HySecure Quick Start Guide

HySecure 5.0

Last Updated: 25 May 2017
The information contained in this document represents the current view of Accops Ltd. on the issues discussed as of the date of publication. Because Accops Ltd. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Accops Ltd., and Accops Ltd. cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. PROPALMS TECHNOLOGIES PVT. LTD. 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 Propalms Technologies Pvt. Ltd.

Contact Propalms Technologies Pvt. Ltd.
Email: info@accops.com
Call: +91 9595 277 001
## CONTENTS

About HySecure.................................................................4
Understanding HySecure..................................................4
   HySecure components ..................................................4
Deployment Method..........................................................6
Hardware Pre-requisites...................................................8
Integration Requirements...................................................9
   Integration with Directory Services for Authentication, Authorization ......................9
Network Requirements....................................................10
Getting Access to HySecure...............................................10
Reaching Accops Support.................................................10
Installing HySecure OS ....................................................11
Prepping HySecure..........................................................12
   Setup Networking.......................................................12
   Bootstrap the HySecure appliance ..................................14
   Enroll First Security Officer Account ................................18
   Sign-in into HySecure Server .........................................19
   Change to Run State ...................................................20
Configuring HySecure......................................................21
   Setup Authentication Server .........................................21
   Configure Authentication Domain ....................................21
   Create an Application ..................................................22
   Create an Application Group .........................................22
   Create Access Control ................................................23
   Install License ..........................................................23
   Change HySecure State ...............................................24
Logging in as a User.........................................................25
ABOUT HYSECURE

Accops HySecure is an enterprise grade SSL/TLS VPN gateway. Accops HySecure installation requires following steps:
1. Understand HySecure components
2. Decide deployment methods
3. Prepare the hardware
4. Install HySecure ISO
5. Basic Configurations Steps
6. Getting First User Logged in

UNDERSTANDING HYSECURE

HYSECURE COMPONENTS

ACCOPS HYSECURE GATEWAY

Accops HySecure Gateway is a highly scalable service that provides secure access to corporate applications for incoming users. HySecure Gateway is responsible for:
- Encryption/Decryption of all VPN traffic
- Session Management
- Application Proxy
- Policy Management
- Audit logging

HySecure is highly scalable in terms of number of users it can handle. It can go from 10 to thousands of users utilizing minimum amounts of hardware resources.

ACCOPS HYSECURE MANAGEMENT CONSOLE

Accops HySecure has a web based management console for easy and centralized user management, session management, policy management and server configuration control. The console also provides a graphical dashboard showing live users, license usage, resource usage and important gateway information. Reports of user activity can be generated and downloaded. The management console has built in granular administrative roles. There are two types of administrators namely Security officers and Administrators. Both security officers and administrators must login using certificates generated from the console.

Accops HySecure management console can be accessed through the Web Portal or HySecure Desktop Client login methods.
ACCOPS HYSECURE WEB PORTAL

Users can login into HySecure using the HySecure web portal interface. Web portal has two modes:

- HyLite: Clientless HTML5 based RDP client for access to hosted virtual applications, virtual desktops and Microsoft RDP type applications
- Hybrid: Client agent enabled access mode to provide full access to web based, client-server based and all other TCP and UDP based applications.

ACCOPS HYSECURE CLIENTS

Users can download and install Accops HySecure desktop client to login into HySecure gateway to access the published applications. HySecure desktop clients are available for following platforms:

- Microsoft Windows operating system
- MAC OSX
- Linux
- Android App
- iOS Mobile App

ACCOPS HYSECURE OS

Accops HySecure OS 5.0 is a security hardened, enterprise class Linux distribution derived from the open source CentOS distribution. HySecure OS comes as an integrated installer for the base OS, dependency services and all HySecure components, in form of an ISO.

When installed, HySecure OS has a small menu driven interface to manage host configuration like network settings modifications or reinstallation of firmware.

HySecure ISO can be burned onto a CD/DVD or can be used to create a bootable USB.

HySecure OS can be installed on any 64bit x86 based hardware platform or on virtual machines.

NB: Installing the Accops OS will erase all existing data off your system without asking about details of partition.

