Accops HyWorks v3.2 Administration

Copyright © 2020, 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

<table>
<thead>
<tr>
<th>Date</th>
<th>Doc Version</th>
<th>Changes</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>02-June-2020</td>
<td>V3.2.0</td>
<td>Draft completed for v3.2</td>
<td>Puneet Shukla</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Controller – Sent for review</td>
<td></td>
</tr>
</tbody>
</table>


Table of Contents

Table of Contents ........................................................................................................................................... 3
About HyWorks Administration .......................................................................................................................... 7
    Target Audience .............................................................................................................................................. 7
    Supported Version ........................................................................................................................................ 7
Introduction to Accops HyWorks ..................................................................................................................... 8
    Overview ....................................................................................................................................................... 8
    Components ................................................................................................................................................. 8
    Terminologies in Accops ............................................................................................................................... 12
Important Ports used by HyWorks .................................................................................................................... 14
HyWorks Controller Management Console .......................................................................................................... 17
    Management Console Browser Compatibility ............................................................................................... 17
    Log in to manage HyWorks .......................................................................................................................... 17
    Administrators of HyWorks .......................................................................................................................... 19
    Log out of HyWorks Management Console ................................................................................................ 19
    Management Console Layout Overview ...................................................................................................... 20
Dashboard – Viewing HyWorks Deployment Details ........................................................................................... 24
Organizations and Multi-tenancy in HyWorks .................................................................................................... 26
    Multi-organization Structuring ...................................................................................................................... 26
    Default Organization .................................................................................................................................. 27
    Organization Configurations .......................................................................................................................... 27
    Organization Resource Sharing Concepts ...................................................................................................... 29
    Organization Management Options ............................................................................................................... 30
Move to Child Organization and Configure Resources at Child Organization ..................................................... 31
Deployment Examples for Different Use Cases .................................................................................................... 32
Functioning of HyWorks in Single/ Multi-organization Deployment .................................................................. 33
Authentication and Authorization in HyWorks .................................................................................................... 34
    Default Authentication and Authorization Configuration Post HyWorks Installation .................................. 34
    System Prerequisites for Adding an Authentication server ....................................................................... 35
    Authentication Servers Management in HyWorks ......................................................................................... 35
    Monitoring Authentication Server Status and Failure Status .................................................................... 38
    Failover Configuration for Authentication Server ....................................................................................... 38
Built-In Directory Server and Local User Management ..................................................................................... 40
    Users ............................................................................................................................................................ 40
    Groups ........................................................................................................................................................... 46
Role based (Delegated administration) from HyWorks Management Console .................................................. 48
    Permissions ................................................................................................................................................... 48
Restoring HyWorks Controller using Backed-up files

Applications and Shared Hosted Desktops Delivery

Supported Platforms

Shared Session Host Management

Session Host Server Teaming and Load Balancing

Applications Delivery

Shared Hosted Desktop Delivery

SHD and Application Delivery in Workgroup (Special Use case)

Dedicated Desktop Delivery in HyWorks

Dedicated Desktop Delivery Model in HyWorks

Dedicated Session Provider Management

Desktop Pools to Deliver Desktops to End-users

Monitoring Desktops

External Session Delivery in HyWorks (TSE and Pano)

External Session Provider Configuration and Desktop Delivery

Additional Configurations for External Session Providers

Connection Profiles

Connection Profile Types

Sessions - Monitoring Logged-in Users/VDI/ Application Sessions

User Sessions

VDI Sessions

App Sessions

Session Provider Management

System

License

HyWorks Backup Configuration

SMTP Configuration

Virtual Profiles

Service Path

Service Config

Advance Config

Syslog Config

Logging and Analysis in HyWorks

Log Database

Viewing Logs on HyWorks Management Console

Log Archiving

Advanced Log Configurations
About HyWorks Administration

*Accops HyWorks Administration* describes how to configure and manage virtual desktop infrastructure using Accops HyWorks.

The guide provides detailed information of step by step processes for effectively deploying and managing VDI infrastructure.

The content in this document includes following information:

- Introduction to HyWorks Components, concepts, and terminology
- Server Configurations of HyWorks
- Virtual Applications and Shared Hosted Desktops delivery
- Dedicated Desktops Delivery

Target Audience

Accops HyWorks Administration guide is intended for system administrators responsible for managing virtual desktop infrastructure using Accops HyWorks.

Supported Version

The content in this document is based on HyWorks v3.2-SP2 release and contains step by step processes as per user interface (Accops HyWorks Management Console) of HyWorks v3.2-SP2 release.

Some of features may not be available in previous releases of Accops HyWorks v3.2.
Introduction to Accops HyWorks

Overview

HyWorks represents product suites to deliver virtualized desktops and applications to authenticated and authorized end-users in a controlled, yet in a very simple manner with minimum complexity.

This section of document consists of following topics:

• Introduction to components of Accops HyWorks
• Important Ports being used by different HyWorks components
• Architectural flow of communication between multiple components
• Terminology

Components

HyWorks is comprised of following important components:

• HyWorks Controller Service
• HyWorks Monitoring Service
• HyWorks Licensing Service
• HyWorks Upgrade Service
• HyWorks Web Interfaces
• HyWorks Session Host Server
• HyWorks DVM Tools
• HyWorks Hyper-V Connector
• HyWorks Endpoints

Each one of these components is briefed in this section:

❖ HyWorks Controller Service

HyWorks Controller service is the core of HyWorks and performs all critical operations centrally. HyWorks controller is primary control layer of HyWorks, to which all HyWorks modules communicates with. HyWorks Controller service operations include:

• Endpoints management and configurations
• User and sessions authentications and management
• Managing session providers and deployment of virtual desktops and application management
• Connection policies management and calculations

HyWorks controller runs as a Windows service and can be installed on Windows server systems (physical or virtual machine), running following operating systems:

• Windows 2008R2-SP1
• Windows 2012R2
• Windows 2016

❖ HyWorks Monitoring Service

Monitoring service collects system performance data from HyWorks Controller server and reports to HyWorks Controller service.

The monitoring service information is used for presenting HyWorks Controller status on dashboard.

❖ Accops HyWorks License Service
Accops HyWorks License Server gets deployed with HyWorks Controller as an add-on Windows service on supported Windows server platforms and is the primary controller layer for managing the licensing. HyWorks License Server can be deployed in separate system as well to serve as a single licensing unit for multi-HyWorks Controller environment.

❖ **Accops HyWorks Upgrade Service**
Accops HyWorks Upgrade Server is required for upgrading the HyWorks DVM Tools on configured Desktops and runs as a Windows service on supported Windows platforms.

❖ **HyWorks Web Interfaces**
An IIS (Web) application installed and managed by HyWorks, to serve following purposes:
- **HyWorks Controller Management Console**: Administrator console for management of HyWorks configurations and deployments
- **HyWorks User Portal**: End-user access portal for accessing virtual desktops and applications
- **HyWorks Reservation Management Portal**: End-user portal for managing and accessing dedicated desktops in lab-based environment.

❖ **Accops HyWorks Session Host Server**
Accops HyWorks Session Host Server module is installed on Microsoft RDS Servers to enable them for serving applications and managed shared hosted desktop sessions.
For enabling real time monitoring of resource consumption on session host servers, HyWorks Monitoring service can also be installed on session host servers. For real time load balancing, monitoring service must be installed and accessible from HyWorks Controller.

❖ **Accops HyWorks DVM Tools**
**Accops HyWorks DVM Tools** is an integrated software package, installed on desktop virtual machines (VMs residing on hypervisors like VMware ESXi, Microsoft Hyper-V or Nutanix AHV). The purpose of HyWorks DVM Tools is to facilitate trouble-free access of desktop to end-users.
Accops HyWorks DVM Tools is comprised of following components:
- Accops HyWorks Desktop Agent
- HyWorks USB Remover Utility
- Built-In USB Redirection Driver (Server-side) module
- Accops Session Server Extensions

**Accops HyWorks Desktop Agent**
Accops HyWorks Desktop Agent gets installed with HyWorks DVM Tools and communicates with HyWorks Controller to achieve following purposes:
- Enabling Remote Desktop services for intended user
- Making the user member of local administrators’ group
- Customizing Desktops being provisioned using HyWorks Controller

**USB Disconnection/Remover Utility**
The utility ensures that all redirected USB devices gets ejected appropriately if user session is disconnected abruptly to avoid possible issues with USB redirection. The utility gets invoked on user session disconnections, system reboot or shutdown.

**Built-in USB Redirection Server module**

HyWorks DVM Tools setup consists of server module of Built-in USB Redirection Driver (to be installed on Desktops) for enabling USB devices redirection plugged on HyWorks Devices. The client-side component is available with HyWorks Clients.

HyWorks also supports ‘Enhanced’ type of USB Redirection Driver also but the server-side component of Enhanced USB Redirection driver must be installed independently.

Important:
- Built-In USB redirection is free and best suited for dedicated Desktop environment.
- Enhanced USB redirection requires additional licensing cost and recommended for session hosted desktops (TSE or Microsoft RDS)

**Accops Session Server Extensions**

Accops Session Server extensions enables monitored and controlled data transfer between Accops endpoints and Accops virtual desktops. Following two server extensions are currently deployed with Accops HyWorks DVM Tools:
- Accops HyPrint PDF Printer: Required for PDF based printing
- Accops HyFr: Required for file transfer between endpoints and virtual desktops

❖ **Accops HyWorks Hyper-V Connector**

HyWorks Hyper-V Connector is required to be installed on Microsoft Hyper-V or SCVMM servers to enable them as desktop provider in Accops deployments.

Hyper-V Connector takes all commands from controller and performs them on Hyper-V or SCVMM servers, which includes:
- Collecting and sharing information of existing VMs
- Power operations on VMs running on Hyper-V or SCVMM servers
- Provisioning of new virtual machines by cloning existing image

❖ **HyWorks Endpoints**

Endpoints running HyWorks Client to facilitate necessary controls and settings for end user to connect to assigned virtual desktops or applications.

These devices can either be Thinclients with integrated HyWorks Client or user desktops running HyWorks Client software. HyWorks supports following types of endpoints in its environment:
- HyWorks Clients for Desktops (Windows/Linux)
- Accops OS or HyOS: Accops customized and preconfigured operating system based on Ubuntu, running integrated HyWorks Client
- HyDesk Devices: Thin-clients which can run in zero or thin-client mode with integrated HyWorks clients, following different HyDesk devices are supported:
  - HY1000
  - HY2000
  - HY3000
Accops HyWorks v3.2 Administration

- HY3020
- HY4000
- HyWorks Clients for MAC OS
- HyLite: Clientless browser-based access enabling end-users to connect from anywhere anytime without requiring any locally installed clients or agents.
Terminologies in Accops

In Accops workspace deployments, following terms can be used frequently:

- **Controller**: Accops HyWorks Controller server
- **Management Console**: Administrator portal for managing HyWorks
- **RMS Portal**: Portal for accessing and managing reservation management system in HyWorks
- **HyLabs**: Reservation management system is referred as HyLabs
- **HySecure**: Accops SSL-VPN software being used for secure access over internet
- **Gateway**: Referred for instances of HySecure servers
- **Endpoints/Devices**: End-user terminals running with Accops HyWorks clients are referred as endpoints or devices
- **HyDesk**: Thinclients embedded with Accops HyWorks Clients
- **HyLite**: Accops HTML5 based access points for connecting applications/ desktops
- **DVM**: Desktop Virtual Machine. Virtual machines configured and managed in HyWorks are referred as DVM.
- **Session Provider**: Session providers are servers which can be used to deliver applications or desktops to end-users. Can be categorized into dedicated, shared, or external providers.
- **Dedicated Session Providers**: Hypervisors (VMware ESXi, Microsoft Hyper-V, Nutanix AHV) or hypervisor management server (VMware vCenter Server, Microsoft SCVMM, Nutanix Prism Central) can be kept under the category of dedicated session providers, which can be used to create and deliver virtual machines as desktops to end-users
- **Shared Session Hosts**: Servers (Microsoft Windows Servers, Ubuntu), which supports multiple user sessions on single instance of servers are referred as Shared Session Hosts.
- **Built-in Directory**: Built-in is HyWorks Controller own user database, can be used for authentication and getting user’s entitlements.
- **Multi-tenancy**: A single HyWorks deployment can be used to serve one or many logical entities of same or different organizations. This kind of deployment structuring is referred as multi-tenancy
- **Organization**: An organization in HyWorks, represents a logical entity, which can be configured to deliver HyWorks managed desktops or applications. The resources in each organization can be shared based on certain rules.
- **Registration**: On first communication with Controller, HyWorks client provides all basic information about endpoint and then controller assigns a unique id for identification of endpoint. The process is known as registration.
- **Heartbeat**: HyWorks clients periodically send status/configuration information to Controller, this periodic status update call is named as heartbeat.
- **Remote Desktop Server (RDS)**: Servers allowing multiple users to remotely access graphical desktops and Windows applications
- **Terminal Server**: Remote desktop servers were previously referred as terminal servers.
- **Shared Hosted Desktop (SHD)**: Servers installed with **HyWorks Session Host Agent** module are referred as shared hosted desktop.
- **Session Host Agent**: HyWorks module responsible for enabling Windows servers to deliver applications and desktops, managing sessions etc.
- **Monitoring Service**: Service responsible for collecting performance data from shared hosted desktop servers and providing it to HyWorks controller on demand.
- **Session Team**: Collection of multiple session host servers, grouped to support load balancing and high availability of shared hosted desktops
- **RemoteApp**: Applications installed on session host servers and configured to be delivered remotely. The RemoteApp once accessed gives, experience of natively installed application only except for the fact that it is running on session host server.
• **Always Seamless**: Application access mode in HyWorks to show remote applications in seamless window with experience of natively installed application. The option is provided in connection profiles.

• **Never Seamless**: Application access mode which basically displays all background activities while sessions are configured. The mode is mostly used for troubleshooting where users are facing connection issues to published applications. The option is provided in connection profiles.

• **Application Publishing**: Process of adding applications in HyWorks is called publishing.
## Important Ports used by HyWorks

Below is the list of ports used by different Accops modules while serving applications or desktop sessions to end-users.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Purpose</th>
<th>Port No.</th>
<th>Protocol</th>
<th>Customizable</th>
<th>Mandatory</th>
<th>If port not open</th>
</tr>
</thead>
<tbody>
<tr>
<td>HyWorks Controller</td>
<td>HyWorks Session Host</td>
<td>Session Info</td>
<td>38871</td>
<td>HTTPS</td>
<td>No</td>
<td>Yes</td>
<td>SHD and application launch will be slow or fail</td>
</tr>
<tr>
<td>HyWorks Controller</td>
<td>HyWorks Session Host</td>
<td>Load Info</td>
<td>38870</td>
<td>HTTPS</td>
<td>No</td>
<td>Yes</td>
<td>Resource based load balancing does not function</td>
</tr>
<tr>
<td>HyWorks Controller</td>
<td>AD / LDAP</td>
<td>User authentication</td>
<td>389</td>
<td>LDAP</td>
<td>No</td>
<td>Yes</td>
<td>User authentication fails</td>
</tr>
<tr>
<td>HyWorks Controller</td>
<td>AD / LDAP</td>
<td>Password Change</td>
<td>636</td>
<td>LDAP</td>
<td>No</td>
<td>No</td>
<td>Password change not possible</td>
</tr>
<tr>
<td>HyWorks Controller</td>
<td>Hyper-V Connector</td>
<td>Hyper-V VM Management</td>
<td>38864</td>
<td>HTTPS</td>
<td>No</td>
<td>Yes</td>
<td>Cannot connect and manage Hyper-V VM</td>
</tr>
<tr>
<td>HyWorks Controller</td>
<td>VMWare vCenter/ESX</td>
<td>VMWare VM Management</td>
<td>443</td>
<td>HTTPS</td>
<td>On</td>
<td>VMWare</td>
<td>Cannot connect and manage VMWare VMs</td>
</tr>
<tr>
<td>HyWorks Controller</td>
<td>Nutanix AHV Server</td>
<td>Nutanix Management</td>
<td>9440</td>
<td>HTTPS</td>
<td>On</td>
<td>Nutanix</td>
<td>Cannot connect and manage Nutanix VMs</td>
</tr>
<tr>
<td>HyWorks Controller</td>
<td>RDS Server Host</td>
<td>RDP Service check</td>
<td>3389</td>
<td>TCP</td>
<td>No</td>
<td>No</td>
<td>RDS service status not checked</td>
</tr>
<tr>
<td>HyWorks Session Host</td>
<td>HyWorks Controller</td>
<td>Session Status</td>
<td>38866</td>
<td>HTTPS</td>
<td>No</td>
<td>Yes</td>
<td>Application launch fails</td>
</tr>
<tr>
<td>HyWorks Controller</td>
<td>HyWorks DVM Agent</td>
<td>DVM Status, Sysprep</td>
<td>38863</td>
<td>HTTPS</td>
<td>No</td>
<td>Yes</td>
<td>Sysprep of clone VM fails, Workgroup login will not work</td>
</tr>
<tr>
<td>Admin Browser</td>
<td>HyWorks Management Console Server</td>
<td>Web Management</td>
<td>443</td>
<td>HTTPS</td>
<td>No</td>
<td>Yes</td>
<td>Admin cannot do management</td>
</tr>
<tr>
<td>HyWorks Client</td>
<td>HyWorks Controller</td>
<td>User login, Device</td>
<td>38866</td>
<td>HTTPS</td>
<td>No</td>
<td>Yes</td>
<td>User login fails, device</td>
</tr>
<tr>
<td>Service Type</td>
<td>Service Name</td>
<td>Service Details</td>
<td>Port</td>
<td>Protocol</td>
<td>RDP</td>
<td>User Access</td>
<td>Failures</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>------</td>
<td>----------</td>
<td>-----</td>
<td>-------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>HyWorks Client</strong></td>
<td>HyWorks Controller</td>
<td>Access over WAN/Internet via Accops Proxy</td>
<td>38861</td>
<td>RDP</td>
<td>Yes</td>
<td>No</td>
<td>User cannot launch desktop/Applications over Internet/WAN when using HyWorks proxy</td>
</tr>
<tr>
<td><strong>HyWorks Client</strong></td>
<td>RDS Server Host</td>
<td>Remote Session login</td>
<td>3389</td>
<td>RDP</td>
<td>No</td>
<td>Yes</td>
<td>User cannot launch desktop/Applications</td>
</tr>
<tr>
<td><strong>User Browser</strong></td>
<td>HyWorks Management Console Server</td>
<td>User Web Portal</td>
<td>443</td>
<td>HTTPS</td>
<td>No</td>
<td>No</td>
<td>User cannot use browser to login. Must use client</td>
</tr>
<tr>
<td><strong>RMS Portal</strong></td>
<td>RMS Portal</td>
<td>RMS Portal</td>
<td>443</td>
<td>HTTPS</td>
<td>No</td>
<td>No</td>
<td>User cannot login into RMS Portal</td>
</tr>
<tr>
<td><strong>Virtual Desktop VMs</strong></td>
<td>HyWorks Upgrade Service</td>
<td>DVM Tools Upgrade</td>
<td>38865</td>
<td>HTTPS</td>
<td>No</td>
<td>No</td>
<td>DVM Tools will not upgrade</td>
</tr>
<tr>
<td><strong>Virtual Desktop VMs</strong></td>
<td>HyWorks Controller Server</td>
<td>Response to Controller Communication</td>
<td>38866</td>
<td>HTTPS</td>
<td>No</td>
<td>No</td>
<td>Response from DVM agents will not be received and functional failures may occur</td>
</tr>
<tr>
<td><strong>HySecure Gateway</strong></td>
<td>HyWorks Controller</td>
<td>User login, app launch</td>
<td>38866</td>
<td>HTTPS</td>
<td>No</td>
<td>Yes</td>
<td>User app list fails, user app launch fails</td>
</tr>
<tr>
<td><strong>HySecure Gateway</strong></td>
<td>AD / LDAP</td>
<td>User authentication</td>
<td>389</td>
<td>LDAP</td>
<td>No</td>
<td>Yes</td>
<td>user authentication fails</td>
</tr>
<tr>
<td><strong>HySecure Gateway</strong></td>
<td>AD / LDAP</td>
<td>Password Change</td>
<td>636</td>
<td>LDAP</td>
<td>No</td>
<td>No</td>
<td>password change not possible</td>
</tr>
<tr>
<td><strong>HySecure Client</strong></td>
<td>HySecure Gateway</td>
<td>User login, app launch</td>
<td>443</td>
<td>HTTPS</td>
<td>Yes</td>
<td>Yes</td>
<td>User login fails</td>
</tr>
<tr>
<td><strong>HyLite Portal</strong></td>
<td>HySecure Gateway</td>
<td>User login, app launch</td>
<td>443</td>
<td>HTTPS</td>
<td>Yes</td>
<td>Yes</td>
<td>User login fails</td>
</tr>
<tr>
<td>Service</td>
<td>Type</td>
<td>Port</td>
<td>Protocol</td>
<td>SSL</td>
<td>Status 1</td>
<td>Status 2</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------</td>
<td>--------</td>
<td>----------</td>
<td>-----</td>
<td>----------</td>
<td>----------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>RMS (Management Console Server)</td>
<td>Both</td>
<td>38866</td>
<td>HTTPS</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Will not be able to get RMS details</td>
</tr>
<tr>
<td>HySecure Gateway</td>
<td>DVMs</td>
<td>3389</td>
<td>TCP</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>User won’t be able to connect to reserved VMs</td>
</tr>
<tr>
<td>HyWorks Controllers</td>
<td>DVMS</td>
<td>3389</td>
<td>TCP</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Controller won’t be able to check RDP readiness of VM</td>
</tr>
<tr>
<td>HySecure Gateway</td>
<td>HyWorks Web Server (RMS)</td>
<td>443</td>
<td>HTTPS</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>HyLite won’t be able to get RMS Data</td>
</tr>
<tr>
<td>Primary HyWorks Controller</td>
<td>Secondary HyWorks Controller</td>
<td>1433</td>
<td>TCP</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Database synchronization, HA will not function correctly</td>
</tr>
<tr>
<td>Secondary HyWorks Controller</td>
<td>Primary HyWorks Controller</td>
<td>1433</td>
<td>TCP</td>
<td>yes</td>
<td>Yes</td>
<td></td>
<td>Database synchronization, HA will not function correctly</td>
</tr>
<tr>
<td>HyWorks Controller</td>
<td>SMTP Servers</td>
<td>25,587, 465 TCP</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Mail notification will not be possible</td>
<td></td>
</tr>
</tbody>
</table>
HyWorks Controller Management Console

As briefly introduced in Introduction section, HyWorks Controller Management Console is a web application providing interface for HyWorks Management.

In later sections of this document, detailed information about all available features and its management using HyWorks Management console will be provided.

In this section, following topics will be covered:

- Management Console Browser Compatibility
- Log in to manage HyWorks
- Administrators of HyWorks
- Log out of HyWorks Management Console
- Management Console Overview

Management Console Browser Compatibility

HyWorks Controller Management console best works with following browsers versions:

- Internet Explorer v11.0 or later
- Google Chrome (Version 46.0.2490.71) or later
- Mozilla Firefox (Version 41.0.2) or later
- Microsoft Edge (Version 25) or later

Log in to manage HyWorks

For administration of HyWorks, user must sign-in into HyWorks Controller management Console:

1. Once HyWorks Controller Service and HyWorks Controller Management Console are installed successfully, open any compatible web browser
2. Type the address as https://Controller-IP or Hostname:<port Number> e.g. https://192.168.1.2/ and press Enter
   a. Port Number (Port configured during installation of management console; default port is 443)
3. HyWorks Controller Management Console login screen will be presented, showing fields Username, Password, Language and Organization

   a. Administrator Credentials
      Default administrator credentials are configured during Accops HyWorks Controller Service installation and same can be used to login to the Management Console
      Or
      Members of AD group (If configured during Accops HyWorks Controller Service Installation) will also be able to login to the Management console using appropriate Username and Password.

   b. Language: The console is accessible in English and Japanese languages and administrator can specify the preferred language on Login screen

   c. Organization: HyWorks supports multi-organization deployments, where the resources can be configured in shared or isolated manner. In such deployments HyWorks Management Console login screen requires organization selection. If the administrator is having access to the selected organization, then it will be directly moved to the selected organization.
      i. In case of single organization, the organization selection screen will not be shown.
4. On successful login admin, will have access to the Accops HyWorks Controller Management Console displaying:
   - Welcome message for logged in user
   - Help button to navigate to Help tab
   - Logout button
   - Dashboard tab (Default tab after login)
Administrators of HyWorks

Administrators in HyWorks can be kept in two categories:

1. Super-administrators (Configured during installation)
2. Designated Administrators (Added later with specific role)

❖ Super-administrators

During HyWorks Controller installation, super-administrators must be configured, which will by default have complete access on HyWorks Controller Management console.

HyWorks Controller can be configured to have following two types of domain administrators:

1. **Type-1**: Create a new user in HyWorks database
   a. Username and password must be specified during installation
   b. A new user with provided details will be created in HyWorks database and will be designated as super-administrator

2. **Type-2**: Configure an active directory group as super-administrator
   a. During installation provide an active directory group, username and password of one of the member user from provided group
   b. Member of active directory group will have super-administrator access)

❖ Role-based access and administration in HyWorks

HyWorks supports delegated administration with access of different screens are controlled using pre-defined roles (administrator, read-only or custom defined)

Once users are configured in HyWorks, with appropriate roles, they can use same login mechanism to access HyWorks using Management console. Delegated administration is covered in detail in later section of this document.

Log out of HyWorks Management Console

To logout of HyWorks Controller Management console,

1. Click on **Welcome Username** shown on top right corner of management console
2. Click on **logout**
3. User will be logged out and navigated back to management console login screen

**Note:**

- HyWorks Controller tasks and processes will continue to run even when administrator has logged-out of HyWorks Controller management console
Management Console Layout Overview

HyWorks Management Console provides a very simple user interface to centrally manage all HyWorks configurations. These configurations are available under various screens as described below:

❖ Top Panel

The top panel on HyWorks Controller Management Console provides access to some very important features. These features are described below:

- Quick Access Toolbar
- Option to configure preferred text size
- Configure Dashboard Graph theme
- Option to Switch Organization
- Logged-in User Details and available operations

Quick Access Toolbar

Quick Access toolbar provides links to most commonly used sections, e.g. User Sessions, App Sessions, VDI Sessions etc. Clicking on any of the option will navigate to corresponding Management Console section.

Current Organization and option to switch Organization

Top panel displays the currently selected organization and enables administrator to move to other organization.

Configure Preferred Text Size

Administrators can also choose preferred text size of HyWorks Management Console, which provides following three text sizes: Small (11 px), Normal (12 px) and Large (13 px).

Currently Logged in User Details and Actions

The top panel also displays the Welcome message along with the currently logged-in administrator details.

The dropdown list, available next to currently logged-in administrator, has the following essential functions:

- Link to Logs
- Link to Help Page
- Option to reset
- Logout: To logout from HyWorks Controller Management console, navigate back to the login screen.

❖ Dashboard

On successful login administrator will be first navigated to Dashboard tab by default displaying summary of HyWorks configurations and deployments in a very easy to read format for quick analysis of current system usage and status monitoring. Following information is available on HyWorks Controller dashboard:

- **System Usage:** Sessions Information, Endpoints information, Information of Desktop Virtual Machines, License Usage, published virtual applications Information
- **Configurations:** HyWorks Controller configuration and status, Shared Session Hosts, Authentication Servers, dedicated session providers information
Monitoring

Monitoring section in HyWorks provides administrator to monitor and manage following objects:

- **Sessions**: Following types of sessions can be monitored and managed from sessions section:
  - User Sessions: Listing and managing all logged-in users
  - App Sessions: Listing and managing all virtual application sessions
  - VDI Sessions: Listing and managing virtual desktop sessions
- **Endpoints**: Listing and managing all registered endpoints. Endpoint management in HyWorks enables administrators to control every aspect of the endpoints e.g. volume control, display management, policy controls etc.
- **Desktop VMs**: Contains all configured desktop VMs and options to manage them using following options:
  - Power Operations
  - Assign/Unassign desktops
  - Remove from pool
  - Refresh Desktop Agent status, Upgrade DVM Tools and download desktop agent logs
- **User Details**: Screen to list all registered users, showing assigned applications, desktops and connection policies. Available options are:
  - View the details of the user
  - Delete user
- **Announcements**: Page containing list of announcements for endpoints and providing options to add, edit and delete announcements. Available options are:
  - View list of announcements
  - Add new announcement
  - Edit existing announcement
  - Delete existing announcement

Workspace

Workspace sections consist of screens for applications, desktop pools, connection profiles and organizations configurations, which eventually defines the workspace of end-users.

- **Applications**: Applications section can be used for following operations:
  - Add/Publish new applications
  - Copy an existing application
  - View details of already added applications in read only mode
  - Modify added applications
  - Delete existing applications
- **Desktop Pools**: Desktop Pools screen provides interface for creating and managing pools of Desktops and associating the Desktops to intended clients. Following management operations are possible:
  - Add/Edit/Delete dedicated desktops’ pools
  - Add/Edit/Delete shared hosted desktop pools
- **Connection Profiles**: Connection profile defines the session experience and connection properties for desktop or applications; following management operations can be performed:
  - Create new connection profiles
  - Modify existing connection profiles
  - Delete existing connection profiles
- **Organizations**: Administrators can have multiple sub-organizations in HyWorks to have logical separation of resources and assigned clients and deliver several types of desktop pools and
applications to the users in distinct organizations. Following actions are available in Organizations:
  o Create a new organization
  o Modify existing organization configurations
  o Delete newly created organizations

❖ Entitlements
Entitlements section can be used to add/edit/delete application and connection profile entitlements for the organization, following types of entitlements are possible:

  • Users
  • Groups
  • OUs
  • Desktop Pools

❖ Server
Server section in HyWorks is consist of pages, which can be used for different types of server configurations, following different types of server configurations are available:

  • **HyWorks Controller**: HyWorks Controller section in HyWorks enables administrator to perform following configurations:
    o View current HyWorks Controller Server and database details
    o Add HyWorks Controller to create cluster
    o Change HyWorks Controller server’s mode
    o Delete HyWorks Controller Cluster Server
  
  • **Authentication Servers**: Section to manage authentication servers for HyWorks configuration. HyWorks supports Microsoft Active Directory, Novell eDirectory, OpenLDAP and Built-in (HyWorks database) as authentication and authorization servers. Admin can do following administrative tasks in **Authentication Server** section:
    o Add authentication server
    o Modify authentication server configurations
    o Delete an existing authentication server

  • **Session Teams**: This section can be used to manage session host server teams. When session host servers are added in a team, application and shared hosted desktops delivery can be load balanced among member session host servers. HyWorks supports Adaptive (Live resource based), Weighted Round Robin and Weighted Least Connection load balancing mechanisms. Administrator can perform following actions:
    o Add new session teams
    o Modify existing session team configurations
    o View/Upgrade and download logs of member session host servers
    o Delete existing session teams

  • **Session Providers**: All types of session providers which can be used to deliver application or desktop sessions to end-users are configured and managed from **Session Providers** section. HyWorks supports three categories of session providers: Dedicated session providers (VMware vCenter Servers/ ESXi Servers and Microsoft SCVMM/ Hyper-V Servers), Shared Session Hosts (Microsoft RDS Servers/ Linux RDS Servers), External Session Providers (TSE and Pano Controller). Following administrative tasks can be done from **Session Providers** section:
    o Add new session provider
    o Modify configurations of existing session provider
    o Delete existing session provider
User Management

User Management section enables administrators to configure local users and groups in HyWorks database itself. These users and groups are then can be used to authentication and authorize access to users. Users and Groups subsections can be used to manage users and groups respectively.

- **Users:** This section can be used for managing built-in users with following actions:
  - Add new users
  - Modify existing users
  - Delete existing users
  - Import/Export users from/to CSV files
  - Download template CSV filers for user import

- **Groups:**
  - Add new groups
  - Modify existing groups
  - Delete existing groups

System

System section in HyWorks is used for most of system configurations. It consists of following important subsections:

- **License:** Dedicated section for viewing, applying and updating licenses in HyWorks.
- **Backup and Restore:** For configuring HyWorks scheduled backups or taking instant backups
- **SMTP Config:** Configuring SMTP server for notifications and backups
- **Virtual Profiles:** Configuring virtual profiles to be used by session host servers
- **Service Path:** Configuring service path for HyWorks controller service
- **Service Config:** Configuring HyWorks Controller discovery service and proxy server configurations
- **Advanced Config:** Important server level configurations, to be used for performance tweaking in HyWorks. To be modified with the help of Accops Support Team.
- **Syslog Config:** For configuring syslog server in HyWorks for logs archiving

Administration

Administration section in HyWorks provides interface to define access and delegated administration policies. Following three sub-sections are available:

- **Permissions:** For adding, removing or changing administrative permissions to the users
- **Roles:** For viewing system defined roles and managing custom roles
- **Client Groups:** For managing client groups which can be used to restrict end-user access to desktops from allowed list of endpoints only based on MAC address, LAN IP or WAN IP rules.

Logs

Dedicate screen for viewing and downloading HyWorks Controller logs.

Help

Section provides links for important help documents and Accops software's download links.
Dashboard – Viewing HyWorks Deployment Details

Dashboard section is used to display the summary of HyWorks Controller configurations with following details of the currently selected organization:

❖ Sessions Details
Dashboard provides following details about sessions in HyWorks:

- **Total User Sessions Count**: Top left section displays User sessions count, suggesting total number of user sessions. Clicking on this section can take you to User Sessions page.
- **Active User Sessions**: Shown as Pie chart suggesting active vs idle session counts. The same section also displays the total number of desktop and application instances launched by users.
  - **Application Count**: Count of total number of application sessions by user.
  - **Desktop count**: Count of total number of desktop sessions

❖ Endpoints Details
Dashboard provides summarized endpoint details in dashboard using following details:

- **Total Endpoint Count**: Total number of endpoints (HyDesk/ HyWorks clients) currently connected to HyWorks Controller are displayed as number and other details are given in *Active Endpoints* pin chart.
- **Active Endpoints**: Pie Chart displaying Active Vs. Idle endpoints and the percentage of active endpoints against the total number of endpoints
  - Count of Offline endpoints
  - Count of Idle endpoints
  - Count of Endpoints with alerts (require attention)

❖ Licenses Details
Following licensing details are available on dashboard:

- **Total number of licenses**: Displaying total number of licenses available in organization
- **License Usage Pie Chart**: Providing details of used and available license in current organization
  - **License Type**: Evaluation, Perpetual or Default
  - **Number of days to expire**

❖ Desktop Details
Following summarized information is available for configured desktops:

- **Count of configured Desktop VMs**
- **Desktop VMs Pie Chart**: Suggesting powered on vs powered off desktop VMs.
  - Count of powered off VMs
  - Count of suspended VMs
  - Count of VMs with alerts

❖ Controller Details
On top right corner status of controllers are shown as *All OK*. Other than that following information on controllers can be seen on dashboard:

- Controller host name
- Controller Server IP Address
- Current CPU, RAM, Hard disk Usage
• Controller Mode (Secondary/ Primary)
• Status as Reachable or not reachable

❖ Authentication Server
Displaying the status of authentication server with following details:
• Server address (IP or hostname as configured) of Authentication server
• Type of authentication server: Primary or secondary
• Reachability of Authentication server
• Is Active: Yes/ No

❖ Assigned Apps
This section provides following details:
• Pie Chart: Displaying percentage of assigned applications
• Count of Total and Unassigned Applications

❖ Assigned Pools
Displays the following content:
• Pie Chart: Displaying % of assigned pools
• % of pool utilization: Suggesting the % of assignments all pools are having
• Empty Pool: Showing count of pools not having Desktops

❖ Shared Session Hosts
The section displays information of Shared Session Hosts configured in this organization with following details of each session host:
• Name and Address of Session host servers
• Resource Utilization: % of CPU, memory and HDD consumption
• Number of Session Counts on Session Host Server
• Score of Session Host Server

❖ Dedicated Session Providers
Displaying information of all configured dedicated session providers, with following details displayed for each session provider:
• Type of session Provider
• Name and Address of session provider
Organizations and Multi-tenancy in HyWorks

A single deployment of HyWorks can be used to serve virtual applications or desktops to end-users belonging to different entities of same or different organizations. Consider the following examples:

- A company named as example.com has multiple units and it is required to deliver virtual applications to each of these units but being managed and licensed separately.
- A vendor/partner wants to deploy HyWorks in cloud and see applications/desktops as service to multiple customers yet keeping them logically separated.

