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		

FIX FOR VULNERABILITIES

DROWN:	Fixed
Secure Negotiation:	Supported
BEAST Attack:	Fixed
POODLE (SSL v3):	Fixed
POODLE (TLS):	Fixed
Downgrade upgrade protection:	Fixed
SSL/TLS compression:	No
Heartbleed:	Fixed
Ticketbleed:	Fixed
OpenSSL CCS (CVE-2014-0224):	Fixed
OpenSSL Padding Vul. (CVE-2016-2107):	Fixed
Strict Transport Security (HSTS):	Yes

SECURE HTTP HEADER

Content-Security Policy:

Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets. Analyze this policy in more detail.

```
default-src blob: https: http: wss: accopshysecureclient: data: 'unsafe-inline' 'unsafe-eval'
```

X-Frame-Options

X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking.

```
SAMEORIGIN
```

Strict-Transport-Security:

HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS.

```
max-age=31536000; includeSubDomains; preload
```

X-Xss-Protection

X-XSS-Protection sets the configuration for the cross-site scripting filters built into most browsers. The best configuration is "X-XSS-Protection: 1; mode=block".

```
1; mode=block
```

X-Content-Type-Options

X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options:

```
Nosniff
```

Referrer-Policy:

Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.

```
origin-when-cross-origin
```

ISSUES FIXED IN 5.0.5035

CLUSTER WHOLE SYSTEM BACKUP

Whole system backup of a cluster system can be taken and applied on a fresh HySecure gateway. The backup must be taken from the Active cluster manager node in the cluster. The backup must be applied to the first node in the cluster.

REINSTALL FIRMWARE OPTION FIXED

When choosing option "Reinstall firmware", it was not uninstalling the cluster module correctly.

SSH CONFIGURATION FUNCTION NOT WORKING ON STANDBY NODE

SSH configuration option is fixed on standby node

HYSECURE SERVICE RESTART DOES NOT FUNCTION FROM OS CONSOLE

The issue in restarting the HySecure service from console is fixed

HYLITE LICENSE SYNC

When HyLite license is applied to HySecure gateway, the license is synchronized with all nodes in the cluster

HYID WORKS FOR NATIVE USERS

When HyID policy is created for native user. OTP is not asking for native user. This issue is fixed in this release.

AUTO-BACKUP OPTION NOT STARTING AFTER REBOOT

If HySecure gateway is restarted, the backup-schedule does not start automatically

FILE SYNCHRONIZATION ISSUE

Following files are not synchronized across the cluster.

SSL/ TLS configuration keep alive settings, time out settings and HyLite license

HYSECURE OS CONSOLE UI ISSUE

The OS version and IP address details on HySecure OS console are not displayed correctly. In this release, this issue is fixed.

IMPROVED PROXY SUPPORT FOR HYSECURE WINDOWS CLIENT.

This release includes HySecure windows client which support proxy. Previous client has issue with proxy. We had fixed this issue.

KNOWN ISSUES IN 5.0.5035

FULL SCREEN OPTION DOES NOT WORK ON HYLITE FOR IE 10

Full screen option does not work for Internet explorer 10 on Windows 8.

JOINING STANDBY GATEWAY REQUIRES REFRESH

When joining standby gateway to cluster, the browser needs to be refreshed to get status of cluster joining.

HYID DOES NOT WORK FOR LDAP USER.

HyID two factor authentication does not work when LDAP server is configured for authentication. The issue will be fixed in the next hotfix.

PASSWORD CHANGE ISSUE FOR CERTIFICATE USER

Security officer, administrator and certificate-based users cannot change the password. The issue will be fixed in the next hotfix.

VPN SERVICES RESTART WHILE ADMIN CHANGE IDLE TIME OUT

The issue is fixed now. VPN service will not be started when idle timeout is changed

IDLE TIME OUT FEATURE STOPS WORKING

In HySecure cluster, once failover to standby gateway is completed, the idle timeout function stops working

BOOTSTRAP PAGE GOES TO NOT RESPONDING STATE

While configuring the HySecure gateway, on bootstrap page, the browser may hang and not show the pass phrase of the first security officer. In such case, there are two options:

7. Reinstall HySecure: Chose reset firmware option from HySecure OS console.
8. Do SSH to HySecure gateway and get the passphrase from this file: /home/fes/firstso.passphrase

VIRTUAL IP ADDRESS FEATURE IS BROKEN

Virtual IP address assignment feature does not work on this release.

ISP LOAD BALANCING

ISP load balancing feature does not work in this release. If admin enable this option user will not be able to login.

HA VIRTUAL IP ADDRESS CHANGE

In HySecure cluster, it's not possible to change the virtual IP address

SOMETIMES COPY-PASTE FUNCTION HANG FOR MS EXCEL APPLICATION ON HYLITE MODE

Sometimes copy -paste operation hangs for Microsoft excel application on HyLite mode.

Workaround: Double click on excel row and try to paste contains.

HYSECURE NON-ADMIN CLIENT DOES NOT SUPPORT HYWORKS APP

HySecure non-admin client does not support HyWorks application. Please use HySecure full client for access HyWorks application via HySecure.

HYSECURE INSTALLATION ON HYPER-V TAKES TIME

When installing HySecure ISO on Hyper-V, it can take quite long to install the ISO. This issue happens on some Hyper-V installations.

KNOWN SECURITY ISSUES IN 5.0.5035

MULTIPLE VULNERABILITIES IN SSH (PORT 22)

Following vulnerabilities exist in SSH service available on HySecure gateway

High Severity

CVE-2016-1908:

<https://nvd.nist.gov/vuln/detail/CVE-2016-1908>

CVE-2015-8325:

<https://nvd.nist.gov/vuln/detail/CVE-2015-8325>

CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012

<https://nvd.nist.gov/vuln/detail/CVE-2016-10009>

<https://nvd.nist.gov/vuln/detail/CVE-2016-10010>

<https://nvd.nist.gov/vuln/detail/CVE-2016-10011>

<https://nvd.nist.gov/vuln/detail/CVE-2016-10012>

CVE-2015-6564, CVE-2015-6563, CVE-2015-5600

<https://nvd.nist.gov/vuln/detail/CVE-2015-6564>

<https://nvd.nist.gov/vuln/detail/CVE-2015-6563>

<https://nvd.nist.gov/vuln/detail/CVE-2015-5600>

CVE-2016-6515, CVE-2016-6210

<https://nvd.nist.gov/vuln/detail/CVE-2016-6515>

<https://nvd.nist.gov/vuln/detail/CVE-2016-6210>

CVE-2014-1692

<https://nvd.nist.gov/vuln/detail/CVE-2014-1692>

Medium Severity

CVE-2015-5352

<https://nvd.nist.gov/vuln/detail/CVE-2015-5352>

CVE-2016-1907

<https://nvd.nist.gov/vuln/detail/CVE-2016-1907>

CVE-2016-0777, CVE-2016-0778

<https://nvd.nist.gov/vuln/detail/CVE-2016-0777>

<https://nvd.nist.gov/vuln/detail/CVE-2016-0778>

CVE-2014-2653

<https://nvd.nist.gov/vuln/detail/CVE-2014-2653>

CVE-2016-3115

<https://nvd.nist.gov/vuln/detail/CVE-2016-3115>

CVE-2014-2532

<https://nvd.nist.gov/vuln/detail/CVE-2014-2532>

MITIGATION: Disable SSH service on HySecure to mitigate all the above vulnerability. SSH service can be disabled from HySecure management console.

5.0.5016

Released on 06 May 2017

HOW TO GET HYSECURE 5.0 BUILD 5016

Download the HySecure ISO from this location:

https://propalmsnetwork-my.sharepoint.com/personal/support_accops_com/_layouts/15/guestaccess.aspx?docid=0d91bd5107fd84b618ba914540a53b958&authkey=Act5Za3bpCXnEM-6zT1oJCI

MD5 Checksum of HySecure ISO: **bd2fdc7650a972e70f553fd4f4f67ecf**

Download the HySecure upgrade patch:

https://propalmsnetwork-my.sharepoint.com/personal/support_accops_com/_layouts/15/guestaccess.aspx?docid=0c09389c4305047da9c3cc554be0fa349&authkey=AfTFhK1t-0mjuc8X_V1y5vE

MD5 Checksum of HySecure upgrade patch: **4eca33052c40c8d69465a3792008eb6d**

NEW FEATURES IN HYSECURE 5.0.1.6

NEW HYSECURE HYBRID PORTAL

A new Hybrid mode of HySecure user portal is available in this release. The new Hybrid mode of user portal use HySecure Windows desktop client as agent. When user chooses the Hybrid mode and logs in, the portal detects if the Windows desktop client is already installed or no on the end user PC. If the client is not installed, the portal downloads the desktop client and installs it.

The portal uses the URL scheme to launch the HySecure desktop client.

The Hybrid portal is supported in Internet explorer 10 and above and Chrome.

The screenshot shows the 'Virtual Workspace Portal' sign-in interface. On the left, there is a welcome message and links to download the HySecure and HyWorks clients. On the right, the 'Sign-in' section includes fields for Username, Password, and a dropdown menu for 'HyLite Mode' (highlighted with a red box). Below this is a language dropdown set to 'English (United States)' and a 'Sign-in' button. A 'Forgot Password' link is at the bottom.

USER BASED ACCESS CONTROL LIST

It is now possible to create access control for individual users. In earlier release, access control could be created only for a group.

The screenshot displays the 'CREATE ACCESS CONTROL' form. Fields include 'Access Control Name' (set to 'Access control'), 'Access Control Description', 'Select HySecure Domain' (set to 'DefaultDomain'), and 'Select Authorization Server' (set to 'AD'). The 'Select Assignment Type' dropdown is highlighted with a red box, and its menu is open, showing 'Select option', 'Users' (highlighted with a red box), and 'User Groups'. Below these are fields for 'Access Control Type' and 'Select User Group' with a search bar. 'Add >>' and 'Delete <<' buttons are at the bottom.

CUSTOM ICON FOR EACH APPLICATION.

Now HySecure administrator can upload custom icon for each application. Create application on HySecure management page and then select application and click on upload icon button to upload application icon. After new icon uploaded when user login into HySecure new icon will be displayed on client /portal.

<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Upload Icon"/>				
#	Application Name	Application Address	Port	Dynamic Port
<input type="checkbox"/>	Hyworks-HA2-205	172.17.8.205	38866	No
<input type="checkbox"/>	Hyworks HA1 206	172.17.8.206	38866	No
<input type="checkbox"/>	PSAppSrv41	172.17.8.41	3389	No
<input type="checkbox"/>	PSAppSrv42	172.17.8.42	3389	No
<input type="checkbox"/>	PSAPPSrv43	172.17.8.43	3389	No
<input type="checkbox"/>	PSAppSrv44	172.17.8.44	3389	No
<input type="checkbox"/>	PSCtrl41	172.17.8.41	38866	No
<input type="checkbox"/>	RDP207	172.17.0.207	3389	No
<input type="checkbox"/>	RDS-JAP-500	172.17.8.134	3389	No
<input type="checkbox"/>	RDS107	172.17.8.107	3389	No
<input type="checkbox"/>	RDS 135-IB500	172.17.8.135	3389	No
<input type="checkbox"/>	RDS 136-IB500	172.17.8.136	3389	No
<input type="checkbox"/> Check all <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Upload Icon"/>				

Once click on upload icon button, administrator need to browse icon and click on submit button to upload icon. Icon should be PNG type and size of 48*48. If administrator wants to reset the application icon to default, then click on reset to default button.

APPLICATION ICON UPLOAD

Application Name

Upload icon for application

The logo should be a png file with dimensions around 48x48.