Installing HySecure OS installs following components
1. Accops HySecure Gateway
2. Accops HySecure web based management console
3. Accops HySecure User web portal
4. Accops HyLite – Clientless HTML5 Hosted Application access portal
5. Accops HyID – Two factor authentication function

ACCOPS HYSECURE CLOUD / VIRTUAL APPLIANCE

Accops HySecure is also available as a virtual appliance with Accops HySecure ISO pre-installed. The Accops HySecure virtual appliance is available for following platforms:

1. Microsoft Azure VM
2. Amazon AWS

Please contact support@accops.com to get the latest virtual appliance.

Accops HySecure can be made available as virtual appliance for deployment on on-premises infrastructure based on VMWare ESX and Microsoft Hyper-V
DEPLOYMENT METHOD

HySecure can be deployed as a standalone gateway or as a cluster.

STANDALONE INSTALLATION IN DMZ

Accops HySecure can be installed on a physical or virtual host with following deployment topology

CLUSTER INSTALLATION IN DMZ

Accops HySecure can be installed on a physical or virtual host with following deployment topology

If installing HySecure as a cluster, follow this guide for detailed steps:

HySecure Cluster Install and Config Guide - 5.0.3.5
HARDWARE PRE-REQUISITES

Accops HySecure Gateway can be installed using ISO on physical or virtual hosts. The configuration requirements are:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Up to 10 user</th>
<th>Up to 100 users</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1 core</td>
<td>4 cores</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB RAM</td>
<td>8 GB RAM</td>
</tr>
<tr>
<td>HDD</td>
<td>50 GB</td>
<td>100 GB</td>
</tr>
<tr>
<td>Network</td>
<td>100 MBps</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

For detailed sizing, please refer to Accops HySecure admin manual. For standalone deployment only one host is required. For cluster deployment, two hosts are required.

**Physical Host:**
The host should be a 64bit processor, capable to run CentOS 7.2 based operating system. Older hardware machine may have compatibility issues with respect to drivers. Hardware should have a USB port or a DVD drive to boot from the ISO.

*Note: follow instructions here how to create a bootable USB with HySecure ISO*

**On-premise Virtual Machine:**
Accops HySecure is tested on VMWare ESX and Microsoft Hyper-V platform. Deploy resources similar to physical host for the virtual machine to install HySecure ISO. Chose the OS as RHEL 7.0 64 bit if CentOS 7.0 or CentOS 7.2 option is not available. Attach a CD ROM to the VM and select the HySecure ISO.

Follow these steps for VMWare ESX:
1. Create a virtual machine and select OS type as RHEL 7
2. Attached a CD ROM to the virtual machine and mount the Accops HySecure ISO
3. At the end, leave the option unchecked to install the OS on finishing the wizard.
4. Start the virtual machine.

Follow these steps for Microsoft Hyper-v:
1. Create a virtual machine and select OS type as RHEL 7
2. Attached a CD ROM to the virtual machine and mount the Accops HySecure ISO
3. For Hyper-v 2008 R2, when selecting a NIC card, select legacy type network card.
4. Start the virtual machine.

**Cloud Deployment:**
If deploying Accops HySecure in Amazon AWS cloud or Microsoft Azure cloud, please deploy the resources equivalent to mentioned above. Chose the respective machine type. Use the Accops HySecure virtual appliance image to deploy in these clouds. If you are using any other cloud, you must install HySecure ISO using the method prescribed by the cloud provider.
Installing on Amazon AWS
Check Amazon AWS market place for the latest HySecure Ami available from Accops. Contact Accops support team for the latest AMI on AWS.

Accops AMI can run on any instance type including t2.micro (up to 10 users), however a t2.medium instance type is recommended as t2.micro has 2 vCPU.

Accops provides a ready to deploy AMI on Amazon AWS. HySecure OS is pre-installed in the AMI. Except for few systems related configurations like network setup, configuration of HySecure is no different than configuring HySecure on any hardware or virtual machine. Please refer to the guide “Installing HySecure on Amazon AWS” for detailed instructions on AWS specific installation instructions.

Installing on Microsoft Azure
Check Microsoft Azure market place for the HySecure image. Contact Accops support team for the latest Azure image.

Accops HySecure can run on any instance type including Standard_A1 (up to 10 users), however a Standard.A2 virtual machine type is recommended.