In this section following points will be covered:

- Multi-organization Structuring
- Default Organization
- Organization Configurations
- Organization Resource Sharing Concepts
- Organization Management Options
- Move to Child Organization and Configure Resources
- Deployment Examples
- Functioning of HyWorks in Single/Multiple Organization Deployments

Multi-organization Structuring

An organization is a logical representation of the resources managed by HyWorks.

If the organization structure is flat and does not require any further logical division then resources can be configured in one default organization only i.e. configure Session host servers, authentication servers etc. However, if the organization structure has multiple segments and each segment should use different resources then, administrator can create multiple organizations and configure with different resources.

An example of organization structure is:

It is important to understand organizational structuring in HyWorks, as multiple resources and configurations are aligned with respective organizations and can be managed from there only.

This section will provide information on following topics:

- Default Organization
- Organization Wizard and Associated Terms
Default Organization
After installation, a system defined organization is present in system and it is termed as Default organization. It is the root organization and no siblings can be created to it.
In deployments, where multi-organization structuring is not needed, default organization can be used.
Name, settings of default organization can be changed as per requirements and will be covered in this section.

Organization Configurations
Configuration of organization defines:
- How users are going to be authenticated and authorized in HyWorks
- Workspace settings to be applied while allowing user access

New organization creation or modification of existing organization can be done from Organizations Workspace -> Organizations.

In this section, details of different configurations available for an organization are described:

❖ **Organization Details:** Basic configurations of an organization
  - **Name:** Provide logical short name for new organization. Name field supports following special characters: _(Underscore) SPACE () # @ :- (Hyphen)
  - **Code:** Short code for organization. Organization code is used for communication between controller and HyWorks endpoints/HyLite. Only _(Underscore), – (Hyphen) and space is allowed (No trailing or leading spaces)
  - **Description:** Logical description of new organization
  - **Parent Organization:** Name of parent organization (Read-only information)
  - **Inherit Resources:** Select the checkbox, if the parent organization’s resources should be shared with this child organization, unchecking the option will make fields **Create Realm** and **Create Auth Domain** as compulsory. Please refer section **Organization Resource Sharing Rules** for detailed information on resource sharing between organizations.
  - Select **Active** to mark organization as active, inactive organizations are not listed on client side on logon
  - Select **Create Realm** to define realm settings specific to this organization (Keep it unchecked to use parent’s realms settings; If Create Realm is unchecked all realm settings will be hidden)
  - Select option **Create Auth Domain** to specify Auth Domain settings for this organization. (If **Create Auth Domain** is unchecked, the tab for Authentication domain will not be displayed, and authentication domain of parent or default organization will be used)
    - If Create Auth Domain is checked, Authentication Domain tab will be enabled and will require appropriate configurations for the child organization. If Inherit Resources option is checked, then administrator will also be able to see and view the authentication servers added in default organization.

❖ **Authentication Domain:** Defines authentication and authorization configurations of an organization.
  - **Authentication Server:** Server to be used for authenticating. All authentication servers added in this organization or inherited from parent organization can be used.
  - **Authorization Server:** Server to be used to authorize application and desktop access. It can be same as authentication server or can be different server. While authorizing HyWorks queries authorization server for user’s membership. Consolidated list of applications and desktops can be assigned to user based on assignment to user, it’s groups or OU.
  - **Domain Name for Remote Desktop Session:** While accessing assigned or desktops, HyWorks provide, domain name prefix to be used for connecting to respective remote
desktop server, this authentication domain, can be auto fetched from authentication server configuration or authorization server configuration or custom defined. For deployments using remote desktop servers in workgroup, domain name can be set as dot ".".

- **Use Credentials for Remote Desktop Server:** When authorization server is set as Built-in, which is presumably for workgroup configurations, administrator can set the options as which credentials to be used while connecting to remote desktop server.
  - **User provided credentials:** Credentials provided by user for authentication will be used, while connecting
  - **Built-in directory credentials:** Credentials of users from built-in directory.
- **User Creation on RDS(s):** If remote desktop servers are in workgroup, new user’s creation method can be defined, as:
  - **Manual Synchronization:** Administrator will initiate user syncing process between remote desktop servers and built-in directory.
  - **Automatically on logon:** No manual synchronization, but users will be created on logon
  - **Do not create:** Users will not be created, and administrator must manage the availability of users on remote desktop servers
- **Populate Users into built-in directory:** Method to push users into built-in directory
  - **Create users in built-in directory:** Users can be created by importing CSVs or specifying details in user creation wizard
  - **Import users from authentication server:** Users can be fetched into built-in directory from authentication server.

❖ **Realm Settings:** Realm settings in organization defines client and user workspace portal behaviour and user interface. In Organization wizard, no such controls or sections with name Realm Settings are displayed, but the combination of following sections is termed as Realm Settings:
  a. **UI Settings:** UI Settings for Client and User Workspace portal having following settings’
    i. **System Tray Pop-up Text:** Text to be displayed for HyWorks Client in system tray
    ii. **Language Configurations:** Language to be used by HyWorks Clients
  b. **Portal Settings:** For defining User Workspace Portal settings
    i. **Enable Portal:** For activating logon through User Workspace Portal
    ii. **Exit Application Session on Close:** Defining if remote sessions to be closed on portal exit
    iii. **Use Custom Logo:** For changing the logo displayed on Client and User Workspace Portal
        1. This provides option to select, crop and upload custom logo for the organization
    iv. **Hide System Tray Icon:** To hide system tray entry of client, when accessed through user workspace portal
    v. **Use Custom Portal Title:** For specifying custom portal title
    vi. **Tile Color:** Tile color for applications user workspace portal
    vii. **Font Color:** Font color to be used for applications on user workspace portal
    viii. **Default Client Type:** Type of client to be used by default with User Workspace portal.
        If client is not installed, on logon, dialog to install client will be displayed and specific type of client will be downloaded. The same settings also govern the type of client to be provide on logon screen Client Download Link.
  c. **Desktop Client Settings:** Configurations for HyWorks clients:
    i. **Enable desktop client:** For activating logon through HyWorks Clients
    ii. **Allow Save Username:** For enabling user to save its username. Last successful logged-in username will be cached and will be displayed on next logon.
iii. **Allow Save Password:** For enabling caching of last successful logon password for the user on client
iv. **Hide App Launcher:** To hide application tray after logon
v. **Use Custom Title for Client:** To configure custom title for client
vi. **Tile Color:** Tile color for applications on client application tray
vii. **Font Color:** Font color to be used for applications on client application tray
viii. **Application Shortcuts Settings**
   1. **Do Not Create Shortcuts:** To disable shortcut creation of applications on user’s desktops
   2. **Delete Shortcuts on Exit:** If shortcuts should be removed on client exit

---

**Organization Resource Sharing Concepts**

HyWorks Organization structure follows some basic rules:

1. With fresh installed HyWorks Controller, a default organization is created
   a. Default organization cannot be deleted, but can be modified
   b. No sibling organization can be created at the default (root) organization level
   c. With only single organization, while logging-in client/management console does not require selection of organization
2. Only parent organization resources can be shared with child organizations and child organizations cannot share resources with sibling organizations or parents
3. **Configurations available at Root organization level (Global Configurations):** Some configurations are global (System) configurations and are either available to super-administrator or at the default organization level only, following are such resources
   a. Role creation
   b. Default Settings for endpoints
   c. Server Configurations – HyWorks Controller for making/managing cluster
   d. System Configurations – License, Backup Restore, SMTP Configurations, Service Path, Service Configurations, Advance Configurations
4. **Resources/Configurations which are not shared among organization:** Few resources are organization specific and cannot be shared, following are such configurations
   a. Connection Profiles
   b. Session Teams
   c. Shared Hosted Session Host
   d. Desktop Pools
   e. Endpoints
   f. Desktop VMs
   g. Built-in Users/Groups
5. **Sharable resources/configurations among organizations:** Few resources are sharable e.g.
   a. Authentication servers
   b. Authentication Domains
   c. Realm Settings
   d. Session Providers (Dedicated and External)
   e. Applications
6. Shared resources cannot be modified at child organization level but can be configured
7. **Configurations getting created for every organization:** With every organization (default or admin created) few resources are created, and these resources cannot be deleted, examples of such resources are:
   a. Default Connection Profile  
   b. Built-in Directory  
   c. Default Session Team  
   d. Default Device Groups
8. Licenses are being shared from default organization only and a child organization is not restricted to use licenses from its parent only.

Based on above few ground rules, organizational structure can be planned and deployed. E.g.
   a. In a deployment where the single authentication server is there but the application servers are in workgroup and not part of domain, a structure can be followed where authentication server will be configured at root level and will be shared with all child organizations and while configure child organizations, every child organization can choose authentication server the one being shared from parent and authorization server as Built-in for workgroup environment.
   b. In another deployment where only one vCenter server is available as session provider, it can be configured at root level and then child organizations can simply use this shared session provider and consume its desktop VMs as needed.

In a deployment, where no sharing is expected and they can use their own authentication server, nothing should be configured and shared from parent, instead each child organization can define resources at its level and consume their only.

**Organization Management Options**
Administrator can perform following management options on organizations:

- Create an organization  
- Modify existing organization  
- Delete a child organization

❖ **Create Child Organization**
   ❖ Login as default super-administrator into HyWorks Controller Management Console  
   ❖ Go to Configuration – Workspace – Organizations  
   ❖ Double click on Default Organization or select Default organization – click on Expand button  
   ❖ **Add** button will be enabled -> Click on **Add** button  
   ❖ Provide appropriate details in different tabs of **Add Organization** wizard  
   ❖ Save the Organization details.  
   ❖ Organization is created and will be available under the currently selected parent node.

❖ **Modify Existing Organization**
An administrator with enough privileges, can modify the settings of the organization. For modifying settings of any organization, follow the below steps:
   1. Go to Workspace -> Organizations section
2. Select the organization to modify and click on *Edit* button
3. *Edit Organization* will be displayed, and all configurations (General configurations, Authentication domain configurations, UI Settings, Portal Settings, Desktop Client Settings) can be modified from here.
4. Once changes are saved, logout and **exit** HyWorks Client and re-launch.

**Note:**
- Organization settings are fetched on registration and thus HyWorks client must be exited and relaunched. On HyDesk endpoints, user may have to reboot the endpoint for settings to come into effect.

**❖ Delete Existing Organization**
Organizations can be deleted from HyWorks, when:
- All references to the organizations are deleted, if any references to organization exist, then organization deletion will fail
- Organization cannot be deleted, if administrator is working at the same organization level -> to delete organization administrator must move one level up and then select the organization to delete
- Default organization cannot be deleted.
Considering that administrator is at parent level, follow the below steps to delete the organization:
1. Go to Workspace -> Organizations section
2. Select the organization to modify and click on **Delete** button
3. **Confirm Action** dialog will be displayed. Click on Delete button to continue deleting the organization
4. Organization will be deleted and will no longer be displayed in HyWorks Configurations.

**Move to Child Organization and Configure Resources at Child Organization**
Once the child organization is created successfully, use the below steps to move to the child organization:

**Move to the Child Organization:** Before configuring the resources, it is required to move to the intended child organization level as all resources are always configured at selected organization level only. Follow the below steps:
1. Login as default super-administrator into HyWorks Controller Management Console
2. At the top right corner, the Organization Selection dropdown labeled as **Current Organization** is available -> Select the child organization, you wish to navigate into.
3. Click on **Select Organization** button
4. Administrator will now be moved to child organization.

**❖ Resource Configurations in Child Organization**
Once administrator has moved to the child organization, all the resources being configured will now belong to this child organization. The resource configuration which can be adding session providers, creating desktop pools or publishing applications are defined in their respective sections.

Addition to above, child organizations inheriting resources from parent can also use shared resources such as Applications for adding entitlements to those applications, Dedicated Session Providers to create Desktop Pools, authentication servers from parent to configure Authentication domains etc.

Deployment Examples for Different Use Cases
As in previous section, multiple concepts of multi-tenancy and multi-organization structuring has been explained, this section will have some use cases and deployment examples:

❖ An organization wishes to deploy HyWorks, where users will be authenticated from active directory but their assignments to be done from built-in directory so that HyWorks administrators do not have to request active directory team for user’s group modifications very often and all remote desktop servers are joined to domain.

**Solution Deployment:** Configure the organization to have following authentication domain settings:
- Authentication Server: Active Directory
- Authorization Server: Built-in
- Domain Name for Remote Desktop Session: Authentication server
- Use Credentials for Remote Desktop Server: User provided credentials
- User Creation RDS(s): Do not create
- Populate Users into built-in directory: Import users from authentication server

**Explanation:** Based on above configuration, users will be authenticated from Microsoft active directory configured as authentication server, administrators will be able to import users from active directory to built-in directory and manage them in different groups. While connecting domain name of active directory will be used and as users are providing credentials of active directory, the same will be used for connecting to remote desktop servers.

❖ An organization wishes to deploy HyWorks, where users will be authenticated from LDAP server but their assignments to be done from built-in directory so that HyWorks administrators do not have to request LDAP team for user’s group modifications very often and all remote desktop servers are to be kept in Workgroup.

**Solution Deployment:** Configure the organization to have following authentication domain settings:
- Authentication Server: LDAP server
- Authorization Server: Built-in
- Domain Name for Remote Desktop Session: Custom as dot "."
- Use Credentials for Remote Desktop Server: Built-in directory credentials
- User Creation RDS(s): Manual Synchronization
- Populate Users into built-in directory: Create users in built-in directory

**Explanation:** Administrator will create users in built-in directory with some random different passwords but same username as LDAP. Users will be synchronized into associated RDS server manually so that users with same username and passwords can be created on RDS(s). While logging-in users’ authentication will be done with the provided credentials against LDAP server but while connecting remote desktop servers, credentials from built-in directory will be used.

❖ An organization wishes to deploy HyWorks, where users will be authenticated from Microsoft active directory server, users and remote desktop servers are managed from domain.
Solution Deployment: Configure the organization to have following authentication domain settings:

- Authentication Server: Active Directory Server
- Authorization Server: Active Directory Server
- Domain Name for Remote Desktop Session: Authentication or authorization server
- User Creation RDS(s): Manual Synchronization (Disabled and do not get used)
- Populate Users into built-in directory: Create users in built-in directory (Default selected but do not get used)

Explanation: As everything is managed through active directory, users will be authenticated from configured authentication server, authorization i.e. assignment of applications and desktops can be done from same authentication server. On logon, users will be authenticated from active directory and will be allowed to connect to remote desktop servers using same credentials.

Functioning of HyWorks in Single/ Multi-organization Deployment

This section of admin guide will provide information on HyWorks functioning in single and multi-organization deployments.

❖ HyWorks Functioning in Single Organization Deployment

With a single organization deployment, HyWorks operates in following manner:

- Organization creation will not be needed
- All resources and configurations can be done on single root (Default) organizations
- License sharing is not needed, and all licenses are consumed at root (Default) organizations
- Resources are not shared
- All information and logs are available in root organization
- While logging into HyWorks, client applications do not require selection of organization and all endpoints by default gets registered in default root organization

❖ HyWorks Functioning in Multi-Organization Deployment

With multiple organization deployment, HyWorks functions in following way:

- Organizations must be created and configured
- Licenses must be shared or allocated to different organizations
- Resources are configurations need to be done at each organization level
  - Resources can be shared or kept for a specific organization level
- All information and logs are specific to organizations, presented at organization level itself
- While logging into HyWorks, client applications require selection of organization and all endpoints will be registered at selected organization level
Authentication and Authorization in HyWorks

Authentication in HyWorks, refers to process of validating user provided credentials against a configured authentication server (which could be Microsoft Active Directory, LDAP server, Novell e-Directory Server or HyWorks built-in directory).

Authorization in HyWorks, represents the process of getting entitlements for user, which can be directly assigned to the user or can be assigned to group(s) or OU, to which user is member of.

Whenever a user (designated administrators from management console) or end-users from device endpoint, logs-in to HyWorks, it is authenticated with the configured authentication server.

Authorization servers need not to be different from authentication server, which means active directory server configured as authentication server can also be used as authorization server however, based on deployment use cases same or different authentication and authorization server configurations can be created.

- Authentication servers are added and managed from HyWorks Management Console -> Server -> Authentication Servers
- Configuring a server as authentication or authorization server is done from HyWorks Management Console -> Workspace -> Organizations

In this section of document, following topics will be covered:
- Default Authentication and Authorization Configuration Post HyWorks Installation
- System Prerequisites for Adding an Authentication server
- Authentication Servers Management in HyWorks
- Monitoring Authentication Server Status and Failure Status
- Failover Configuration for Authentication Server

Default Authentication and Authorization Configuration Post HyWorks Installation

After a fresh installation of HyWorks, as no additional authentication server is configured, HyWorks uses its in-built directory server to define authentication domain, having following configuration:

- Authentication Server: Built-in
- Authorization Server: Built-in

Built-in is user database of HyWorks Controller, which can be used for authentication and authorization. Built-in directory server will be covered in a later section of the document.

This configuration is saved in Authentication Domain configuration of organization. Details of organization and respective configurations are already covered in previous section Organizations and Multi-tenancy in HyWorks of this document.

Which means if any user will try to log into HyWorks, then it will be authenticated with built-in directory server and its authorization will also be done from built-in directory server.

In most cases, organizations have their own AD or LDAP server available and require the same server to be used as centralized authentication authority and thus post installation, super-administrator must add respective authentication server into HyWorks configurations, explained in next section.
System Prerequisites for Adding an Authentication server

Configuration of authentication server may fail if HyWorks Controller is not able to connect and resolve authentication server due to any of the following facts:

- HyWorks Controller machine is not in domain
- HyWorks Controller is in some other domain
- HyWorks Controller is not able to connect to domain

And thus, it is important to make sure HyWorks Controller can connect to authentication server and for achieving this, on system where HyWorks Controller is installed:

- Primary DNS should be configured as the authentication server being configured
- Appropriate Hosts entries should be created in Hosts file located at 'C:\Windows\System32\drivers'
- All required ports to authenticate users from HyWorks Controller to authentication server are open, e.g. 389 (default active directory port for non-SSL communication, port 636 for SSL communication with AD)

E.g. if the active directory propalmsnetwork.com (IP = 192.168.1.1) is being configured as authentication server then the primary DNS server on HyWorks Controller machine should be 192.168.1.1 and hosts file should have entries as '192.168.1.1 propalmsnetwork.com'

Let us understand the management of authentication server in HyWorks.

Authentication Servers Management in HyWorks

Authentication tab in Server section can be used to manage the authentication servers. Configured authentication servers can be used as authentication or authorization server in authentication domain of an organization.

By default, every organization has one built-in authentication server which is also set as default authentication and authorization server in authentication domain of that organization and should be updated as per requirement.

Administrator can add several types of authentication servers into configurations. HyWorks deployment supports following types of authentication servers:

- Microsoft Active Directory
- Open LDAP/ Novell eDirectory
- Built-in

❖ Add New Authentication Server

To configure authentication server, follow the below steps:

1. Login into HyWorks Controller Management Console using appropriate admin credentials
2. Go to Server tab and expand the Authentication section
3. Click on + Add button to open Add Authentication Server dialog
4. In Add Authentication Server dialog: Configure distinct types of authentication servers as per below steps:
   a. Microsoft Active Directory
      i. Select Appropriate Server Type as Active Directory
      ii. Provide appropriate Server address e.g. 192.168.1.1 or accopsad.com in Address field (if providing domain name then it should be resolvable from HyWorks Controller server)
iii. Provide appropriate **Domain** name which could be NetBIOS Name for domain (this domain name information will be used for signing into remote sessions).

iv. **Port Number** to be used to communicate with authentication server (default is 389)

v. **Enable SSL** (Check this checkbox if configured Active directory only supports secure communication, in this case default port will be changed to 636)

vi. Provide Base DN information (**optional** for Microsoft Active Directory)
   a) All users, groups and OUs will be fetched if Base DN information is not provided
   b) On providing specific Base DN information users, groups or OUs will be fetched accordingly.

vii. Provide administrator credentials (Domain username and password) with rights to read and write access to user account managements

viii. **User Search Attribute**: User search attribute. For active directory default search attribute is SAMAccountName. HyWorks will use this search attribute to search users.

b. OpenLDAP/ Novell eDirectory

i. Select Appropriate Server Type as Novell Directory/ OpenLDAP

ii. Provide appropriate Server address e.g. 192.168.1.1 or accopsad.com

iii. Provide appropriate **Domain** name which could be NetBIOS Name for domain (this domain name information will be used for signing into remote sessions).

iv. **Port Number** to be used to communicate with authentication server (default is 389)

v. **Enable SSL** (Check this checkbox if configured Active directory only supports secure communication, in this case default port will be changed to 636)

vi. Provide Base DN information (**Mandatory** for Novell Directory/OpenLDAP e.g. o=qa)

vii. Provide administrator credentials with rights to read and write access to user account managements

viii. **User Search Attribute**: User search attribute. For LDAP default search attribute is cn. HyWorks will use this search attribute to search users.

c. Workgroup

**Note:**

➢ In HyWorks v3.0 or later, built-in directory support has been added, which is an improvisation over workgroup authentication server and should be preferred. Workgroup support will be stopped in future HyWorks releases.

i. In case of workgroup configuration, HyWorks Controller serves as a directory server and its local users are used to authenticate the user logon.

ii. Select Appropriate Server Type as Workgroup

iii. Provide appropriate Server address of HyWorks Controller itself e.g. 192.168.1.1 or hysrv.accops.com

iv. Provide administrator credentials with rights to read and write access to user account managements

5. Click on **Test Connection** button to check server reachability

6. Once the successful connection message appears, click on **Add** button
7. Authentication Server is configured now and ready for use

❖ **Modify a Configured Authentication Server**
Administrator can modify a configured authentication server. But it's important to understand what information can be updated and what could be the impact of updating an existing Session Provider:

**Modifiable Fields and Impact**
Following fields in authentication server configuration are modifiable and these fields are equally critical than configuration as any misconfiguration in any of these fields could lead to failed deployment. Thus, administrator should be extra cautious while configuring such critical settings.

- Address: Critical
- Domain: Critical
- Port Number: Critical
- Enable SSL: Critical
- Base DN: Critical
- Username: Critical
- Password: Critical
- User Search Attribute: Critical

**How to Modify Configured Authentication Server**
1. Go to Server – Authentication section
2. Select authentication server and click on Edit button
3. In **Edit Authentication Server** wizard -> Provide appropriate entries for modifiable fields
4. Click on **Test Connection** button to verify if provided entries are working
5. Click on **Update** button to update the authentication server settings

❖ **Delete authentication Server**
As mentioned in Built-in authentication server section that built-in authentication server cannot be deleted but any admin configured authentication server can be deleted if it is not being configured in any current or child organization’s authentication domain.

To delete any configured authentication server, follow the below steps:
1. Select the authentication server to be deleted and click on **Delete** button
2. Clicking on **Delete** button will prompt **Confirm Action** dialog, showing warning that all assignments related to this authentication server will also be removed. Click on **Delete** button to confirm the authentication server delete operation.
3. Authentication server will be deleted and will not be displayed in Management Console

**Note:**
- Current version of HyWorks does not delete any entitlements of users on removal of authentication server configured as authorization; but the users will not be able to authenticate unless the same authentication server is added again and configured as authorization server.
Monitoring Authentication Server Status and Failure Status
Once added into HyWorks, authentication server status i.e. connectivity with HyWorks is continuously monitored and displayed at various screens:

1. **Authentication Server Page:** The server status is shown as reachable or unreachable against each of the added authentication server. If any of authentication server is not reachable or failed to connect, **Authentication server** page is shown in red color with number against it, suggesting one or multiple authentication servers are not reachable.

2. **Dashboard:** Status of Authentication server is also shown in Dashboard, which also starts displaying status as Need Attention to attract administrator’s attention in case of connectivity issues with authentication server.

Failover Configuration for Authentication Server
Unavailability of authentication server could lead to user logon failures and thus it is important to make sure that authentication server is always available and reachable from HyWorks Controller.

To keep the availability of authentication servers, HyWorks supports the configuration of secondary authentication server which can be used to authenticate users when primary authentication server is not available.

❖ **Supported Authentication Servers**
Secondary authentication server is currently supported for **Microsoft Active Directory** server only.

❖ **How to configure secondary Active Directory Server**
To configure secondary authentication server, follow the below steps:

1. Login into HyWorks Controller Management Console using appropriate admin credentials
2. Go to **Server** tab and expand the **Authentication** section
3. Click on + **Add** button to open **Add Authentication Server** dialog or click on **Edit** button if authentication Server of type Active Directory already exists
4. In **Add/Edit Authentication Server** dialog:
   a. Make sure **Server Type** is **Active Directory**
   b. Provide appropriate Server address e.g. 192.168.1.1 or hyAuth.com
   c. Provide Base DN information (optional for Microsoft AD)
      i. All users, groups and OUs will be fetched if Base DN information is not provided
      ii. On providing specific Base DN information users, groups or OUs will be fetched accordingly.
   d. Provide administrator credentials with rights to read and write access to user account managements
   e. Select the checkbox **Add Secondary Authentication Server**, this will enable the fields for secondary authentication server
      i. Provide appropriate Server address e.g. 192.168.1.2 or hyAuth2.com
      ii. Provide Base DN information (optional for Microsoft AD)
         a) All users, groups and OUs will be fetched if Base DN information is not provided
         b) On providing specific Base DN information users, groups or OUs will be fetched accordingly.
iii. Provide administrator credentials with rights to read and write access to user account managements
5. Click on **Test Connection** button
6. Once the successful connection message appears, click on **Add** button
7. Authentication servers will be added and will be shown in **Authentication** section

❖ **Authentication Server Failover Mechanism**

Authentication server’s failover works in the same manner as Session Provider Failover works, which means:

1. **When both servers are up**
   Primary authentication server will be used to authenticate users.
2. **When secondary is down, and primary is up**
   Primary authentication server will be used to authenticate users.
3. **When Primary goes down and secondary is up**
   HyWorks Controller will automatically switch to secondary authentication server and secondary server will be used to authenticate users.
4. **Primary comes up and secondary goes down**
   HyWorks Controller will automatically switch to primary authentication server and user authentication will be done using Primary authentication server.
5. **When both goes down and either of the server comes up**
   HyWorks Controller will use authentication server whichever comes up first and reachable to authenticate users.
6. **Primary goes down – Comes up again**
   If primary server goes down, HyWorks Controller will start using secondary server and when primary server comes up again, it will keep primary in the standby mode only which means it will continue to use the secondary server only.
   Administrator will be displayed option to switch to Primary Authentication server by using **Make Primary** button which will configure the Primary authentication server as active server.
   There on authentication will happen using Primary authentication server.
Built-In Directory Server and Local User Management

As mentioned briefly in section of authentication and authorization servers, HyWorks supports workgroup-based environments with an in-built directory server, where local users and groups can be defined into HyWorks database and can be used for authentication or authorization.

To add/remove/modify users or groups in this built-in directory, User Management section is used. User Management section provides administrator to manage the users to be used in built-in directory. User Management section consists of following two sub-sections:

- **Users**: For managing users
- **Groups**: For managing groups

**Users**

Users subsection under User Management section, enables administrator to manage users (Add/Remove/Modify), change their Group memberships, create/remove session team association, synchronizing users into session providers.

This section will provide all necessary details to manage users, which includes:

- Add/Update/Delete Users
- Import users from CSV

**Add Users**

Users can be added in to HyWorks Built-in directory by following two methods:

1. Add Users Manually
2. Import Users using CSV

**Add Users Manually**

To add users manually, follow the below steps:

1. Go to User Management section - > Users subsection
2. Click on Add button
3. Add User wizard will be displayed
4. Provide the following details in User Details screen
   a. **Display Name**: Display name for new user (for display purpose)
   b. **Username**: Username for new user (to be used for login)
   c. **Active**: Checkbox to activate user. Inactive users will not be allowed to login into HyWorks
   d. **Password & Confirm Password**: Password fields for new user. Password must be 8 characters long.
5. Click on Next button to proceed to Assign Groups section
6. **Assign Groups** screen can be used to make user member of any existing user groups
   a. To add any groups, click on Add Group button
   b. **Available Groups** dialog will be displayed, which can be used to locate desired group
   c. Select and click on OK button
d. Selected group will be added, and administrator will be navigated back to **Assign Groups** screen
7. Click on **Next** button to proceed to **Session Team** screen
8. **Session Team** screen can be used to associate user with session team. On synchronizing users will then be synchronized into member session host servers of selected session team.
   a. Select the desired session team from the displayed list
9. Click on **Save** button to save user. User will be added with provided details and **Users** section will start showing the details of the added users.

**Add User Wizard – Advanced Configurations**
Default screen to Add User does not display advanced configurations to avoid complexity in user creation. These controls can be enabled from System - Advance Configurations screen. Following advance configurations can be enabled for user account:

- **Authorization Only**: (Deprecated: Field is no longer available), if the user account should be used for authorization purpose only. Selecting this checkbox will disable **Passwords** fields.
- **Password Management**:
  - **Auto Disable (in days)**: User account will be disabled automatically after configured number of days from the date of creation
  - **Change Password at next logon**: If user should be prompted to change password on next logon
  - **User cannot change password**: if user should be restricted to change password

**Import Users (Add Users Automatically using CSV Import)**
HyWorks v3.0 or later supports adding multiple users at a time by importing users from CSV files. The CSV file should be properly formatted and should use only predefined columns. Any deviation from the specification may result in user import feature.

**CSV Template**
For ease of administrator User Management – User section provide option to download CSV Template.

**Downloading CSV Template**
To download CSV Template, follow the below steps:
1. Go to User Management – **User** section
2. Click on **Download Template** button
3. CSV File template will be downloaded in zipped format with name **En_UserImportCSV**
4. Extract the CSV file to be used for providing user details.

**CSV Template Fields and Import Behavior**
Below is the list of fields which are defined as columns in downloaded CSV files:
- Display Name: Display name of the user
- Username: Username for the new user
- Delete User: Keeping it as true will delete the user from HyWorks configuration on successful CSV import and will delete from session providers on next synchronization. Should be kept False for new users or if existing users need not to be deleted. The field cannot be left blank and accepts values True or False only.
- Group Names: For specifying names of groups for the user.
  - On import user will be made member of specified groups.
  - Multiple groups can be specified using semicolon separated values.
  - If a group does not exist, it will be created on import
  - If group is not specified, then all group membership of the user will be removed
- Session Teams: For specifying names of sessions teams for new user
  - User will be associated with specified session teams on import
  - Multiple session teams can be specified using semicolon separated values
  - If specified team does not exist, then error will be displayed
  - If Session teams column is left blank, then user’s association with all session teams will be removed
- Applications: Name of applications for new users
  - User will be assigned with provided applications
  - If applications do not exist, then appropriate error will be displayed on CSV import
  - Multiple applications can be assigned using semicolon separated values
- Password: The password for the new user
  - Cannot be left blank
  - Should be at least 8 characters long and following special characters are supported: aA1~!@#$%^&*()_+{|}\_\|./ ?

Important Points while Populating CSV with User Details:
- CSV file encoding is UTF-8 and must not be changed.
- Do not change the order of the columns. Do not delete any columns from the file.

CSV Import Process
To import users into HyWorks using CSV Import feature, follow the below steps:
1. Fill all the details cautiously using the above rules and prepare CSV file
2. Click on button Import
3. Import dialog will be displayed, listing the type of CSV file format, following file formats are supported
   a. ANSI
   b. Unicode
   c. UTF_8
   d. Shift_JIS
4. Choose required file format and click on *Import* button
5. **Choose File to Upload** window will be prompted
   a. Select appropriate CSV file and click on *Open*
6. All user records which can be imported will be displayed
7. Click on *Save* button to continue saving the records
8. Controller will start processing the records
   a. If records do not have any misconfigurations, then success dialog will be displayed
   b. If any issues are detected, then error will be displayed for failed records in the same *Import File Records* dialog with option to download the logs
      i. Only records with error will be skipped and all other records will be imported into HyWorks
   c. Click on *OK* button to dismiss the dialog
9. All imported records will now be listed in User Management – Users section.

### Add Users from Authentication Server

In specific deployment pattern, users can be fetched from configured authentication server in organization. Possible use case could be administrator of HyWorks does not want to manage user groups on active directory but create groups in local built-in directory and add users from active directory into respective groups for application and pool assignments.

To achieve this, auth domain configuration should be kept as below:
- Authentication Server: Active Directory
- Authorization Server: Built-in
- Domain name for remote desktop session: Authentication Server (Considering all machines to be accessed are domain joined)
- User Credentials for remote desktop servers: User provided credentials
- User Creation on RDS(s): Do not create (Considering all machines to be accessed are domain joined)
- Populate users into built-in directory: Import users from authentication server

Once above configuration is set in Organization – Auth domain section, users can be pulled from active directory into HyWorks and then can be managed into different groups for authorization.

To import users into HyWorks built-in directory, follow the below steps:
1. Make sure Auth domain configurations are set as described above
2. Go to User Management – Users
3. Click on *Add* button to invoke *Add User* wizard
   a. Click on *Add Users* button
   b. Search and select users to be added and click on *OK* button
   c. Go to next screen to associate users with any existing built-in groups
   d. In next screen, keep option *All Session teams* checked to associate users with all available session teams
4. These users are now added in to HyWorks built-in directory and can be used for direct entitlements or group-based entitlements.

In a similar manner, users can also be added from Groups wizard, where while adding or editing a group, presents option to add users from authentication server.
❖ Edit User
Administrator can modify the details of a user using followings steps:

1. Select a user from the list displayed in User Management – Users section
2. Click on button Edit
3. Edit User dialog will be displayed, with following modifiable sections/ controls:
   a. User Details:
      i. Display Name: Editable
      ii. Username: Not editable
      iii. Active: Editable
      iv. Change Password: Select this checkbox to provide new password for the user
   b. Assign Groups: To assign new groups or unassign existing groups
   c. Session Teams: To modify associations of users with session teams
4. Change required details and click on Save button
5. All details will be saved and on next synchronization, details will be updated on shared session host server as well.

❖ Delete User
Following two methods can be used to delete users from HyWorks:

Delete Manually
To delete users manually, follow the below steps:

1. Select one or multiple users from the list of users displayed in User Management - Users section
2. Click on Delete button
3. Confirm Action dialog will be displayed, click on OK button to continue deleting the selected users
4. Users will be deleted from HyWorks Configuration

Delete Automatically using CSV Import
As specified in section CSV Template Fields and Import Behavior that specifying value True in column Delete User deletes the user from HyWorks Configuration. Thus, below steps can be followed to delete multiple users:

1. Export the existing users list into CSV file in required file format
2. For all the users to be deleted, specify value as True in column Delete User

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User Name</td>
<td>Delete User</td>
<td>Group</td>
<td>Status</td>
<td>Session</td>
<td>Team</td>
<td>Password</td>
</tr>
<tr>
<td>2</td>
<td>abca1</td>
<td>abca1</td>
<td>FALSE</td>
<td>abcgrp</td>
<td>built-in</td>
<td>abc123@</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>abca2</td>
<td>abca2</td>
<td>FALSE</td>
<td>abcgrp</td>
<td>built-in</td>
<td>abc123!</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>abca3</td>
<td>abca3</td>
<td>FALSE</td>
<td>abcgrp</td>
<td>built-in</td>
<td>abc123^</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>abca4</td>
<td>abca4</td>
<td>FALSE</td>
<td>abcgrp</td>
<td>built-in</td>
<td>abc123@</td>
<td></td>
</tr>
</tbody>
</table>
3. Import the CSV file using process specified in section **CSV Import Process**

4. All users specified with value **True** in **Delete User** column of imported CSV will be deleted and on next sync will be removed from respective session host servers as well.

❖ **Sync Users**

User synchronization refers to the process using which users (created manually or created using CSV Import) will be created and updated into member session host servers of associated teams. Considering that all users are added/updated in HyWorks Controller, follow the below steps to synchronize them into session host servers:

1. Go to User Management – Users section
2. Click on **Sync Users** button
3. **Confirm Action** dialog will be displayed, showing list of Session Teams
4. Select appropriate session teams in which users must be synchronized and click on button **Yes** to continue
5. Success status message will be displayed in the top bar.
6. All the users associated with the selected session team will be sent to all the member session host servers and following logs will be created on session host server
7. HyWorks Session Host Server, will create the users if they do not exist and will update them if already exist on session host server
8. On completion of the operation the logs will be sent to controller stating the number of users created, updated, deleted, or failed. (See screenshot above) (Please refer section **Syncing Mechanism** for detailed information)
9. Now on successful login from client, these built-in users will be able to connect to assigned applications or shared hosted desktop sessions.