Set default icon for application

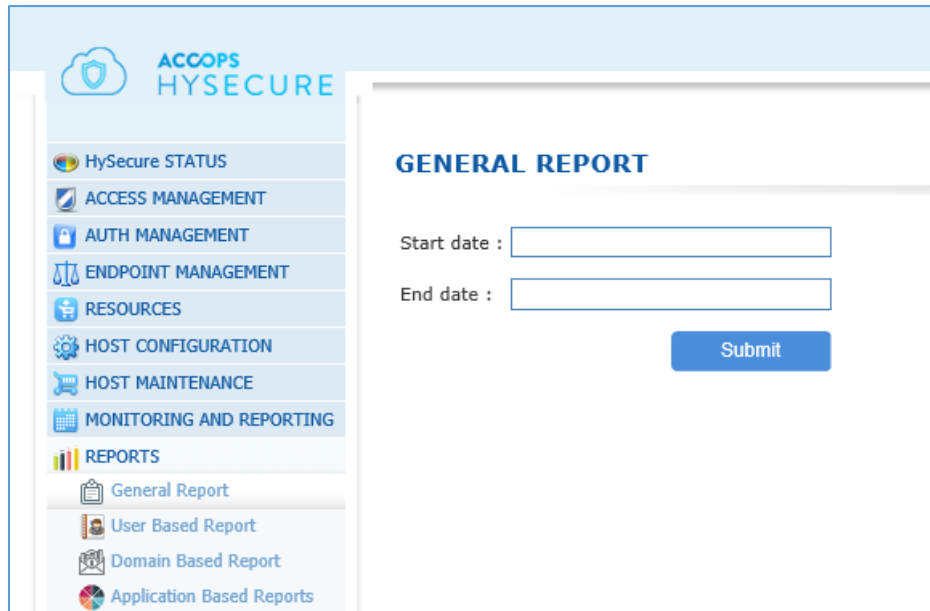
REPORTING OPTION IS AVAILABLE FOR LOG AUDIT

In this release, new reporting option has been added to generate and download various reports. Using this reporting feature administrator can generate custom reports for specific user, domain and application. Following reporting options are available

- General Reporting
- User Base Reporting
- Domain Base Reporting
- Application Base Reporting

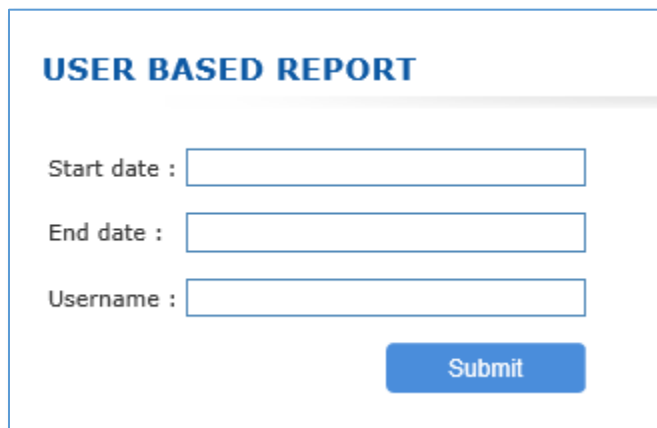
All the reports can be downloaded based on the start date and end date provided by administrator. The report is downloaded as PDF.

General Reporting: This report contains all the summarized reports for the provided start date and end date.



The screenshot shows the Accops HySecure web interface. On the left is a sidebar menu with the following items: HySecure STATUS, ACCESS MANAGEMENT, AUTH MANAGEMENT, ENDPOINT MANAGEMENT, RESOURCES, HOST CONFIGURATION, HOST MAINTENANCE, MONITORING AND REPORTING, REPORTS, General Report, User Based Report, Domain Based Report, and Application Based Reports. The 'REPORTS' section is expanded, and 'General Report' is selected. The main content area is titled 'GENERAL REPORT' and contains two input fields: 'Start date :' and 'End date :'. A blue 'Submit' button is located below these fields.

User Base Reporting: Using this report, user-based reports can be downloaded for a specific user. The report provides information like last session details, application accessed by user, etc.



The screenshot shows the 'USER BASED REPORT' form. It has three input fields: 'Start date :', 'End date :', and 'Username :'. A blue 'Submit' button is positioned at the bottom right of the form.

Domain Base Reporting: This report gives summarized access details for a specific HySecure domain

DOMAIN BASED REPORT

Start date :

End date :

Domain :

Application Base Reporting: This application base report will give details specific HySecure application activity log.

APPLICATION BASED REPORT


Start date :

End date :

Application name :

OPTION TO DISABLE UNSECURE TLS PROTOCOL

It is possible to disable TLS 1.0 and TLS 1.1 support on HySecure.



- HySecure STATUS
- ACCESS MANAGEMENT
- AUTH MANAGEMENT
- ENDPOINT MANAGEMENT
- RESOURCES
- HOST CONFIGURATION
 - Network Configuration
 - Route Configuration
 - Proxy Server
 - SMTP Server
 - SMS Gateway
 - Global Settings**
 - Client Settings
 - Password Expiry Time
 - Database Password
 - SSH Configuration

Current SSL Timeout(Mins): 2
New SSL Timeout

SSL Version 3.0 Support OFF

TLS 1.0 Support ON

TLS 1.1 Support ON

Connection KeepAlive OFF

SUPPORT FOR MORE SECURE TLS CIPHERS

Support for more secure ciphers is added and unsecure ciphers are unchecked by default.

Select New SSL Ciphers

Select cipher

- ☒ ECDHE_RSA_AES256_GCM_SHA384
- ☒ ECDHE_RSA_AES256_SHA384
- ☒ ECDHE_RSA_AES256_SHA
- ☐ DHE_RSA_AES256_GCM_SHA384
- ☐ DHE_RSA_AES256_SHA256
- ☐ DHE_RSA_AES256_SHA
- ☒ RSA_AES256_GCM_SHA384