Accops provides a ready to deploy virtual machine image for Azure. HySecure OS is pre-installed in the virtual machine image. Except for few systems related configurations like network setup, configuration of HySecure is no different than configuring HySecure on any hardware or virtual machine. Please refer to the guide “Installing HySecure on Microsoft Azure” for detailed instructions on Azure specific installation instructions.

INTEGRATION REQUIREMENTS

INTEGRATION WITH DIRECTORY SERVICES FOR AUTHENTICATION, AUTHORIZATION

HySecure can use existing Microsoft Active Directory, LDAP directory services, Novell e-Directory or RADIUS server for user authentication and authorization.

Following are the details required to configure user authentication:

1. Hostname or IP address of the directory server
2. Search path (domain root or an OU) under which all the target user account exists
3. A service account with credentials (non-interactive login user) with “Account Operator” rights, in FQDN format
4. Shared secret in case of RADIUS server
5. Required port opening from HySecure to the authentication server
   a. Microsoft AD/LDAP: port 389 for user authentication, port 636 for user password change or secure authentication
   b. UDP port 1812 when integrating a RADIUS server
NETWORK REQUIREMENTS

With a single node deployment HySecure needs only 1 IP address. When deployed in DMZ, firewall must allow inbound traffic on port 443 to HySecure from WAN or LAN to DMZ and allow outbound connections on required application ports from HySecure to application servers, DMZ to LAN.

If HySecure is to be accessible over Internet, port 443 on firewall should be set in NAT for HySecure IP address.

When deploying a cluster, each HySecure node requires an IP address for the HySecure host. In addition to IP address for HySecure host, an additional IP address in same network is required as Virtual IP address for the cluster.

Users will use this virtual IP address to access the cluster. On firewall, inbound traffic on port 443 should be allowed to HySecure hosts. Outbound traffic from HySecure hosts should be allowed from DMZ to LAN for the required application port. On firewall, inbound port 443 should be set in NAT for the virtual IP address assigned to HySecure cluster.

GETTING ACCESS TO HYSECURE


REACHING ACCOPS SUPPORT

Accops support is available at support@accops.com or https://support.accops.com.
INSTALLING HYSECURE OS

1. Attach the bootable DVD drive with the physical host or virtual machine and start the host.
2. On the installer prompt, press Enter key to start installing using DVD drive.

![Image of installer prompt]

3. Installation of HySecure OS will start and it will take approximately 10 minutes based on hard disk size to complete. The installation process will not require any input.

4. After installation is completed, the host will reboot. Remove the bootable DVD drive and let the host reboot.

5. After completion of the installation, following prompt will come up

```
Accops HySecure OS VERSION: 5.0.0.0
Accops HySecure SERVER VERSION: 5.0.2.3

eth0 [STATIC] [UP] 172.17.9.100

Login using console administrator account.
Default Username: consoleadmin
Default Password: adminconsole
hysecuresslvpn login: _
```
PREPARING HYSECURE

Perform following tasks to configure HySecure
1. Set up Networking
2. Bootstrap the appliance
3. Create the gateway self-signed SSL certificate
4. Create first Security Officer (HySecure administrator)
5. Configure basic settings
6. Change to run mode

SETUP NETWORKING

The default IP Address assigned to the first network interface card of HySecure is a static IP address 172.17.9.100.
All networking settings can be done from HySecure web management console by visiting https://hysecure-IP-address in local browser of PC.
If HySecure OS does not have a valid IP address, and to setup other basic networking settings, login into HySecure OS Console as user “consoleadmin” with default password “adminconsole”.
Choose “Network Configuration” (Enter 1) and then Choose “Configure Ethernet Device” (Enter 1).
Select 0 to choose eth0 interface. If you see a different interface name like eth1 or eth2, select the numeric digit to select the network interface. For e.g. enter 1 for eth1 and 2 for eth2.

It is recommended to do all other network settings from HySecure Web based management console.
BOOTSTRAP THE HYSECURE APPLIANCE

Follow below steps to configure HySecure for use

1. Launch the local web browser of your PC and go to URL  https://HySecure_ip_address/
2. Click on the Configure **HySecure Now**

3. **SYSTEM – CONFIGURATION**
   1. When installing on a local physical host or virtual machine, choose the option for the same to configure network settings.
   2. When installing on public cloud like Amazon Web Services or Microsoft Azure, choose the respective option. When selecting this option, there is no option to set network settings. All network settings including hostname must be done through the management console provided by the cloud vendor.