❖ **Syncing Mechanism**

Following mechanism is used for user synchronization in HyWorks:

1. HyWorks sends list of users to each member session host server of session team
2. On Session host server, checks the members of local group with name “Accops_group”.
   a. If user in list does not exist on HyWorks Session Host server, then user will be created and will be made member of Accops_group.
   b. If user exists on session host server but does not belong to Accops_group, then user details are updated (password, display name and Accops_group membership)
   c. If the user belongs to the “Accops_group”, and the user is included in the list, the user details are updated, like password & display name
   d. If the user belongs to the “Accops_group”, and the user is not included in list from controller, the user is deleted from the RDS server. The profile of the user is also deleted.
   e. If the user list received from HyWorks is blank, HyWorks session host will delete all users who belong to “Accops_group”.
3. Once all the users provided in user list are synced, then session host servers will send summary of synchronization, providing information of added, updated, deleted or failed users count.

“User synchronization response from server ‘mytesthyworks’: Added Users:10, Updated Users:2, Deleted Users:5, Failed Users:3”
4. If any synchronization failures are observed, session host server logs can be analyzed for details, default directory of HyWorks session host server is as follows:

C:\Program Files (x86)\Accops\HyWorks\SessionHost\Logs

Example of detailed logs are provided below:

```


2017-02-12 17:50:25,858 [11] DEBUG EDCLog - User 'test user' is added to 'Accops_group' group
```

❖ Export Users

If administrator requires modifying list of users using CSV, then list of users can be exported in the CSV format and can be re-imported with modified details. Following steps can be used to export users list:

1. Go to User Management – Users section
2. Click on Export button
3. Select CSV File format in Export dialog and click on button Export
4. Controller will process all the records and will display dialog suggesting the status of export operation with Download button

```
Export

Export Processed Successfully.

Download Cancel
```

5. Click on Download button – CSV file in selected file format will be downloaded
6. Administrator can use this exported file to modify the details and then further re-import to update the details.

Populate users from authentication server

Groups

Groups subsection under User Management, can be used to manage built-in user-groups. Following management operations are available:

- Add Group
- Delete Group
- Edit Group
❖ **Add Group**

To create new user-group, follow the below steps:

1. Go to User Management – Groups section
2. Click on Add button
3. **Add Group** wizard will be invoked, requiring following details:
   a. **Groups Details** screen:
      i. Name: Logical name for new group
      ii. Description: Optional description of new group
      iii. Active: Unselect the checkbox to make user-group inactive, group-based entitlements will not work for inactive groups
   b. Click on Next button
   c. In **Assign Users** screen,
      i. Click on Add Users button to search and select intended users into this group
      ii. Added users can be removed by selecting and clicking on Remove Users button
4. Click on Save button to save the group
5. **Groups** section will now start showing the newly created group

❖ **Edit Group**

An existing group can be edited to update its description or changing active state or for modifying user assignments. To modify any existing group:

1. Go to User Management – Groups section
2. Select intended user-group from displayed list
3. Click on Edit button
4. **Edit Group** wizard will be launched
5. Update required modifiable field and click on Save button
6. Group information will be updated

❖ **Delete Group**

Using the same process as specified above, user-groups can also be deleted. Follow the below steps to delete user-group from HyWorks:

1. Go to User Management – Groups section
2. Select intended user-group from displayed list
3. Click on Delete button
4. **Confirm Action** dialog will be displayed, click on Delete button to continue deleting the user group
5. Group will be deleted and will not be displayed in User Management – Groups section

**Impact of Group Deletion**

1. Deleting a user group does not delete the group from entitlements or desktop pools.
2. Running sessions will not get affected
3. Users belonging to the deleted group will not be able to get assigned applications or desktops
Role based (Delegated administration) from HyWorks Management Console

HyWorks Controller enables role-based administration from HyWorks Management Console, where users on successful authentication will get

HyWorks supports delegated administration to enable following objectives:
1. Role based administration
2. Object/Resource level permissions
3. Organization wise permission configurations

The following sub-sections are available for administration management:
- Permissions
- Roles

Permissions

Permissions section in Administration can be used to designating users with built-in or custom defined roles (Refer section Roles for detailed information on roles).

Following options are available in Permissions section:
- Add Permission
- Edit Permission
- Delete Permission

Follow this section to get detailed information on Permissions operations.

❖ Add Permission

Administrator can designate a user with built-in or custom defined roles to enable that user as administrator of HyWorks. To add permission, follow the below steps:
1. Login as administrator with appropriate privileges on Permissions
2. Go to Administration – Permissions section
3. Click on button Add Permission
4. Add Permissions wizard will be invoked, displaying User/Group tab
5. In User/Group screen
   a. Click on Add Users/Groups button to invoke Available Clients dialog
      i. In Available Client dialog
         1. Set appropriate search options (Client Type as User or Groups, Search By, Search Option)
         2. Provide appropriate search text
         3. Select one or multiple users/groups from search results and click on button OK
         4. Administrator will be navigated back to Users/Groups tab, displaying added users/groups
6. At the bottom of *Add Permissions* wizard, checkbox *Propagate to Child* is shown. Selecting the checkbox will allow the same permissions to be propagated to child organizations, which means this new administrator will be able to login and do administrative tasks on child organization as well.
   a. The access of Propagated permissions can be later revoked using Restrict Access or overriding its role. (To be explained later in this section)
7. Click on **Next** button to proceed to **Role** screen
8. On **Role** screen, all built-in or custom defined roles (except super-administrator) will be listed
   a. Select one of the listed roles
   b. Propagate to child checkbox will be available on this screen as well and can be used to propagate the permissions to the child level.
9. Click on **Save** button to save the settings
10. Permissions will be added and will be listed in **Permissions** section
11. The user added with specific role will be able to login and manage following organizations
    a. Current organization where its defined
    b. Child organizations (if propagated and not restricted)

### Permission Propagation

Permission propagation refers to defined behavior using which the permissions of one organizations can be inherited into child organizations.

Option to enable propagation appears during *Add/ Edit Permissions* wizard.

Example: Permission is created for user ‘Admin1’ at Root organization with administrator role and *Propagate to child* is enabled.

User ‘Admin1’ will have access to root organization as well as all child organizations with role administrator because permissions are propagated.

![Permission Propagation Diagram]

### Disable Propagation

Propagation can be disabled at any level of organization hierarchy, following two scenarios are explained:

- **Disable Propagation at Definition level**: While adding/editing permissions at current organization level (where permissions are defined), uncheck *Propagate to child* to disable propagation. Now administrator won’t have permissions on child organizations.
  
  Example: Please refer image shown in section *Permission Propagation*
Create permission for user ‘admin2’ at organization root with **Propagate to child** unchecked. Login into management console with user ‘admin2’. Admin2 will have access to only root organization. He will not be able to see or enter other organizations.

- **Disable Propagation at child organization level:** It is possible to disable propagation at child organization level by editing the permissions at child level:
  
  Example: Please refer image shown in section **Permission Propagation**
  
  1. Create permission for user ‘admin3’ at organization ‘root’ with **Propagate to child** checked.
  2. Edit permission for user admin3 to **uncheck Propagate to child** at child organization ‘Org 1’.
  3. Login into management console with user ‘admin3’. ‘Admin3’ will not be able to see/modify organizations ‘Org 1.1’ and ‘Org1.2’ since propagation is disabled at organization ‘Org 1’.

**Edit Permission**

Permissions can be modified either at definition level or at child level and depending on the level it is being invoked, options are enabled or disabled.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Logged-in user cannot modify its own permissions and thus, for modifying permissions of any user, it is must to login with super-administrator credentials or other user credentials with enough rights on permissions.</td>
</tr>
</tbody>
</table>

**Edit Permission at Parent (Definition) Level**

1. Login as administrator with appropriate privileges on Permissions into organization where the permissions to be modified is defined
2. Go to Administration – Permissions section
3. Select any administrator user - click on button **Edit**
4. **Change Access Permission** dialog will be displayed, allowing following options:
   i. Role Selection: To designate a new role to the user
   ii. Propagate: To enable or disable propagation
5. Modify available options as needed and click on **OK** button to save the changes
6. Role changes will come into effect immediately, whereas propagation changes will require user to re-login

**Edit Permission at Child Level**

It is possible to modify the permission of the user at child level as well. Follow the below steps:

1. Login as administrator with appropriate privileges on Permissions into child organization
2. Go to Administration – Permissions section
3. Select any administrator user - click on button **Edit**
4. **Change Access Permission** dialog will be displayed, allowing following options:
i. Role Selection: To designate a new role to the user, by changing the role of a user at child organization, its permissions can also be overridden.

ii. Propagate: To enable or disable propagation

iii. Restrict Access: To disable administrator access on this child organization level

5. Modify available options as required and click on **OK** button to save the changes

6. Changes will be saved and following impact of permission modification will be available:
   i. Role changes will come into effect immediately
   ii. Propagation changes will come into effect from next login
   iii. Restrict Access changes will come into effect from next login
   iv. Once the permissions are modified at child level, its definition level is changed to current organization (child) as well, and it becomes object of that organization.

慎重にアクセス

慎重にアクセスオプションは、プロパゲーションされた管理者ユーザーに対してのみ、子組織レベルで利用可能。この機能は、プロパゲーションされた管理者ユーザーのアクセスを禁止するために使用されます。

例: 请参阅在权能プロパゲーションセクションに示す図

1. Create permission for user ‘user4’ at organization ‘root’ with **Propagate to child** checked.
2. Edit permission for user ‘user4’ at child organization ‘org2’ with ‘restrict access’ enabled.
3. Login into management console with user ‘user4’.
4. User4 will not be able to see/modify into organizations ‘org2’ and ‘org2.1’ since access is restricted in those organizations.
   a. Once the definition level of permission changes, it will not be affected by the changes being done at parent level and its properties should be modified at all definition level.

削除権能

削除権能は可能ですが、権能を削除する地点が権能を削除した地点であるときに、ユーザーは自分の権能を削除することはできません。以下の手順に従って、ユーザーの権能を削除します:

1. Login as administrator with appropriate privileges on Permissions into organization where the permissions to be modified is defined
2. Go to Administration – Permissions section
3. Select any administrator user - click on **Delete** button
4. **Confirm Action** dialog will be displayed, click on **Remove** button to continue removing the permissions
5. Permissions will be removed and will not be displayed in the permissions list.
6. User will not be login into organization after deletion.

権能オーバーライド

権能オーバーライドは、二つの方法で起こります:

1. Permissions are first defined at parent level with propagation and at child level its redefined to have a new role
   a. On parent level user will have access as per defined role in that organization
   b. On child level user will have access as per new role
2. Permissions are defined for a user group and then for individual user as well
a. On parent level, user will have access as per his permissions overriding permissions coming from group
b. On child level, access and privileges will be provided as per user’s individual permissions

Roles

Roles sub-section under Administration section can be used to view the default available roles and for creating custom roles as per requirement.

Roles defines the privileges, that user is going to have on HyWorks/RMS resources.

Roles are critical for organizational access and thus are accessible to super-administrator only. Based on access, roles can also be classified into HyWorks and RMS roles:

❖ Built-in Roles

Following pre-defined roles are available in HyWorks configurations, HyWorks management roles are defined in detail in this section, whereas RMS roles will be briefly introduced and will be covered in detail in reservation management guide.

1. Super-administrator
2. Administrator
3. Helpdesk
4. Read-only

Following pre-defined HyLabs roles are available in HyWorks Configurations:

1. Reservation Admin
2. Incharge
3. Assistant
4. Participant

Super-Administrator

Root user of HyWorks, having below key facts associated with it

1. Super-administrator can be defined during installation only
2. Super-administrator role cannot be modified
3. No users (other than local user or group defined as super-administrator during installation) can be designated with super-administrator role.
4. User/ Group, once designated with super-administrator role during installation, cannot be deleted
5. Super-administrator is by-default propagated to child organizations
6. Super-administrator has all the configurational access in HyWorks, including system level configurations.

Administrator

Next to super-administrator but does not have access to system level configurations.

1. The second most powerful user after super-administrator except some system level configurations
2. Administrator (Built-in) role cannot be deleted but the user assigned with administrator role can be removed
3. Administrator user/group permissions can be over-ridden at child level by not propagating to child or by assigning some other role to user

Helpdesk
1. Level-3 administrator role, having write access to limited modules.
2. Helpdesk (Built-in) role cannot be deleted but the user assigned with administrator role can be removed
3. Helpdesk user/group permissions can be over-ridden at child level by not propagating to child or by assigning some other role to user

Read-Only
1. Role with having view only permissions on limited modules
2. Built-in role in HyWorks which cannot be deleted
3. Read-only user/group permissions can be over-ridden at child level by not propagating to child or by assigning some other role to user

❖ Role Management Options
Following role management options are available for HyWorks administrators:

• View Privileges
• Add Role
• Edit Role
• Delete Role

Let us understand each of these operations in detail.

View Privileges
To view associate privileges of any role following steps can be used:
1. Go to Administration – Permissions – Roles section
2. Click on any role-name or select and click on button View Details
3. Administrator will be navigated to Privileges page, displaying HyWorks resources and associate rights of that role

Add Role
If needed a custom role, can also be defined and can be assigned to users for creating administrator with defined privileges.

To add a new role, follow the below process:
1. Login as Super-administrator
2. Go to Administration -> Roles
3. Click on Add button
4. In Add Role wizard
   a. Provide appropriate Name for new role
   b. Provide some Description (Optional) for new role
   c. Select Status checkbox to make role Active or keep role as unchecked to make it Inactive (Inactive roles do not appear while adding permissions)
d. Select appropriate **Role Classification** i.e. Administrator, RMS-Incharge, RMS-Assistant or RMS-Participant.
   i. This role classification determines the basic level of access in RMS e.g. an incharge classified role will also have incharge like permissions.

e. Select appropriate privileges on resources for new role (Use search controls to locate any specific permissions)
   i. Privileges on system level resource cannot be given to custom roles and will appear as disabled, example of such resources are:
      1. Role Management
      2. Client Software Settings
      3. Server Configurations
      4. HyWorks Controller
      5. Backup and Restore
      6. License Management
      7. RDP Proxy Settings
      8. SMTP Configuration

5. Click on **Add** button to save the new role
6. Role will be saved and will now be displayed in the list of roles. The custom role can now be assigned to users from **Permissions** section.

**Edit Role**

As already specified, system defined roles cannot be modified (**Edit** button gets disabled) but administrator can modify a custom defined role using following steps:

1. Login as Super-administrator and go to Administration -> Roles
2. Select any custom defined role and click on **Edit** button
3. In **Edit Role** wizard, following fields will be editable:
   a. Name
   b. Description
   c. Statue
   d. Privileges (Use search controls to locate any specific permissions)
4. Modify all fields as needed and then click on **Update** button
5. Role will be saved with new configurations and new privileges will come into effect on next logon of the user.

**Delete Role**

**Delete** button will be disabled on selecting system defined roles but administrator can delete a custom defined role, by following the below steps:

1. Login as Super-administrator and go to Administration - > Roles
2. Select any custom defined role and click on **Delete** button
3. **Confirm Action** dialog will be displayed, click on **Delete** button to continue deleting the role
4. If the role is associated with any permissions, then it will show error else the role will be deleted and will not be displayed in **Roles** section.
## Role Privileges Comparison
The table below gives the overall comparison of several roles and their respective privileges on HyWorks resources:

<table>
<thead>
<tr>
<th>Module Name</th>
<th>Role</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Add</td>
<td>Edit</td>
</tr>
<tr>
<td>Permissions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(Y)</td>
</tr>
<tr>
<td>Role Management</td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(X)</td>
</tr>
<tr>
<td>Application Definition</td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(Y)</td>
</tr>
<tr>
<td>Application Entitlements</td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(Y)</td>
</tr>
<tr>
<td>Desktop Pools</td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(Y)</td>
</tr>
<tr>
<td>Desktops VMs</td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(Y)</td>
</tr>
<tr>
<td>Default Device Settings</td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(X)</td>
</tr>
<tr>
<td>Section</td>
<td>Super-Administrator</td>
<td>Administrator</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Device Settings</td>
<td>(Y)</td>
<td>(Y)</td>
</tr>
<tr>
<td>Device Group Management</td>
<td>(Y)</td>
<td>(Y)</td>
</tr>
<tr>
<td>Device Management</td>
<td>(Y)</td>
<td>(Y)</td>
</tr>
<tr>
<td>HyWorks Logs</td>
<td>(Y)</td>
<td>(Y)</td>
</tr>
<tr>
<td>Client Software Settings</td>
<td>(Y)</td>
<td>(Y)</td>
</tr>
<tr>
<td>Remote Support</td>
<td>(Y)</td>
<td>(Y)</td>
</tr>
<tr>
<td>Server Configurations</td>
<td>(Y)</td>
<td>(Y)</td>
</tr>
<tr>
<td>Authentication Servers</td>
<td>(Y)</td>
<td>(Y)</td>
</tr>
<tr>
<td>Category</td>
<td>Role</td>
<td>Helpdesk</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(X)</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------</td>
<td>-----</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(X)</td>
</tr>
<tr>
<td>License Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(X)</td>
</tr>
<tr>
<td>RDP Proxy Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(Y)</td>
</tr>
<tr>
<td>SMTP Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(Y)</td>
</tr>
<tr>
<td>Built-in Directory Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(Y)</td>
</tr>
<tr>
<td>Connection Profiles</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(Y)</td>
</tr>
<tr>
<td>Organizations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(Y)</td>
</tr>
<tr>
<td>Virtualization Profiles</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Super-Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Helpdesk</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Read-Only</td>
<td>(Y)</td>
</tr>
<tr>
<td></td>
<td>Custom Defined</td>
<td>(Y)</td>
</tr>
</tbody>
</table>
Endpoint Management in HyWorks

All client-based endpoints once communicate with HyWorks Controller, they are permanently registered and can be managed centrally from HyWorks. Management of endpoints involves controlling and providing all configurations required for secure, managed and efficient remote sessions.

In this section of HyWorks administration, all endpoint management aspects will be covered in detail.

- Viewing list of registered endpoints
- Viewing details of registered endpoint

Viewing List of Registered Endpoints

All registered endpoints are listed in Monitoring -> Endpoints page. On navigating to Endpoints page following details can be seen:

- Name/ Username
  - Name: Showing the current display name of the device. Default name of device is created by appending the MAC address of the device to text ‘HyDesk’ e.g. HyDesk-40:e2:30:ec:de:71.
  - The name of device is configurable and can be changed from Device Settings dialog.
  - Username: Username of currently logged-in user from the listed device.

- Model: Displaying the type of registered device based on the system on which HyWorks Client (HyWorks client software).
  - The possible values (based on supported endpoints) could be
    - Hy1000/HY2000/HY3000/HY3020/HY4000
    - Windows Client
    - Windows On-demand Client
    - Ubuntu Client

- IP Address: Network IP address of registered device (as provided by ISP).
  - In case of LAN based configurations, the Network IP address and local IP address both appears as same
  - In case of WAN or internet configurations the network IP address can defer with the local IP address

- MAC Address: MAC address of the registered device

- Status: Status column provides the status of the device, which can have following possible values
  - Active: Devices with running desktop or application sessions (Colour: Green)
  - Idle: Devices with no desktop or application sessions but in actively communicating with Controller (Colour: Yellow)
  - Offline: Devices not sending heartbeats to controller and not connected with controller (Colour: Grey)
  - Disabled: Device is disabled from HyWorks Controller Management console and connected HyWorks Controller
  - Enabled: A disconnected device, which was disabled before, is enabled from HyWorks Controller Management console. -> Devices will be moved to Idle status
  - Shutting Down: Device shutdown power operation has been initiated from HyWorks Controller Management Console
Rebooting: A powered on (connected) device has been rebooted from HyWorks Controller Management Console

Powering On: Device power-on operation has been initiated from Controller will be shown status. The status is intermediate and will be changed after some time, once the device is up and connected with controller.

- **Last Seen**: Last seen information reflects the duration when the device has last contacted the server. Hovering mouse over *Last Seen* information displays exact time stamp at which the device has last communicated with Controller.

- **Profile**: Current assigned profile on the device is displayed under the Connection Profile column. The new connection profile can be assigned from Device Settings dialog or from Assign Connection Profile dialog.

- **Group**: Displaying the current group name to which device belongs

Following UI actions are available for administrator for ease of administration:

- **Refresh**: Re-fetching all latest information from HyWorks Controller service for listed devices
- **Sorting**: Clicking on column header can sort the endpoints. The feature is available on following columns: Name, IP address, Connection status or Connection profile values
  - **Default Sorting**: By default, devices will be sorted by Connection Status only which means all Active devices will appear first and will be sorted alphabetically.
- **Search**: Administrator can search any specific device, by providing appropriate search string. Clearing the search will start displaying list of endpoints again.
- **Number of endpoints per page**: By default, endpoints are shown dynamically as per available browser area, however administrator can change count to show from 10 to 150 endpoints per page. The settings are not remembered and navigating away from endpoints page or reload will reset the list again to be shown dynamically.

**View Endpoints in Group View**

HyWorks v3.0 or later supports grouping of endpoints into device groups for efficient management. The list view can also be changed in HyWorks – Endpoints section to view endpoints in group view.

1. Go to Monitoring – Endpoints section
2. Click on button *Group View*
3. To view all endpoints from a specific group, click on group

**Getting Detailed Information of an Endpoint**

To view detailed information of an endpoint, click on *Device Name*, which opens the *Device Details* page, showing all relevant information of the device:

<table>
<thead>
<tr>
<th>Property</th>
<th>Purpose</th>
<th>Possible Values</th>
<th>Is Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Name</strong></td>
<td>Display name of the device</td>
<td>By default, generated by the HyWorks Controller as - HyDesk + ‘MAC Address’</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Admin can configure the name for device as per his</td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC Address of device</td>
<td>MAC Address</td>
<td>No</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------</td>
<td>-------------</td>
<td>----</td>
</tr>
<tr>
<td>Device IP Address</td>
<td>IP Address of device</td>
<td>IP Address</td>
<td>No</td>
</tr>
<tr>
<td>Network IP Address</td>
<td>IP Address of Network where device is located</td>
<td>As provided by ISP or in case of LAN environment same as Device IP</td>
<td></td>
</tr>
<tr>
<td>Serial No.</td>
<td>The serial number of Device</td>
<td>e.g. XYZ45024</td>
<td>No</td>
</tr>
<tr>
<td>Model No.</td>
<td>Model number of devices</td>
<td>e.g. HY3000</td>
<td>No</td>
</tr>
<tr>
<td>Hardware Version</td>
<td>Details of the hardware of the device</td>
<td>e.g. ETCC00XC0480</td>
<td>No</td>
</tr>
<tr>
<td>Software Version</td>
<td>Software version running on the device</td>
<td>e.g. 257</td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>The language currently set on the device</td>
<td>e.g. US or German</td>
<td>No</td>
</tr>
<tr>
<td>Registere d On</td>
<td>The time on which device was registered with Accops HyWorks Controller Service</td>
<td>e.g. 25-Jun-2015 05:20:56 PM</td>
<td>No</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The time on which last time controller has made communication with device</td>
<td>e.g. 25-Jun-2015 05:23:56 PM</td>
<td>No</td>
</tr>
</tbody>
</table>
| Status            | Status of the device | Active: Device with running session  
Offline: Device not communicating with controller  
Idle: Devices connected with controller but does not have any desktop or app sessions | No |
| Connecti on Status| Connection Status of device | Reachable: Device is communicating with Controller  
Unreachable: Device is not in connection with Controller  
Connecting: Checking the status of the device | No |
| Connecti on Profile| Assigned connection profile to the device. User will be getting the remote sessions as per the assigned connection profile | Default Profile: The system generated default profile, assigned to devices by default  
User assigned profiles | Yes |
Device Configurations

Endpoints page can be used to update the devices configurations. Devices can be configured by using three layers of settings:

- Default Settings
- Group Settings
- Device Settings

❖ Effective or Applicable Settings on Endpoints

As mentioned in the above section that device configurations can be done using three layers of settings i.e. Default Settings, Group Settings and Device Settings.

How the effective settings can be derived?

The effective settings on a device are determined by the priorities of the different layers of configurations. The priorities are as follows:

Device Settings (Highest) > Group Settings (Medium) > Default Settings (Lowest)

Let us try to understand this by few examples:

Example# 1: Volume settings are configured in the following manner:

- Default Settings: 100
- Group Settings: 61
- Device Settings: 50

Now effective volume settings on device will be 50 as Device Settings are having highest priority.

Example# 2: The table below consists of more examples for effective device configurations on endpoint:

<table>
<thead>
<tr>
<th>Configuration Attribute</th>
<th>Default Settings</th>
<th>Group Settings</th>
<th>Device Settings</th>
<th>Effective Settings on Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Redirection Driver</td>
<td>Built-In</td>
<td>Inherit</td>
<td>Inherit</td>
<td>Built-In</td>
</tr>
<tr>
<td>USB Redirection Driver</td>
<td>Enhanced</td>
<td>Built-In</td>
<td>Inherit</td>
<td>Built-In</td>
</tr>
<tr>
<td>USB Redirection Driver</td>
<td>Enhanced</td>
<td>Built-In</td>
<td>Enhanced</td>
<td>Enhanced</td>
</tr>
<tr>
<td>Desktop Mode</td>
<td>KIOSK</td>
<td>KIOSK</td>
<td>Set Manually - Desktop</td>
<td>Desktop</td>
</tr>
<tr>
<td>Desktop Mode</td>
<td>KIOSK</td>
<td>Inherit</td>
<td>Set Manually - KIOSK</td>
<td>KIOSK</td>
</tr>
<tr>
<td>Desktop Mode</td>
<td>Desktop</td>
<td>KIOSK</td>
<td>Inherit</td>
<td>KIOSK</td>
</tr>
</tbody>
</table>

Default Settings

Default Settings affects all the devices which are already registered or the devices which are going to be registered in future.

Default Settings are the first layer of configurations which can be overwritten from Group Settings (Second Layer) or Devices Settings of specific device which is the third and final layer of configurations.
Opening Default Settings dialog:
1. Make sure to log-in as super administrator and currently selected organization is Default
2. Go to Endpoints tab (Make sure no devices are selected)
3. Click on Default Settings button

Note:
- Default Settings will only be available in Default organization only
- Default Settings button will only be available if no devices are selected.

Default Settings dialog provides the following configurations to be configured for devices:

- Configurations
  - Screen Resolution
  - Volume
  - USB Redirection Driver
  - Connection Profile
  - Language
  - Banner Image
- Login Settings
  - Auto Login Checkbox
  - Ask Credentials at first logon
  - Set Credentials
  - Windows Login
- UI Controls
  - Display or Hide UI Controls on HyWorks Client Login Screen E.g. Show/ hide Shutdown,
    Settings, Info, Accops Logo, Network Settings tab, Remember Me checkbox
  - Password Protect UI Controls and specify the password e.g. password protect Shutdown,
    Settings, Mode change etc.
- Desktop Mode
  - Default Desktop Mode for HY3000, HY2000, HY3020, HY4000, Windows Client and Linux
    Client
- Upgrade Settings
  - Auto Upgrade – Enable/ Disable
  - Upgrade Source: Currently upgrade from controller is supported
- Power Saving Mode
  - Enable/Disable
    - Device Turn Off Timeout in Minutes
- Advance Settings
  - Session Shell
  - Session Control
- Custom Links

We will be going through each of these configurations in details in the later section of the document.

❖ Configurations Tab in Default Settings
Configurations screen of Default Settings provides following options:
**Screen Resolution**

The **Screen Resolution** settings in Default Settings dialog is no longer used and thus should be avoided while configuring Default Settings.

Earlier this setting was used to configure a common resolution on all the devices. The display configurations for different devices are now controlled through Device Settings.

The default value is native, which indicates the device’s settings being accepted. The other supported resolution values are:

- 800 x 600
- 1024 x 768
- 1280 x 720
- 1280 x 768
- 1280 x 1024
- 1366 x 768
- 1450 x 1050
- 1440 x 900
- 1600 x 900
- 1680 x 1050
- 1920 x 1080

**Volume**

Administrator can set the default volume for the devices using Volume options in Default Settings.

The devices which are inheriting volume settings from the Default Settings will be affected and will get set to volume specified in Default Settings dialog.

For changing the Volume level in Default Settings:

1. Change the volume value using the slider feature
2. Click on **Save** button

Following devices will be unaffected from the Volume changes in Default Settings:

1. Devices not inheriting Volume Settings i.e. Device Settings of such devices are either Set Manually or User’s Settings
2. Windows Clients – Assuming such devices to be under the control of users any such configurations are ignored

**Note:**

➢ Volume settings in Default Settings are primary layer of volume configurations and can be overwritten from Device Settings of specific device. Please check Device Settings section for more details.

**USB Redirection Driver**

**USB Redirection Driver** from Default Settings determines the default USB Redirection Drivers to be used by all the existing devices or devices to be registered later.

**Default Value:** By default, USB Redirection Driver is set as **Built-In** in Default Settings which means all newly registered devices will be using Built-In USB Redirection Driver.

Devices which will be affected by USB Redirection Driver Changes in Default Settings:

1. Devices which are inheriting the USB Redirection Driver configurations from Group Settings and Group Configurations are inheriting USB Redirection Driver configurations from Default Settings
2. New Devices to be registered later

Devices which will not be affected by USB Redirection Driver Changes in Default Settings:

1. Devices not inheriting the USB Redirection Driver configurations from Default Settings i.e. Device Settings of such devices are configured as Set Manually
Changing USB Redirection Driver Configurations in Default Settings:

1. Open Default Settings dialog from Endpoints page
2. In Configuration section – USB Redirection Driver
3. Select desired USB Redirection Driver as Built-In or Enhanced
4. Click on Save button to save the settings

**Supported USB Redirection Drivers**

HyWorks 3.0 or later supports following types of USB Redirection Drivers:

- **None**: No USB Redirection Drivers will be used and attached USB devices won’t be redirected
- **Built-In**: Built-In USB Redirection Driver: Best suited for dedicated VDI infrastructure
- **Enhanced**: Best fit in HyWorks deployment with shared hosted desktops

**Note:**

- USB Redirection Driver changes requires the device to be rebooted therefore if any changes are made in Default Settings, all devices inheriting the USB Redirection Drivers settings from Default Settings will be rebooted and will be configured with newly configured redirection drivers.
- On Windows Applications, USB Redirection Driver changes won’t require machine reboot, only HyWorks Client application will be restarted.

A more detailed article ‘USB Redirection in HyWorks’ for detailed information on USB Redirection will be published on Support portal. Please contact Accops support for any specific information on USB Redirection.

**Language**

A language can be specified to be used along with native language for newly registered devices so that the user logging in from the devices will have two language choices; one as native and another one as language specified in Default Settings dialog.

Changing the language in Default Settings dialog does not affect the existing registered devices; the language is specific to newly registered devices only.

**Note:**

- The language configured in Default Settings dialog does not force language settings to all the devices and/or does not overwrite any device specific language selection by user from devices end or in device specific settings
- Administrator will be able to overwrite the device specific default language from the Device Settings dialog
- Organizational level language configurations can be defined from Organizations -> Realm Settings. Please refer section Organizations for detailed information on language configurations.
Upload Banner Image

Upload banner image can be used to insert a specific banner image on the device login screen. The inserted banner image will be available on all registered devices’ login screens.

Note:
- HyWorks v3.0 or later Clients do not use Banner image and thus Banner Image configuration does not apply to v3.0 or later Clients.
- Banner Image configuration will continue to work for v2.5 clients.

Banner Image configuration provides two options to the administrator:

- **Use Default Banner:** ‘Use Default Banner’ is used by default and could be used when administrator wants to change the banner from custom banner to default. The setting will use the default banner delivered with the Accops HyWorks Controller Service. To configure default banner image on HyWorks Client Login screen
  1. Check the checkbox **Use Default Banner** to enable this setting
  2. Click on **Save** button to apply the settings

- **Upload (Custom) Image:** Administrator can also insert custom image as banner. Below are some key details for files to be used as banner image:
  - Supported File Formats for upload image: jpg, jpeg, gif, png
  - Maximum File Size supported for upload image: 4 MB
  - Image Dimensions supported is 700 X 175

To use a custom image as banner for all registered devices:

1. Click on **Upload Image** control to open the wizard for choosing the custom banner image.
2. Select your image file and click on **Open** button
3. On **Crop Banner Image** screen, select the area of image and click on **Save Banner Image** button.
4. Click on **Save** button on Default Settings dialog.
5. All the devices will start downloading and displaying new banner after it is saved.

Login Settings

Login Settings section of Default Settings dialog provide options to configure Automatic login settings on devices.

Automatic Login

Automatic login configuration enables the automatic connection to the configured Desktops.

- **Available Auto-Login Options**

Following types of Auto Login settings can be configured on devices:

1. **Set Credentials:** Devices will be automatically connected to configured Desktops using the credentials set by Administrator in Default Settings/ Device Settings
2. **Ask Credentials at first Logon:** On first login users will be displayed with default login screen and on successful logon, the provided credentials will be cached. Same
credentials will be used for automatic connection to the configured Desktops from next device reboot.

3. **Windows Login**: Configured Desktops will be connected on the devices without any credentials and users will be needed to provide credentials in the remote session.

**Note:**
- Windows login does not work with NLA (Network Level Authentication) enabled on devices.

- **Enable Auto Login Configurations from Default Settings**
  1. Go to Endpoints page – Open Default Settings dialog
  2. Go to Login Settings section
  3. Select the Auto Login checkbox to enable the auto login setting
  4. Choose desired **Auto Login Type** as per requirement and provide appropriate details as per selected Auto Login Type
     a. Ask Credentials at First Logon – Won’t require any other details
     b. Windows Login – Won’t require any other details
     c. Set Credentials – Will require username and password
  5. Click on **Save** button to save the Default Settings
  6. On Confirm Action Dialog
     a. Select checkbox ‘Reboot the device(s) now. Connected user(s) will be disconnected.’ to immediately reboot and configure auto login settings and click on **Save** button
     Or
     b. Keep checkbox ‘Reboot the device(s) now. Connected user(s) will be disconnected.’ unselected, if willing to reboot devices manually later or willing to configure the settings on next device reboot

**Note:**
- All auto login setting changes require device to be rebooted.
- Enabling Auto login settings in Default Settings with option ‘Reboot the device(s) now. Connected user(s) will be disconnected.’ Will reboot all the devices which are inheriting the Auto login settings. The default Auto login configuration in Device Settings is ‘Inherit’ which means all the registered devices will be rebooted and will be configured with auto login settings.
- Devices which will be registered later to HyWorks Controller will also start using the Auto login settings due to Inherit configuration of Auto login in Device Settings.

More detailed information will be provided on Auto login in the later section of the document.

**UI Controls**

**UI Controls** section in Default Settings provide UI customization of HyWorks Client Login screen which means administrator will be able to enable or disable various controls on HyWorks Client Login screen.

UI Control configurations are provided on HyWorks Controller to prevent accidental changes in HyWorks Client configurations or hiding information from end users.
**Show/Hide UI Controls:**

To show a UI Control, follow the below steps:

1. Select the checkbox displayed against the control and uncheck the checkbox to hide it on HyWorks Client Login screen
2. Click on **Save** button to save the Default Settings
3. All devices inheriting UI Controls (by default all devices inherits UI Control property) will start showing or hiding respective UI Controls on HyWorks Client login screen

- **UI Controls Which can be shown or hidden:**
  - *Information* Button
  - *Shutdown* Button
  - *Settings* Button
  - *Network Settings* tab in *Settings* window
  - *Accops* Logo
  - *Remember Me* checkbox
  - *Virtual Keyboard*
  - *USB Redirection Driver*

**Password Protect UI Controls**

To make any UI Control password protected, follow the below steps:

1. Go to UI Controls section in Default Settings dialog
2. Select the checkbox against it and to keep it unprotected uncheck the checkbox.
3. Provide appropriate password if making any UI Control Password protected
4. Click on **Save** button to save Default Settings
5. All devices inheriting UI Controls (by default all devices inherits UI Control property) will now start using Password Protection settings
6. If UI Controls are made password protect, accessing those control will start prompting for password and will be accessible only on providing correct password
7. UI Controls which are not made password protected will be accessible without any password

- **UI Controls Which can be Password Protected**
  - *Shutdown* Button
  - *Settings* Button
  - *Mode Change* (Desktop Mode Change from HyWorks Client Login screen using secret key combination
  - *Virtual Keyboard*
  - *USB Redirection Driver*

**Note:**

➢ *UI Controls* settings in *Default Settings* dialog are primary layer of UI Control configurations and can be overwritten from Device Settings of specific device. Please check Device Settings section for more details.