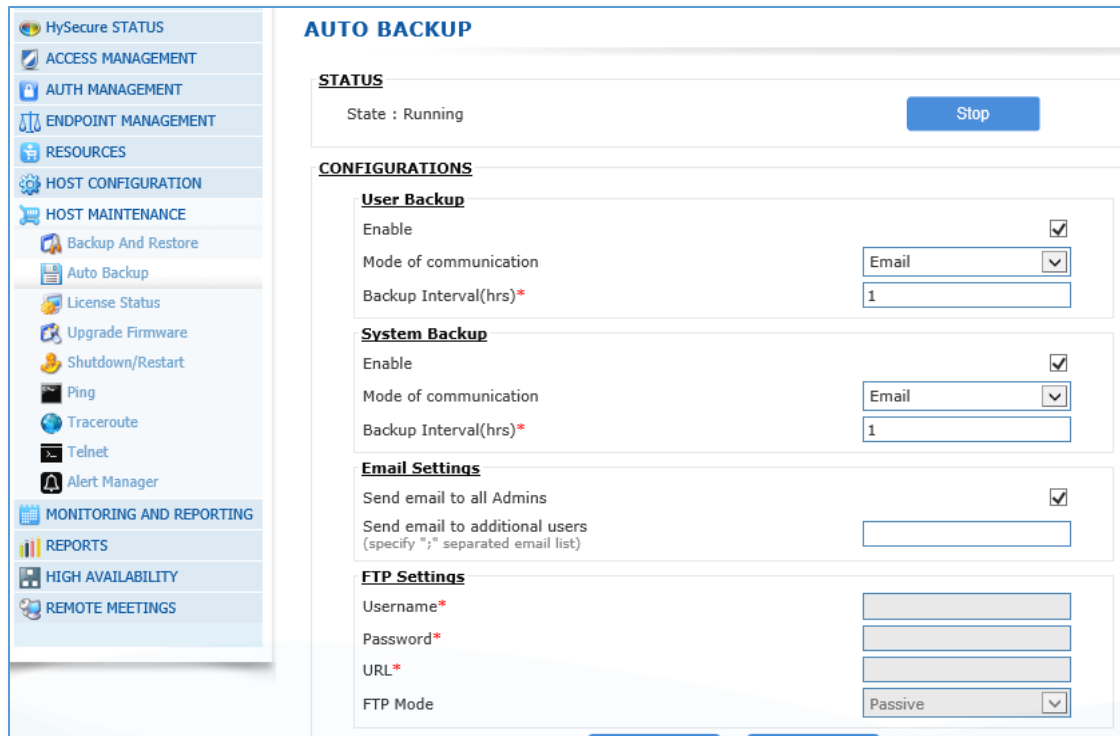
Submit

Note:

1. Default entry is ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256.
2. Selected entries are current ciphers.
3. Ciphers are listed in strengthwise descending order.

AUTO BACKUP OF HYSECURE GATEWAY CONFIGURATION.

New feature to automatically backup HySecure configuration is added in this release. HySecure gateway will generate backup of the configuration and send to specified location or email ID. The configuration backup file can be sent over email to all administrators registered on HySecure or it can be sent to specific email ID. The configuration backup can also be sent to an FTP site. For configuring Auto backup go to Host Maintenance->Auto Backup. Start the auto-backup module first and refresh the screen to check that it's in running status. There are two types of backup, user backup and whole system backup. User backup includes all user and application related configuration. This backup does not include system files and SSL certificates. Such backup can be used to replicate the configuration on a HySecure gateway which is already configured and running. The System backup includes all system files and SSL certificates required to setup a new HySecure gateway.



HYSECURE RESOURCE ALERT MANAGER

This release includes an alert manager to send email notifications when certain resources are under stress. HySecure gateway can send notifications about high CPU, RAM, HDD and Swap space usage. It can also send alerts related to high license utilization.

Configuration option is available Under **Host Maintenance -> Alert Manager**

On Global setting:

Alert Title Prefix*: The subject of email notifications starts with this prefix. The prefix can be used to identify the HySecure cluster identifier.

Data Sampling rate(secs)*: Enter the time in seconds for data sampling

On Alert Setting:

Resource Type: Select the resource type for which alert is to be configured.

Threshold value: Specify the threshold value, when this value is reached, the alert email will be triggered

Alert Rate: Specify this time in minutes as frequency of sending the same alert.

Alert Title: Set the complete subject of the email. The **Alert Title Prefix** is prepended to this title.

Log Alerts in file: If this option is enabled then the alert is also logged in log file.

Enable Email Alert: Enable sending alert over email

Send Alert to all Admin Users: If this option is enabled then resource utilization high alert email will go to all HySecure administration user.

Send Alert to all Security Officers: Send alert email to all HySecure administrators

Send Alert to additional Users: Send alert to additional email IDs

ALERT MANAGER

STATUS
State : Running Stop

CONFIGURATIONS

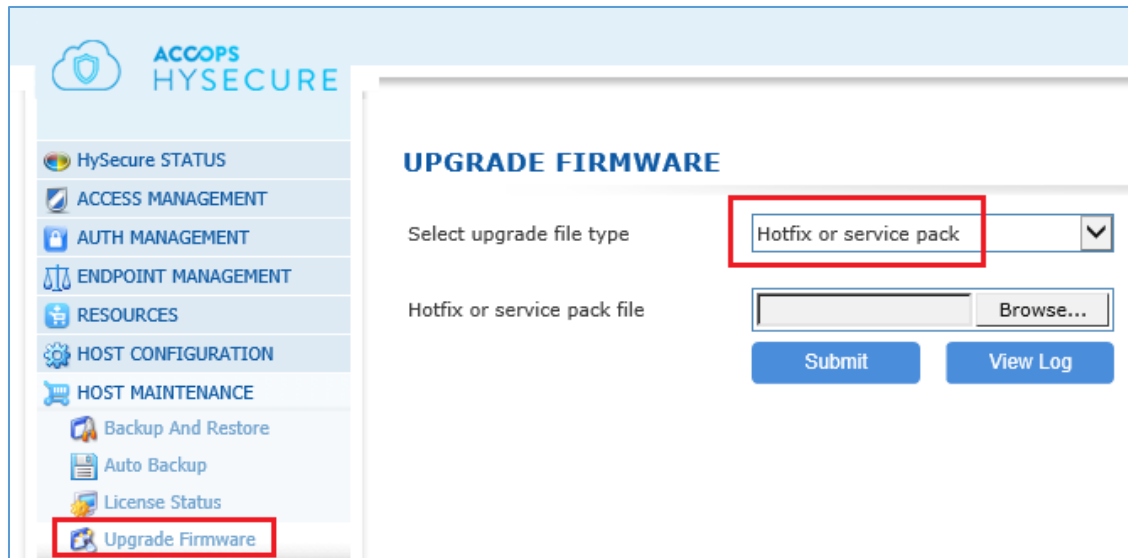
Global Settings
Alert Title Prefix*
Data Sampling rate(secs)*
(Rate at which resource usage should be checked)

Alert Settings
Resource Type
Enable ☒
Threshold value(%)*
Alert Rate(mins)*
Urgency Level
Alert Title*
Log Alerts in file ☒
Enable Email Alert ☐
Send Alert to all Admin Users ☐
Send Alert to all Security Officers ☐
Send Alert to additional Users
(Specify email list separated by ";")