4. **HYSECURE – SYSTEM CONFIGURATION**
   1. Use this screen to configure network settings
   2. Make sure to configure the hostname on this screen. Hostname cannot be changed after HySecure is configured. This hostname need not be a public DNS name. The initial self-signed SSL certificate is created using this hostname, however the self-signed certificate can be replaced later.
3. Setup IP address, default gateway, DNS and date and time settings. All these settings can be configured later from HySecure web management console.

4. When installing on a public cloud, only date and time settings can be changed on this screen.

5. Select Submit to next screen.

5. SYSTEM CONFIGURATION : INSTALLATION TYPE: Select if installing a standalone gateway or a HySecure cluster. For details on cluster installation, refer to the cluster installation guide: “HySecure Cluster Install and Config Guide”

SYSTEM CONFIGURATION : INSTALLATION TYPE

In case you have a system backup file for HySecure gateway, you can restore the backup from this screen.
6. CA CERTIFICATE: Select to create a self-signed CA certificate

**CA CERTIFICATE**

Certificate Authority Mode
- External CA
- Default Propalms Internal CA

Submit  Reset

7. CREATE SSL CERTIFICATE: Create self-signed SSL certificate

**CREATE SSL CERTIFICATE**

Certificate Authority Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>&lt;Company Name&gt;</td>
<td>Name of the company to which Certificate will be issued.</td>
</tr>
<tr>
<td>Country</td>
<td>&lt;Country Name&gt;</td>
<td>Name of the country where Certificate will be issued.</td>
</tr>
<tr>
<td>State</td>
<td>&lt;State Name&gt;</td>
<td>State where company is based.</td>
</tr>
<tr>
<td>City</td>
<td>&lt;City Name&gt;</td>
<td>City where company is based.</td>
</tr>
<tr>
<td>Validity (days)</td>
<td>&lt;No. of Days&gt;</td>
<td>Validity period for the Certificate. Enter 3650 for 10 year validity</td>
</tr>
</tbody>
</table>

Security Officer Account

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td></td>
</tr>
</tbody>
</table>

Submit  Reset
<table>
<thead>
<tr>
<th><strong>Security Officer Account</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>&lt; First Security Officer</td>
<td>Full name of First Security Officer.</td>
</tr>
<tr>
<td>Email</td>
<td>&lt;Username@domain</td>
<td>Email address of First Security Officer.</td>
</tr>
<tr>
<td>User ID</td>
<td>&lt;User Name&gt;</td>
<td>Basic Authentication Login ID for First</td>
</tr>
</tbody>
</table>
8. On clicking submit, the first security officer (administrator) is created and a passphrase is generated. The passphrase is used to create the SSL client certificate. Security officer (administrator) must always login with SSL Client certificate to administer HySecure.

Copy the passphrase and use it to enroll the security officer SSL certificate.

**ENROLL FIRST SECURITY OFFICER ACCOUNT**

1. On a Microsoft Windows PC, download and install Accops HySecure client from web page [https://hysecure-ip-address](https://hysecure-ip-address)

2. Launch Accops HySecure client, enter HySecure IP Address and select “Login with digital certificate”. In Action file menu, select “Enroll Client SSL Certificate”

3. Enter the passphrase and set password for the security officer account.
4. The enrollment process creates a SSL Client certificate on the user PC. The SSL Client certificate is signed by the CA certificate of HySecure gateway and is installed in the certificate store of the browser. The certificate is non-exportable from the machine.

6. HySecure administrator can be done only from this PC.

7. Note: The passphrase once used cannot be reused on any other machine. To manage HySecure from another PC, create another security officer from HySecure management console.

8. The option “Allow me to export the certificate for mobility” is a special mode to generate exportable certificate. This option can be enabled by a special setting, before using the passphrase to generate the certificate.

SIGN-IN INTO HYSECURE SERVER

Use Accops HySecure client to login into HySecure gateway. Select option “Login with a digital certificate” and select the newly install security officer certificate.
Once authenticated, HySecure management console will open up.