**Desktop Mode**
‘Desktop Mode’ section in Default Device Setting dialog enables administrator to configure the default desktop mode for different endpoint devices. The default configurations of desktop mode in Default Settings are as follows:

- HY1000: KIOSK
- HY2000: KIOSK
- HY3000: KIOSK
- HY3020: KIOSK
- HY4000: KIOSK
- macOS Client: Desktop
- Ubuntu Client: Desktop
- Windows Client: Desktop
- Windows on-demand Client: Desktop

To change Desktop Mode configurations in Default Settings:
1. Go to Desktop Mode section in Default Settings dialog
2. Select appropriate desktop mode (Desktop or KIOSK) for the desired type of device (e.g. if willing to keep Linux clients in Desktop mode then change mode against Linux Client)
3. Click on Save button to save Default Settings

Note:
- Desktop Mode configurations in Device Settings are set as ‘User Settings’ which means whatever desktop mode user is currently using will be kept as it is and will not be changed and thus changing Desktop Mode configurations in Default Settings will not affect the devices.

Note:
- Desktop Mode configurations in Default Settings are primary layer of Desktop Mode configurations and can be overwritten from Device Settings of specific device. Please check Device Settings section for more details.
- Any changes in Desktop Mode configurations will require devices to be rebooted (if the device settings are being changed) and thus administrator will be careful while making changes in Default Settings as all devices inheriting Desktop Mode configurations will be rebooted and may cause running sessions to be disconnected.
- On Windows clients, desktop mode changes from HyWorks Controller do not work to avoid possible corruption of end user environment on Windows machines. However, desktop mode can still be changed on Windows machines from HyWorks Client login screen and secret key combinations.

❖ Upgrade Settings
Administrator can check Auto Update Client checkbox available in Upgrade Settings section to enable automatic upgrade of devices.

Once enabled, devices will start downloading and installing the latest hotfixes available on HyWorks Controller.

By default, Auto Update Client setting is not enabled to avoid any accidental updates on registered devices.
Enabling **Auto Update Client** will upgrade the HyWorks Client application on device and the following type of devices will be affected:

- Newly registered devices
- Devices currently inheriting the Auto Update Client settings from Default Settings

**Note:**

- Devices will be updated only when clients are currently in idle state (Not having any running desktop sessions)
- The upgrade may cause reboot of devices
- **Auto Update Client** settings in **Default Settings** can be overwritten by **Group Settings** or **Device Settings**

In the later section of the document, more information and conceptual details of Device upgrade will be provided.

❖ **Power Saving Mode**

Enabling **Power Saving Mode** on devices will automatically turn off the devices when the specified turn-off timeout limit is reached.

Enabling Power Saving Mode in Default Settings will affect following type of devices:

- Newly registered devices
- Devices currently inheriting the **Power Saving Mode** settings from Default Settings

Power Saving Mode does not turn off the devices; if:

- Session is running on devices
- Devices are configured with Automatic Login
- User is actively operating on the devices (Mouse and Keyboard events are being observed)
- Device model is Windows client i.e. HyWorks client running from user desktop

❖ **Advanced Settings**

**Advanced Settings** section currently provides option to enable or disable the **Remote Shell** and **Remote Control** options on devices. The options available in Advanced Settings are:

- **Remote Shell:** It allows administrator to enable/disable the SSH on the devices and thus affects only HY3000, HY2000, HY4000 and Linux Clients only. Once enabled administrator will be able to **SSH** to specific device with root credentials and provided password (If not specified default password will be set, contact **Accops Support** for default password). The option provides administrator to work on devices in case of any issues or specific configurations.

- **Remote Control:** It allows administrator to enable/ disable VNC on the devices and thus applies to HY3000, HY2000, HY4000, and HyWorks Client on Accops OS only, HyWorks Client installed on Ubuntu OS i.e. Linux Client will require manual installation of VNC servers on system to make this option work. Once enabled administrator will be able to view and work on devices remotely using VNC viewer. The option provides administrator to work on devices in case of any issues or specific configurations.
By default, the options are disabled in Default Settings. To enable Advanced Settings configurations in Default Settings:

1. Go to Advanced Settings section in Default Settings dialog
2. Select on Remote Shell checkbox to enable shell access to the endpoints – Selecting Remote Shell option enables the following controls
   a. Set Custom Password: Select this checkbox to provide custom remote shell password, if custom password is not set then devices will use default password.
   b. Show: Option to show the password in text format
3. Select Remote Control checkbox to enabled remote control of endpoints using VNC clients – Selecting Remote Control checkbox enables following controls
   a. Require User Confirmation: If user working on device should be prompted for confirmation for taking remote control
   b. Set Custom Remote Control Password: Like, Remote Shell a custom password can be set for accessing remote session of endpoints. If password is not specified, it will not require any password to connect to devices using VNC
4. Click on Save button to save Default Settings

Below is the list of endpoints which support Remote Session - Advanced Settings configurations:

Remote Shell:
- HY2000
- HY3000
- HY4000
- Linux Clients

Remote Control:
- HY2000
- HY3000
- HY4000
- Linux Clients

Note:
- **Advanced Settings** configurations come into effect after reboot of endpoint devices and thus changing the configurations will reboot the devices, without prompting the user on it and thus should be configured cautiously.
- Advanced Settings configurations in Default Settings are primary layer of Advanced Settings configurations and can be overwritten from Device Settings of specific device. Please check Device Settings section for more details.

Custom Links

Some organizations have web applications which must be available to end-users all the time even when they are not able to access assigned desktop or applications. Such URLs can also be managed from endpoints page and published on HyWorks Clients.

On clicking on these URLs, HyWorks Client launches default browser of the system, opens the published URL.

To publish URL for all endpoints, which are inheriting Custom URLs, follow the below steps:

1. Go to Default Settings – Custom Links
2. Provide appropriate **Name** and **URL** for links to publish
3. Choose an icon by clicking on Browse button from a predefined list
4. Click on **Add** button
5. Click on **Save** to update configurations.
6. All endpoints will get published URLs in next heartbeat and users can click on Links to access provided URLs.

**Group Settings**

HyWorks Controller enables administrators to group devices into multiple groups for ease of management. Device grouping helps administrator as follows:

- Easy identification of devices belonging to a group
- Keeping common settings for the group of devices
- Applying settings to only group of devices

Administrator can configure Group settings by modifying an existing group (Update Group dialog) or by adding a new group (Add Group dialog). Following configurable settings are provided in Group Settings:

**Configurations**

Following settings can be configured in Configurations screen of Group dialog:

- **Group Name**: Mandatory Field, logical name for the new group
- **Description**: Optional, logical description for group
- **Volume**: Default value 'Inherit'
  - Inherit (Inherit from Default Settings)
  - Set Manually
- **USB Redirection Driver**: Default Value 'Inherit'
  - Inherit
  - Set Manually
    - None
    - Built-In
    - Enhanced
- **Default Language**: by default, Native is selected or administrator can select a specific default language for the group.

**Login Settings**

Following Login Settings can be configured from Add/Update Group dialog to enable/disable automatic login on devices.

Devices belonging to the group and inheriting the Group Setting will be rebooted to take effect of configured Auto Login settings.

- Inherit: Default value
- Enable:
  - Ask Credentials as first logon
  - Windows Login
  - Set Credentials
    - Username
    - Password
UI Controls

UI Controls screen in Add/ Update group dialog enables administrator to customize the device login screen by showing/ hiding/ password protecting UI controls.

Devices belonging to the group and inheriting the Group Setting will take new configuration on next heartbeat. Following configurations are available:

- **UI Control Source:**
  - Inherit
  - Set Manually
    - Show/ Hide Controls
      - **Shutdown** Button
      - **Settings** Button
      - **Info** Button
      - **Network Settings** tab in **Settings** window
      - **Accops** Logo
      - **Remember Me** checkbox
    - Password Protect Controls
      - **Shutdown** Button
      - **Settings** Button
      - **Mode Change**
      - **Password** and **Confirm Password** textbox

Desktop Mode

Desktop mode configurations in Group Settings, determines the desktop mode in which devices belonging to this group will be running.

By default, groups inherit the desktop mode settings from Default settings, but administrator can alter the configurations as per group requirements.

Devices belonging to group and inheriting Desktop mode settings will be rebooted to take effect of new Desktop Mode configurations.

- HY1000 – Inherit (Default value), KIOSK, Desktop
- HY2000 - Inherit (Default Value), KIOSK, Desktop
- HY3000 - Inherit (Default Value), KIOSK, Desktop
- HY3020 - Inherit (Default Value), KIOSK, Desktop
- HY4000 - Inherit (Default Value), KIOSK, Desktop
- macOS Client - Inherit (Default Value), KIOSK, Desktop
- Linux Client - Inherit (Default Value), KIOSK, Desktop
- Windows Client - Inherit (Default Value), KIOSK, Desktop

Upgrade Settings

Upgrade Settings are used to enable automatic upgrade of HyWorks Client hotfixes.

Devices inheriting Upgrade Settings from Group Settings will be affected. Following configurations are possible for Upgrade Settings in Add/ Update Group dialog:

- Inherit (Default Selected) – Inheriting the upgrade settings from default settings which means Default Settings will determine the effecting upgrade settings
- Enable – Upgrade will be enabled for all devices belonging to this group
- Disable – Upgrade will be disabled for all devices belonging to this group

❖ Power Saving Mode

If administrator requires to configure power saving mode for a specific group of devices, the objective can be achieved from Group Settings dialog – Power Saving Mode screen. Administrator has following options:

- Inherit the settings from Default Settings: Use the Power Saving Mode settings as configured in Default Settings
- Set Manually
  - Enable and Configure the Turn-Off time out in Minutes
  - Disable: Devices will not get turned off

Updating the Power Saving Mode configurations in Group Settings will affect the following devices:

- Devices going to be inserted into the group
- Devices currently member of this group and inheriting the Power Saving Mode settings from Group Settings

Windows Client devices will not be affected by the Power Saving Mode settings.

This section now concludes the Devices screen which can be used to add registered devices in group. Now brief details of available configurations in Add/ Update group dialog have been given. Refer section Group Management for more details of Group operations and their impact on devices.

❖ Advanced Settings

Advance Settings screen consists of Remote Session settings for the devices. By default, groups inherit the Default settings however administrator can always alter these configurations as per group requirements. Following configurations are possible:

- Remote Session:
  - Inherit
  - Set Manually
    - Remote Shell
    - Remote Control

❖ Devices

Device screen in Add/ Update Group dialog provides the following options to administrator:

- **Add**: To add Devices into this group
- **Remove**: Remove already added devices
- **Search**: To search any already added Devices
- **Refresh**: To refresh the list of already added Devices

✱ Add Devices to Group

For adding devices to group:

1. Click on Add button. This will invoke Available Device Dialog.
2. Displays list of all registered devices in HyWorks Controller (except devices which are already added in this pool).

In Available Devices dialog, administrator has the following options
• **Refresh** the list of Devices to get a fresh list of Devices registered with HyWorks Controller
• **Search:** Any specific Device
• **Select Single, Multiple or Select All** devices using respective checkboxes

3. In Available Devices dialog, select all required devices and click on **OK** button to add them in group.
   Administrator will be navigated back to Device screen in Add/ Update Group dialog, displaying all selected devices as added.

#### Remove Devices from Group
To remove added Devices from group, select the devices from Devices screen and click on **Remove** button. Selected devices will be removed from devices screen and will be available in Available devices list now.

**Note:**
- Devices removed from any group will become member for Default group of that organization
- Devices cannot be removed from Default group of specific organizations
- Default group of any organization cannot be deleted

#### Refresh List of Added Devices
To refresh already added devices in Devices screen, click on **Refresh** button.

#### Search Any Device in Added Devices list
For searching any specific device(s) in added devices list, enter any appropriate search text in Search text box and press Enter key or click on **Search** icon displayed.
The devices matching the search criteria will now be highlighted and be displayed first.

### Device Settings

'Device Settings' enables administrators to apply specific Device Settings to existing devices individually. Device Settings is the third layer of device configurations and has the highest priority and thus can be used to overwrite Default Settings or Group Settings, if need to be.

To open Device Settings dialog, select a registered device and then click on button **Device Settings**. Only one device can be edited at a time; selecting multiple devices will make the setting disabled in the Action toolbar.

Device Settings dialog provides following options to the Administrator:
- **Configurations**
  - Device Name
  - Group Name
  - Volume
  - USB Redirection Driver
  - Desktop Mode
  - Default Language
  - Connection Profile
  - Software Version (Information Only)
• Login
  o Auto Login Dropdown
    ▪ Inherit
    ▪ Enable
    ▪ Disable
    • Ask Credentials at first logon
    • Set Credentials
    • Windows Login

• Display Settings
  o Configure resolution and refresh rate on connected monitors on device
  o Multimonitor configurations
  o Change Primary Monitor
  o Change Multimonitor Mode

• UI Controls
  o Display or Hide UI Controls on HyWorks Client Login Screen E.g. Show/ hide Shutdown, Settings, Info, Accops Logo, Network Settings button
  o Password Protect UI Controls and specify the password e.g. password protect Shutdown, Settings, Mode change button

• Upgrade Settings
  o Inherit
  o Enable
  o Disable

• Advance Settings
  o Session Shell
  o Session Control

• Custom Links

❖ Configurations
Following settings are available in Configurations section of Device Settings:

🔍 Device Name
Renaming the devices can help a lot in HyWorks Management and thus the same option is provided in Device Settings dialog.

To change name of the device:
1. Select the device and click on Device Settings button
2. In Device Settings dialog, go to Configurations section
3. Type appropriate name for the device
4. Click on Save button to save Device Settings
5. Device name will be changed and will start reflecting all relevant sections where the selected device is configured e.g. Endpoints tab, Sessions tab, Desktops VMs tab etc.

💡 Group Name
Displays the name of the group to which this device belongs. The group cannot be changed from Device Settings dialog.
**Volume**

A device can be configured to use specific volume settings. By default, Volume is configured as Inherit in Device Settings which means all devices will use volume settings from Group Settings. Volume configurations in Device Settings could be used for overwriting the Group or Default Settings configuration.

**To change the volume setting of a specific device:**

1. Select the device and click on **Device Settings** button
2. In Device Settings dialog, go to Configurations section
3. Select appropriate Volume settings
   a. **Inherit**: Use the volume settings as configured in Group Settings
   b. **User's Settings**: Let the device use its settings and do not force settings from HyWorks Controller
   c. **Set Manually**: Specify Volume manually for the device. Set the volume slider to desired level
4. Click on **Save** button to save Device Settings
   a. Device volume will be changed as per configured settings in next successful heartbeat

**Note:**

- Any difference between the Device Settings and current user settings will be represented by exclamation mark with red color on device page.
- Windows Clients (HyWorks Clients running on Windows Desktops) does not support volume changes from HyWorks Controller to keep user's settings intact. Thus, while modifying the Device Settings of a Windows Client all such inapplicable settings are disabled. The behavior of disabling inapplicable settings is termed as **Model based behavior** and will be explained in detail in later section of the Admin guide.

**USB Redirection Driver**

USB Redirection Driver option in Device Settings dialog provides opportunity to administrator to enable specific USB Redirection Driver configuration for the specific device. USB Redirection Driver configuration is set to Inherit to use the USB Redirection Driver configurations from Group Settings, but Device Settings provides the option to overwrite USB Redirection Driver settings.

**To change the USB Redirection Driver setting of a specific device:**

1. Select the device and click on **Device Settings** button
2. In **Device Settings** dialog, go to **Configurations** section
3. In **USB Redirection Driver** dropdown list
   a. Select **Inherit** to use USB Redirection Drivers configurations from **Group** Settings
   b. Select ‘Set Manually’ and specify the USB Redirection driver to be used by the device
      i. Built-In (Recommended for dedicated VDI deployments)
      ii. Enhanced (Recommended for shared VDI deployments)
4. Click on **Save** button to save Device Settings
5. If any change in USB Redirection Driver (currently used by device) is detected, device reboot will be required, and a Confirm Action dialog will be prompted
6. Click on **Save** button to confirm the action
7. Device will be rebooted and will start using new USB Redirection Driver configurations after restart

**Note:**
- Supported USB Redirection Driver list is populated as per installed USB Redirection Drivers on the device e.g. Linux Client does not support Enhanced USB Redirection Driver and thus when using Linux Client, Redirection Driver dropdown will not display the Enhanced option
- USB Redirection Driver settings changes require device reboot and thus any active session will be disconnected, and device will be rebooted
- As mentioned in Default Settings - USB Redirection Driver section, on Windows machines, system restart will not be required, and HyWorks Client application will be closed and reopened to use new USB Redirection Driver settings

Please read 'USB Redirection in HyWorks' manuals for detailed information on USB Redirection.

**Default Language**
Default language option can be used to set the default language for the device and to provide language choices to the user on the HyWorks Client login screen.
The default value is always native using the native (EN-US) language of the device until another language is specified on HyWorks Controller.
In Default Language option administrator will be able to configure the following language configurations:
- Add More Languages
- Remove Added Languages
- Select Default Language

- **Add More Languages**
  Adding multiple languages for the device provides end user options to select language of their choice. To add multiple languages for the device, in Device Settings dialog - Configuration screen:
  1. Click on **Add More Languages** button.
  2. On **Select More Languages** dialog, select multiple languages using ctrl + mouse click or shift + mouse click operations.
  3. Click on **Right** arrow button
  4. Click on **Add** button
  5. All the selected languages will then appear on the **Selected Languages** drop down list
  6. Click on **Save** button to save the Device Settings
  7. Default Language changes in Device Settings require device reboot and thus Confirm Action dialog will be displayed with checkbox **Reboot the device now. Connected user will be disconnected**.
     a. Enabling this option will reboot the device immediately and language changes will be applied
     b. Keeping this option as unchecked will not reboot the device and changes will be applied on next device reboot
  8. Rebooting the device will enable the Keyboard control on login screen with all above language changes available.
• Removing Languages
Administrators can also remove additional languages by selecting the languages from language list on right side.

1. Click on Left arrow button.
2. Click on Add button.
3. Default Language changes in Device Settings require device reboot and thus Confirm Action dialog will be displayed with checkbox **Reboot the device now.**
   - Enabling this option will reboot the device immediately and language changes will be applied
   - Keeping this option will not reboot the device and changes will be applied on next device reboot
4. All the selected languages will be removed from Default Language drop down list.
5. Rebooting the device will enable the Keyboard control on login screen with all above language changes available.

**Note:**
➢ Administrator will not be able to remove the Default Language using above steps.

• Selecting Default Language for Device
Administrator can specify a default language for any specific device, but user will always have option to change the keyboard layout based on the provided options.

1. Selecting any language from Default Language drop down will make that language default language for the device.
2. Default Language changes in Device Settings require device reboot and thus Confirm Action dialog will be displayed with checkbox **Reboot the device now.**
   - Enabling this option will reboot the device immediately and language changes will be applied
   - Keeping this option will not reboot the device and changes will be applied on next device reboot
3. In case of no other language is selected by the user during login, the default language specified in Device Settings should be used.

**Connection Profile**
Device Settings - > Configurations - > Connection Profile dropdown option can be used to specify connection profile for the selected device.

Connection profiles are used to configure user experience options in the Desktop sessions and can be created from HyWorks Controller Management Console - > Setup - > Connection Profile section.

**To configure a new connection profile:**
1. Select the device and click on **Device Settings** button
2. In **Device Settings** dialog, go to **Configurations** section
3. In **Connection Profile** dropdown list, select the option **Set Manually** (Default configuration is Inherit -> Which means devices will use the connection profile as defined in Device group)
4. Select the desired connection profile from Connection Profile dropdown list
5. Click on **Save** button to save Device Settings
6. New Connection profile will be configured on the device and will be used in the very next session

Connection profile can directly be configured using **Assign Profile** dialog. See section **Assign Connection Profile** for more details.

Use link 'View Profile Details' to directly open the details of selected profile.

Please see Setup - Connection Profile section for more details on Connection Profiles and its attributes.

**Note:**
- The connection profile changes do not get applied on the currently running sessions.

**Software Version**

This field will be used to display the current client version of the device. In case of any difference between the current version and available software version on HyWorks Controller, an **alert** icon (exclamation sign with red/orange color) will appear, representing out of sync client version.

The alert can be used to change the device settings to enable/disable the Auto Update Client settings.

**Login**

Auto Login settings in Device Settings can be used to configure specific auto login settings on the selected device. Following configurations are possible:

- **Inherit**: The default Auto Login configuration in Device Settings. Specifying the device to inherit the login setting from Group Settings and thus device will use Auto Login settings as configured in Group Settings e.g. if Auto Login in Default Settings is configured as Windows Login and if Device Settings – Auto Login is set as Inherit then it will get Auto Login configuration as Windows Login.

  Image displayed next to Auto login checkbox reflects the status of Auto Login configurations in Default Settings
  - A Cross sign [X] reflects that Auto Login is disabled in Group Settings
  - A Tick sign ☑ reflects that Auto login is enabled in Group Settings.

- **Enable**: Selecting Auto Login as Enable in Device Settings will enable the automatic login on selected device irrespective of Default Settings configurations. Once Auto Login is set to Enable one of the following configurations needs to be selected:
  - **Set Credentials**
    Devices will be automatically connected to configured Desktops using the credentials set by Administrator in Default Settings/ Device Settings
  - **Ask Credentials at first Logon**
On first login users will be displayed with default login screen and on successful logon, the provided credentials will be cached. Same credentials will be used for automatic connection to the configured Desktops from next device reboot.

- **Windows Login**
  Configured Desktops will be connected on the devices without any credentials and users will be needed to provide credentials in the remote session.

**Note:**
- Windows login do not work with NLA (Network Level Authentication) enabled on devices.

- **Disable:** Specifies that selected device will not use automatic login settings and thus manual login will be enabled on device.

❖ **Enable Auto Login Configurations from Device Settings**

1. Go to Endpoints page – Select a device – Click on *Device Settings* button to open Device Settings dialog
2. Go to Login Settings section
3. Select the Auto Login checkbox to enable the auto login setting
   a. Choose desired auto login configurations
     i. Ask Credentials at First Logon
     ii. Windows Login
     iii. Set Credentials
       1. Provide appropriate credentials
4. Click on *Save* button to save the Default Settings
5. On Confirm Action Dialog
   a. Select checkbox ‘Reboot the device now. Connected user will be disconnected.’ to immediately reboot and configure auto login settings and click on *Save* button
   b. Keep checkbox ‘Reboot the device now. Connected user will be disconnected.’ unselected and click on *Save* button to save the settings on the device. Auto Login settings will then start functioning in next device reboot.

❖ **Display**

Device Settings are the primary control layer for Display configurations on the device and it does not take configurations from the Default or Group settings.

❖ **How Does It Work?**

Devices once connected with HyWorks Controller share their monitor and available display settings as per provided details HyWorks Controller enables appropriate display options for the selected device. E.g. if selected device is having only single monitor then HyWorks Controller will provide options to configure resolution and refresh rate options for single monitor and if device is having monitors, HyWorks Controller will provider options for both the monitors, selecting primary monitor etc.

❖ **Display Configurations**
• **With Single Monitor**

When connected device is having only single monitor connected then it allows administrator to configure following display settings:

- **Resolution**: Default value is Native and dropdown list will have options as shared by device
- **Refresh Rate**: Default value is Native and dropdown list will have options as shared by device

To change any off the above two settings, select appropriate values from the respective dropdown lists and click on **Save** button.

Device Settings will be saved and from next heartbeat device will start using new display settings.

• **With Multiple Monitors**

If connected device is having multiple monitors plugged in, then following display settings are enabled in Device Settings – Display section:

- **Display Mode Configurations**: Following display modes are available:
  - Native (Referred as default configuration for newly registered device)
  - Single Display (Multiple Monitors connected but specifying to use only one display)
  - Multiple Display (Known as True Multimonitor as well: This mode supports displaying different applications in different monitors)
  - Duplicate Display (In this mode both monitors display same data)
  - Extended Display (Known as Spanning as well: This mode extends the display on both monitors)
  - Vertical Multiple Display (Vertical version of Multiple Display, different applications can be displayed in different monitors)

- **Configure Primary Display**: Configuring which one of the two monitors will function as the primary monitor

- **Screen Resolution** and **Refresh Rate** settings for connected displays

❖ **Configuring Display Settings in Device Settings**

1. Select device – Click on **Device Settings** button to open Device Settings -> Go to Display tab
2. Observe available options (if settings are as per single monitors or multiple)
3. Configure appropriate display settings:
   a. Display Mode as per requirement
   b. Change resolution and refresh rate of connected monitors
   c. Specify primary monitor settings (if needed)
4. Click on **Save** button to save the settings
5. Logoff any running session and wait for settings to get applied (Default is 40 seconds)
6. Re-logon using appropriate credentials
7. New session should be displayed as per configured display settings.

**Note:**
- Display settings do not affect any running sessions on the device and thus also gets applied only when the session is disconnected
- With Auto Login settings enabled, devices require reboot to apply display settings
➢ Display settings will not have any impact on Windows clients as per assumption that the user must be running with best display configurations of its choice.

For details on Multimonitor configurations, please refer HyWorks Multimonitor Configuration Guide.

❖ UI Controls
UI Control section in Device Settings provide UI customization of HyWorks Client Login screen for a specific device which means administrator will be able to enable or disable various controls on HyWorks Client Login screen.

UI Controls in Device Settings is secondary layer which can be used to overwrite the Default Settings – UI Controls configurations.

Following settings are possible in Device Settings – UI Controls:

- **Inherit:** To inherit UI Controls configurations from Default Settings and thus effective UI will be customized as per Default Settings – UI Controls configurations.

- **Set Manually:** Specifying UI Control settings and thus over writing the Default Settings. Following settings will get enabled once UI Controls Source is selected as ‘Set Manually’
  - Show/Hide Controls
  - Password Protect Controls

❖ Show/Hide UI Controls
To show a UI Control,

1. Select the checkbox displayed against desired UI Control in UI Controls section of Device Settings and to hide it uncheck the checkbox.
2. Click on Save button to save the Device Settings
3. Selected device will start showing or hiding respective UI Controls on HyWorks Client login screen

- **UI Controls Which can be shown or hidden:**
  - Information Button
  - Shutdown Button
  - Settings Button
  - Network Settings tab in Settings window
  - Accops Logo
  - Remember Me
  - Virtual Driver
  - USB Driver

❖ Password Protect UI Controls
To make any UI Control password protected,

1. Go to UI Controls section in Device Settings dialog
2. Select UI Controls Source dropdown as Set Manually
3. Select the checkbox displayed against desired UI Control to make it password protected
   uncheck the checkbox to keep it unprotected
4. Provide appropriate password if making any UI Control Password protected
5. Click on Save button to save Device Settings
6. The selected device will now start using Password Protection settings
7. If UI Controls are made password protect, accessing those control will start prompting for password and will be accessible only on providing correct password
8. UI Controls which are not made password protected will be accessible without any password

• UI Controls Which can be Password Protected
  o Shutdown Button
  o Settings Button
  o Mode Change (Desktop Mode Change from HyWorks Client Login screen using secret key combination
  o Virtual Keyboard
  o USB Driver

Note:
➢ UI Controls settings in Default Settings are primary layer of UI Control configurations and can be overwritten from Device Settings of specific device. Please check Device Settings section for more details.
❖ Upgrade Settings
Using Auto Update Client option in Upgrade Settings screen in Device Settings dialog, administrator can overwrite the auto update settings specified in the Default Settings.
Auto update client option in Device Settings is set as Inherit by default to use Auto Update Client settings from Group Settings.
Once Auto Update Client is enabled then devices will be downloading latest hotfixes from HyWorks Controller and will get upgraded to latest version and vice versa if Auto update client is disabled the devices will not download the update patches from HyWorks Controller.

To change Auto Update Client configurations for a specific device:
1. Select the device and click on Device Settings button
2. In Device Settings dialog, go to Configurations section
3. In Auto Update Client dropdown list select appropriate option. The following three viable options can be set for a device from Device Settings dialogs:
   a. Inherit: Set the device to be updated as per Group Settings.
   b. Enable: Update the specific device, irrespective of Group Settings.
   c. Disable: Do not update the specific device, irrespective of Group Settings.
4. As per configured option, selected device will be set for upgrade

Important to know that current Auto Update Client configuration in Default Settings is displayed next to Auto Update Client dropdown in Device Settings to help appropriate settings.
• A cross sign [x] represents Auto Update Client is disabled in Default Settings.
• A tick sign [✓] represents Auto Update Client is enabled in Default Settings.
**Note:**
- Devices with running session may initiate upgrade patch download from HyWorks Controller (if Auto Update Client is enabled) but will only be upgraded when the session is not running.
- Upgrade patch installation on device may take some (Appropriate message will be prompted on the device during the operation) and requires device reboot.

In the later section of the document, more information and conceptual details of device upgrade will be provided.

❖ **Power Saving Mode**

Power Saving Mode section in Device Settings dialog provides administrator to set specific settings for a device and over-writing Power Saving Mode configurations pushed by Group Settings or Default Settings.

Following configurations are possible:
- Inherit: Use the settings being configured in the group this device belongs to
- Set Manually
  - Enable (Select the checkbox *Power Saving Mode*) and specify Device Turn-off timeout
  - Disable (Disable the Power Saving Mode) feature for the specific device

❖ **Advanced Settings**

Advanced settings in Device Settings provide options to reconfigure Remote Session settings on devices. Administrator can configure following configurations in Advanced Settings of the device:

- **Session Shell:** It allows administrator to enable/disable the SSH on the devices and thus applied to HY2000, HY3000, HY4000 and Linux Clients only. Once enabled administrator will be able to *SSH* to specific device with root credentials and default password (Contact Accops Support for default password).
- **Session Control:** It allows administrator to enable/ disable VNC on the devices and thus applies to HY2000, HY3000, HY4000 and HyWorks Client on Accops OS only, HyWorks Client installed on Ubuntu OS i.e. Linux Client will require manual installation of VNC servers on system to make this option work.

To enable or disable above two configurations, administrator must select appropriate option from Remote Session dropdown list:

1. **Remote Session:** Dropdown list to select the source of the Remote Session settings on device. Select appropriate option from following possible configurations:
   - User Setting: Means current user settings will remain configured. User can configure these settings from HyWorks Client Login Screen – Settings – Diagnostic tab. If User Setting is selected, then it also displays the current configured settings with controls disabled.
   - Inherit: Inherit remote session configurations from Default Settings. If Inherit is selected, then screen will display current Advanced Settings configurations in Default Settings with controls disabled.
   - Set Manually: Manually specifying remote session settings. If configured as 'Set Manually' then administrator can configure Session Shell and Session Control settings as per need.
2. Click on **Save** button to save device settings
3. Remote session configurations will be enabled or disabled as per provided configurations.

**Device Group Management**

With no device selected, Device tab displays button **Group Management**, which invokes Group Management dialog to enable administrator to manage device groups:

To open Group Management dialog:

1. Go to **Endpoints tab** in HyWorks Controller Management Console
2. Click on button **Group Management**
3. Group Management dialog will be displayed, enabling administrator to perform following operations
   a. Create a new group
   b. Update existing groups
   c. Delete existing group

Let us try to understand the impact of group management operations before performing any.

❖ **Impact of Group Management on Devices**

All group management operation (i.e. add group, update group, delete group, and move devices to group) affects the devices belonging to the group or being moved to the group and these configuration changes may cause configuration changes on devices and may require and cause device reboot.

Let us try to understand the above things by example:

➢ Administrator adds a new group, with following configurations
   1. USB Redirection Driver now set to None
   2. Added 5 devices

   **Impact:** As by default devices belong to group ‘Default Group’ with USB Redirection Driver as Inherit (= Built-In) and now this device is being move to new group with USB Redirection Driver as None, it will be rebooted and then will take effect of USB Redirection Driver settings.

➢ Administrator updates an existing group, with following configurations:
   1. Login settings changed from Inherit to Enable – Windows Login
   2. Group consists of 2 devices

   **Impact:** All 2 devices will be rebooted and will start using automatic login settings as Windows Login

➢ Administrator deletes a group, which has following configurations:
   1. Login Settings as Enabled – Windows Login
   2. USB Redirection Driver as – None
   3. Advanced Settings as Set Manually with both Remote Shell and Remote Control enabled
   4. Group has 3 devices

   **Impact:** Whenever a group is deleted, all devices belong to the group will be moved to default group and thus there will following configuration changes, which will require and cause device reboot:
   1. Previous Login Settings Enabled – New Login Settings Inherit from Default (=Disabled)
   2. Previous USB Redirection Driver Settings None, new USB Redirection Driver Settings Inherit = Built-In
3. Previous Advanced – Remote Session setting enabled, and new Remote Session settings disabled

Now due to the configuration changes of point (a) and (b), devices will require and cause reboot whereas configuration changes of point c will cause all remote shell and VNC session on devices to be disconnected.

Now we understand how group management operations can affect device configurations, let us learn how to perform group management operations in below section.

❖ **Group Management Operations**

Following device group management options are available in HyWorks:

❖ **Create a New Group**

Follow the below steps to create new groups:

1. In HyWorks Controller Management Console go to **Endpoints tab**
2. Click on **Group Management** button
3. In Group Management dialog, click on **Add** button
4. In Add Group dialog, modify the settings as per requirements
   a. Configurations
      i. Group Name and Description
      ii. Volume: Inherit or Set Manually
      iii. USB Redirection Driver: Inherit or Set Manually as None, Built-In or Enhanced
      iv. Default Language: As per requirement
   b. Login: Inherit, Disable or Enable with Set Credentials, Ask Credentials at first logon or Windows Login
   c. UI Controls: Show, Hide or Password Protect UI Controls
   d. Desktop Mode: As Inherit, Desktop or KIOSK
   e. Upgrade Settings: Inherit, Enable or Disable
   f. Advanced Settings: Inherit, Users Settings or Set Manually
   g. Devices: Add devices to group
5. Administrator can select checkbox **Add more groups** before saving the group if willing to create more groups
6. Once all the configurations using different screens of Add Group dialog are completed, click on **Save** button
7. Confirm Action dialog box will be displayed stating devices being moved to this group may reboot due to configuration changes
8. Click on **Save** button on Confirm Action dialog to continue saving the group
9. New group will be created, and appropriate status message will be displayed, and administrator will be navigated back to respective page as per selection of checkbox **Add more groups**
   a. Devices screen if **Add more groups** checkbox was not selected
   b. Group Management dialog if **Add more groups** checkbox was not selected
10. Devices being moved to this new group will be configured as per new group settings, the new configurations may cause device reboot as well as explained in section **Impact of Group Management Operations**

❖ **Update Existing Group**

Follow the below steps to update settings of an existing group:
1. In HyWorks Controller Management Console go to **Endpoints tab**
2. Click on **Group Management** button
3. In Group Management dialog, click on Edit button displayed against any existing group
4. Update group dialog will be displayed
5. In Update Group dialog, modify the configurations as per requirement
6. Administrator can select checkbox **Update more groups** before saving the group if willing to update more groups
7. Click on **Update** button
8. Confirm **Action** dialog will be displayed, stating devices belonging to this group will be affected and may require and cause device reboot.
9. Click on **Update** button on **Confirm Action** dialog to continue saving the group
10. New group will be created, and appropriate status message will be displayed, and administrator will be navigated back to respective page as per selection of checkbox **Update more groups**
   i. Devices screen if **Update more groups** checkbox was not selected
   ii. Group Management dialog if **Update more groups** checkbox was not selected
11. Devices belonging to this group will be configured, the new configurations may cause device reboot as well as explained in section **Impact of Group Management Operations**

### Delete Existing Groups

Administrator can use Group Management dialog to delete existing groups with the following exception for Default group that **Default Group cannot be deleted.**

Follow the below steps to delete an existing, manually created device group:

1. In HyWorks Controller Management Console go to **Endpoints tab**
2. Click on **Group Management** button
3. In Group Management dialog, click on Delete button displayed against any existing group
4. Confirm Action dialog will be displayed, stating that devices belonging to this group will be moved to Default Group and may cause devices to reboot
5. Click on **Delete** button on **Confirm Action** dialog to continue deleting the group
6. Group will be deleted; appropriate status message will be displayed, and administrator will be navigated back to Group Management dialog
7. Devices belonging to deleted group will be moved to default group and will start using default group settings and may require and cause device reboot for new configurations to take effect.