Submit

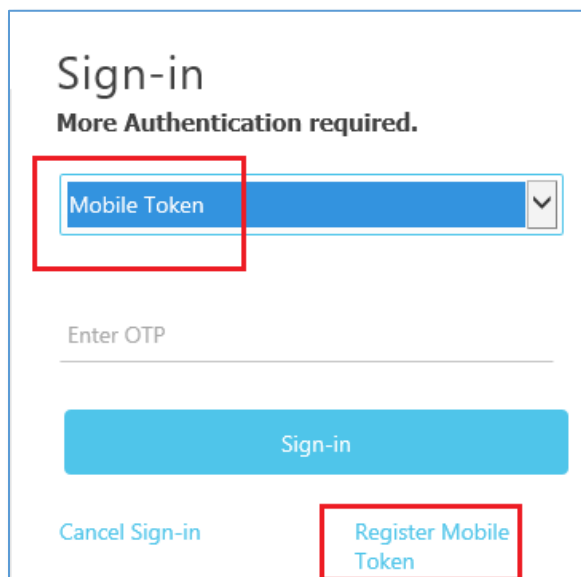
OPTION TO APPLY HOTFIX WITHOUT RESTARTING HYSECURE

When applying upgrade patch to HySecure, gateway state must be changed to Configuration state, which restart the HySecure service and active connections get disconnected. However certain hot fixes do not require HySecure service restart. A new hotfix mode is added so that HySecure service do not require restart.



MOBILE TOKEN REGISTRATION

The version enables end users to self-register Accops HyID mobile app for mobile token registration. Users can open HySecure user portal and login. If HyID two factor authentication is enabled for the user, user can see the option to register the mobile app token. For registration of mobile token, email or SMS based OTP is also required.



Now mobile token registration window will pop up. Select Mobile or Email OTP to get OTP and click on send button.

Mobile Token Registration

ACCOPS
HYSECURE

How do you want to get one time password?

Email OTP
SMS OTP

Cancel Send

Mobile Token Registration

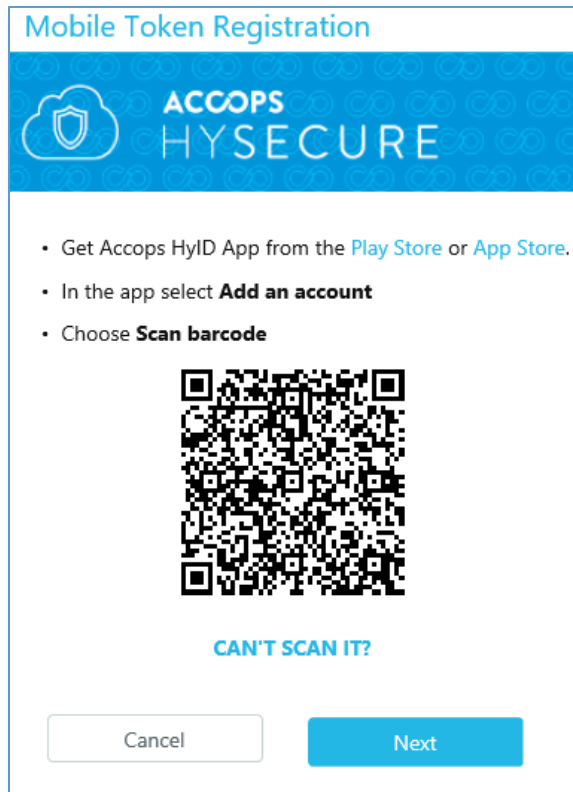
ACCOPS
HYSECURE

Enter one time password

Didn't get it? Resend

Back Next

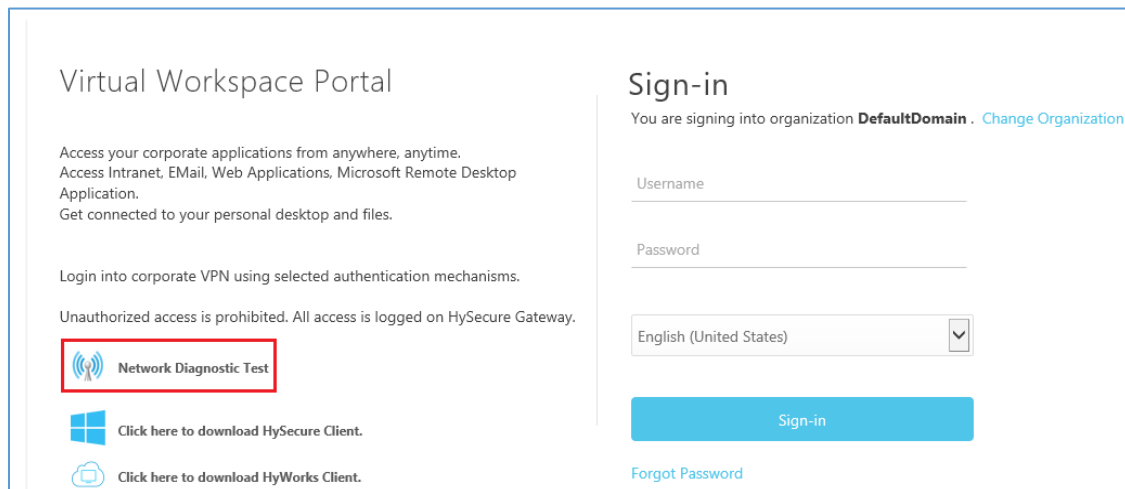
Scan this QR code using Accops HyID app. If QR code is not working, then click on CAN'T SCAN IT? link to get registration key for manual registration.



User can download HyID mobile application from google app play or iOS apps store. Using this HyID app user need to scan QR code or manually enter registration number. Once token is configured then user can verify the token using this portal also.

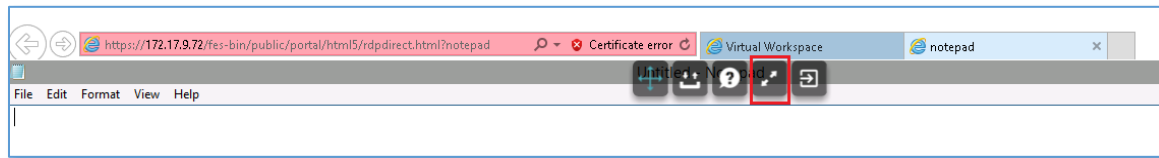
NETWORK DIAGNOSTIC TEST OPTION FOR END USER.

