Release Notes

HySecure Gateway Hotfix V6.0.3.3

Last Updated: 06 April 2020

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

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

Contact Accops Systems Private Limited.
Email: info@accops.com
Call: +91 9595 277 001

CONTENTS

OVERVIEW

This document outlines the "HySecure Mac ID validation through external API and user active session" feature and how to apply hotfix on HySecure gateway. It is recommended to apply this hotfix on gateway version 5.2.3.0.

Note: Down time is required while applying this hot fix.

6.0.3.3

Released on 06 April 2020

HOW TO APPLY HOTFIX

UPGRADE COMPATIBILITY OF HOTFIX V6.0.3.3

HySecure Web Login Restriction Hotfix is compatible with HySecure V5230 Setup only.

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

HOW TO GET HYSECURE HOTFIX V6.0.3.3

Download the HySecure Hotfix:
https://propalmsnetwork-my.sharepoint.com/:u:/g/personal/support_accops_com/EdmZ_vuAa7VOlO1XXEicQqQBkFYAHzjMEazriXjeBISKQ?e=WdY9tW

MD5 Checksum of HySecure Web login restriction hotfix: **5824dddd44f438554244701e6dc13f78**

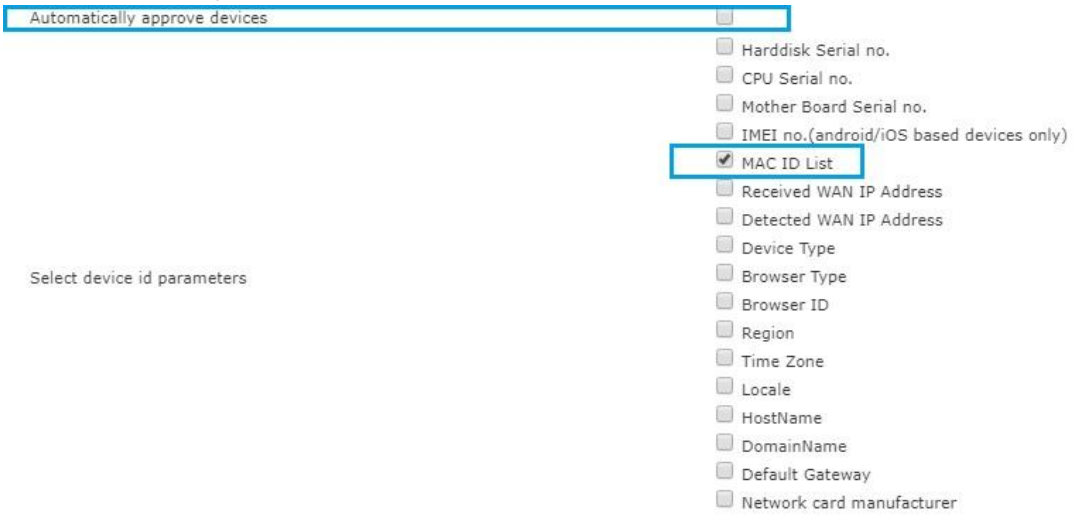
NEW FEATURES IN HYSECURE HOTFIX V6.0.3.3

MAC ID VALIDATION USING EXTERNAL API:

For verifying the authenticity of the device from which user is logging into HySecure gateway, HySecure gateway validate several device parameters like WAN IP, Domain, Mac ID etc. In this Hotfix V6.0.3.3, we have provided support to validating the device's Mac ID using external API.

To configure Mac ID validation using external API, follow below steps:

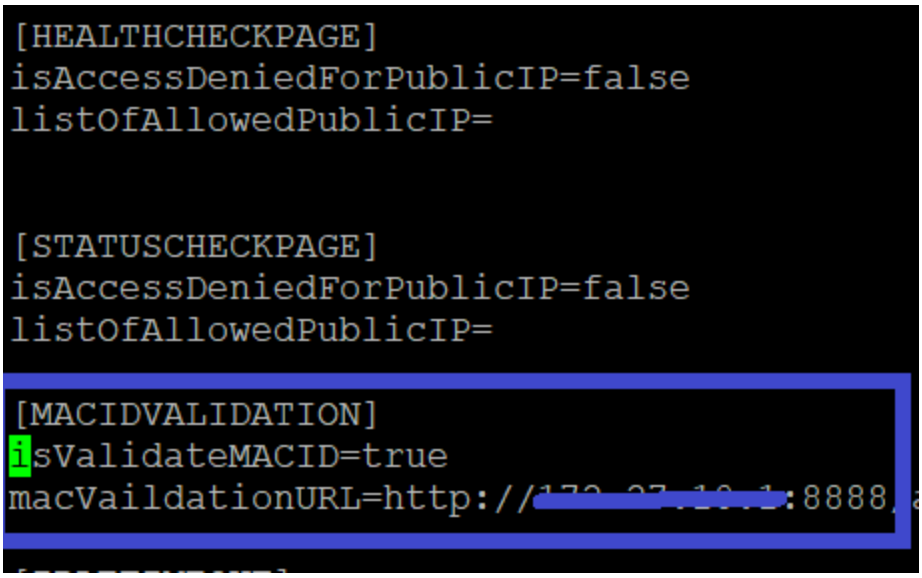
1. Create a device policy for user whose Mac ID should be validated using API.
2. **Uncheck Automatic approval and select MaC ID list as device parameters**.(Refer screenshot below)



3. Take SSH of HySecure gateway Active node.
4. Open local.conf using command: **vim /home/fes/local.conf**
5. Find tag "**isValidateMACID**" and set as true(Refer screenshot below)
6. Find tag "**macVaildationURL**" and set value as URL of Mac ID validation API.(Refer screenshot below)
7. After doing above changes, enter command: **pkill fes**
8. Enter next command: **/home/fes/fes /home/fes**
9. **Follow steps 3-8 in all HySecure gateway nodes.**

Note: After doing any changes in local.conf, fes needs to be restarted.
To restart fes, follow these steps:

- After doing changes, enter command: **pkill fes**
- Enter next command: **/home/fes/fes /home/fes**



Note: isValidateMACID=true means Mac ID will be validated using external API. **To disable Mac ID validation through provided API** set tag *isValidateMACID=false*

How Mac ID validation using external API will work:

When user login from device for the first time, user device Mac ID will be sent to external API for validation. If external API verifies MaC ID, then HySecure will consider above device as authentic device and approve the device for future login.

If user device is found as unauthenticated by API, HySecure will consider device as unapproved and will not allow login from that device.

LOGGING OF ACTIVE USER SESSION:

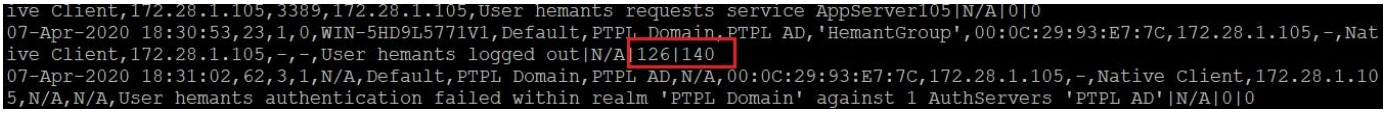
In this Hotfix V6.0.3.3, we have provided support to log the active session out of total user session. This active user session will be calculated by subtracting idle timeout of the user from user's total session time.

Total session time of a user = User logout time – User login time

Active User session = Total session time of a user – Idle time of a user

To check Active user session time:

- Take SSH of HySecure gateway Active/Standby node.
- Open UserLog file using command: **vim /home/fes/logs/UserLog** (Refer screenshot below)



In the above screenshot, 126 is the active user session time while 140 is total user session time.

KNOWN ISSUES IN HYSECURE HOTFIX V6.0.3.3

LOCAL.CONF FILE NOT SYNCHRONIZING AMONG NODES:

Local.conf file does not synchronize among HySecure gateway nodes. So, changes done in Local.conf needs to be done in all HySecure nodes.

APPENDIX A: UPGRADING HYSECURE CLUSTER

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

To upgrade HySecure cluster, follow these main steps:

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

UPGRADING REAL HYSECURE CLUSTER NODE:

1. Connect to Real HySecure Cluster node as Security Officer.

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

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

- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the hotfix installation logs.

UPGRADING STANDBY HYSECURE CLUSTER MANAGER NODE:

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

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

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

UPGRADING ACTIVE HYSECURE CLUSTER MANAGER NODE:

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

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

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

DISABLING MAINTENANCE MODE IN STANDBY NODE

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

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

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

DISABLING MAINTENANCE MODE IN REAL NODE

- Connect to Real HySecure node as Security Officer.

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

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

About Accops

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

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

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