### Operations on Endpoints

Apart from changing the devices configurations using Devices Settings (for individual devices), Group Settings (for group of devices) or Default Settings (for all or new registered device), administrator can perform various other tasks on the devices by selecting one or multiple devices and selecting appropriate action from Actions tool bar. The Action toolbar provides the following options to administrator:

- Assign Connection Profile to single or multiple devices
- Enable or Disable single or multiple devices
- Device Logs (Viewing, Collecting or Deleting) for single device
- Deleting single or multiple devices
- Device Power Operations
  - Power On
Let us walk through each of these actions on devices in details:

❖ **Move to Group**

To move one or multiple devices to a specific group follow the below steps:

1. In HyWorks Controller Management Console – **Endpoints tab**
2. Select one or multiple devices
3. Click on button **Move to Group**
4. **Please select group** dialog will be displayed, consists of all available groups with option to select only one group at a time
5. Select the desired group and click on button **Move**
6. Confirm Action dialog will be displayed, stating that devices being moved to the group may require reboot - Click on Move button to continue with operation
7. Appropriate status message will be displayed; selected devices will be moved to the selected group and will get configured as per new group settings.

**Note:**

➢ Please note **Move to Group** operation may cause devices to reboot due to the configuration changes between current settings and new groups settings. Refer section **Impact of Group Management Operations** for more details.

❖ **Assign Connection Profile**

Administrator can assign a connection profile to one or more registered devices using **Assign Profile** option.

To assign a connection profile:

1. Select one or more devices and click on **Assign Profile** button in the **Action** toolbar.
2. In Assign Connection Profile dialog select the profile and click on **Assign** button to save the settings.
3. All selected devices will be assigned with new connection profile and will start using the new connection attribute from the next session.

**Note:**

➢ Assigning a new connection profile does not affect the currently running sessions and comes into effect only for the new connections only.

❖ **Enable / Disable Device**

Administrator can enable or disable one or multiple registered devices by clicking on **Enable/Disable** button on the **Action** toolbar.

Depending on the selected device's status the Enable or **Disable** button will be displayed. In case of multiple selections, the button will appear as per the first selected device e.g.

- **Single Selection**
  - Selected single device with enabled state - **Disable** button will be displayed
Selected single device with disabled state - **Enable** button will be displayed

- **Multiple Selection**
  - Multiple devices selected with different states but first device in enabled state - **Disable** button will be displayed
  - Multiple devices selected with different states but first device in disabled state - **Enable** button will be displayed

**Impact of disabling device(s):**
- The selected device(s) will be disabled, and user will also be notified that **Administrator has disabled your device**.
- Any desktop sessions are running, then the desktop sessions will be closed, and user will be notified that **Administrator has disabled your device**.
- User will not able to login from the device anymore.

**Device Logs**
For troubleshooting purpose or simple monitoring of device activities, administrator can view, refresh, download or delete device logs.
Device logs operation can be done only on single and reachable device only, selecting multiple devices will prompt appropriate error and selecting an unreachable device will display error in device logs page.

Once device logs are enabled HyWorks Controller will send the request to selected device -> Device will upload the first chunk of device logs after first successful heartbeat.

**View/ Download Device Logs**
To **view device logs**, administrator will be needed to perform the following steps:
1. Select the registered device from Device tab
2. Click on **Logs** button as shown in below image
3. Wait for 1 heartbeat to be exchanged between controller and device, it can take from 40-120 seconds for logs to be retrieved
4. The device logs will start appearing on the same window as shown in Device Logs window also only latest 1000 lines of device logs are displayed only.
5. To **update or refresh** the available logs, administrator will be needed to click on the Refresh Device **Logs** button explicitly as devices logs do not get refreshed automatically.
6. To download the logs to a txt file, click on the **Download Logs** button
7. As mentioned earlier also once device log window is opened devices will send the first chunk of logs to HyWorks Controller. HyWorks Controller will keep the logs file in the following directory with the name of device registration id:
   **Device Logs Path:**
   
   < C:\Program Files (x86)\Accops\HyWorks Controller\Service\Contents\DeviceLogs>

Every time the device logs are refreshed then the device logs will be updated in the respective folder.

However, if administrator chooses to not to keep device logs, device logs can be **deleted** using **Delete Logs** button. All the logs being saved on HyWorks Controller till time will be deleted and fresh logs request will be sent to device.
Note:
➢ Delete Logs operation will delete the entire directory created under Device Logs folder for the selected device.

Disabling/ Stopping Device Logs
The device logs will stop coming to the Device Logs settings as soon as administrator closes the Device Logs Settings dialog, however the old logs which are already downloaded, will re-appear on the Device logs windows on re-opening the Device logs window for the same registered device.

Delete Device
Administrator can delete one or multiple registered devices by selecting the option Delete from Action dropdown list or Delete button on the Action toolbar.

Impact of deleting device(s):
1. Any running session will be closed, and the selected device(s) will be deleted from the management console
2. All corresponding data of deleted device will also get deleted which includes running session information, Desktop assignments, Profile assignment and configuration changes
3. If the device is powered on it will get re-registered as a fresh device with all previous settings reset.
4. If the device is in disconnected state and not reachable then device will not appear on management console again.

Device Power Operations
HyWorks Controller Management Console - Endpoints page provides the options to perform power operations on the selected devices also. Following are the possible power operations on the devices:

1. Power On: If the selected device is in powered off state, selecting the device and clicking on 'Action Toolbar - More - Power On' option will turn on the device

Note:
➢ Power on operation is supported only for following models, that too with specific BIOS version.
   o HY3000
   o HY4000

2. Shutdown: If the selected device is in powered on state, selecting the device and clicking on 'Action Toolbar – More dropdown - Shutdown' button will shut down the device (running session will be closed)

Note:
➢ Windows Client machines do not support remote power operations thus reboot, power on or shutdown operation won’t work on them though initiating the action on client will not be prohibited on HyWorks Controller Management Console and will also change its status in management console, won’t have any impact on devices.
3. **Reboot**: If the selected device is in powered on state, selecting the device and clicking on ‘Action Toolbar – *More* dropdown- *Reboot’ button will reboot the device (running session will be closed)

**Applicable Settings on first Time Registration**

The table below specifies the available configuration on newly registered devices on a fresh HyWorks Controller which means all configurations in Default Settings and individual Device Settings are kept as default.

<table>
<thead>
<tr>
<th>Configuration Attribute</th>
<th>Default Settings</th>
<th>Group Settings</th>
<th>Device Settings</th>
<th>Implemented Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Screen Resolution</strong></td>
<td>Native (Not Used)</td>
<td>NA</td>
<td>Native (Best Resolution on Device side)</td>
<td>Native</td>
</tr>
<tr>
<td><strong>Volume</strong></td>
<td>100</td>
<td>Inherit</td>
<td>Inherit</td>
<td>100</td>
</tr>
<tr>
<td><strong>USB Redirection Driver</strong></td>
<td>Built-In</td>
<td>Inherit</td>
<td>Inherit</td>
<td>Built-In (Inherited)</td>
</tr>
<tr>
<td><strong>Language</strong></td>
<td>Native</td>
<td>Inherit</td>
<td>Native</td>
<td>Native (En-US)</td>
</tr>
<tr>
<td><strong>Banner Image</strong></td>
<td>Default</td>
<td>NA</td>
<td>NA</td>
<td>Default</td>
</tr>
<tr>
<td><strong>Connection Profile</strong></td>
<td>Default</td>
<td>Inherit</td>
<td>Inherit</td>
<td>Default Profile</td>
</tr>
<tr>
<td><strong>Auto Update Client</strong></td>
<td>Disabled</td>
<td>Inherit</td>
<td>Inherit</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Login Settings (Auto Login)</strong></td>
<td>Disabled</td>
<td>Inherit</td>
<td>Inherit</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>UI Controls</strong></td>
<td>Show: All except <em>Remember Me</em> Password Protect: None</td>
<td>Inherit</td>
<td>Inherit</td>
<td>Show: All except <em>Remember Me</em> Password Protect: None</td>
</tr>
<tr>
<td><strong>Desktop Mode</strong></td>
<td>HY2000 - KIOSK</td>
<td>Inherit</td>
<td>Inherit</td>
<td>KIOSK</td>
</tr>
<tr>
<td></td>
<td>HY3000 - KIOSK</td>
<td>Inherit</td>
<td>Inherit</td>
<td>KIOSK</td>
</tr>
<tr>
<td></td>
<td>HY3020 - KIOSK</td>
<td>Inherit</td>
<td>Inherit</td>
<td>KIOSK</td>
</tr>
<tr>
<td></td>
<td>HY4000 - KIOSK</td>
<td>Inherit</td>
<td>Inherit</td>
<td>KIOSK</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td>Linux Client - KIOSK</td>
<td>Windows Client - Desktop</td>
<td>Session Shell - Disabled</td>
<td>Remote Control - Disabled</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Inherit</td>
<td>Inherit</td>
<td>Inherit</td>
<td>User Setting</td>
<td>User Setting</td>
</tr>
<tr>
<td>Inherit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KIOSK</td>
<td></td>
<td></td>
<td>As per current user settings</td>
<td>As per current user settings</td>
</tr>
</tbody>
</table>

Configuration changes of all above attributes are already covered in detail in Device Configurations section of this document.

The below section will brief details about what are the configurations available in Default Settings, Group Settings or Device Settings.

**Automatic Upgrades and Endpoint Software Version Management**

All registered endpoints can be centrally managed from HyWorks Controller. This section of document can be used to push automatic upgrades to endpoints from HyWorks Controller.

❖ **Software Version Check and Alerts on Management Console**

HyWorks Controller is having version information files in its installation directory and it matches software version of each client, on finding client software version being lower than version available on server (controller), it starts showing alert for such endpoint.

<Install Directory>\Service\Contents\Firmware\<PlatformId>

- **List of Platform Ids with Model Name**

<table>
<thead>
<tr>
<th>Sr, No.</th>
<th>Endpoint Model</th>
<th>Platform Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Windows Client</td>
<td>EDCMS01WIN000</td>
</tr>
<tr>
<td>2</td>
<td>Windows on-demand Client</td>
<td>EDCMS01WIN100</td>
</tr>
<tr>
<td>3</td>
<td>macOS Client</td>
<td>EDCA00MAC000</td>
</tr>
<tr>
<td>4</td>
<td>Hy1000</td>
<td>EDCDB09ARMHF</td>
</tr>
<tr>
<td>5</td>
<td>Hy2000</td>
<td>ETCC00ARMUBU012</td>
</tr>
<tr>
<td>6</td>
<td>Hy3000 (OS 4.8)</td>
<td>ETCC00XC0480</td>
</tr>
<tr>
<td>7</td>
<td>Hy3000 (OS 6.2)</td>
<td>ETCC00XC0620</td>
</tr>
<tr>
<td>8</td>
<td>Hy4000 (OS 4.8)</td>
<td>ETCC01XC0480</td>
</tr>
<tr>
<td>9</td>
<td>Hy4000 (OS 6.2)</td>
<td>ETCC01XC0620</td>
</tr>
<tr>
<td>10</td>
<td>Ubuntu Client</td>
<td>EDCOS01UBU012</td>
</tr>
</tbody>
</table>

- **Version Info file Contents**
FileName=HyWorksClient_Installer_UPGRADE_HYCLIENT-UBUNTU.7z
Version=321129

Where
- **FileName** is name of upgrade file, kept at following location:
  - `<Install Directory>\Service\Contents\Firmware\Upgrade`
- **Version** is software version of upgrade file, the same is used to compare versions

❖ **Pushing Upgrade from HyWorks Controller**

To push upgrade to specific endpoint model, following steps can be used:

1. Identify Hardware Id of the model or type of devices to be upgraded e.g. Hy4000 (ETCC01XC0620) needs to be upgraded
2. Download latest upgrade patch from Accops website and copy at the following location:
  - `<Install Directory>\Service\Contents\Firmware\Upgrade`
3. Update settings in info.ini file at following location:
  - `<Install Directory>\Service\Contents\Firmware\ETCC01XC0620`
    a. Set FileName= <name of downloaded file> e.g. FileName=HyWorksClient_Installer_UPGRADE_321154_HY3000.7z
    b. Set Version= <version of file> e.g. Version=32154, please see the below screenshot for reference
4. Login into HyWorks Controller Management Console – Endpoints, follow below alternate process to push upgrade to one/ multiple or group of devices:
   a. **Push updates to Specific Device**: To push updates to specific device,
      i. Search and select endpoint from list
      ii. Click on **Device Settings** - Go to **Upgrade Settings** tab
      iii. Set **Auto Update Client** as **Enabled**
      iv. **Save** settings. Controller will share upgrade details and client will download the updates automatically.
   b. **Push updates to all endpoints of same model**: To push updates to all endpoints of same model, upgrade can be enabled from **Default Settings**, with assumption that devices are inheriting upgrade settings from Default.
      i. Consider upgrade file has been copied to respective location and info file has been updated
      ii. Go to Endpoints – Default Settings – Upgrade Settings
      iii. Select checkbox **Auto Update Client**
      iv. Endpoints, which satisfy following conditions will start getting updates:
         1. Inheriting Upgrade Settings from Default
         2. Belong to model for which update files are available and running with lower version than mentioned in info file

❖ **Upgrade File Extensions**

Commonly used upgrade file extensions are:

1. `.tgz` (Old upgrade files for Linux based HyWorks Clients)
2. `.7z` (new upgrade file format for Linux based HyWorks Clients)
3. `.zip` (Windows based HyWorks Clients)
Endpoint Behavior Management using HyWorks Advance Configurations

Advance Config sub-section under System is very critical system level configurations and can be used to tweak endpoint behaviors. Below are some of such configurations, which have been used in different customer environments:

❖ **Change Heartbeat Timeouts for better Controller Performance**

By default, HyWorks Clients send heartbeat to Controller in every 40 seconds, but as number of endpoints increase HyWorks controller may face performance overhead, and following configurations can be used to change default behavior of HyWorks Clients:

1. Go to HyWorks Controller Management Console -> System -> Advanced Config
2. Search for following configuration *Heartbeat Interval*
3. Click on *Edit* button and change the value
4. Click on *Update* to save configurations

Now endpoints will send heartbeats as per new interval. The value must be a number and should not be less than 5 seconds.

❖ **Controlling Endpoints Time and Timezone Settings**

Endpoints of type thinclient e.g. Hy1000, Hy2000, Hy3000, Hy4000, Hy3020 sync times with HyWorks Controller for better management, however if required, behaviour can be managed using following configurations:

- **Stop Controller-HyDesk Date Sync**: If this is set then Controller will stop sending Date to HyDesk on registration, HyDesk devices will not sync date with controller. Default value is false.
- **Enforce time zone**: If controller should specify timezone to be set on endpoints. If this is set to True, then settings *Define/Specify device time zone* must be configured correctly.
- **Define/Specify device time zone**: Based on above configuration, timezone can be specified to set on HyDesk endpoints.

**Note:**

➢ Windows desktop endpoints do not set time related configurations and above configurations are applicable for Linux based or HyDesk endpoints only

❖ **TCP Timeouts for endpoints in indecent network**

Latest v3.2 HyWorks Clients for Linux based platforms such as Hy3000/Hy4000, Ubuntu or Accops OS, have better control and stability in fluctuating networks. The behaviour can be further controlled using Controller provided advanced timeouts for sessions:

- **KeepAlive interval**: Keepalive interval is the duration between two successive keepalive retransmissions, if acknowledgement to the previous keepalive transmission is not received. Value in Second, Default value is 3.
- **KeepAlive count**: Keepalive count is the number of retransmissions to be carried out before declaring that remote end is not available. Value in Second, Default value is 2.
- **KeepAlive idle**: Keepalive Idle is the duration between two keepalive transmissions in idle condition. Value in Second, Default value is 5.
- **TCP user timeout**: The TCP user timeout controls how long transmitted data may remain unacknowledged before a connection is forcefully closed. Value in Second, Default value is 9.
Licensing in HyWorks

License Management section in System section is used for managing the licenses on HyWorks Controller.

Accops License service by default gets installed with HyWorks Controller setup and responsible for managing the licensing.

License Types

HyWorks Controller currently supports following types of licenses:

- **Based on License Duration**
  - Default
  - Evaluation
  - Perpetual

- **Based on Licensing Attribute**
  - Concurrent Session Based Licenses
  - Number of Registered Devices
  - Named user Licensing

**Based on License Duration**

- **Default License**: The license of 30 days for 10 devices is provided by default with HyWorks Controller setup which can be used for initial trial of the software and this is termed as default license. Default license is not extendable. Serial Keys are not required and not displayed for Default Licenses.

- **Evaluation License**: Evaluation license is time bound license and can be extended further. Accops Sales or support team should be contacted for getting any evaluation license. Evaluation license can be used for further evaluation of HyWorks Controller with more devices, users, Desktops etc.

- **Perpetual License**: Once product is purchased by customer, a perpetual license will be provided, which does not get expired with time and could be used forever. However, this does not necessarily make it eligible for latest version download or installation. Latest version of HyWorks Controller may be made available with new licenses only though old licenses will continue to work.

**Grace Period**: Grace period of 7 days is given for default or evaluation licenses post expiration date so that license expiration will not cause immediate shutdown of HyWorks. But after the grace period is over, the system will be expired and users as well as administrator won’t be able to use the HyWorks until appropriate license is applied on HyWorks Controller.

Perpetual licenses will not go into grace period as the perpetual licenses are forever.

However, in case the license files on HyWorks Controller goes missing or corrupted, the system will go into grace period of 90 days to provide continuity to running operations through HyWorks Controller.

**Based on License Attribute**
Based on License attribute following two types of licenses can be applied on HyWorks Controller:

- **Concurrent Session Based Licenses**
  Session based licenses will have restrictions over number of sessions with HyWorks Controller, which means any number of devices can be configured with HyWorks Controller, but concurrent sessions will be allowed as per license configurations. E.g. a session-based license with 10 sessions allowed will allow any number of devices to be connected to HyWorks Controller but only 10 sessions will be allowed.

- **Named User Licenses**
  Licensing restrictions based on total number of registered users. Once all licenses are consumed new users will not be allowed to login.

- **Number of Registered Devices**
  Licenses based on number of registered devices will simply allow only those many devices which are configured in the license e.g. if license is configured for 10 devices then 11th device will not be allowed to be registered.

**Important Licensing Details**

We will try to outline few key facts and details about HyWorks Controller Licensing:

- **Impact on HyWorks deployment after license expiry**
  System has already passed the default, evaluation or grace period time. In case where HyWorks Controller gets expired:
  1. HyWorks Controller will stop communicating with registered devices and causing entire deployment to be down until the license is activated
  2. On user logon, errors will be displayed regarding license expiry
  3. Please note as HyWorks Controller is continuously declining client’s request the HyWorks Controller may display lot of repetitive errors depending on the connected devices
  4. Management console will be blocked except access of Dashboard, License Server section in **Setup** tab and **Logs** tab.

- **Applying Same License Keys on Different Servers**
  - License keys in HyWorks controllers are tightly coupled with Hardware keys of server machine and thus, once one serial key is used to activate one HyWorks Controller, same key cannot be used with any other hardware.

- **Reactivating HyWorks Controller with same serial key**
  - HyWorks Controller can be activated multiple times with same serial key, but the license duration will remain same.

**License Key Activation on HyWorks Controller**

License can be applied on HyWorks Controller using following two methods.

- **Online Activation**: Online activation requires internet connection on HyWorks Controller so that HyWorks Controller can directly communicate with License Server and activate license.
- **Offline Activation**: Method can be used when HyWorks Controller does not have internet connection and HyWorks Controller cannot connect to License server.
Online License Activation on HyWorks Controller

If HyWorks Controller has internet access and able to connect to License Server, then license can be activated online.

Pre-Requisites:

1. HyWorks Controller should be connected to internet
2. Appropriate serial keys and user credentials are available (Contact Accops Support team for getting all required information)

Steps:

1. Go to System - License section
2. Click on button **License Activation or Apply New License** to enable **License Activation** wizard
3. In **License Activation**, sub-section
   i. Provide appropriate entry in Serial Key
   ii. Provide appropriate Username and Password text boxes
4. Click on button **Activate License Online**
5. License will be activated, appropriate status message regarding successful activation will be displayed
6. Dashboard and License Server section in **Setup** tab will start reflecting the new license details.

Offline License Activation on HyWorks Controller

Offline license activation is required in cases, when HyWorks Controller server does not have internet connection and cannot communicate with license server.

Pre-requisites:

1. Appropriate serial keys and user credentials are available (Contact Accops Support team for getting all required information)
2. Access HyWorks Controller Management Console from machine where internet connection is available

Steps:

1. Access HyWorks Controller Management Console from machine where internet connection is available
2. Go to System - License section
3. Click on button **Apply New License** to enable **License Activation** sub-section
4. Provide appropriate entries in Serial Key, Username and Password text boxes in **License Activation** sub-section
5. Click on button **Generate Offline Activation Data**
6. HyWorks Controller will generate offline activation data and **Offline Activation Data** sub-section will be displayed under **License Management** section
7. Click on link **Click here to copy Offline Activation Data to clipboard and go to License Server** to automatically copy the offline activation data to clipboard and go to license server

**Note:**
- Pop-up blocker from browser may block, navigation to License server and thus should be unblocked for uninterrupted navigation to license server

8. Login to License Server user portal using the same user credentials being used to generate offline activation data
   i. On successful login, user will be navigated to License Server user portal
   ii. Go to **Offline Activation** tab on License Server user portal and paste the offline activation data copied from HyWorks Controller in **Offline Activation Data** text area
9. Click on **Activate** button
10. License server will validate the data being provided by HyWorks Controller and on successful validation will navigate the user to next screen which displays the license details as shown below
11. Click on **Continue** button
12. Next screen on License Server, will display the License’s Encrypted Data, copy the **License’s Encrypted Data** content
13. Navigate back to HyWorks Controller
14. Paste the **License’s Encrypted Data** content (copied from License Server) in the **Encrypted License Details** field as shown below
15. Click on button **Activate License Offline**
16. License will be activated, appropriate status message regarding successful activation will be displayed
17. Dashboard and License Server section in **Setup** tab will start reflecting the new license details.

**Cluster License or Licensing in HyWorks Controller Clusters**

With HyWorks Controllers configured in cluster, same license can be activated on both servers to enable both HyWorks Controllers to support same number of devices without additional licensing cost.

To configure cluster license, follow the below steps:

1. **Activate License on Primary Controller Server**:
   a. One server to be kept as primary should be activated first with provided serial key using the steps specified in above License - **License Activation on HyWorks Controller** section.
**Note:**

❖ When controllers are in cluster, then **Join Cluster License** checkbox is displayed on both controllers, but the option **should not be selected** while activating the license on Primary HyWorks Controller.

b. Once activated the configuration will start showing appropriate licensing details in License and Dashboard section.

2. **Activate License on Secondary Controller Server:** Considering that primary HyWorks Controller is already activated (Step#1), now secondary HyWorks Controller should be activated using appropriate cluster license.
   a. Go to **System** tab -> **License** section
   b. Click on button **Apply New License**
   c. Provide appropriate details for all License Activation section (copied in step# 3)
      i. Username
      ii. Password
      iii. Serial Key
   d. Select the checkbox **Join Cluster License**

3. Rest of the license activation process is same as specified in section **License Activation on HyWorks Controller** *(Either of license activation methods i.e. Online or Offline activation can be used to activate cluster license on secondary HyWorks Controller.)*

4. Same license will get activated on secondary HyWorks Controller

5. License Management section and dashboard of secondary HyWorks Controller will start displaying new license details.

License Allocations/Sharing in Multi-Organization Structure

HyWorks supports multi-organization structure with license allocations. License allocations enables administrator to distribute licenses to multiple organizations and restrict license usage in specific organizations.

❖ **License Details shown at root (default) Organization**

System level license details are always shown at Default organization and as Default level is also an organization its own license usage is also shown. At default organization level, following licensing information is available:

❖ **System Level (License usage)**

  **Total Licenses:** Total number of licenses installed on HyWorks [Read only information and cannot be changed]
  **Total Reserved:** Total number of licenses reserved by all organization [Read only information and cannot be changed]
  **Available to reserve:** Total number of licenses which can be reserved [Read only information and cannot be changed]
  **Total Shared:** Total number of licenses which are available as shared pool and can be used at any organizational level [Read only information and cannot be changed]
This Organization (Organization Name)

**Currently Used:** Actual usage of licenses in this organization. [Read only information and cannot be changed]

**Reserved:** Total number of licenses reserved for this organization. Modifiable and cannot be greater than total number of licenses in system.

**Limit License Usage:** Must be enabled if this organization need to use shared or unreserved licenses.

**Maximum allowed usage:** Maximum number of licenses which can be used at this organization level (Cannot be greater than reserved + total unreserved licenses in system)

Reserving Licenses at Organization Level

It is most likely possible that administrator wants to keep some minimum number of licenses available at organization level. For this Reserved License count be set to that minimum number.

The licenses will be reserved for this organization and cannot be used by any other organization.

- Reserved License count cannot be greater than total number of licenses in the system.
- Reserved License count cannot exceed total number of available licenses in system. (Total Licenses installed – Reserved – Used from Shared Licenses)

Creating or Sharing Licenses with other Organization

Even after some licenses are reserved for an organization, administrator may wish to keep some licenses in spare which can be used by any sub-organization on need basis. This can be achieved by keep some of the licenses for sharing. Use below steps to share licenses among child organizations:

1. Go to organization1, System – License section
2. Keep some of licenses as reserved (if needed), if not keep it as zero (organization will not have any reserved licenses)
3. Select check box *Limit License Usage*
4. Provide an appropriate count for field *Maximum allowed Usage*
   i. Entry in this field enables the use of shared licenses maximum up to available licenses.
5. Click on button *Update License Distribution* button
6. Now this organization will be able use:
   i. Minimum number of licenses which are mentioned in *Reserved*
   ii. Maximum number of licenses as mentioned in *Maximum allowed Usage*

Key Facts of Organizational Licensing

1. On license activation, all licenses are allocated to default organization
2. On creating new organization, default allocation for this organization is zero
3. On deleting the organization, licenses will be allocated back to default organization.

Monitoring License Usage and Freeing Up Licenses

In above sections, we have checked all the configurations related to licensing in HyWorks, the following screens in HyWorks management console can be used to view license usage.
Viewing License Usage
Licensing information is available in following screens:

- **Dashboard:** Management Console – Dashboard displays the summarized information of license usage, for currently selected organization, which includes:
  - **Licensing Type:** Default, Evaluation or Perpetual
  - **Overall License Usage:** Used vs Available Licenses in chart
  - **Number of days to expire**

- **License (In System):** Management Console – System – License screen displays all the information about licensing.
  - **Super-administrator View:** Super administrator in HyWorks, can view following information:
    - Overall license usage of HyWorks (all organizations)
    - Current Organization License Usage
    Please refer section License Allocations/Sharing in Multi-Organization Structure, for more details.
  - **View for other administrator users:**
    - License usage in current organization

**Note:**
- Non-super administrator users are not shown with system level license usage.

Freeing Licenses
Administrators can free up licenses from different screens based on type of license in use. This section will provide information about all types of licenses:

- **Registered Devices:**
  - As covered in section Endpoint Management in HyWorks, all devices post registration, are listed in Monitoring – Endpoints screen.
  - Registered devices do not get deleted automatically and thus once an endpoint has registered with Controller, it consumes one license.
  - **To free up licenses,** administrator can manually delete offline or online endpoints from Monitoring – Endpoints screen. Steps to delete endpoints are provided in Endpoint Management in HyWorks section.

- **Named User Licenses:**
  - Every user gets registered in HyWorks after its successful login for the first time and consumes one license if HyWorks is installed with Named user licenses.
  - The registered users can be seen in Monitoring – User Details section.
  - HyWorks does not delete any registered user and thus if administrator wants to free-up any licenses, then users must be deleted manually from Monitoring – User Details section. The steps to delete named users are provided in section Registered User Management in HyWorks.

- **Concurrent Sessions:**
  - HyWorks, on configuration with Concurrent Session based licenses, uses one license for every user session. This license consumption is not dependent on applications or desktop sessions by end-users.
  - License will be consumed when users are logged-in and will be freed automatically when user logs-out from HyWorks.
Even if administrator needs to free up licenses, user sessions can be deleted from *Monitoring – Sessions – User Sessions*. The detailed steps are provided in section Session Management in HyWorks.
Registered User Management in HyWorks
HyWorks v3.2 or later registers every user on their first successful logon. All registered or named users can be managed from Management Console – *Monitoring – User Details* section.

Listing of Registered Users
*Monitoring – User Details* section lists all registered users with following details shown in tabular format:

- **User Id**: Logon name or username of user. The User Id field is also consisting of link to view detailed information of user.
- **Display Name**: Actual display name of user
- **Last Login**: Information of last logon of user. On mouse hover, it displays exact date and time, when user had logged-in last.
- **Authorization Server**: Authorization server from where it was authorized
- **User DN**: Full distinguished name of user

Viewing detailed information and Login simulation
Clicking on User Id displays out detailed information about the user. The information displayed is based on following actions which includes:

- Login Simulation
- Fetching user information and group membership from AD
- Fetching user assignments

The detailed information includes following details:

- **User Information**: Displaying information of user with following sub-sections

  - **User Information**: User information sub-section includes following details:
    - User Id
    - Display Name
    - First Name
    - Last Name
    - Email
    - Phone Number
    - First Logon time

  - **Directory Service Details**:
    - Authentication Server
    - Authorization Server
    - Domain
    - Distinguished Name
    - Groups: the user is member of

  - **Last Login Details**
    - Last Login Time
    - Authentication Server
    - Authorization Server
    - Device Type
    - WAN IP Address

- **User Desktops**: Displaying the list of desktops which will or may get assigned to user. Details shown may be different for dedicated and shared hosted desktops as described below:
**Dedicated Desktops**
- **Pool Name**: Name of desktop pool from which desktop is getting assigned
- **Display Name**: Display name of desktop pool
- **Virtualization Type**: Desktop pool type e.g. Shared hosted desktop, Persistent Virtual Desktop or Non-persistent Virtual Desktop
- **Desktop Name**: Name of desktop assigned to user
- **OS**: Operating system of desktop
- **Desktop Provider**: Desktop provider on which desktop/VM is running
- **IP address**: IP address of Desktop VM
- **DNS Name**: FQDN of Desktop VM
- **DVM Assignment**: Assignment life span e.g. personal, floating
- **DVM Persistence**: Desktop persistence as persistent or non-persistent
- **Assigned from**: How the Desktop VM is getting assigned to user (Directly assigned to user or being assigned as a group/OU membership)
- **Applicable Profile and how is it getting assigned**: Which connection profile will get applied when user will connect to this desktop. If connection profile is directly applied to desktop pool, then it will not show any inheritance information.
- **Power Status**: Current power status of desktop VM

**Shared Hosted Desktops**
- **Pool Name**: Name of desktop pool from which desktop is getting assigned
- **Display Name**: Display name of desktop pool
- **Virtualization Type**: Desktop pool type e.g. Shared hosted desktop, Persistent Virtual Desktop or Non-persistent Virtual Desktop
- **Team Name**: Session host team name which is being assigned
- **Session Provider**: Type of session provider
- **Assigned from**: How the shared hosted desktop is getting assigned to user (Directly assigned to user or being assigned as a group/OU membership)
- **Applicable Profile and how is it getting assigned**: Which connection profile will get applied when user will connect to this shared hosted desktop. If connection profile is directly applied to desktop pool, then it will not show any inheritance information.
- **Status**: Current status of shared hosted desktop

**User Applications**: Displaying list of applications assigned to user and details of assigned application assignment.

**Application assigned to User**: List of application directly assigned to user with following details:
- **Application Name**: Name of application
- **Application Internal Name**: Internal name of assigned application
- **Launch Mode**: Launch mode of the application e.g. RemoteApp or Shell
- **Applicable Profile**: Connection profile to be applied when user will access this application
- **Description**: Description of the application

**Application assigned from Group**: List of application assigned to user from group memberships
- **Application Name**: Name of application
- **Application Internal Name**: Internal name of assigned application
- **Group Name**: Name of user groups, which is getting entitlement for user
- **Launch Mode**: Launch mode of the application e.g. RemoteApp or Shell
- **Applicable Profile**: Connection profile to be applied when user will access this application
- **Description**: Description of the application
**Application assigned from OU:** List of application assigned to user from OU membership
- Application Name: Name of application
- Application Internal Name: Internal name of assigned application
- OU Name: Name of organizational unit, which is getting entitlement for user
- Launch Mode: Launch mode of the application e.g. RemoteApp or Shell
- Applicable Profile: Connection profile to be applied when user will access this application
- Description: Description of the application

**User Policy:** Policies which will get applied on user sessions:

**User Applicable Profile:** Applicable connection profile details
- Profile Name: Name of connection profile
- Description: Description of connection profile
- Assigned from: How the connection profile is being assigned.

**Session Timeout Policy:**
- On Client-Disconnect: Action to be taken on client disconnect. HyWorks can logout the user session or can keep it disconnected
- Enable User Inactivity Monitoring: If applicable profile is monitoring inactivity of user. True/False
- Mark User Session Idle In: If Enable User Inactivity Monitoring is true, then after how many minutes of inactiveness, user session should be considered as idle
- Expire Idle Session In: In how many minutes, idle session should be expired
- On Expire: Action to be taken on session expiry, disconnect the session or logout the session.
- Set Max session Timeout: If you want to enable maximum session timeout. True or false
- Force Terminate User Session In: Timeout in minutes for which session will be allowed
- On Exceeding Max Session Timeout: Action to be taken after max timeout is achieved. Logout the user session or disconnect the user session.
- Logoff Disconnected Sessions after: After how many minutes, disconnected user session will be logged off.

**User Details a Powerful Tool for Troubleshooting**
Though **User Details** screen is simply used for displaying user information but the same can also be used for understanding or determine following delivery aspects:

- **User Assignments:** Troubleshooting what applications or desktops are getting assigned to the user and how are they getting assigned
  - Applications
  - Desktops
- **Applicable connection profiles for:** What connection profile will be used for an application or desktop session and thus understanding if user experience is getting set correctly or not.
  - Applications
  - Desktops
- **User Policies:** What connection profile/ timeouts will be applied for user session.

**Deleting registered users**
Use below steps to delete registered users from HyWorks:
1. Go to HyWorks Controller Management Console – Monitoring – User Details
2. Select one or multiple users from list of users
3. Click on button **Delete User**
4. Confirm the action, users will be removed from HyWorks.

**Note:**
- You cannot delete a user from User Details, if user is currently logged in.

❖ **Important points for User deletion**
  - With **Named User License**, every registered user consumes one license and thus by removing users from **User Details** screen, licenses can be freed.
  - You cannot delete users who are currently logged-in
  - Registered users do not affect any license usage with device based or concurrent user session-based licenses.
HyWorks Controller Clustering and High Availability

HyWorks Controller is the core component of HyWorks VDI environment and unavailability of HyWorks Controller may cause complete VDI environment to be down. Thus, in a production environment it is very critical to keep HyWorks Controller always up and functioning. 

**HyWorks Controller** section in **Server** tab enables administrator to configure two HyWorks Controllers in cluster to maintain availability of HyWorks Controllers.

HyWorks Controller clustering provides following **benefits**:

1. High Availability of HyWorks Controller - New session can be provided from second HyWorks Controller when first HyWorks Controller is down
2. Common license for both HyWorks Controllers
3. Running sessions won’t get disconnected
4. Only Primary server establishes and makes active communication with providers, thus the traffic on providers (E.g. VMware, Hyper-V etc.) is not doubled due to two HyWorks Controllers.
5. Continuous synchronization between member HyWorks Controllers

We will learn about the HyWorks Controller cluster, concepts, mechanism and concepts in this section.

Concepts and Terminologies

Following terms will be used frequently in this section:

- **HyWorks Controller Modes**: HyWorks Controller, when configured in cluster, can be in following modes:
  - **Primary**: When running in Primary mode, HyWorks Controller will be the active server between the configured cluster servers and will be processing all device or resource related operations.
  - **Secondary**: In HyWorks Controller cluster, there cannot be two primary servers and thus one server works as a primary, other server changes its mode to secondary. In Secondary mode or standby mode, HyWorks Controller only communicates with Primary HyWorks Controller to keep on syncing its configuration and availability of primary server and discards any other client request.
  - **Fault Mode**: HyWorks Controller mode in which it cannot function correctly, but HyWorks Controller Service is running, e.g. database services are down, or license services are down.
  - **Maintenance Mode**: HyWorks Controller mode in which it does not interact with another server in cluster. Maintenance mode can be used to do some management activities on the controller to avoid any synchronization e.g.