On HySecure portal, user can check the health of network to confirm that they do not have any network related issue when accessing the application.



FULL SCREEN OPTION ON HYLITE.

A new menu option is added on HyLite portal to switch to full screen mode.



HYWORKS APPLICATION PUBLISHING

To publish HyWorks via HySecure, Create applications of two type:

- a. HyWorks – Controller (Primary)
- b. HyWorks – Application Server

In case HyWorks secondary server is available, publish another application of type HyWorks – Controller (Secondary).

Important: If HyWorks Controller is published with hostname in HyWorks management console, then publish the controller with hostname. Port number for HyWorks Controller is 38866.

Shared Hosted Desktop and hosted application: Publish each Microsoft RDS Session Host server as *HyWorks – Application Server* in HySecure. Specify the same hostname or IP address as published in HySecure, with port 3389.

Virtual Desktop: Publish an application in HySecure of network type application to allow access to the full subnet in which Virtual Machine exists. There is no *HyWorks – Application Server* to be created for Virtual Desktop access.

The name of the application given to HyWorks object is not visible to end users.
All names must be in English and non-English characters are not supported.

HYWORKS ORGANIZATION MAPPING

HySecure VPN realms must be same as HyWorks Organization names.
HySecure does not support non-English realm names.

LDAP SUPPORT (AUTHENTICATION SERVER)

New option to add LDAP as a separate authentication server is added.

Go to AUTH MANAGEMENT -> Authentication Servers. Click on Add button and select AD/LDAP. Now select LDAP as server type and enter LDAP details information.

CREATE AD/LDAP AUTHENTICATION SERVER

Server Type: LDAP

Server Name: TestLDAP

IP Address/Host Name: 172.17.6.3

Port: 389

Admin Bind DN: cn=admin,dc=accops,dc=com

Admin Password:

Base DN: 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: ☐

User Interface Configuration

Message for Users:

Username label: Username

Password label: Password

Test Connection Submit Reset

HYLITE (HTML5) SUPPORT AUDIO ON IE BROWSER.

Support for audio for Internet explorer 10 is added.

SUPPORT FOR 2-BYTE CHARACTER

Support for 2-byte character on login screen is blocked. The option is configurable, but option is not available on management console.

HYSECURE WINDOWS CLIENT - 5042

The new client includes following features:

- Hostname resolution support for 64bit applications is added
- Fall back to LSP mode-based filtering when driver fails to load. This scenario is possible on Windows 10 OS with SecureBoot option on where the HySecure client driver may not install.

IMPROVED ENDPOINT SECURITY SUPPORT

The new client has improved support for endpoint security. If HySecure endpoint security module cannot detect the antivirus and firewall based on WMI, then it falls back to heuristic based search.

HYSECURE NON-ADMIN WINDOWS CLIENT

HySecure client has a new mode called On-Demand mode. The On-Demand mode is a Windows installer which does not require admin rights on end user machine. On-Demand can be downloaded and provided to users from following path.

<https://hysecuregateway/fes-bin/public/NVPNClientSetup.exe>

Following are key differences between HySecure Full client (requires admin rights) and On-Demand client

1. On-Demand client installs the files in %localappdata\Accops HySecure Client% directory on user PC and hence does not require admin rights on end user PC
2. On-Demand client does not install a kernel driver or Windows LSP and NSP modules which require admin rights for installation.

KNOWN ISSUES IN 5.0.5016

FULL SCREEN OPTION DOES NOT WORK ON HYLITE FOR IE 10

Full screen option does not work for Internet explorer 10 on Windows 8.

JOINING STANDBY GATEWAY REQUIRES REFRESH

When joining standby gateway to cluster, the browser needs to be refreshed to get status of cluster joining.

HYID DOES NOT WORK FOR LDAP USER AND NATIVE USER.

HyID two factor authentication does not work when LDAP server or local database of HySecure is configured for authentication. The issue will be fixed in the next hotfix.

PASSWORD CHANGE ISSUE FOR CERTIFICATE USER

Security officer, administrator and certificate-based users cannot change the password. The issue will be fixed in the next hotfix.

FILE SYNCHRONIZATION ISSUE

Following files are not synchronized across the cluster.

SSL/ TLS configuration keep alive settings, time out settings and HyLite license

SSH CONFIGURATION OPTION IS NOT WORKING

On standby gateway SSH configuration option not showing.

BOOTSTRAP PAGE GOES TO NOT RESPONDING STATE

While configuring the HySecure gateway, on bootstrap page, the browser may hang and not show the pass phrase of the first security officer. In such case, there are two options:

9. Reinstall HySecure: Chose reset firmware option from HySecure OS console.
10. Do SSH to HySecure gateway and get the passphrase from this file: `/home/fes/firstso.passphrase`

VIRTUAL IP ADDRESS FEATURE IS BROKEN

Virtual IP address assignment feature does not work on this release.

ISP LOAD BALANCING

ISP load balancing feature does not work in this release. If admin enable this option user will not be able to login.

HYSECURE OS CONSOLE UI ISSUE

The OS version and IP address details on HySecure OS console are not displayed correctly.

VPN SERVICES RESTART WHILE ADMIN CHANGE IDLE TIME OUT

If admin changes idle timeout settings, HySecure service restarts, disconnecting all users.

IDLE TIME OUT FEATURE STOPS WORKING

In HySecure cluster, once failover to standby gateway is completed, the idle timeout function stops working

UDP SUPPORT

UDP support is not supported in this release

HA VIRTUAL IP ADDRESS CHANGE

In HySecure cluster, it's not possible to change the virtual IP address

AUTO-BACKUP OPTION NOT STARTING AFTER REBOOT

If HySecure gateway is restarted, the backup-schedule does not start automatically

5.0.5005

Released on 15 Feb 2017

NEW FEATURES IN 5005

HYWORKS INTEGRATION

In this release we have added support of Accops HyWorks integration. So that HyWorks application can be easily accessible from WAN. HySecure administrator need to create HyWorks Controller type and HyWorks Application server type application on HySecure gateway.