**CHANGE TO RUN STATE**

In order to access HySecure as a non-admin user a Security officer or Administrator needs to move the server into RUN state. This is performed in the Management Console under VPN Status > VPN Server State. Simply click Run State to change the status.
Minimum configuration of Accops HySecure involves following steps:
1. Setup authentication server
2. Configure HySecure realm
3. Create Application
4. Create Application Group
5. Create Access Control List
6. Install License
7. Change to Run State

**SETUP AUTHENTICATION SERVER**

Open HySecure management console, and go to **AUTH MANAGEMENT** section and then **AUTHENTICATION SERVER** page.
Add a new authentication server. You can configure existing Microsoft Active Directory, LDAP or RADIUS server. For details, please refer to HySecure Admin guide.
If you do not want to use external directory server, local database of HySecure can be used.

**CONFIGURE AUTHENTICATION DOMAIN**

Go to **AUTHENTICATION DOMAIN** screen under **AUTH MANAGEMENT** section and edit the default authentication domain. Add the newly create authentication server as server at priority 1. If using the HySecure local database, leave the server at priority 1 as **Native**.
CREATE AN APPLICATION

Under **ACCESS MANAGEMENT** section, go to **Application** page to create an application. It is possible to publish internal web portals as HTTP or HTTPS application, RDP connections, access to Linux servers via SSH, or any client server application.

To publish Propalms TSE, create following type of applications

1. Propalms TSE Web
2. Propalms TSE Application Server: publish each server separately
3. Propalms TSE Print Server: publish each server separately

To publish Accops HyWorks, create following type of applications

1. HyWorks Controller
2. HyWorks Session Host: publish each server separately
3. Publish network range/Subnet when publishing the VDI

CREATE APPLICATION

(Auto Configuration of Standard Applications)
* Mandatory fields.

Basic Options

- **Type**
- **Name**
- **Description**
- **Application Server Address**
- **Application Port**
  Specify comma or "~" separated list. Max. 3 elements.
- **Protocol**
- **Web URL**
- **Hidden Application**
- **Hide Access Pop-up**

Advanced Options

- **Show Real IP Address of Server**
- **Enable Compression**
- **Clustered Application**
- **Enable Session caching**
- **Site to Site Application**
- **Remote Server Name**

Add Application to Application Group

Selected Application Groups

Add Application to Application Group

Submit

CREATE AN APPLICATION GROUP

Add an application group and add the applications created to the application group.
CREATE ACCESS CONTROL

Under **ACCESS MANAGEMENT** section, go to **Access Control** screen and create an access control to allow a user group access to the application group.

**CREATE ACCESS CONTROL**

- **Access Control Name**: TestACL
- **Access Control Description**:
- **Select HySecure Domain**: DefaultDomain
- **Select Authorization Server**: AD
- **Select Assignment Type**:
- **Select User Group**:
  - Search a Group...
  - Add >>
  - Delete <<
- **Select Application Group**
  - Add >>
  - Delete <<
- **Access Filter**: ANY TIME
- **Access Control State**: Enable

INSTALL LICENSE

When freshly installed, HySecure is pre-configured with a trial license for 5 concurrent users valid for 30 days. To install a new trial license or a production license a new serial key can be installed.

Under **HOST MAINTENANCE** section, go to **License Status** screen and add a new license.

To get a new serial key, send a request to license@accops.com
CHANGE HYSECURE STATE

When freshly installed, HySecure is in configuration state. For HySecure to start accepting user connection, change HySecure status to Run mode. Go to **HySecure STATUS** section and **HySecure Gateway State**. Change the gateway state from Configuration to Run state. HySecure services will restart. Logout of HySecure and login again.
LOGGING IN AS A USER

To login as a user, use following access methods

1. Visit HySecure web portal and use Hybrid portal mode
2. Download HySecure client on user PC

HySecure user portal is accessible at https://hysecure-ip-address

User can login into the portal using the configured authentication server. If the configured authentication server is Microsoft Active Directory, user can now login using their domain credentials.

Upon login, with Hybrid mode of portal, the portal will check for client presence and will download and install the client for first time login from user PC.

About Accops

Propalms Technologies Pvt. Ltd. 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 Propalms Technologies Pvt. Ltd. Other names may be trademarks of their respective owners. Propalms 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 © 2016, Propalms Technologies Private Limited. All Rights Reserved.