- **Pulse**: Test request from HyWorks Controllers to check each other’s status when configured in cluster (Default pulse interval is 45 seconds)
- **Heartbeat**: Request and response mechanism between devices and HyWorks Controller to maintain connectivity and updating the configurations. System default heartbeat interval is 40 seconds.
- **Cluster License**: Licensing mechanism which allows same license to be applied and available on different HyWorks Controllers configured in cluster.

HyWorks Controller Cluster Mechanism

1. Once HyWorks Controller cluster is configured, which means administrator has successfully configured the second HyWorks Controller. Following updates are going to happen:
   a. Devices connected to primary HyWorks Controller, will be communicated with the available HyWorks Controllers details i.e. details of both primary and secondary servers
b. Secondary HyWorks Controller will start syncing its database with Primary HyWorks Controller
   i. The syncing happens in every 60 seconds so that secondary HyWorks Controller is always having most recent details from primary server.
   c. Secondary HyWorks Controller will stop all its active services i.e. broadcasting, communication with Session Providers
   d. Secondary HyWorks Controller will start refusing HyWorks Client’s heartbeats and registration requests
2. Device will keep the details of HyWorks Controller cluster configuration on use these values in the following order:
   a. Connect to Primary HyWorks Controller – All devices will eventually come to primary HyWorks Controller
   b. Connect to Secondary HyWorks Controller if primary HyWorks Controller is not available

Configuration of HyWorks Controller Cluster

HyWorks Controller cluster can be configured as described below:

❖ Pre-requisites to Configure HyWorks Controller Cluster

1. Two HyWorks Controllers are installed
   a. On two different windows servers with same configurations e.g. 2 Windows 2008 R2 servers with 4 GB RAM and 4 vCPUs
   b. Same version of HyWorks Controller is installed on both servers.
   c. SQL Server is configured to use static port and to allow remote connections
   d. Installation using SQL Server database, HyWorks Controller high availability is not supported for HyWorks Controllers with Embedded database
   e. Microsoft Synchronization framework 2.1 is installed on both HyWorks Controllers
2. Time is perfectly synchronized between the two HyWorks Controllers
3. Both HyWorks Controllers can connect to each other and able to resolve respective hostname of another server
4. Date and time are correctly synced among two controller servers
Refer document ‘HyWorks Controller HA Configuration’ for detailed instructions on prerequisite configurations and configuration process.

❖ Configuration Process

Follow the below steps to configure HyWorks Controller Cluster:

1. Assuming following configuration is ready in the environment:
   a. Two HyWorks Controllers (hySrv1 and hySrv2) are installed using SQL Server
2. Access HyWorks Controller Management Console of one HyWorks Controller to be configured as Primary HyWorks Controller initially say hySrv-1
3. Login with appropriate admin credentials
4. Go to Server tab -> HyWorks Controller section
5. In HyWorks Controller section, it will display information about the current HyWorks Controller server using the following sections:
   a. HyWorks Controller: Displaying information about the controller using columns Name, IP Address, Version, Mode, Status and Actions
b. Database Information: Details of HyWorks database server configurations displaying Controller server host name, database name, database type and database location.

c. Add button to configure more HyWorks Controllers in cluster

6. Click on Add button to open Add HyWorks Controller dialog

7. In Add HyWorks Controller dialog:
   a. Provide Host Address of second HyWorks Controller in the following format:
      https://HyWorks Controller IP or hostname>:<Port>; Port is the port number, on which HyWorks Controller Service is running. By default, HyWorks Controller Service is configured on port 38866.

8. Click on Test Connection button to verify the availability of second HyWorks Controller.
   a. If server is reachable then Save button will remain enabled
   b. If server is not reachable then Save button will be disabled which means second HyWorks Controller must be available for being configured in HyWorks Controller cluster.

9. Click on Save button to save the configuration.

10. Configuration will be saved, appropriate status prompt will be displayed on top of HyWorks Controller Management Console

11. HyWorks Controller section will start displaying information of both servers

12. Activate cluster licenses on HyWorks Controllers to maintain same capabilities on both the servers to serve same number of devices or sessions. Please refer section Cluster License for detailed instructions of activating cluster license.

Now we have successfully configured the HyWorks Controller cluster, it’s important to understand how this HyWorks Controller cluster functions to maintain high availability. Refer section HyWorks Controller Cluster Mechanism for detailed information.

**HyWorks Controller Cluster Management Operations**

The section will give brief details about the available management operations on HyWorks Controller cluster:

❖ **Changing Server Modes**

Administrator can manually change the server modes from HyWorks Controller section.

The feature is useful when administrator wants to do some maintenance activities (e.g. Upgrade) on one server and willing to keep services down for some time. In such cases administrator can change the modes of servers using following steps:

1. Access HyWorks Controller Management Console of one HyWorks Controller
2. Login with appropriate admin credentials
3. Go to Server tab and expand HyWorks Controller section
4. Click on button Change Mode, which will present Change Mode wizard
5. Configure appropriate modes for both the servers and click on button Save
6. Appropriate status prompt will be displayed on top bar
7. Eventually servers may be shown with same status, but it will get updated as soon as the services adapt the applied changes.

❖ **Removing HyWorks Controller from Cluster**

Administrator can remove one HyWorks Controller from cluster by following the below steps in below mentioned two situations:

 Idol When Both Controllers are Reachable:
It is highly recommended to remove HyWorks Controllers from cluster when both servers are reachable for maintaining the environment on Primary server. Follow the below steps to remove HyWorks Controller from cluster when both controllers are reachable.

1. Access HyWorks Controller Management Console of any of the HyWorks Controller (recommended Primary Controller)
2. Go to **Server** tab -> **HyWorks Controller** section
3. HyWorks Controller section will list both the servers with displaying **Delete** button against the second HyWorks Controller (1\(^{st}\) server is the one from where management console has been accessed, 2\(^{nd}\) server is the other server in cluster)
4. Click on **Delete** button
5. Confirm the action by clicking on **Delete** button in **Confirm Action** dialog
6. Selected controller will be removed from the cluster and both controllers will start functioning independently as Primary server.
   a. Second controller will have exactly same data as first controller and thus could also create conflict in the environment
      i. It is not advised to have two controllers in same environment running independently and thus the second server should be kept down.
   b. No data synchronization will happen once controllers are separated out
   c. Devices already registered with controller, will communicate with last accessed primary server and in the next communication with server, update their controller entries so that next time they won’t go to secondary server.
7. First HyWorks Controller which was used to activate the license will continue to have the same license as before
8. Second HyWorks Controller on which cluster license was activated will go into grace period.

**When One HyWorks Controller is down:**

Though it’s not recommended to remove HyWorks Controller from cluster when it’s not reachable, but still this can be done using below steps:

1. Access HyWorks Controller Management Console of HyWorks Controller currently reachable
2. Go to **Server** tab -> **HyWorks Controller** section
3. **HyWorks Controller section** will list both the servers with displaying Delete button against the second HyWorks Controller (currently not reachable)
4. Click on **Delete** button
5. Confirm the action by clicking on **Delete** button in **Confirm Action** dialog
6. It will check the HyWorks Controller unavailability and will display error in **Confirm Action** dialog
7. Click on button **Force Delete** to continue deleting the HyWorks Controller from cluster
8. Server2 will get deleted from Server1 and server1 will start functioning as an independent primary server
9. As Server2 is down and not having any information of removal of cluster, so when it will come up again, it will continue to work as secondary and to avoid any further invalid synchronization of data among two servers. The entry of first server must be deleted from this.
10. Access Management Console of second HyWorks Controller
11. Go to **Server** tab -> **HyWorks Controller** section
12. Click on **Delete** button displayed against the Server1 which it considers to be primary server
13. Confirm the action by clicking on **Delete** button in **Confirm Action** dialog
14. Server1 will get deleted from Server2 and now Server2 will also start functioning as independent primary server with license of second server will get reset to grace period reset as it was using the cluster license.

**Limitations of HyWorks Controller Clustering**

1. Time synchronization must be manually achieved
2. With data synchronization happening in 60 seconds duration, configuration changes (happened between last sync and server down) may get lost, which may cause
   a. Most recent session disconnection happened in that duration
   b. Data duplication if the same configuration is done on new primary server, once the old primary comes up from down status
3. Banner and HyWorks Client upgrade configurations which are handled using files are currently not synced and thus may either show alerts or change the banners. Client may show the version mismatch alerts.

**Note:**

- Detailed information about HyWorks Controller installation for cluster configuration, prerequisite configuration, failover points and behavior of several types of client can be found in document **HyWorksController-v3.0_Clustering_and_HighAvailability**
SMTP Configuration for Email Notifications

*SMTP Config* sub-section in *System* section enables HyWorks Controller to send email alerts (e.g. Backup emails) to configured email IDs.

SMTP configuration in HyWorks Controller requires, HyWorks Controller to connect to SMTP server else the configurations will fail in send emails.

**SMTP Configuration Process**

1. In HyWorks Controller Management Console, Go to *System - SMTP Config*
2. Provide the following details
   a. **SMTP Server:** Mandatory field requires hostname or IP of SMTP Server
   b. **Connection Type:** Type of connection SMTP supports according to its security configurations. Available options are *None, StartTLS, SSL/TLS*
   c. **SMTP Port:** Mandatory field requires SMTP Port on which SMTP server can be connected
   d. **Enable SMTP Authentication:** Select the checkbox if SMTP server requires authentication
   e. **SMTP Username:** Mandatory field requires Username to authenticate with SMTP server in the format of username@domain.com.
   f. **SMTP Password:** Mandatory field requires Password of configured SMTP user
   g. **Confirm Password:** Requires same password as SMTP Password
   h. **SMTP Email Sender:** Mandatory, account of user which will appear as Email sender in the format of username@domain.com.
3. **Send Test Mail:** Once all SMTP configuration fields are filled with appropriate details, administrator can validate the configuration by sending a test mail to any email address. To send test email address:
   a. Provider appropriate details in Test Email Address field in the format of username@domain.com
   b. Click on button *Send Test Email*
   c. Email will be sent to the provided email id and appropriate status prompt will be displayed on top of management console stating Test mail sent successfully
   d. Click on *Save* button to save the SMTP configuration.
   e. SMTP Configuration will be saved, and appropriate status prompt will be displayed on top of management console stating SMTP Configuration saved successfully.

**SMTP Configuration Usage**

Once SMTP configuration is done successfully, HyWorks can use these settings to send e-mail notifications to configured administrators.

Currently HyWorks supports e-mail notifications for following configurations:

1. HyWorks Controller backup: Administrators can schedule periodic backup along with e-mail notifications to get controller backup file over e-mail.
2. RMS (now HyLabs) reservation notifications

**Resetting SMTP Configuration**

If administrator does not wish to keep SMTP configuration, it can simply click on *Reset* button, displayed at the bottom of *SMTP Configuration* page.
**Confirm Action** dialog will be displayed and on confirming the reset operation, all SMTP Configurations will be erased from HyWorks Controller.
HyWorks Controller Database Backup and Restore

Backup configuration in HyWorks Controller enables the automatic backup of HyWorks Controller database.

This backup can be used to restore the configuration using HyWorks Controller installation wizard.

_Beckup Restore_ section can be used for following purposes:

- Take immediate backup
- Configure the Backup schedule
- Configure Email Address

**Backup Now - Manual Backup**

For creating a database backup manually, administrator can follow the below steps:

1. Go to **System – Backup Restore** section
2. Click on button **Backup Now in Backup Restore** section to initiate HyWorks Controller database backup.
3. HyWorks Controller will immediately create a backup file, will display the status of the backup operation.
4. The backup file is saved locally on HyWorks controller with appropriate time stamp in zipped format. The detailed information of backup file can be found in controller logs.
   a. **Database configured with SQL Server Authentication** - Location of Database Backup: 
   C:\Windows\TEMP\DB\BACKUP
   b. **Database configured with Windows Authentication** - Location of Database Backup: 
   C:\Users\<Username>\AppData\Local\Temp\DB\BACKUP
5. Backed up database file can be used later to restore the HyWorks Configuration, "**HyWorks Controller Restore using Backup**" for detailed instructions.

**Configure Backup Schedule – Automatic Backup**

Backup schedule enables automatic backup creation of HyWorks Controller database as per configured schedule. Follow the below steps to configure the Backup Schedule:

❖ **Backup Scheduler**

1. In HyWorks Controller Management Console -> Go to **System – Backup Restore** section
2. In Backup Scheduler, sub-section, provide the following details:
   a. Select checkbox **Schedule Backup** (Backup after every _ days and Backup time fields will get enabled)
   b. Provide appropriate number in **Backup after every field** e.g. if willing to take backup after every 7 days, then enter 7
   c. Provide details of time when you want to schedule backup in time format HH:MM
3. Click on **Save** button shown at the bottom of the **Backup Restore** section
4. Backup scheduler will be enabled
5. As per configured schedule, backup will be taken and saved at the following location on HyWorks Controller with time stamp
   a. **Database configured with SQL Server Authentication** - Location of Database Backup: 
   C:\Windows\TEMP\DB\BACKUP
b. **Database configured with Windows Authentication** - Location of Database Backup: 

C:Users\<Username>\AppData\Local\Temp\DB\BACKUP\n
❖ **Email Backup File**

Administrator can also configure the email address as well on which scheduled backup will be mailed. To configure backup email, follow the below steps:

1. In System – Backup Restore section
2. Provide following appropriate details in **Email Configuration** sub-section
   a. Select checkbox **Email Backup File** (Send to Email Id, Subject and Message fields will get enabled)
   b. Provide appropriate Email Id in format username@domain.com in Send to Email Id field
   c. Provide appropriate text for the backup email in **Subject** field
   d. Provide appropriate text for the body of backup email in **Message** field
3. Click on **Save** button shown at the bottom of the Configuration Backup section
4. Backup scheduler will be enabled and will start sending Backup file to the configured Email address

**Note:**

❖ For sending backup email, SMTP configurations should be done correctly, and HyWorks Controller should have access to SMTP server. Refer section **SMTP Config** for detailed information.

❖ If HyWorks Controller fails to connect to SMTP server at the time of backup, mail will not be sent, however backup will be taken.

**Restoring HyWorks Controller using Backed-up files**

HyWorks supports restoration of whole deployment using restoring backed-up database. Please refer document **HyWorks Restore Mechanisms** for detailed information.
Applications and Shared Hosted Desktops Delivery
With HyWorks one of delivery aspect is to virtualize and deliver applications and shared hosted desktops to end-users.

HyWorks supports application and shared hosted desktop delivery from Windows and Linux platforms. This section of HyWorks administration will provide details on following topics:

- Platform Support for application and shared hosted desktop delivery
- How to add and manage session host servers in HyWorks
- Session teaming and load balancing
- Application delivery, management, and application session management
- Shared hosted desktop delivery, management, and session management

Supported Platforms
HyWorks supports applications and shared hosted desktops deliveries from Windows and Linux platforms. Below is the list of different supported server versions:

- **Windows:**
  - Windows 2008R2-SP1
  - Windows 2012R2
  - Windows 2016

- **Linux:**
    - V1.6

Shared Session Host Management
For delivering applications or shared hosted desktops to end-users, session host servers (Linux/Windows), should be added into HyWorks configuration and then appropriate applications or shared hosted desktops should be published for end-users. As part of session host server management, following operations can be done:

- Add/Edit/Delete Session Host Servers
- Mark session host server as inactive for maintenance activity
- Server status monitoring

Preparing Servers for Application and Shared Hosted Desktop Delivery
This section will briefly give details for preparing servers for application and shared hosted delivery in HyWorks.

- **Windows Session Host Server Preparation:** Follow the below steps to configure Windows server:
  1. Install supported Windows server as virtual machine or on physical hardware
  2. Configure machine into domain or workgroup as per requirement
  3. Install all pre-requisites for session host agent installation
  4. Install HyWorks session host module – Windows server is ready for application and shared hosted desktop delivery

- **Linux Session Host Server Preparation:** Follow the below steps to configure Linux server for application and shared hosted delivery:
  - Install Linux SHD server using ISO released by Accops team
  - Install latest offline packages and Linux DVM Tools
Configure machine for LDAP, Microsoft Active Directory or Workgroup authentication
Linux shared session host server is ready for application and shared hosted desktop delivery

**Note:**
➢ Refer relevant installation and configuration guide for Linux and Windows servers for detailed information.

Adding ‘Shared Session Host’
Shared session host category refers to Microsoft Windows servers running Accops HyWorks Session Host module. Following prerequisites are mandatory for configuring a HyWorks Session Host Server under Shared Session Host Category:

**Pre-requisites**
1. Supported Windows Server platform (Windows 2008R2, Windows 2012R2, Windows 2016) is up and running
2. Accops HyWorks Session Host Server (Session Host Agent and Monitoring Service is running)

**Step by step process to Add Shared Session Host**
Follow the below steps to add Microsoft Windows server with appropriate prerequisite as shared session host:
1. Go to Server – Session Providers section
2. Click on **Add** button to invoke **Add Session Provider** wizard
3. **General Configurations:** Following general configurations should be done with appropriate details:
   a. Select **Category** as **Shared Session Host**
   b. Select **Type** as
      i. **Microsoft RDS Server** for Windows Session Host Servers
      ii. **Linux RDS Server** for Linux shared hosted desktops
   c. Provide appropriate logical name in **Name** field
   d. In **Host Address**, provide appropriate host address or IP

**Important Notes:** If providing host address, then make sure it is being resolved correctly from Controller
➢ Controller uses configured address for providing connection details to endpoints and thus if hostname is configured, it must be resolvable from endpoints as well.
➢ With HySecure being used appropriate host entries should also be made on HySecure Host Configurations
➢ Avoid using localhost as the hostname as it will not get resolved while accessing Apps/Desktops.

a. **RDP Port:** Session host server port on which it will accept the remote connection. Default value is 3389 but can be modified as per server configurations.
b. **Session Team** select appropriate session team for session host server. Refer section **Session Host Server Teaming and Load Balancing**.
i. Linux Session teams should be chosen for Linux shared session hosts and Windows session teams should be chosen for Windows shared session hosts

ii. By default, a Linux and a Windows session team exists in system which cannot be deleted.

c. Based on team selection, following things will happen

i. **Check the Session Team Type:** Weight is required for Weighted Least Connection or Weighted Round Robin load balancing, which means if selected team is using either type of load balancing then **Weight** filed will be enable, if it’s using Adaptive load balancing then **Weight** filed won’t get enabled.

ii. Check HyWorks Session Host Modules: On Selection of team, controller attempts to connect to Session Host and Monitoring service (progress bar will come for a short duration)

1. If it is able to connect, then will proceed without any exception

2. If it is not able to connect then it will display the error

**Note:**

➢ Administrator will be able to add session host servers even when its showing error for Session Host Service or Monitoring Service or Both, but Application or Shared Hosted Desktops will not be delivered until these services are running.

d. Select **Active** checkbox to make session provider as active.

i. Inactive session providers are not considered while providing the sessions.

e. Keep other options i.e. **Enabled Diagnostics** and **Enable Virtual IP** should be kept unchecked until they are really required and recommended by Accops team. Please refer **Advance Shared Session Host Configurations** for more information about these options.

f. Once all required options are configured, click on Test Connection button to check the availability of session host server on configured RDP port

**Note:**

➢ **RDP Port** configuration is not available in v.3.0 release and thus HyWorks Session Host Servers can only communicate on default RDP Port (3389)

2. Once connection is successful, success message will be displayed and clicking on Add button will add the session host server

3. Administrator will be able to see configured session host server in Session Providers screen with appropriate status.

**Advance Shared Session Host Configurations**

Though not tagged as advance configurations, following Shared Session Host specific configurations can be kept in advance category. These options are available for **Microsoft RDS Server** type shared session hosts.

4. **Enable Remote Control:** Select this option if session shadowing to be used for user desktop or application sessions from this server. Option to take session shadow is available from
5. **Enable Diagnostics**: An advanced configuration for enabling advanced diagnostics of session host server, to be kept unchecked until affirmed by Accops Support team during.

6. **Enable Virtual IP**: This option can be used to provide virtual IPs to either RDS sessions or any remote applications being published in HyWorks.

![Configuration settings for enabling virtual IP](image)

7. Following configurations should be done while enabling virtual IP on session host server
   a. **Interface**: Listing available network adapters on the session host server, one of the network adapters to be selected.
   b. **IP Virtualization Type**: Read-only with default option as RDS
   c. **IP Type**: Currently only IPv4 is supported and thus the field is disabled, and default option is IPv4.
   d. **IP Virtualization Mode**: Can be selected as per session or per program
      i. **Per Session**: Each RDS session will be assigned one virtual IP. All application sessions under single RDS session will be assigned same virtual IP. For Per Session IP Virtualization mode, specific Virtualization profile is not needed.
      ii. **Per Program**: Per program IP virtualization mode, assigns virtual IP to specific program (Application) in RDS session. **Per Program Virtualization** mode, requires application to be assigned with specific Virtualization Profile with **Virtualization** enabled.

**Note:**
- Not specifying Virtualization profile in Application or specifying virtualization profile with **Virtualization as disabled** will not assign Virtual IP to remote application.
- Virtualization Profile can be assigned while adding or editing application in **Additional Settings** tab.
Use Specific Range: Selecting this option enables administrator to specify the network range, from which virtual IPs will be assigned. Enabling this option will require following fields to be filled with appropriate details:

i. **Start IP Address**: First IP Address
ii. **End IP Address**: Last IP Address
iii. **Subnet Mask**: Appropriate Subnet mask

Administrator can enable these two configurations as well in addition to all important configurations while adding session host servers.

Once configured successfully, added session host server can be used to deliver shared virtual desktop or applications to end users.

Deleting a Shared Session Host Server

Follow the below steps to delete a session provider:

1. Select session provider to be deleted and click on **Delete** button
2. **Confirm Action** dialog will be displayed stating all the consequences of deleting session provider.
3. Confirm the operation by clicking on **Delete** button on the confirmation dialog
4. Session provider will be deleted from HyWorks configuration with following impact.

**Impact of Deleting Session Host Server**

When a shared session host is deleted from HyWorks Controller, following things can be affected:

1. The provider will be removed from all HyWorks configurations
   - a. Session providers: Management of deleted provider will not be possible
   - b. Session teams: Deleted server will no longer be part of session teams and hence it will not participate in session load balancing
   - c. Applications/Shared hosted desktop pools: Application sessions from the server will not be given from deleted server

Update Shared Session Host Configurations

**Editable Fields and Impact of Changes**

While modifying shared session host configurations, following configurations can be changed:

- **Name**: Changes in name will not affect any services. It is not critical to any delivery aspects.
- **Host Address**: **Critical** field and should be updated only when the same server has been migrated to different IP or host address as using this information only HyWorks Controller fetches the information of Desktops and assignments etc. If somehow the same server is not available on the same host address, then existing configuration may get corrupted. Administrator should be very cautious while updating host address field.
- **RDP Port**: **Critical** filed, controller will check session host server reachability on this port. Modify only when it has been changed on session host server configurations as well.
- **Active**: **Critical**, it is already specified in configuration of each type of Session Provider that not selecting Active checkbox will mark the Session Provider as inactive and it will be ignored while fetching Desktop information for the client.
Administrator should be cautious while marking any Session Provider as inactive as all associated clients will stop getting Desktops.

- With adaptive/least connection load balancing, adding new session host server can put immediate load on newly activated server and hence should be considered carefully as per load analysis.

- **Changing Session Teams: Critical.** Changing session server team should be done very carefully as it can affect the load balancing of sessions and delivery to end-users. Depending on new session server team, Weight configuration can be shown to be changed or specified.

- **Weight: Critical.** Weight of a session host server affects the number of sessions to the server directly. Consider changing weight as per capacity of servers.

- **Other configurations:**
  - **Enable Remote Control:** Check or un-check to enable/disable. Not critical
  - **Enable Diagnostics:** Not critical but should be enabled as advised from Accops team recommendations.
  - **Enable Virtual IP:** Requires server reboot and critical. Change configurations as per requirement.

**Editing Session Host Server**

Once changes are identified, administrator can update configured session host server details using following steps:

1. Select the session provider to be modified
2. Click on **Edit** button
3. **Edit Session Provider** dialog will be displayed
4. Update the fields as required and click on **Update** button.
5. Changes will be saved, and user’s sessions will be given from new session host servers.

**Special Case: Marking Session Host Server Inactive**

In deployments, sometimes it is required to perform maintenance activities on one or multiple session host servers of a team and thus, administrators require these servers not to be used for providing application or shared hosted desktop by end-users.

Changing Session host server mode to inactive serves this purpose and once session host server is marked inactive, following activities will be stopped:

- Health check of session host server reachability, this involves
  - Check connections on RDP port
  - Session host agent service
  - System resource (Hard disk, Memory and CPU usage), HyWorks monitoring service
- No new sessions will be given to inactive servers so that maintenance activities can be done
- Existing sessions will still be managed but on re-logon and attempt to reconnect will give sessions from Active servers only,

**Shared Session Host Status Monitoring**

For smooth delivery of applications and shared hosted desktops, session host servers must be up and running. For any specific analysis and troubleshooting details are provided below:
Monitoring Server Health

HyWorks Controller gets information of CPU, RAM and Hard-disk utilization from all configured shared session hosts and display it at following location:

1. Dashboard -> Details of all server will be shown with respective resource values

For resource values HyWorks need connection to monitoring service and if monitoring service cannot be reached, it is shown as yellow alert for respective session host server and current usage data is not shown.

2. Server -> Session Teams -> Click on respective session team -> details of all servers will be shown

Session host server reachability

HyWorks controller periodically checks session host server reachability for following perspective:

1. Configured RDP port: Unreachable RDP port shows the server is not usable and HyWorks does not give any sessions from that server, The status will be reflected as red count against Server -> Session provider page.
2. Session Host Server Agent: As session host server agent is responsible module for mediating all sessions. Unreachability of it is reflected in Server Session Teams page.
3. HyWorks monitoring service: An important service to share system resource values and communication failure of monitoring service will affect load balancing. Status can be checked on dashboard and server -> Session Teams page.

Sections to check for troubleshooting

When application or shared hosted desktop deliveries are functioning normal, monitoring is not needed but, in any case, if users are facing issues in connecting to any provider, then following sections can be checked for server status:

1. Server -> Session providers
2. Server -> Session teams
3. Logs -> Appropriate warning or error logs are generated when accessed session host is facing any problems or controller is facing problems in connecting to respective session host server.
4. Dashboard
Session Host Server Teaming and Load Balancing

Session Team in HyWorks is a team of session host servers which will be load balanced based on the type of load balancing mechanism configured. In HyWorks, shared hosted desktop sessions or applications are delivered from a session team instead of independent session host servers.

Session Team sub-section under Server section provides options to manage session host servers team. Administrator can perform multiple management options from Session Teams page, details of these options will be provided in this section.

Session teams can be created for Linux or Windows session host servers.

Navigating to Server – Session Teams page, lists the available session team and displays the following details of the session team using different columns:

- **Team name**: Name of session team
- **Team type**: Type of session team
- **Use restrict session**: If any resource-based restriction is applied
- **Load balancing type**: Type of load balancing mechanism
- **Defined In**: If this session team is defined in the current organization

Administrator can search a session team by searching with appropriate search string in search textbox.

Before moving ahead in Session Teams configuration and management it’s important to understand the session team load balancing in HyWorks.

**HyWorks Session Team Load Balancing**

Once two or more servers are added to a single session team then HyWorks Controller starts load balancing the sessions among the member session host servers.

Based on load balancing mechanism, HyWorks Controller supports following types of load balancing:

- Weighted Round Robin
- Weighted Least Connection
- Adaptive

Let us understand each of these load balancing types in detail:

**Weighted Round Robin**

Usually Round Robin refers to a mechanism where sessions are given one by one from all servers, but in HyWorks the Weighted Round Robin load balancing uses a unique formula, where the load balancing is done in following manner:

1. While adding session host servers to session team with **Load Balancing Type** as Weighted Round Robin, weight of each server is taken. The weight could be a number ranging from 2 to 100.
2. Controller performs addition of weight of all servers and stores this number and assigns a range to each server e.g. three session host servers say srv1, srv2 and srv3 are added with weight 10, 50 and 100 respectively. Then number range for each server could be:
   a. Sum of weights = 10 + 50 + 100 = 160
   b. Srv1 (Weight = 10): Range 1 – 10
   c. Srv2 (Weight = 50): Range 11 – 60
   d. Srv3 (Weight = 100): Range 61 – 160

3. Whenever any session requests (Application/ Shared Hosted Desktop Session) comes to controller
   a. Controller picks a random number between 1 to sum of weight of all servers (in above example number could be 1 to 160)
   b. Controller verifies, picked number falls in which range and that range belongs to which session host server
   c. Session is given from session host server in whose range the picked number falls

4. On every session request, the same process is repeated.

**Session Stickiness in Application Delivery in Remote App Mode**
If applications are configured to be delivered in *Remote Application* mode, which means all the application sessions will be running in single RDS session, then controller stores the session host server details from where the application has been served.

If another application session request comes which can be delivered from the same server, then controller ignores the load balancing and provide the application sessions from the same server.

The phenomenon is called the session stickiness and is applicable only in application delivery in *Remote App* mode.

**Reconnection (Shared Hosted Desktop Session and Application Sessions in Remote App Mode)**
Another important phenomenon in HyWorks Controller, where controller will ignore load balancing mechanism is *Reconnection*.

In cases, when user’s shared hosted desktop session or application sessions in Remote App mode is already lying in running or disconnected mode, then Controller ignores the load balancing and first provides the reconnection of same desktop or remote application sessions to the users.

**Application Delivery in Shell Mode and True Load Balancing**
As application delivery in *Shell* mode, launches each application session in new RDS session, HyWorks Controller does not consider session stickiness or reconnection phenomenon and calculates the most suitable session host server as per its Weighted Round Robin mechanism every time.

The application delivery in Shell mode is termed as *True* load balancing.

**Cases in Which Controller Won’t Provide Session from Eligible Session Host Servers**
In few cases controller does not provide session from eligible session host server and recalculates the suitable session host server based on Weighted Round Robin load balancing mechanism, following is the list of such cases:
1. **Session Host Server is down**: Controller monitors the availability of each session host server and if session host server goes unreachable, it does not give session from that server though, session may fall in the range of eligible server.

2. **Session Host Agent Service is down**: If controller cannot communicate with session host server then also sessions from that server will not be given.

3. **CPU or RAM Threshold Reached**: In session team if *Use restrict session* is enabled and memory or CPU or both resource utilization has crossed specified limit then, sessions from that respective session host server will not be given.

4. **Limit of No. of Application Instances Per Server Has Reached**: If number of application instances per server is configured and number of application sessions from one session host server has already reached, then while providing that application session, then the server which has already reached the limit will be skipped and session from other servers will be given.

### Weighted Least Connection

Weighted least connection in HyWorks provides sessions from session host servers using following mechanism:

#### Weighted Least Connection Load Balancing Mechanism

1. While adding session host servers to session team with *Load Balancing Type* as Weighted Least Connection, weight of each server is taken. The weight could be a number ranging from 1 to 100.

2. Score for each server is calculated using the following formula and server with least connection will be given the sessions:

   \[
   \text{Score Calculation Formula: } \frac{(\text{No. of Sessions} \times 10000)}{\text{Weight}}
   \]

3. Whenever any session requests (Application/ Shared Hosted Desktop Session) comes to controller
   
   a. With zero sessions, the score of session host server will also be zero (displayed as Hyphen “- ”)
      
      i. If all session host servers are having zero (-) score, controller will pick any session host server randomly to provide session
      
      ii. With one server is having zero sessions and zero (-) score, then that server will be used first
   
   b. Once at least one session from each of the session host server is provided, then controller will check the score to provide the next session.
      
      i. If servers are having same score, then again controller will randomly pick one of the session host servers
      
      ii. If not having same score, then session from server with least score will be provided.

4. On every session request, the same process will be repeated.

### Session Stickiness in Application Delivery in Remote App Mode

Session stickiness mechanism is same as specified in section **Session Stickiness in Application Delivery in Remote App Mode**
Reconnection (Shared Hosted Desktop Session and Application Sessions in Remote App Mode)
Reconnection mechanism in Weighted Least Connection will work in the same manner as being used in Weighted Round Robin load balancing mechanism. Please refer section Reconnection (Shared Hosted Desktop Session and Application Sessions in Remote App Mode).

Cases in Which Controller Won’t Provide Session from Eligible Session Host Servers
Controller skips providing sessions from session host server in specific cases mentioned in detail in section Cases in Which Controller Won’t Provide Session from Eligible Session Host Servers.

Adaptive Load Balancing
Adaptive load balancing in HyWorks refers to mechanism for sessions from team of session hot servers based on current load (CPU/Memory) consumption.

In Adaptive load balancing controller continuously updates its database with CPU and memory consumption of session host servers using monitoring service running on session host servers.
Score of each session host server is calculated based on current CPU and memory consumption and session is provided from session host server with least score.

Score Calculation Formula: CPU (%) + Memory (%)

Note:
➢ Monitoring service on session host server sends an average of last 3 memory and CPU usage in every 30 seconds and then sends the data to controller in every 30 seconds. Which means the controller usage a little old data, but this also helps in avoiding intermittent spikes in CPU or memory usage.

Weighted Least Connection Load Balancing Mechanism
1. Score for each server is calculated using the following formula and server with least connection will be given the sessions:
   Score Calculation Formula: CPU (%) + Memory (%)
2. Whenever any session requests (Application/ Shared Hosted Desktop Session) comes to controller
   a. If servers are having same score, then controller will randomly pick one of the session host servers
   b. If not having same score, then session from server with least score i.e. server with least consumption will be provided.
3. On every session request, the same process will be repeated.

Session Stickiness in Application Delivery in Remote App Mode
Session stickiness mechanism is same as specified in section Session Stickiness in Application Delivery in Remote App Mode.
**Reconnection (Shared Hosted Desktop Session and Application Sessions in Remote App Mode)**

Reconnection mechanism in Weighted Least Connection will work in the same manner as being used in Weighted Round Robin load balancing mechanism. Please refer section [Reconnection (Shared Hosted Desktop Session and Application Sessions in Remote App Mode)](#).

**Cases in Which Controller Won’t Provide Session from Eligible Session Host Servers**

Controller skips providing sessions from session host server in specific cases mentioned in detail in section [Cases in Which Controller Won’t Provide Session from Eligible Session Host Servers](#).

In addition to the cases mentioned above monitoring service (and resource consumption) becomes the critical and can affect session host server selection in following manner:

1. **Sessions will not be provided if Monitoring Service is down:** Monitoring service is not considered in Weighted Round Robin and Weighted Least Connection load balancing types, but if session team is using Adaptive load balancing and monitoring service is not running on specific Session Host Server then sessions from that session host server will be skipped.

**Default Teams (Concept and Usage)**

As specified in [Organization](#) section, that every organization has two default session teams: one for Windows session host servers and other for Linux session host servers:

- Default team cannot be deleted.
- If any session team is deleted, then all session host servers of that team are moved to default teams.

**Default Team Configurations**

The default configurations of default team in root (default) organization is as follows:

1. Team Name: Windows Default/ Linux Default

**Note:**

- If the organization is admin created organization, then the name of default team of that organization will follow below naming convention: Default Team_<OrgName> e.g. if organization name is Accops, then name of the default team of organization Accops will be: Default Team Accops.
- Modifying the organization name does not modify the name of default team.

2. Team Type: Shared Session Host (Read-Only)
3. Load Balancing Type: Weighted Round Robin
4. Use restrict session: Not enabled
5. Session Provider: List of session host servers (if any)

**Viewing Session Team Members and Management Options**

Clicking on the session team name, opens page displaying all member session host servers and displaying some essential information to administrator:

1. At Title bar along with team name, load balancing type is specified
2. Displaying lists of session host servers with following details:
   a. **Name:** Name of session host server
   b. **Address:** IP or hostname of session host server
   c. **Version:** Version of HyWorks Session Host Server module
   d. **Server Status:** If session host server is reachable on specified RDP port
   e. **Session Host Agent Status:** If session host server module is up and running
   f. **Monitoring Service Status:** Reachability of monitoring service from HyWorks Controller
   g. **Sessions:** Number of HyWorks sessions on session host server
   h. **CPU (%):** CPU (%) usage on session host server
   i. **RAM (%):** RAM (%) usage on session host server
   j. **Disk (%):** Disk (%) utilization on session host server
   k. **Score:** Current score of session host server (Calculated and displayed for load balancing types, Weighted Least Connection and Adaptive)
   l. **Weight:** Weight of session host server (Weight is configured while adding session host server into team with load balancing type as Weighted Round Robin or Weighted Least Connection.