CREATE APPLICATION

(Auto Configuration of Standard Applications)

* Mandatory fields.

Basic Options

Type: HyWorks - Controller (Primary) ▼

Name*: Accops HyWorks Controller

Description:

Application Server Address*: 172.17.9.160

Application Port*: 38866

Specify comma or "." separated list. Max 5 elements.

Protocol: TCP ▼

Hidden Application: ☐

Hide Access Pop-up: ☐

Advanced Options

Show Real IP Address of Server: ☐

Enable Compression: ☐

Clustered Application: ☐

Enable session caching: ☐

Auto Launch: ☐

User Options

Enable Single Sign-On: ☒

Use HySecure Credentials: ☒

Domain:

Test Connection

1. Create a new app of type "HyWorks Controller – Primary". Any name can be specified. Server address must be same as the same value specified in HyWorks Controller setting. If the HyWorks controller host address specified on HyWorks management as hostname, provide the hostname here. Port number of HyWorks services is 38866. Leave all other options unchecked with default value
2. Create a new app of type "HyWorks- Application Server". Any name can be specified. Server address must be same as the same value specified in HyWorks Controller setting. If the HyWorks controller standby host address specified on HyWorks management as hostname, provide the hostname here. Leave all other options as default.

Publish HyWorks - Application Server application for each Microsoft RDS Server in the HyWorks cluster

Application Group:

It is recommended to create 1 application group for each VPN Domain (sub-organization) containing only following types of applications:

- HyWorks Controller – Primary
- HyWorks Controller – Secondary
- HyWorks – Application Server: All application servers part of this organization.

Create one application group for each sub-org.

Access Control:

1. One Access control must be created for each VPN domain.
2. Access control should have following details:
 1. Access control name: ibaraki-acl
 2. HySecure Domain: ibaraki (VPN domain for ibaraki)
 3. Select authorization server as common LDAP server.
 4. Access control type: Application Access
 5. Select User Group:
 6. Select the common LDAP group listed in the control
 7. Select Application Group:
 8. Select the ibaraki application group name: ibaraki-app-group

Create one ACL for each sub-org. Each sub-org must have access only to their own application-group created on HySecure. That means user of sub-org A cannot access RDS server of sub-org B

LDAP SUPPORT (AUTHENTICATION SERVER)

In this release HySecure server can support LDAP user database. Now HySecure administrator can integrate LDAP on HySecure server.

Go to AUTH MANAGEMENT ->Authentication Servers. Click on Add button and select AD/LDAP. Now select LDAP as server type and enter LDAP details information.

MOBILE TOKEN REGISTRATION

Now end user able to do Accops mobile token registration using online. If administrator assign HyID mobile token to end user. Then open and try to login using web portal. Select Mobile token and click on link called “Registered Mobile Token”

Now user need to select email or SMS OTP. Then OTP will be sending to user’s email id or mobile number. Next screen user needs to enter received OTP and click on next button to get mobile token registration code/QR code.

User should download HyID software from google app play or iOS apps store. Using this HyID app user need to scan QR code or manually enter registration number. Once token is configured then user can verify the token using this portal also.

NEW HYSECURE WINDOWS CLIENT

New HySecure windows client 5.0.1.1 added in this release. We have fixed some bugs and crashed in this client. This windows client supports HyWorks application. If HyWorks application is publish on HySecure gateway. Then user can access HyWorks application using this client.

NEW HYSECURE NON-ADMIN WINDOWS CLIENT

We have released new non-admin client. Which does not need any administrator right at the time of HySecure installation. Basic or non-admin user can install this client.

NEW WEB PORTAL LOGIN MODE.

In this release Hybrid login mode for web portal added. Using this mode user can login into HySecure gateway can access web, RDP application. This mode will support almost all HySecure client features. At the time of login user need to select Hybrid mode. While user will use this mode Accops client software need to download and install on user machine.

ACCOPS HYSECURE

Virtual Workspace Portal

Access your corporate applications from anywhere, anytime.
Access Intranet, Email, Web Applications, Microsoft Remote Desktop Application.
Get connected to your personal desktop and files.

Login into corporate VPN using selected authentication mechanisms.

Unauthorized access is prohibited. All access is logged on HySecure Gateway.

Network Diagnostic Test

Click here to download HySecure Client.

Click here to download HyWorks Client.

Sign-in

Username

Password

HyLite Mode

English (United States)

Sign-in

[Forgot Password](#)

HYLITE ADVANCE SETTING

In this release we have added more advance HyLite setting. Following setting we have added like display setting and Local setting.

Display setting: HySecure administrator can select color depth and enable touchpad mode.

Local setting: Using local setting administrator can control following HyLite setting.

- Remote audio playback: Controlling audio via HyLite
- Quality of audio: Controlling audio quality via HyLite.
- Enable Clipboard: Enable /disable clipboard.
- Enable Printing: Enable /disable clipboard
- Remote Printer Name: Edit HyLite printer name
- Enable Uploading/Downloading files: Enable /disable file copy.
- Shared Disk Name: Edit shared disk name

The screenshot shows the 'HyLite Settings' window with three main sections: Display Settings, Local Settings, and Advanced Settings. The Display Settings section includes 'Color depth' set to '16 bit' and 'Enable Touchpad mode(Relative mouse movement)' which is unchecked. The Local Settings section includes 'Remote audio playback' set to 'Do not play', 'Quality of audio' set to 'Low', 'Enable Clipboard' checked, 'Enable Printing' checked, 'Remote Printer Name' set to 'Accops Hylite Printer', 'Enable Uploading/Downloading files' checked, and 'Shared Disk Name' set to 'Accops Hylite Storage'. The Advanced Settings section includes several unchecked checkboxes for 'Enable Desktop background', 'Enable Font smoothing', 'Enable Desktop composition', 'Enable Show window contents while dragging', 'Enable Menu and window animation', 'Enable Theme', 'Enable Persistent bitmap caching', and 'Enable RemoteFX'. It also has 'Choose your connection speed to optimize performance' set to 'WAN (10 Mbps or higher with high latency)' and 'Network Level Authentication' set to 'Disable'. A 'Submit' button is at the bottom right.

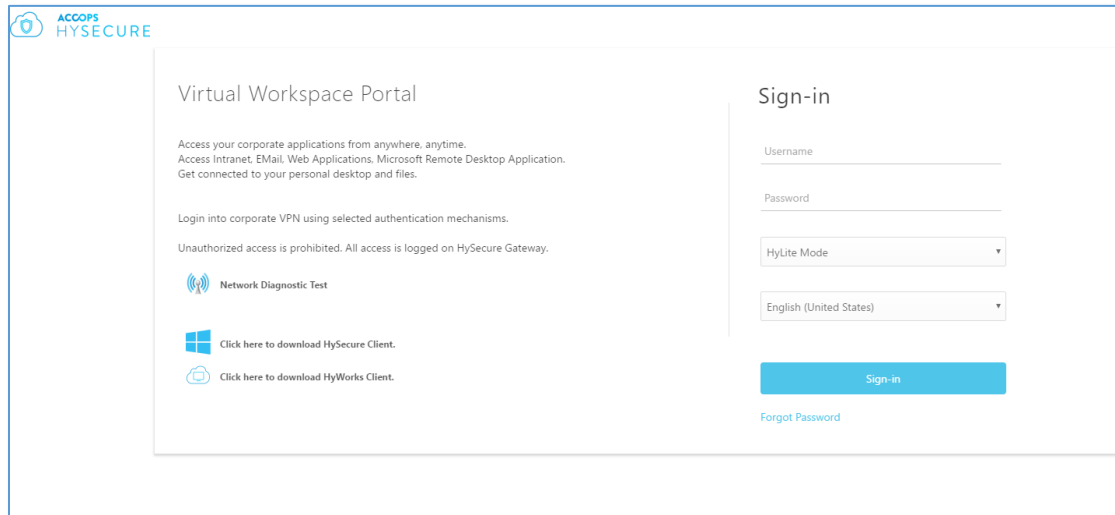
HyLite Settings	
Display Settings	
Color depth	16 bit
Enable Touchpad mode(Relative mouse movement)	<input type="checkbox"/>
Local Settings	
Remote audio playback	Do not play
Quality of audio	Low
Enable Clipboard	<input checked="" type="checkbox"/>
Enable Printing	<input checked="" type="checkbox"/>
Remote Printer Name (Default is "Accops Hylite Printer")	Accops Hylite Printer
Enable Uploading/Downloading files. (Drag files to your screen after connected).	<input checked="" type="checkbox"/>
Shared Disk Name (Default is "Accops Hylite Storage")	Accops Hylite Storage
Advanced Settings	
Enable Desktop background	<input type="checkbox"/>
Enable Font smoothing	<input type="checkbox"/>
Enable Desktop composition	<input type="checkbox"/>
Enable Show window contents while dragging	<input type="checkbox"/>
Enable Menu and window animation	<input type="checkbox"/>
Enable Theme	<input type="checkbox"/>
Enable Persistent bitmap caching	<input type="checkbox"/>
Enable RemoteFX	<input type="checkbox"/>
Choose your connection speed to optimize performance	WAN (10 Mbps or higher with high latency)
Network Level Authentication. ("auto" will connect without NLA at the first time, reconnect with NLA if the connection failed)	Disable
Submit	

HYSECURE HIGH AVAILABILITY (HA)

In this release we have improved HySecure HA. So, this ISO can be installed on HA mode. For details please follow HySecure Cluster Installation document. We have fixed some critical bugs on HA as well as improved the performance of HA.

NEW WEB PORTAL UI

In this release we have improved HySecure web portal UI. Like login page, all button on portal and message dialog box.



NEW ACCOPS HYSECURE OS 5.0

HySecure OS is now based on CentOS 7.2.

KNOWN ISSUES IN 5005

INTERNET EXPLORE NEED TO REFRESH WHILE JOIN STANDBY GATEWAY

At the time of joining standby gateway into HySecure HA cluster using IE browser, administrator need to refresh IE browser manually to get the status of joining.

USE ACTIVE GATEWAY TO DO ANY ADMINISTRATIVE OPERATION.

HySecure administrator should login into active gateway to do any administrative operation on HySecure gateway. Like application creation, authentication server configuration, access control creation etc.

HYID NOT WORKING FOR LDAP USER.

For LDAP user OTP will not work.

LICENSE APPLY STATUS DISPLAY ISSUE.

While apply HySecure license on HySecure gateway, here is issue of display status of license.

PASSWORD CHANGE ISSUE FOR CERTIFICATE USER

Certificate user not able to reset password using client.

HYSECURE VM INSTALLATION ISSUE ON HYPER-V

HySecure VM not able to install on Hyper-V

FILE SYNCHRONIZATION ISSUE

In HA cluster following setting not able synchronize. So HySecure administrator need to do these setting on specific gateway.

SSL version, keep alive, time out

SSH CONFIGURATION OPTION IS NOT WORKING

On standby gateway SSH configuration option not showing.

BOOTSTRAP PAGE GOES TO NOT RESPONDING STATE

Sometimes while do bootstrap of active gateway bootstrap page goes to not responding state and it will not display passphrase of first security officer. But administrator can get the passphrase from firstso.passphrase file from location /home/fes.

SELF-SERVICE PORTAL (SSP) NOT WORKING ON HA SETUP

On HySecure HA setup SSP does not working.

VIRTUAL IP DOES NOT WORK.

Virtual IP feature does not work on this release.

ISP LOAD BALANCING

ISP outbalancing feature does not work on this release. If admin enable this option user will not be able to login.

HYSECURE OS CONSOLE UI ISSUE

HySecure OS console UI issue. IP address and version is display issue

DHCP IP ISSUE ON HYSECURE GATEWAY

If IP address is assigned to HySecure gateway using DHCP. Then try to do pre-boot configuration, automatically HySecure IP address will be unassigned.

VPN SERVICES RESTART WHILE ADMIN CHANGE IDLE TIME OUT

IDLE TIME OUT ISSUE

In HySecure HA setup, if gateway failover is happened. Then Idle time out does not work.

UDP NOT SUPPORT

This release does not support UDP.

HA VIRTUAL IP CHANGE

In HySecure HA setup virtual IP of cluster not able to change once it is assigned.

LOCAL USER GROUP HYID ISSUE

HySecure local user group OTP assignment, does not work.

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 © 2017, Accops Systems Private Limited. All Rights Reserved.