Administrator can use this information to analyze the overall status of the session host server, especially information of statuses, sessions, resource (RAM, CPU and Disk) is important and should be monitored regularly.

**Session Host Server Operations from Session Teams Page**
Following options can be performed on Session Host Servers from Session Teams page:
   1. Upgrade Session Host Server
   2. Download Session Host Server Logs

**Upgrade Session Host Server**
Session Host Servers upgrade can be initiated from HyWorks Controller Management Console. Following prerequisites should be fulfilled to perform session host upgrade successfully from management console:

**Prerequisites:**
   1. Session Host Server Agent is up and running
   2. Session host upgrade file is available on HyWorks Controller (Usually copied during HyWorks Controller upgrade, but if provided separately, then should be copied at the following location: <HyWorks Controller Installation Directory>/Accops/HyWorks/Service/SessionHost/
   
   Below is the default location:
   C:\Program Files (x86)\Accops\HyWorks\Service\SessionHost

**Upgrade Process:**
Once all the prerequisites are fulfilled, upgrade process is very simple as described below:
   1. Select session host server to be upgraded from the list
   2. Click on button Upgrade SHS
3. **Confirm Action** dialog will be displayed, with following details:
   a. If remote sessions exist on selected session host server, then it will prompt error for remote sessions and administrator must remove all sessions from server before initiating upgrade.
   b. If no remote sessions exist on session host server then **Confirm Action** dialog will be displayed.

   **Note:**
   - Having existing remote sessions on session host server could affect installation of HyWorks components and it's recommended to logout all sessions before upgrade
   - Once upgrade is initiated no more sessions will be allowed on the respective session host server.

4. Confirm the upgrade option by clicking on **Upgrade** button
5. All remote sessions will be removed, and upgrade will be initiated
   a. Refresh the session teams page to check the status of session host server upgrade
   b. Session host server will go into maintenance mode for upgrade to avoid any connection requests during upgrade and after successful upgrade
6. Version of session host server should now be displaying newer version.
7. Check logs for more details on session host upgrade

**Download Session Host Server Logs**
Administrator can download the session host server logs from Session Teams page. To download session host server logs, follow the below steps:
1. Go to **Server – Session Teams** page
2. Click on Session Team name to view list of session host servers
3. Select the session host server
4. Click on button **Download Logs**
5. Logs will be downloaded in zipped format and success status will be shown.

**Add New Session Team**
Follow the below steps to add a new session team:
1. Go to **Server – Session Teams** page
2. Click on **Add Team** button to launch **Add Session Team** wizard
3. Provide the following details in **Session Team Basic Info** tab:
   a. **Team for:** Select from option Windows/ Linux based on type of session host servers to be added into this team
   b. **Team Name:** Any logical name for the new session team, following special characters are supported in Team Name field: _ SPACE () {} # @ : -
   c. **Team Type:** Read-only field and default value is Shared Session Host
4. Following details to be filled in **Load Balancing** tab
a. **Load Balancing Type**: Select appropriate Load Balancing Type, following types of load balancing is supported
   i. **Weighted Round Robin**
   ii. **Weighted Least Connection**
   iii. **Adaptive**
   Please see section [HyWorks Session Team Load Balancing](#) for more details.

b. Use Restrict Session: Enable **Use Restrict Session** option to stop providing sessions from session host server reaching the either of the following two configurations
   i. CPU Max Limit
   ii. RAM Max Limit

5. Click on **Save** button to save the session team
6. New session team will be created and will be displayed in Session Teams page. The team now will also be displayed in Session Provider section while adding the Shared Session Host.

### Modify Session Team
Administrator can modify the session team configurations as well by following the below steps:

1. Go to **Server – Session Teams** page
2. Select session team to be modified
3. Click on **Edit** button
4. Change the configurations as needed in **Edit Session Team** wizard, following configurations can be changed:
   a. Session Team Basic Info tab:
      i. Team Name
   b. Load Balancing tab:
      i. Load Balancing Type
      ii. Use Restrict Session
5. Click on **Save** button to save the changes
6. Session teams’ configurations will be modified, and controller will start using new configurations from next session.
7. Team information will be updated in all associated configurations e.g. Session Providers, Desktop Pools etc.

### Impact of Changing Session Team Configurations
Changing Load Balancing Type could affect the configuration of the member session host servers in the following manner. Consider the following scenario:

1. Two session host servers are added into a session team (with adaptive Load balancing).

### Note:
- Adding session host servers into Adaptive load balancing team, it does not require any weight configuration, on the other hand configuration of Weighted Round Robin or Weighted Least Connection requires weight configuration.
2. Now if administrator is changing the load balancing type from Adaptive to Weighted Round Robin or Weighted Least Connection then session host servers will be required to have some weight configuration.

3. **Impact on Member Session Providers:** Default weight of a session host server will be set to 100 in following conditions
   a. *Load Balancing Type* of session team is changed from *Adaptive* to *Weighted Least Connection*
   b. *Load Balancing Type* of session team is changed from *Adaptive* to *Weighted Round Robin*

4. **Impact on Associated Users (Built-In):** No adverse impact is expected on user/group configuration.

5. **Impact on running session:** No adverse effect is expected

6. **Impact on Built-in User Association:** No adverse effect

7. **Impact on Desktop Pools:** No adverse effect

### Delete Session Team
Administrator can delete a session team from Session Teams sub-section using following steps:

8. Go to *Server – Session Teams* page
9. Select session team to be modified
10. Click on *Delete* button
11. **Confirm Action** dialog will be displayed, click on *Delete* button to continue deleting the session team.
12. Session Team will be deleted and following impact could be there:
   a. **Impact on Member Session Providers:**
      i. Session host servers, members of deleted session team will move to Default session team
      ii. Default weight of a session host servers will be set to 100 in following conditions
         1. Admin configured session team with *Load Balancing Type* as *Adaptive* is deleted and default team is of type *Weighted Least Connection*
         2. Admin configured session team with *load balancing type* as *Adaptive* is deleted and default team is of type *Weighted Round Robin*
   b. **Impact on Associated Desktop Pools:**
      i. Desktop Pools will be deleted, and users won’t be able to get new sessions from the same team (member session host servers) any more
      ii. Running sessions won’t get disconnected/ removed
   c. **Impact on Applications:**
      i. Applications and entitlements will remain same
   d. **Impact on Built-in users:**
      i. Built-in Users association with session team will be deleted and thus the user accounts won’t be able to get any new sessions. Pl. Note this behavior is for Built-in users only.

### Add Session Host Server into Session Team
Session Host servers can be added into session teams from Session Provider section using *Add* or *Edit Session Provider* wizards.
Session host servers will get added to session team selected in Add/Edit Session Provider wizard – Session Team dropdown.

Applications Delivery

Applications sub-section in Workspace can be used to Add/View/Update/Delete Applications.

Publish (Add) Applications

Prerequisites: For creating any new application for end users, it is necessary to have following pre-configurations to be done on HyWorks Controller

- HyWorks Session Host Server is already configured as Session Provider. Refer section Shared Session Host Management for detailed information on adding and managing session host servers in HyWorks.

Use the below steps to configure applications:

1. Launch browser and open Primary HyWorks Controller Management Console
2. Login using Organization administrator credentials and selecting appropriate organization
3. Go to Configuration -> Workspace -> Applications section
4. Click on Add ‘+’ button to invoke the Add Application wizard
5. In Add Application Wizard, first tab is Application Information. Provide the following details
   a. Application Platform set as Windows for publishing and delivering application from Windows session host servers and set as Linux for publishing and delivering application from Linux session host servers
   b. Application Display Name to be displayed to user *Mandatory Field
   c. Application Path: Full path of the application exe *Mandatory Field
   d. Application Internal Name: Actual internal name of the application *Mandatory Field
   e. Application Description: Optional description of the application
   f. Application Command Line: Optional command line parameter to be used while launching the application
   g. Application Status: Enabled/ Disabled, disabled applications are not shown to the users though assigned.
   h. Application Icon:
      i. Get Icon Automatically: To use icon fetched from application exe
      ii. Use Default Icon: Use Accops HyWorks Default Icon
      iii. Use Custom Icon: To browser and fetch custom icon for the application

Note:

➢ Application details (Full Path/ Internal Name and Icon) will be fetched automatically, when administrator will type the application exe path and will move to the next tab (using key entry Tab or by using Mouse click). Refer Section: Get Application Details by Providing Full Application Path
   o This does not work for applications from
➢ Administrator can also navigate to configured Session Host Server directory to browse and get the application details. See section: Browse Application in Session Host Server Directory

6. Click on Next button to proceed to Additional Settings section
7. In **Additional Settings** tab, following configurations can be done:
   a. **Folder Information**: Create a new folder or select an existing folder, under which the application will be displayed on client side.
   b. **Launch Settings**: Following launch settings can be configured as per requirement
      i. **Specify Connection Profile**: To be configured if any specific connection profile must be used for application access. Please refer section, Application Specific Connection Profile for more details.
      ii. **Virtualization Profile**: If this application should use any specific Virtualization profile to support Virtual IP.
      iii. **Limit Total Concurrent Sessions**: Specify the total number of concurrent sessions to be allowed for the application.
      iv. **Limit Total Concurrent Sessions per server**: Specify total number of concurrent sessions per server should be allowed.
      v. **Limit Single Instance per user**: Specify if only single instance of application should be allowed for one user. If checked, user will be able to access
      vi. **Auto Launch**: If application should be auto-launched as soon as the user logs-in.
   c. **Access Settings**: Defines from where application can be accessible. Following options are available for **Publish the Applications on**:
      i. **Portal and Client**: Select this option to publish applications to be shown on client and HyLite.
         1. **Add to Favorites**: To specify if Application should be listed in **Favorites** Folder on client side.
      ii. **Create Desktop shortcut**: To specify if application shortcut should be created on
         1. **On User PC**: Along with publishing applications on client and portal, applications shortcuts can be created on user PC. Selecting this option will create application shortcuts on user desktops
         2. **On Shared Hosted Desktop**: With desktop customization or HyShell is enabled on session host servers, this published application shortcuts will be created in user’s desktop on shared hosted desktop. Refer **HyShell** section for more information on this.
      iii. **Pin Applications to Start Menu**: To specify if application start menu shortcut should be created or not. The deletion of **Start Menu Shortcuts** will be handled using Organization realm settings.
         1. **On User PC**: Selecting this option will pin application shortcuts on user desktops
         2. **On Shared Hosted Desktop**: Select this option to pin application shortcuts on shared hosted desktop. Refer **HyShell** section for more information on this.

8. Click on **Next** button to proceed to **Select Servers** section
9. In **Select Servers** section, select the servers from which the application can be published. Please refer section Server Selection for Application publishing on detailed information.
   The wizard by default verifies if published application is available or not on the defined path. If the application is not available on the provided path, Select Servers tab can be used to browse to the application directory as well.
10. Click on **Next** button to proceed to **Entitlements** tab
11. **Entitlements** tab can be used to modify the assignments of the applications to users, groups or OUs.
   a. To add new entitlements, click on **Add** button to open **Available Clients** dialog
i. Search with appropriate string to get required users/ groups, OUs or Pools
   ii. Select Users/ Groups/ OUs or Pools (User based)

   b. To remove existing entitlements, select the user/group/OU and click on button **Remove**
   c. Administrator can also search already added clients in the **Entitlements** tab of
      Application wizard

12. Click on **Save** button to complete the application creation process.
13. Once application is saved, administrator will be navigated back to the Applications section and
    application will be listed.
14. Use all the steps mentioned in this section to publish multiple applications to be used by end
    users.

Now we have all the required applications published correctly. The next section will provide steps to
creating users locally and on respective RDS server (syncing), making entitlements.

### Application Publishing Facts and Concepts

#### Browse Application in Session Host Server Directory

1. Select **Session Team** using dropdown in **Browse Application Details** section
2. Select RDS Server from next dropdown screen
3. Click on **Browse** button to open **File System** dialog
4. In **File System** dialog, click on any displayed drive to navigate to application path
5. Navigate to the folder where application exe can be found and select the application.exe (Google
   chrome application is selected in below image)
   a. It will automatically fetch the icon and will show success message in the same dialog
   b. Click on **Get Details** button to go back to **Add Application** wizard
6. **Application Path** and **Application Internal Name** will get filled automatically

#### Get Application Details by Typing Full Application Path

An additional shortcut method is also available to get application details automatically, following steps
can be used to get all the application details automatically:

1. In **Add Application** wizard
   a. Type the full path of the exe in **Application Path** field
   b. Change the focus using tab or mouse click on some other field
2. All the application details (Full Path/ Internal Name and Icon) will be fetched automatically

#### Server Selection for Application publishing

1. The list of servers includes all the session host servers added in the current organization
2. If the selected servers are members of session team, then while providing the application session,
   server will be selected as per load balancing mechanism
3. If the selected servers do not belong to the same session team, then it won’t follow any load
   balancing mechanism and session can be given from any server
   a. If the Authorization server is built-in, then the session for the session will be provided
      from the session host server from which the user belongs to.
4. While selecting a server which does not have the application installed, will be shown with a cross (X) and should not be selected.
   a. Selecting such server will continue to give application from the server and then may result in failed session when given from server.

**Application Specific Connection Profile**

In HyWorks deployment, if any specific connection profile must be used for an application then that can be done by specifying the connection profile for the application.

Application specific connection profile takes priority only when

1. When the access mode in connection profile is selected as Shell mode
2. In case of Remote App mode, application specific connection profile will only be used if that application is the first from the specific session host server. If the application is accessed after invoking any other application, applying new connection profile, won’t be possible.

Connection profile for an application can be specified in Additional Settings section of Add or Edit Application wizard.

**Application in Shell and RemoteApp mode**

In HyWorks, applications can be accessed in RemoteApp or Shell mode, which are briefly explained below:

- **Shell mode:** In shell mode, published application is opened in shell (Black background) where only accessed application will be shown. For each application instance a separate RDS session is created.
  - Shell mode is more user friendly in HyLite, which creates a new tab for new RDS session and thus different applications are available in different tabs.
  - Shell mode is recommended while being accessed from HyWorks client for Linux or MAC platforms

- **RemoteApp mode:** Seamless application mode, which appears like native applications. Multiple instances of applications in RemoteApp mode can be opened from single RDS session.
  - Remote App mode gives better user experience while being accessed from HyWorks Client on Windows platforms.

**How to enable Shell/RemoteApp mode:** To enable specific mode, configure a connection profile having specific mode and then assign it to application.

In case, where only Windows based clients are there default profile can be used with RemoteApp mode and similarly cases where only HyLite based deployment is preferred, connection profile can be modified to use Shell mode

**Always Seamless and Never Seamless Access Experience**

Seamless mode refers to access experience where user is shown progress bar until its session gets prepared on session host server and thus user gets a seamless experience.

Never Seamless mode displays a window with all session loading information showing always and post launch of application the window will still be there as a parent window.

**Use Cases for configuring never seamless mode:**

1. Application launch is not working
2. User input is needed for completing logon process but with seamless mode is not showing that and thus session fails to launch application

**How to configure Never Seamless mode**

1. Add/Edit connection profile
2. Go to *Application Access Settings* screen
3. Set *Session Experience Option* as *Never Seamless*

**Using Folders to Categorize Application**

Administrator can choose to categorize the application, as how they will be shown on client side using putting applications in a container referred as *Folder*.

1. Folders can be created or modified in *Create Application* or *Edit Application* wizard only. To create a new folder, select option *Create New* in *Folder Information* section and provide appropriate name for the folder.
2. To use an existing folder, select option *Use Existing*, in *Folder Information* section in *Additional Settings* screen of *Add* or *Edit Application* wizard. All existing folder names will be displayed in dropdown list.
3. Administrator can choose to edit an existing folder by clicking on *Edit* button. The folder name will be modified with new folder name provided in *Edit Folder* wizard.

When user logs in from HyWorks Client, the applications will be shown in respective folders only.

![Image of Accops HyWorks Client](image)

Please note, once created, folders cannot be deleted. However, applications can easily be moved out by selecting folder as None.

**Publishing Application for Shared Hosted Desktops only/ Desktop Customization/ HyShell**

In deployments, if users must be given full desktop access but at the same time display the applications which are published to it. HyWorks desktop customization can be used.

Desktop customization refers to process, where user session on shared hosted desktop will be customized to show application shortcuts on desktop and start menu for ease of access.

To enable desktop customization following two changes must be done:

1. **Enable desktop customization on shared session hosts**
   a. Windows Session Host Servers:
i. Registry Location:
   \KEY\LOCAL\MACHINE\SOFTWARE\Accops\Controller\EDC\SESSIONHOST
ii. ISDESKTOPCUSTOMIZATIONENABLED set as TRUE
iii. Restart HyWorks Session Host service

b. Linux:
i. Connect to Linux SHD server via SSH Client (if ssh enabled) or console session
ii. Open HyShell configuration file
   ```
sudo vi /etc/edcdvm/linuxDVM/hyShell/hyshell.config
   ```
iii. Set the value for IS_HYSHELL_ENABLED to 1.
iv. Restart DVM Agent Service, by using following command,
   ```
sudo systemctl restart edcdvm
   ```

2. Configure Applications for HyShell
While HyShell has been enabled on shared session hosts, applications can be configured to be enabled for HyShell, follow the below steps:

a. In Application Add/Edit wizard, go to Additional Settings screen
b. In section Access Settings: Defines from where application can be accessible. Following options are available for Publish the Applications on:
   i. Create Desktop shortcut
      1. On Shared Hosted Desktop: With desktop customization or HyShell is enabled on session host servers, this published application shortcuts will be created in user’s desktop on shared hosted desktop. Refer HyShell section for more information on this.
   ii. Pin Applications to Start Menu:
      1. On Shared Hosted Desktop: Select this option to pin application shortcuts on shared hosted desktop. Refer HyShell section for more information on this.

c. Save the application and desktop shortcuts in user session on session host server will be created.

Note:
- HyShell supports only those application shortcuts in session, which are assigned to user and published from this server. If any application is not available or published on current server it will not create the shortcut.

View, Edit, Copy or Delete Applications
From Applications tab, administrator will be able to view the details of existing applications, edit an existing application, delete an existing application or copy the application.

View Published Application Lists
Go to Workspace -> Applications page to view list of published applications. The tabular list provides following information

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Application Name</td>
<td>Displays the name of application</td>
</tr>
<tr>
<td>2</td>
<td>Folder Name</td>
<td>If application is kept under specific folder</td>
</tr>
<tr>
<td>3</td>
<td>Description</td>
<td>Application description</td>
</tr>
<tr>
<td>4</td>
<td>Session Settings</td>
<td>Connection profile, if any specific connection profile is provided</td>
</tr>
<tr>
<td></td>
<td>Application Status</td>
<td>Enabled/ Disabled</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5</td>
<td><strong>Application Status</strong></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><strong>Defined In</strong></td>
<td>If application is defined in current organization level. “This” means application has been published in current organization</td>
</tr>
<tr>
<td>7</td>
<td><strong>Application Platform</strong></td>
<td>Windows or Linux as icon</td>
</tr>
</tbody>
</table>

**View Application Configurations**

Clicking on Application Name from the application list or selecting an application and clicking on View Details button opens the application in read only mode.

Applications cannot be modified in read-only mode. Clicking on Edit button enables administrator to modify application from read-only mode.

**Edit Applications**

To modify the configurations of an existing application, Edit Application wizard can be used. Applications can be opened in Edit mode, following two methods can be used:

1. Select application and click on Edit button
2. Open application in read-only mode and then click on Edit button (See section View Details for reference.)

**Copy Application**

Copying an application enables administrator to easily clone the same application with all similar configurations and entitlements.

To copy an application, follow the below steps:

1. Select application from the list and click on Copy button.
2. **Copy Application** dialog will be displayed to provide new name for the new application. Default name uses format: Application Name-Copy.
3. Provide appropriate name and click on Save button.
4. New application will be created by cloning an existing application with the provided name and will be displayed in the list.
   a. Application copy operation creates exact same application with all configuration from source application, which can be later modified to change few settings.

**Delete Application**

Existing applications can be deleted by selecting the application and clicking on Delete button.

Confirm Action dialog will be displayed, click on Delete button to continue deleting the application.

Deleting an application will have the following impact on different user sessions:

1. **New Sessions:** Users on fresh logon won't be displayed with deleted applications
2. **Existing Sessions:**
   a. User who have already logged-in
      i. Deleted application will be deleted on refreshing the application list
      ii. On clicking on application name, error ‘No Apps found’ will be displayed
   b. Users with running sessions of the applications will continue to use the application, until user logs out or session expires as per configured timeouts.
**Disabling Application**

Instead of deleting an application, application can be marked as **Disabled**. Disabling an application can have similar impact as deleting, except application can be enabled in future with same configurations.

**Impact of disabling an application:**

1. New Sessions: Users on fresh logon won’t be displayed with disabled applications
2. Existing Sessions:
   a. User who have already logged-in
      i. Disabled application will be disappeared on refreshing the application list
      ii. On clicking on application name, error ‘Application is disabled by administrator’ will be displayed
   b. Users with running sessions of the applications will continue to use the application, until user logs out or session expires as per configured timeouts.

To disable an application, following steps can be used:

1. In Add Application wizard, keep **Application Status** as Disabled.
2. Select application -> Click on **Edit** button -> In Edit application wizard -> Set **Application Status** as disabled.

**Application Entitlements Management**

Entitlements section under Configuration can be used to manage application and connection profile assignments to following objects:

- Users
- Groups
- OUs
- Pools

This section will describe the entitlements management for these objects.

**Users**

**Users** section in Entitlements displays the current entitlements to the users and can be used to manage entitlements and connection profile assignments.

**Viewing User Entitlements**

Navigating to Users tab in Entitlements screen, displays the list of Users having one or more application entitlements or having assigned connection profiles.

Following information is displayed in respective columns:

1. Username: Username of the user
2. Connection Profile: Assigned connection profile
3. No. of Applications: Number of applications assigned to selected user
4. Authorization Server: Auth server details from where users are fetched

Administrator from Users section under Entitlements, can also search user entitlements by providing appropriate search string in the provided search box.

**Viewing Entitlements of a Single User**

To view entitlements of any specific user:
1. Select a single user from Users list and click on **View Details** button or click on username
2. All entitlements to the user will be displayed in following two sections
   a. Applications directly assigned to the user
   b. Application assigned to the user through group or OU

**Note:**

➢ From **Users** tab in **Entitlements** section, applications directly assigned to user can be deleted.
➢ On client side, only the final set of applications (removing duplicate assignments through groups or OUs) are shown.

**Add User Entitlements**

To add new user entitlements, follow the below process:

1. Go to Entitlements -> Users section
2. Click on **Add Entitlement** button
3. In Users – Add Entitlement wizard
   a. Click on Add Users button
   b. Available Clients dialog will be displayed, search with appropriate search string to get users list
   c. Select intended users and click on OK button
   d. Selected users will be added in Add Entitlements wizard
4. Click on **Next** button to proceed to **Applications** screen
5. In **Application** screen, select applications to be assigned to selected user(s)
6. Click on **Next** button to proceed to **Connection Profiles** screen
7. In **Connection Profiles** screen
   a. Select any appropriate connection profile to be assigned to users
   b. Keep connection profiles unchecked if no specific connection profile must be assigned
8. Click on **Save** button to save the entitlements
9. All user entitlements will be saved and now the Users screen will start displaying the list of users having entitlements.
10. On logon, user will be displayed with updated list of applications.

**Edit User Entitlement**

Like adding user entitlements, administrator can also modify the user entitlements as well. To modify entitlements of a user:

1. Select a single user from Users list and click on **Edit Entitlement** button
2. List of assigned applications will be displayed with selected checkboxes and unassigned applications will be listed with unchecked checkboxes
3. Select or deselect applications as per requirement
4. Click on **Save** button to save entitlement changes
5. Application entitlements will be updated and user entry in entitlements list will now be displayed with respective application count.
6. On new logon, user will be displayed with updated list of applications.
**Remove Entitlement**
A user’s entitlements can be removed from using following steps:

1. Select a single user from Users list and click on *Remove Entitlement* button
2. **Confirm Action** dialog will be displayed, click on *Delete* button to continue removing the entitlements
3. User entitlements will be removed and if user is not assigned with connection profile, its entry from Users section under Entitlements will also be removed.

**Note:**
- Entry of a user/group or OU in Entitlements section remains until it is assigned with at least on application or it is assigned with connection profile.

**Assign Profile**
Administrator can also assign any specific connection profile to one or more users by following the below steps:

1. Select one, more or all users displayed in *Users* section under Entitlements
2. Click on button *Assign Profile*
3. **Connection Profiles** dialog will be displayed with list of connection profiles
4. Select appropriate connection profile and click on *Save* button
5. Connection profile will be assigned to all the users selected and on next logon connection profile will be applied in user session.

**Unassign Profile**
Like assigning profile, administrator can also unassign connection profile from a single user, multiple users or all users listed in *Users* section under Entitlements. Follow the below steps to unassign connection profiles from user entitlements:

1. Select one, more or all users displayed in *Users* section under Entitlements
2. Click on button *Unassign Profile*
3. Connection profile will be unassigned and now users will be listed with no connection profile entry against them

**Note:**
- If users are not having any entitlements, then on Unassigning the connection profiles, their entry from Entitlements section will be removed.

**Groups**
*Groups* section in *Entitlements* displays the current entitlements to the groups and can be used to manage entitlements and connection profile assignments.

All operations for group based entitlements remain same as specified in section *Users* above.

Following operations on group entitlements can be performed:

1. View List of Group Entitlements
2. View Application Entitlements of a group
3. Add Group Entitlement
4. Edit Group Entitlement
5. Remove Group Entitlement
6. Assign Profile
7. Unassign Profile

Note:
➢ In HyWorks v3.0, group-based entitlements are not supported for Open LDAP or Novell eDirectory authentication servers.

**OUs**

**OUs** section in *Entitlements* displays the current entitlements to the OUs and can be used to manage entitlements and connection profile assignments.

All operations for OUs based entitlements remain same as specified in section *Users* above.

Following operations on OUs entitlements can be performed:

1. View List of OUs Entitlements
2. View Application Entitlements of an OU
3. Add OU Entitlement
4. Edit OU Entitlement
5. Remove OU Entitlement
6. Assign Profile
7. Unassign Profile

**Pools**

Direct application entitlements to a desktop pool can be managed from *Pools* section under *Entitlements*, if it satisfies the following conditions:

1. If it’s a USER BASED desktop pool
2. It’s a shared virtual desktop pool

Making the entitlements to desktop pool, indirectly assigns the applications to all the users belonging to the desktop pool.

All operations for Pools based entitlements remain same as specified in section *Users* above.

Following operations on Pools entitlements can be performed:

1. View List of Pools Entitlements
2. View Application Entitlements of a Desktop Pool
3. Add Pool Entitlement
4. Edit Pool Entitlement
5. Remove Pool Entitlement
6. Assign Profile
7. Unassign Profile
This section will give detailed information of these server configurations.

**Application Sessions Management**
Now all details to provide applications are already covered in previous sections, this section will provide details of administrating application sessions.

**Application access details in User Sessions**
Whenever a user connects to HyWorks and accesses any published applications, it is reflected as a count in User Sessions page, e.g. a user has initiated 3 application instances then *Application Sessions* column will show as 3.

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Username</td>
<td>Displays the username of the logged in user</td>
</tr>
</tbody>
</table>
2. IP Address | IP address of the server from app session is provided
3. Session ID | Remote Desktop Server session id of the user
4. No of Applications | Count of application sessions
5. Status | Status of User session, which could be Running/Initializing/Disconnected

Clicking on username, expands the details of app sessions running for the user and following information is displayed for application sessions:

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Application Name</td>
<td>Display name of the application, accessed by user</td>
</tr>
<tr>
<td>2</td>
<td>Server name</td>
<td>Name of session host server on which remote session (app session) is running in</td>
</tr>
<tr>
<td>3</td>
<td>Status</td>
<td>Status of app session, which could be Running/Initializing/Disconnected</td>
</tr>
</tbody>
</table>

**Application Session Removal**
Administrator can choose to remove specific application sessions and the section enables administrator to remove all the application sessions from all session host servers or terminate specific application sessions.

1. **Terminate Specific Application Session**: To terminate specific application session for a user, below mentioned steps can be used:
   1. Go to Monitoring – Sessions – App Sessions
   2. Click on Username (User whose application session needs to be terminated)
   3. This will expand and display the list of the application sessions running for the user
   4. Select the application needs to be closed
   5. Click on button **Remove App Session(s)**
   6. On Confirm Action dialog,
      a. Select option Show message to specify custom message to be displayed to user while terminating the app session
      b. Specify Wait Time in minutes to allow user to keep the session for the specified time
      c. Click on **Remove** button
   7. Selected remote app session will be closed and user will be notified as per specified options in **Confirm Action** dialog

Administrator can opt to remove single or multiple app sessions at a time.

2. **Terminate Provider Session or Remove RDS Sessions of a user**: In certain situations, administrator can opt to remove all application sessions of a user, termed as provider session removal. To remove provider session of a user, following steps can be used:
   1. Go to Monitoring – Sessions – App Sessions
   2. Select the Username (User whose application sessions/ provider sessions need to be removed)
   3. Click on button **Terminate Process(s)**
4. Click on **Remove** button on **Confirm Action** dialog
5. User remote session from all the session host servers will be completely removed.

**Shared Hosted Desktop Delivery**

To provide shared hosted desktop access to end-users, configured session host servers can be used in shared hosted desktop pools. This section will provide detailed information on how shared hosted desktop can be delivered and managed in HyWorks Controller.

**Creating a Shared Hosted Desktop Pool**

HyWorks v3.0, supports shared hosted desktop deliveries from a load balanced team of session host servers and creating a shared hosted desktop pool will require following requisites to be preconfigured in HyWorks:

**Shared Hosted Desktop Pools Pre-Requisites**

For creating a Desktop Pool following pre-requisites must be configured:

- **Reachable Shared Session Provider** (i.e. HyWorks Session Host Server) is configured
- **Authorization/Authentication Server** is configured (If User based pool need to be created) and post pool creation for authenticating the user session
- **Registered Devices in** HyWorks Controller (If Device based pool needs to be created): As shown in image below the devices are registered, renamed for better identification

Once above pre-requisites are configured in HyWorks Controller, administrator can proceed with Desktop Pool creation.

**Shared Hosted Desktop Pool Creation Process**

Considering that all session host servers are configured in appropriate session teams, following steps can be followed to create a shared hosted desktop pool:

- Login to HyWorks Controller Management Console using appropriate admin credentials
- Go to **Workspace** -> **Desktop Pools** tab
- In **Desktop Pools** screen, click on **Add New Pool** button
- **Add Desktop Pool** wizard will be launched
- In **General** screen, provide the following details to proceed:
  a. **Name**: Mandatory field* for providing logical name for Desktop Pool which will be used to identify Desktop Pool.
     i. Two desktop pools with same name cannot exist in HyWorks organization).
     ii. Only following special characters are supported: _ SPACE () {} # @ : -
  b. **Description**: Optional field for logical description for desktop pool, can be used by administrator to define Desktop Pool’s purpose and associated details.
  c. **Entitlement Type**: Defines the type of the clients to be configured and given access of desktop session. A Desktop in HyWorks deployment can be associated with a device or a user and thus Desktop Pools in HyWorks can be of two types:
     i. **Device Based**: Desktop Pools in which Desktops are assigned to devices and thus any valid user login from the device always gets the session of same Desktop which is assigned to the device from where user is logging-in.
     ii. **User Based**: Desktop Pools in which Desktops are assigned to users and thus a valid user logging-in from any device or location gets the session of same Desktop which is assigned to this user.
Entitlement Type selection in General screen also enables the corresponding client type screen in Desktop Pool wizard, e.g. Selecting Entitlement Type as Device based will enable Devices screen, where as selecting Entitlement Type as User based will enable Users screen (For configuring users as clients) (Refer below image)

d. Desktop Virtualization Type: Desktop Virtualization Type field describes the kind of desktops to be delivered to the clients. Select as Shared Hosted Desktop.
e. Connection Profiles: Connection profiles dropdown field can be used to use specific connection profile for this pool.
   i. On specifying connection profile, desktop connection will be provided as per configured profile
   ii. On specifying connection profile as None, applicable connection profile will be derived as per Connection Profile fallback model. Refer section Connection Profiles for more details on Connection Profile Fall Down model.
f. Active/ Inactive Pools: A Desktop Pool can be made active/ inactive from Add/Edit Desktop Pool wizard. When user logs-in, only active pools are searched for assignments, inactive pools are ignored while providing Desktops to clients (devices or users).
   i. To make a pool active, keep Active checkbox as selected in General screen of Desktop Pool wizard, uncheck Active checkbox for making a pool inactive.
g. Maintenance Mode: Shared hosted desktop pool can be put into maintenance mode to avoid any access from users during some configuration period. However, maintenance mode is more significant for dedicated desktop pools.

❖ Click on Next button to proceed
❖ Configure Clients in Desktop Pool
It’s important to understand that the client in Desktop Pools can be either a device or user and this is determined by Entitlement Type attribute in General Settings of Add Desktop Pool wizard.

a. Device based: Assuming administrator has selected Pool Type as Device based, which will now enable Devices screen in Add Desktop Pool wizard. Device screen provides following options to administrator:
   i. For adding devices to Desktop Pool, click on Add Device button. This will invoke Available Device Dialog
   ii. In Available Devices dialog, administrator has the following options
      1. Select Single, multiple or select all devices using respective checkboxes, click on OK button to add them in Desktop Pool.
      2. Administrator will be navigated back to Device screen with displaying all selected devices as added.

b. User based: *Recommended, if administrator wants to assign shared hosted desktop to users, then selecting Entitlement type as User based, Users screen to configure users as clients will be shown.
   i. For adding users to Desktop Pool, click on Add button. This will invoke Available Client Dialog
   ii. In Available Client dialog, search and select multiple users, groups, OUs from configured authentication server. Searching client provides some advance options for optimizing search queries:

Note:
➢ Groups or OUs are not supported with Workgroup and LDAP/Novell eDirectory type authentication servers and thus if configured authentication server is either of
Accops HyWorks v3.2 Administration

Workgroup or Novell eDirectory then Available Clients dialog will not display any group or OUs in respective tabs.

- **Client Type Selection:** Option to specify, the type of client to be searched, this could be user, group or OU
- **Search by Attribute:** Administrator can specify what search attribute to be used for searching the client e.g. for Microsoft Active Directory this search attribute could be SAM Account Name, Name or Display Name
- **Search Option:** Administrator can also specify the search option as Starts with, End With, Contains or Equals to narrow down the searches

❖ Click on *Next* button to proceed
❖ Configure *Client Groups* optionally, to restrict shared hosted desktop access to only those users which are connecting from specific LAN or WAN or MAC. Refer section *Client Groups* section To enable restricted client groups access,
  a. Select access policy as *From specific client groups only*
  b. It will list down all the added client groups
  c. Select client groups and move to allowed list.
❖ Save the desktop pool by clicking on *Finish* button
❖ User can login from respecting endpoints and they will be able to access shared hosted desktops.

**Important points for shared hosted desktop pools:**
➢ One session host server team can be used only once in HyWorks deployment and hence only one shared hosted desktop pool created for one session host server team.

**Managing Shared Hosted Desktop Pools**
This section will cover management of shared hosted desktops pool.

❖ **Viewing added desktop pools**
All added desktop pools are listed in Workspace -> Desktop Pools. The tabular listing provides following information about desktop pool:
Once Desktop Pools are created by providing appropriate details in *Add Desktop Pool* wizard, Desktop Pools page is refreshed and displays following information of configured Desktop Pools using different columns.

- **Pool Name and Type:**
  o Desktop Pool Name and Entitlement Type as provided in General screen
- **Provider/Team Name and Type**
  o Name of session provider or session host team
  o Type of session provider
- **Desktop Provisioning and Connection Profile**
  o Desktop Provisioning configuration as Deployed for dynamic and None
  o Connection Profile if configured else None
- **Assignment Life Span:** Permanent or Temporary
- **Desktops Ready**
  o Total number of ready Desktops
  o Not applicable (NA) for Microsoft RDS Server Desktop Pools
• **Desktops in Use**
  o Desktops already assigned or being used in session
  o Not applicable (NA) for Microsoft RDS Server Desktop Pools

• **Free Desktops**
  o Unassigned Desktops in Pool, available for assignments and connection

• **Status**
  o Ready (Normal font)
  o Ready in maintenance (Red Font)
  o Cloning Desktops (If provisioning is in progress, for dedicated desktops)

• **Active**
  o If Desktop Pool is active or not

❖ **Modifying Shared Hosted Desktop Pool**
As per requirement, administrator can modify shared hosted desktop pool using following steps:

1. Selected shared hosted desktop pool
2. Click on **Edit** button
3. Modify properties listed below, as per requirement
   - **Name:** Not critical and modifiable and changing pool name will not affect any end-user access
   - **Description:** Not critical and modifiable
   - **Entitlement Type:** Cannot be changed
   - **Desktop Pool Type:** Cannot be changed
   - **Server Team:** Critical and modifiable, as user will now be given connection of servers from new team
   - **Connection Profile:** Critical and modifiable, connection timeouts, experience is derived from connection profile so changing it can affect all users.
   - **Active/ Inactive:** Critical and modifiable, unchecking **Active** checkbox will deny any connection requests for this desktop pool.
   - **Maintenance Mode:** Critical and modifiable, enabling maintenance mode will stop user access but controller will keep on monitoring the desktop pools.
   - **Clients:** Critical and modifiable, added clients (Users or devices) can be removed or more clients can be added as per requirement. Removed clients will lose access to desktop pools and added clients will get access to
   - **Client Groups:** Critical and modifiable, restricting desktop pools with client groups will affect end-user access.
4. Click on **Finish** button to save settings

❖ **Delete Shared Hosted Desktop Pool**
Once shared hosted desktop pool is not in use, it can be deleted from HyWorks Controller.

1. Selected shared hosted desktop pool
2. Click on **Delete** button
3. Click on **Delete** button on **Confirm Action** dialog
4. Shared hosted desktop pool will be deleted
   a. It does not delete shared session host team or shared session hosts
Shared Hosted Desktop Session Management

**Shared Hosted Desktop access details in User Sessions**
Whenever a user connects to HyWorks and accesses any shared hosted desktops, it is reflected in User Sessions page, e.g. a user has initiated shared hosted desktop then *Virtual Desktop Session* column will show as **checked**.

![User Sessions](image)

**Desktop Sessions Detailed View and Management**
To view and manage shared hosted desktop session, go to Monitoring -> VDI Sessions section and it will provide following details:

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Username</td>
<td>Displays the username of the logged in user</td>
</tr>
<tr>
<td>2</td>
<td>Device Name</td>
<td>Displays the name of the device, if user has logged in from HyDesk or HyWorks Client</td>
</tr>
<tr>
<td>3</td>
<td>IP Address</td>
<td>IP address of the machine from where the user has logged in. In case of HyLite, this will be IP address of HySecure Gateway</td>
</tr>
<tr>
<td>4</td>
<td>Session Id</td>
<td>Remote Session Id on Session Host Server</td>
</tr>
<tr>
<td>5</td>
<td>Pool Name</td>
<td>Name of the desktop pool from where sessions are coming</td>
</tr>
<tr>
<td>6</td>
<td>Desktop Name</td>
<td>Name of session host server from which session has been provided</td>
</tr>
<tr>
<td>7</td>
<td>Desktop IP Address</td>
<td>IP Address of session host server from which session has been provided</td>
</tr>
<tr>
<td>8</td>
<td>Status</td>
<td>Status of the desktop session (Connected/ Disconnected)</td>
</tr>
<tr>
<td>9</td>
<td>Remote Control</td>
<td>If Remote Control is enabled for shared session hosts, button will be shown</td>
</tr>
</tbody>
</table>

❖ **Remove VDI Session**
To remove shared hosted desktop session:

1. Select VDI session
2. Click on button **Remove Session(s)**
3. In **Confirm Action** dialog, click on **Remove** button
4. User’s shared hosted desktop session will be removed from HyWorks as well as from respective session host server.
   a. All user’s unsaved data will be lost.
SHD and Application Delivery in Workgroup (Special Use case)

HyWorks supports workgroup deployment and the mechanism used is very user-friendly. But as workgroup environment does not have any centralized authentication mechanism and users exist locally on session host servers, some appropriate configurations must exist, which will be covered in this section.

Session Host Server – User Mapping

**Point# 1:** In workgroup environment as users are not centrally managed thus user accounts must be created on all possible session host servers from where application or SHD sessions can be given. This can be done easily using initiating user creation process in HyWorks explained in detail in [Built-In Directory Server and Local User Management](#) section.

**Point# 2:** However, while providing session HyWorks must check if user exist on target session host server or not and this is taken care by aligning users with session teams.

**Point# 3:** While publishing applications only session host servers are considered and thus it is not known if assigned users exist in session host server or not.

**Point# 4:** Thus, on user logon, HyWorks checks if application is published from session host server which is member of session team to which user is also added. While adding users from management console or using CSV administrator should specify specific session teams.

What does it mean:

In case a user account is not created on a session host server, but the user has access to an application published from that RDS server, the application will not be visible to the user.

HyWorks v3.0 or later has the support for feature of user to session host server and application mapping and access, where user will be displayed those applications which are coming for session host server to which the user belongs. E.g. consider the following configuration

- An organization has 4 session teams with each session team having 1 session host server
- User1 belong to Team1 (SHS1) so the user account is created (synched) only with SHS1
- App1 is published from all session host servers
- App2 is available only on SHS1
- App3 is available on SHS2, SHS3 and SHS4
- User is assigned all applications; App1, App2 and App3

When User1 logs in, user will see icons for only App1 and App2, as User belongs to SHS1 and applications App1 and App2 are from SHS1. Also, when user1 will access App1, its session will only come from SHS1 not from SHS2, SHS3 or SHS4.
Dedicated Desktop Delivery in HyWorks

HyWorks can be configured to deliver single user Windows or Linux desktop systems to end-users. Dedicated desktops delivery in HyWorks refers to the model where one desktop system is allocated to one user at a time only. For that delivery aspect, HyWorks support both Linux and Windows platforms. HyWorks can be used to delivery following dedicated desktops to end-users:

- Windows
  - a. Windows 10
  - b. Windows 8.1
  - c. Windows 7
- Linux
  - a. Ubuntu Gnome 16.04.3/4
  - b. CentOS 7.4.1708

In this section of HyWorks administration, following topics will be covered:

- Dedicated desktop delivery model in HyWorks
- Dedicated session provider configurations and management
- Desktop pools concepts, management and user cases
- Desktop management

Dedicated Desktop Delivery Model in HyWorks

As explained above, HyWorks can provide dedicated desktops to end-users. But to delivery these desktops, they must be hosted somewhere, these hosting servers are known as Hypervisors. Some popular Hypervisors are provided by VMware, Microsoft, Nutanix and many more. And now with cloud Azure/ AWS can also be used to host dedicated desktops. Each of such hypervisors uses its own technology to run operating systems as virtual machines and then these virtual machines can be given access to end-users.

HyWorks can connect to these hypervisors to fetch/provision virtual machines and then assign them to end-users, along with powerful management capabilities. Thus, HyWorks uses the below model to deliver desktops to end-users:

As per above model, to delivery desktops to end-users, administrator will be needed to

1. Manage dedicated session providers
2. Create desktop pools (Containers which contain dedicated desktops and clients) and manage those desktops and entitlements.
3. All these administration concepts will be covered in this section.
Dedicated Session Provider Management
Administrator will be able to add, update, delete and monitor dedicated session providers in HyWorks.

Supported Dedicated Session Providers
HyWorks supports hypervisors and management softwares from VMware, Microsoft and Nutanix, detailed information is provided in next section.

Provider Support Version vise
Below table provides information of types of dedicated provider supported and their respective supported versions

<table>
<thead>
<tr>
<th>Provider</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESXi</td>
<td>6.7  6.5  6.0  5.5  5.0 (May require additional patching)</td>
</tr>
<tr>
<td>VMware vCenter Server</td>
<td>6.7  6.5  6.0  5.5  5.0 (May require additional patching)</td>
</tr>
<tr>
<td>Microsoft Hyper-V (Core)</td>
<td>Windows 2016</td>
</tr>
<tr>
<td>Microsoft SCVMM</td>
<td>Windows 2016  Windows 2012R2</td>
</tr>
<tr>
<td>Nutanix AHV</td>
<td>PE v5.11  PE v5.10  PE v5.8.2</td>
</tr>
<tr>
<td>Nutanix Prism Central</td>
<td>PC v5.8.2</td>
</tr>
</tbody>
</table>

Functioning Support Provider vise
Dedicated desktops delivery can be done in various ways and thus they can be sub-divided into multiple functions. This section will briefly provide details of functional support of different providers

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sub Feature</th>
<th>Nutanix AHV</th>
<th>VMware</th>
<th>Microsoft</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Prism Central</td>
<td>Prism Element</td>
<td>vCenter Server</td>
</tr>
<tr>
<td>Deploy pool with existing VMs</td>
<td>Deploy pool with existing VMs</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Desktop VM Provisioning</td>
<td>Clone Type</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Full clone</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Add Dedicated Session Providers
Configuration of dedication session providers can be done from HyWorks Controller Management Console -> Server -> Session Providers section.

Add Microsoft Hyper-V/ SCVMMM as Dedicated Session Provider
Microsoft Hyper-V Servers are independent hypervisors from Microsoft, which can be used to host desktop virtual machines, whereas SCVMM (System Center Virtual Machine Manager) is top layer management server which can be used to manage multiple Hyper-V servers.

HyWorks Controller can be configured with both types of Microsoft Servers to deliver dedicated desktops to the end users. Following pre-requisites are must for configuring Microsoft Hyper-V or SCVMM in Dedicated Session Provider category:

Pre-requisites
1. **Hyper-V Server:**
   a. Running appropriate supported Hyper-V Server (2012R2, 2016 (GUI)/ 2016 (Core))
   b. **Accops Hyper-V Connector** is installed on Hyper-V server in Hyper-V mode, configured and reachable from HyWorks Controller (Please refer HyWorks Hyper-V Connector Installation Guide for reference)
      - Port 38864 is used to connect to VMware servers
2. **SCVMM Server:**
   a. Running appropriate supported SCVMM Server:
      - SCVMM 2016

<table>
<thead>
<tr>
<th>Clone from Snapshot</th>
<th>Clone from Snapshot</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>No</th>
<th>Yes (2016)</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk persistence</td>
<td>Persistent VM Deployment</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes (2016)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Non-persistent VM Deployment</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes (2016)</td>
<td>No</td>
</tr>
<tr>
<td>Desktop Power Operations</td>
<td>Desktop Power Operations</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OSes Support on Provider</td>
<td>Windows Desktops</td>
<td>Windows 7</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Windows 8.1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Windows 10</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Windows Servers</td>
<td>Windows 2012R2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Windows 2016</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Linux Desktops</td>
<td>CentOS 7</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Ubuntu 16</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
b. **Accops Hyper-V Connector** is installed on SCVMM server in **SCVMM** mode, configured and reachable from HyWorks Controller (Please refer **HyWorks Hyper-V Connector Installation Guide** for reference)

**Process to Add Microsoft Hyper-V or SCVMM Server as Dedicated Session Provider**

1. Go to Server – Session Providers section
2. Click on **Add** button to invoke **Add Session Provider** wizard
3. Select **Category** as **Dedicated Session Provider**
4. Select **Type** as **Microsoft Hyper-V/ SCVMM Server**
5. Provider a logical name in **Name** field
6. In **Host Address**, provide appropriate host address or IP (If providing host address then make sure it’s being resolved correctly from Controller)
7. **RDP Port:** Port number on which the desktop virtual machines can be accessed remotely,
   a. While providing connection settings to client HyWorks provides the same port as specified here
   b. HyWorks controller also checks configured port for accessibility of respective DVMs
   c. Please note it is **not** the port of session provider but the port on which hosted desktops will be reached
8. Select **Active** checkbox to make session provider as active. Desktops from inactive session providers are not considered while providing the sessions to end users.
9. Click on **Test Connection** button to check the configurations.
10. Once connection is successful, success message will be displayed and clicking on **Add** button will add Hyper-V or SCVMM server as dedicated session provider
11. Administrator will be able to see configured Hyper-V or SCVMM server in Session Providers screen with appropriate status.
12. Session Provider will be added, and HyWorks Controller will start synchronizing the data with configured Hyper-V or SCVMM Dedicated Session Provider.
13. Once synchronization is completed, Session Provider status will change to **Reachable** suggesting that HyWorks Controller has successfully connected to Dedicated Session Provider and fetched all desktops information.
   a. The added Dedicated Session Provider row will now display the Desktop count as well.
14. Now administrator create dedicated desktop pools using desktops from configured Hyper-V/ SCVMM dedicated session providers.

**Adding VMware/ vCenter Server as Dedicated Session Provider**

VMware ESXi servers are independent hypervisors from VMware, which can be used to host desktop virtual machines, whereas vCenter Server is top layer management server which can be used to manage multiple ESXi servers.

**Pre-requisites**

1. Supported version of VMware/ vCenter Server is up and running
   a. Port 443 is used to connect to VMware servers
2. Appropriate user credentials with adequate rights of VMware servers are available.
   a. Provided user must have appropriate rights to read all VMs information, create/ delete resource pools and virtual machine rights
b. If the configured user is not having enough privileges then it may fail the process of getting desktop details, performing power operations, provisioning etc.

**Process to Add VMware/ vCenter Server as Dedicated Session Provider**

1. Go to Server – Session Providers section
2. Click on Add button to invoke Add Session Provider wizard
3. Select Category as Dedicated Session Provider
4. Select Type as VMware/ vCenter Server
5. Provider a logical name in Name field
6. In Host Address, provide appropriate host address or IP (If providing host address then make sure it’s being resolved correctly from Controller) of VMware ESXi or vCenter Server
   a. Controller automatically detects, if it’s an independent ESXi server or a vCenter server.
7. **RDP Port:** Port number on which the desktop virtual machines can be accessed remotely,
   a. While providing connection settings to client HyWorks provides the same port as specified here
   b. HyWorks controller also checks configured port for accessibility of respective DVMs
   c. Please note it is not the port of session provider but the port on which hosted desktops will be reached
8. Provide user credentials to connect to VMware server
   a. User must have adequate rights as specified in pre-requisite
9. Select Active checkbox to make session provider as active. Desktops from inactive session providers are not considered while providing the sessions to end users.
10. Click on Test Connection button to check the configurations.
11. Once connection is successful, success message will be displayed and clicking on Add button will add VMware ESXi or vCenter server as dedicated session provider
12. Administrator will be able to see configured Hyper-V or SCVMM server in Session Providers screen with appropriate status.
13. Session Provider will be added, and HyWorks Controller will start synchronizing the data from VMware/ vCenter Server Dedicated Session Provider.
14. Once synchronization is completed, Session Provider status will change to Reachable.
   a. The added Dedicated Session Provider row will now display the Desktop count as well.
15. Dedicated Session Provider of type VMware is ready for providing dedicated desktops sessions to end users using existing or provisioned desktops.

**Adding Nutanix AHV as Dedicated Session Provider**

Nutanix AHV servers can be configured using same steps as VMware, where prism central or prism element can be configured.

**Pre-requisites**

1. Supported version of Nutanix prism central or prism elements are running and ready
   a. Port 9440 is used to connect Nutanix servers
2. Appropriate user credentials with adequate rights of Nutanix servers are available.
   a. Provided user must have appropriate rights to read all VMs information, create/ delete resource pools and virtual machine rights
b. If the configured user is not having enough privileges then it may fail the process of getting desktop details, performing power operations, provisioning etc.

**Process to Add Nutanix as Dedicated Session Provider**

16. Go to Server – Session Providers section
1. Click on *Add* button to invoke *Add Session Provider* wizard
2. Select *Category* as *Dedicated Session Provider*
3. Select *Type* as *Nutanix*
4. Provider a logical name in *Name* field
5. In *Host Address*, provide appropriate host address or IP (If providing host address then make sure it’s being resolved correctly from Controller) of VMware ESXi or vCenter Server
   a. Controller automatically detects, if it’s an independent ESXi server or a vCenter server.
6. **RDP Port:** Port number on which the desktop virtual machines can be accessed remotely,
   a. While providing connection settings to client HyWorks provides the same port as specified here
   b. HyWorks controller also checks configured port for accessibility of respective DVMs
   c. Please note it is **not** the port of session provider but the port on which hosted desktops will be reached
7. Provide user credentials to connect to VMware server
   a. User must have adequate rights as specified in pre-requisite
8. Select *Active* checkbox to make session provider as active. Desktops from inactive session providers are not considered while providing the sessions to end users.
9. Click on *Test Connection* button to check the configurations.
10. Once connection is successful, success message will be displayed and clicking on *Add* button will add VMware ESXi or vCenter server as dedicated session provider
11. Administrator will be able to see configured Hyper-V or SCVMM server in Session Providers screen with appropriate status.
12. Session Provider will be added, and HyWorks Controller will start synchronizing the data from VMware/ vCenter Server Dedicated Session Provider.
13. Once synchronization is completed, Session Provider status will change to Reachable.
   a. The added Dedicated Session Provider row will now display the Desktop count as well.
14. Dedicated Session Provider of type VMware is ready for providing dedicated desktops sessions to end users using existing or provisioned desktops.

**Deleting a Session Provider**

A session provider can be deleted once it is not being used further in HyWorks Controller configuration. Follow the below steps to delete a session provider:

1. Select session provider to be deleted and click on *Delete* button
2. *Confirm Action* dialog will be displayed stating all the consequences of deleting session provider.
3. Confirm the operation by clicking on *Delete* button on the confirmation dialog
4. Session provider will be deleted from HyWorks configuration with following impact.
Impact of Deleting Session Provider
Deleting a session provider can have following consequences:

- Deleting a Dedicated Session Provider may result in deletion of all associated data such desktop Pools, desktops and assignments from HyWorks. Therefore, it is highly recommended to be very cautious with session provider deletion. Running session may not be disconnected on client side but will be removed from controller side.
- On deletion of session provider, HyWorks does not delete any configured desktop VMs from respective session provider and thus any such residual must be cleaned up manually or any such desktop pools or desktops should be deleted before deleting session provider.

Modify a Configured Session Provider
Administrator can modify a configured Session Provider. But its important to understand what information can be updated and what could be the impact of updating an existing Session Provider:

Modifyable Fields and Impact
Editing an existing Session Provider, enables following fields for modifications:

- **Name**:
- **Host Address: Critical**: field and should be updated only when the same server has been migrated to different IP or host address as using this information only HyWorks Controller fetches the information of Desktops and assignments etc. If somehow the same server is not available on the same host address, then existing configuration may get corrupted. Administrator should be very cautious while updating host address field.
- **Username and Password (In case of Dedicated Session Provider - VMware/ vCenter Server or Nutanix): Critical**: field and should be updated only when the new user being provided has appropriate privileges on VMware/ vCenter Server. In case of updating with inappropriate user may result in ambiguous configuration.
- **Active: Critical**, it is already specified in configuration of each type of Session Provider that not selecting Active checkbox will mark the Session Provider as inactive and it will be ignored while fetching Desktop information for the client. Administrator should be cautious while marking any Session Provider as inactive as all associated clients will stop getting Desktops.

How to Modify Configured Session Provider
2. Select the session provider to be modified
3. Click on Edit button
4. Edit Session Provider dialog will be displayed
5. Update the fields as required and click on Update button.
6. Changes will be saved, and user’s sessions will be given from new session host servers.

Update Configured Session Provider to Update Desktop Provider Cache
HyWorks Controller keeps all details of desktop in its memory and refreshes this information in an hour. In some cases, if the details need to be updated immediately, updating session provider without changing any configuration can help.

The operation of updating Session Provider without modifying the information reestablishes the connection with Session Provider and re-synchronizes the data.

Periodic Updates:
Desktops cache for all configured Dedicated Session Providers (e.g. VMware ESXi/ vCenter Server, Microsoft Hyper-V/ SCVMM Server or Nutanix) is updated in every 60 minutes. The periodic update of Desktops cache helps in maintaining most recent list of available Desktops from Dedicated Session Provider.

**Marking Session Provider as Inactive**
Sometimes when session provider is not in use or some maintenance is going on, administrator can mark session provider is inactive. When a session provider is marked as inactive:

1. HyWorks does not sync or communicate with provider for updating any desktop details.
2. HyWorks will not process any desktop connections from inactive session provider

**Session Provider Section Status in Setup Page**
Based on the status of each of the configured Session Provider’s status overall status of Session Provider section is determined:

The following possible values may appear:

- **Not configured**: No Session Provider is configured (Color: Orange)
- **Need attention**: One of the configured Session Provider is not reachable (Color: Red)
- **Configured**: All the Session Providers are reachable (Color: Green)

If Session Provider status becomes unreachable post configuration, the status of Session Providers section will become need attention.

**Desktop Pools to Deliver Desktops to End-users**
The primary objective of HyWorks deployment is to provide desktop/ application sessions to its intended client. The client could be a device, a user, a group of users etc. and thus it is important to associate target desktops with appropriate clients.

**Desktop Pools** tab provides interface for creating and managing pools of Desktops and associating the Desktops to intended clients.

**Desktop Pool Categorization**
Desktop pools can be kept into distinct categories based on following factors:

- Desktop Virtualization Type
- Desktop Provisioning
- Entitlement Type
- Assignment Lifespan
As shown in above diagram, as per end-user needs multiple options are available in HyWorks to deliver desktops. Appropriate choices should be made to serve the purpose in most efficient manner. In section we will try to understand available options and their respective use cases.

❖ **Desktop Virtualization Type:** Administrator must choose what kind of virtualization type must be done, which can be:
  - **Persistent Virtual Desktops:** Dedicated desktops which will not be reverted to fresh state and will retain all changes done by user. Applicable for existing desktops and provisioned desktop pools
  - **Non persistent Virtual Desktops:** Applicable for provisioned desktops only, where changes done to desktop VMs by users will be reverted after users have logged-out.
  - **Shared Hosted Desktop:** For delivering shared hosted desktops to end-users

❖ **Desktop Provisioning:** HyWorks can deploy new virtual machine on respective session provider from a pre-configured gold image or source. The process is termed as desktop provisioning. Now if an environment is having VMs pre-existing then they can be re-used instead of deploying new. HyWorks can be used to deliver dedicated desktops to end-user. The choice is given during desktop pool creation as **Provisioning**, which can be set as:
  - **None:** To use pre-existing desktop VMs on session provider
  - **Dynamic:** To provision new VMs in desktop pool.

Once **Provisioning** is set it can be changed.

❖ **Entitlement Type or Client Type:** HyWorks can assign desktops either to registered endpoints or to users. If desktops are assigned to registered endpoints it can works as office workplace, where user will get the assigned desktop only when logging in from device. If desktops are directly assigned to users, then user will get desktop irrespective of endpoints it is logging-in. The choice is shown as **Entitlement Type** in **Desktop Pool** wizard, which can be set as:
  - **Device based:** for entitling desktops to registered endpoints
  - **User based:** for assigning desktops to users from configured authentication server

**Entitlement type** can be configured during pool creation and cannot be changed afterwards.

❖ **Assignment Lifespan:** Assignment lifespan defines lifespan of desktop assignment to the client. The available options are:
  - **Personal:** Personal assignment will keep the assignment for client unless it is manually revoked by the administrator
• **Floating:** The floating assignment will be removed on user logout. The floating assignment can be further sub-divided into following two use cases:
  - **On demand:** Desktop will be assigned whenever user requests access
  - **On Login:** Desktop will be assigned on user logon itself

More details about desktop pools creations and management will be provided in next sub-sections.

**Configuration Options for Dedicated Desktop Pools**
Desktop pool configurations can be separated into two major part:

1. **Common Configurations:** Configurations which will be common across the desktop pools
2. **Critical Configurations affecting deployment type:** Configurations which will affect the whole deployment of desktops in HyWorks.

Let us try to understand these configurations in detail.

**Common Configurations**
Below is the list of configurations which are common for all desktop pools and could be used as per requirement.

**General Screen**
1. **Name:** Name of desktop pool, this is shown to end-users on logon
2. **Description:** For providing logical details of desktop pools
3. **Connection Profiles:** To assign any specific connection profile for desktop pool. Connection attributes will be decided as per provided connection profile
4. **Active:** To mark desktop pool as active or inactive. For inactive desktop pool, HyWorks stops processing desktops and does not provide access to clients on logon from inactive desktop pools
5. **Maintenance Mode:** To enable maintenance mode in desktop pool. In maintenance mode HyWorks keeps on processing the desktops but does not provide access to end-users.

**Clients (Users/ Devices) Screen**
**Devices/ Users:** Based on **Entitlement Type** selected, screens **Devices/ Users** will be shown. The screen can be used to add/remove devices, users/groups or OUs respectively.

**Important Points for Adding Groups or OUs as Client:**
1. If groups or OUs are being added as clients for permanent dedicated Desktop Pools, then assignments should be kept Automatic as one virtual machine can be assigned to only one user (client) at a time.
2. If the assignment is kept manual then none of the users (members of added group/OU) will be given session of desktops, as assignment is automatic.

**Desktop Assignment**
How does assignment should happen automatically, or administrator should assign desktops to different clients manually.

1. In automatic assignment, HyWorks assigns desktop using its mechanism to identify best desktop pool.
   a. Default for provisioned desktop
   b. Should be used when trying to entitle desktops to groups/ organizational units
2. Whereas in non-automatic assignment, administrator will be required to assign desktops to clients.
   a. Can be used for desktop pool with pre-existing VMs

**Note:**
- While creating desktop pool with Dynamic Desktop Provisioning, Desktop Assignment screen is not displayed, as all cloned VMs are going to have same configurations and assignment will be done automatically to clients (as per configured Assignment Type).

**Client Groups**
Configure **Client Groups** optionally, to restrict shared hosted desktop access to only those users which are connecting from specific LAN or WAN or MAC. Refer section **Client Groups** section To enable restricted client groups access,

1. Select access policy as **From specific client groups only**
2. It will list down all the added client groups
3. Select client groups and move to allowed list.

**Advanced Configurations**
Following advanced configurations are commonly configured for users:

❖ **Advanced Screen**
1. **Keep desktops in power on state:** Configurations to set if associated desktops should also be kept in powered on state. Administrator can have following options:
   a. **Not configured:** Desktops will remain in power-state as managed by administrator or users
   b. **All Desktops:** If all desktops to be kept power on
   c. **Specified Desktops:** Minimum number of desktops which should be kept powered-on always.

2. **Power on state timing:** if option **Keep desktops in power on state**, set as **All Desktops** or **Specified Desktops** then this option gets enabled. Which can be used to specify the time from which desktops should be checked for powered-on state and should be turned on if found in powered-off state. The possible configuration can be:
   d. **Always:** Which means specified or all Desktops will be always kept powered on
   e. **Before Specified Timing:** To be entered in HH:MM TT format and specifies when the Desktops will be powered on if found powered off. HyWorks Controller starts the Desktops power on process before the specified timing to get them ready before the specified time.

3. **Power action when user logs off:** The setting **Power action when user logs off** specifies what action will be taken by HyWorks Controller once the user will log off its session. Possible actions can be:
   a. **Not Configured:** Do not take any action
   b. **Power Off:** Power off the Desktop, once user has logged off the session
   c. **Suspend:** Suspend the Desktop, once user has logged off the session
   d. **Restart:** Restart desktop on user logoff
   e. **Shutdown:** Shutdown desktop on user logoff
Note:
➢ The setting Power action when user logs off will not be enabled when the **Keep Desktops in Power On state** is configured as **All Desktops** due to the reason that keeping all the desktops in Powered on state will contradict with the setting of power action on user log off.

4. **User Permission (Add user to local Administrator group):** Selecting the option will make the logged in user a member of local administrator group on the target Desktop. Unchecking will not modify the user privileges on the Desktops.

5. **Dedicated Linux VM Pool:** A special configuration to be used when Linux based dedicated desktops to be delivered to end users.

6. **Use last known good IP address:** A very specific advanced settings, which enables HyWorks to use last cached good IP address of desktop if it does not receive IP address from respective session provider.

7. **Assign Network Ready Desktops:** Again, a very specific advanced setting which will enable delivery of only those desktops which are found ready for desktop connection based on reachability on configured RDP port. If enabled:
   a. HyWorks checks the reachability of desktops in virtual machines periodically
   b. If any desktop virtual machine is found not reachable on RDP port, then it will not give session of that machine to end-user.

8. **Use Connect Console:** This feature is only available for Hyper-V dedicated session providers, where VMs console session can be connected. Enabling this feature will require,
   a. Provider must be a Hyper-V server
   b. User credentials having authority to connect to console of VM.
   c. Port 2179 to be accessible from endpoints to Hyper-V server
   d. Feature is supported on HyDesk Hy3000/Hy4000, Windows Clients, Hy1000, Ubuntu Clients
   e. Hy2000, HyLite do not support Console Connect feature

9. **Use Pool Credential:** A very deployment specific setting, where every desktop connection will use a common pool credential. This can be very useful in deployments where user profiles can be highly reduced as all users will login with respective credentials but on connection these configured pool credentials will be used. Following details need to be enabled for using pool credentials:
   a. **Username:** Username to be used for logon
   b. **Password:** Password of the user
   c. **Domain:** Domain name/ NetBIOS name to be used to logon. For local users specify dot (.)

10. **Auto upgrade desktop agent:** To be used to upgrade HyWorks DVM tools. All desktops will be notified about desktop agent upgrade and will be upgraded as per available version of DVM Tools. Following additional configurations can be done:
    a. **HyWorks Desktop Agent:** For upgrading desktop agent upgrade
    b. **HyWorks Printing Module:** To be enabled to upgrade HyWorks printing module
    c. **HyWorks USB cleaner:** To upgrade HyWorks USB cleaner utility
    d. **HyWorks USB Redirection Driver:** For upgrading Built-in USB redirection driver (server side) module

Specific component or all components can be selected to be upgrade. Usually this option is enabled post desktop pool creation when HyWorks DVM Tools need to be upgraded.

Administrator should configure appropriate **Advance settings** as per requirements in **Advance** screen and can move to **Summary** screen for verifying the configured options.
❖ **Summary Screen**

Summary screen provides the information of all configurations done to revalidate settings before committing the changes. Administrator can go back using **Back** buttons on respective screens to modify the configurations if required or click on **Finish** button to commit the pool changes. HyWorks Controller will start the operations required after pool creation e.g. Desktop Provisioning or getting Desktop details etc.

**Important Configurations Affecting Deployment**

Some configurations which decides the deployment of desktop virtual machines will be briefly discussed this section.

**General Screen**

❖ **Entitlement Type**: This affects the deployment as client for desktops will be changed. Selecting as,
   1. **Device based** will show the **Devices** screen to configured registered devices as clients.
   2. **User based** will change screen to **Users**, which can be used to add/remove users from configured authorization server

❖ **Desktop Virtualization Type**: Desktop virtualization type simply decided what type of desktops will be given to the end-users. Each of available option further enables or disables other controls.
   1. **Shared hosted desktop**: To be used for shared hosted desktop delivery and not for dedicated desktops. Refer section [Shared Hosted Desktop Delivery](#) for detailed information.
   2. **Persistent Virtual Desktops**: Selecting **Virtualization Type** as **Persistent Virtual Desktops** will have following impact:
      a. **Select Session Provider**: Listing all configured session providers
      b. **Provisioning**: Enabling, both options, **None** for existing VMs and **Dynamic** for provisioning desktops
   3. **Non-persistent Virtual Desktops**: Selecting **Virtualization Type** as **Non-persistent Virtual Desktops** will have following impact:
      a. **Select Session Provider**: Listing all configured session providers which supports deployment of non-persistent desktops.
         i. It will list SCVMM server, VMware vCenter Server or Nutanix server, if configured.
         ii. It will remove any configured ESXi servers or Hyper-V Servers
      b. **Provisioning**: Only **Dynamic** option will be shown and will be selected by default.

❖ **Provisioning Type**: Type of dedicated desktops to be used in this pool
   1. **None**: For using existing desktops **Provisioning Type** to be selected as **None**. This enables
      a. **Desktops** tab to be used to get desired dedicated desktops from selected dedicated session provider.
      b. **Desktop Assignment** tab for assigning desktops to clients
      c. **Session Providers** dropdown control will list down all configured session providers
   2. **Dynamic**: For provisioning new desktops by cloning gold image, **Provisioning Type** should be selected as **Dynamic**. Selecting **Provisioning Type** as **Dynamic**, enables
      a. **Session Providers** dropdown control will list down all configured session providers which support provisioning
         i. It will list Hyper-V, SCVMM server, VMware vCenter Server or Nutanix server, if configured.
         ii. It will remove any configured ESXi servers from the list
b. **Deployment** and **Customization** tabs, to be used for provisioning and preparing customized new desktops

c. Will remove **Desktop Assignment** screen, as dynamically provisioned desktops are assigned automatically.
   i. Logically all desktops are going to have same configuration, thus it is not required to assign them manually.
   ii. Desktops are going to be created on demand and thus prior assignment will not be possible.

❖ **Assignment Lifespan**: This option defines, if the client assignment to the Desktop will persist after session or not. Based on the persistence of assignment, Desktop Pools can be of following two types:

1. **Personal**: Desktop Pools in which Desktops are permanently assigned to the clients (Devices or Users) and thus the same Desktop is provided to same client (User or Device) on every successful login. The client to Desktop assignment is always remembered.

2. **Floating**: Desktop Pools in which assignments do not persist after the session is removed, which means on every successful logon the session to different Desktop can be provided. The client to Desktop assignment is removed and is not remembered. Floating assignment can be further subdivided into following two types based on when assignments should be done:
   a. **On Login**: The configuration is shown in **Advanced** screen and specifies to assign desktop on user logon itself.
   b. **On Connect**: Selecting this option will not assign desktop on logon itself but desktop assignment will happen, when user will initiate the connection to desktop.
      • When **On connect** option is selected, administrator must specify another option that when desktop session is disconnected, after how much time assignment should be removed.

❖ **Deployment Screen**

When administrator configures desktop pool to use **Provisioning** as **Dynamic**, then deployment screen is enabled, and desktop screen is removed. Deployment screen provides options for deployment of virtual machines. Let us try to understand the option available in **Deployment** screen and its meaning.

❖ **Source VM**

Source VM also termed as gold image, will be copied multiple times to provision multiple Desktops. Following important configurations should be remembered while selecting the Source VM:

- **Source VM Format on Dedicated Session Provider**: The source VM must be a virtual machine and cannot be a template.
- **VMware Tools (VMware), Integration Services (Microsoft) or Nutanix Guest Tools (Nutanix)**
- **HyWorks Desktop Agent Installation**: Source VM should have HyWorks Desktop Agent installed as HyWorks Desktop Agent is required for post installation customization of virtual machine and ensures remote access for new valid users.
- **Source VM Power State**: Should be in running state which helps HyWorks Controller to determine the HyWorks Desktop Agent availability in the Source VM. However, if administrator knows that all prerequisites are correctly installed and configured in gold image then gold image machine can be kept in powered-off state as well.
- **Source VM should be a Fresh Installed Image**: Source VM should preferably be a fresh installed virtual machine. Using a virtual machine as source VM which was created using provisioning may result in customization failure since customization can be done only once on virtual machines.
Note:
➢ While selecting a source VM, if it is in powered off state or HyWorks is unable to connect to desktop agent, it will show warning message. However,
   o If Administrator is sure about the selected Desktop (Any displayed configuration error can be ignored) click on **Continue Anyway** button to proceed or click on **Cancel** button to cancel the Source VM selection dialog and correcting the issues on virtual machine

❖ **Clone from Snapshot**
Select this option, if clones should be created from specific snapshot/ checkpoint on virtual machine. Please note, not all providers support this operation and thus if selected provider does not support this, the option will be disabled. Selecting **Clone from snapshot**, enables option to select snapshot, which provide list of all available snapshots.

❖ **Desktop Name Prefix**
HyWorks uses the desktop name prefix with appending unique number to create desktops on respective Hypervisor.

1. HyWorks append a hyphen(-) and number in XXXX format e.g. a prefix as AccVDI, controller will create VMs with name as AccVDI-0001, AccVDI-0002, AccVDI-0003 and so on.
2. Including hyphen and number as XXXX, 5 more characters are added in desktop name and thus administrator must consider that the name of VM should not exceed allowed number of characters in VMware

Note:
➢ Providing a prefix with text which will make a duplicate name after appending the number is not validated in **Desktop Pool** wizard and thus results in Desktop creation failure.
➢ It’s a mandatory field in Deployment screen, keeping it blank will display relevant error.

❖ **Clone Type**
Clone type field in Desktop deployment defines the type of clones to be created of source VM. Following two types of clone Desktops can be created:

1. **Full Clone:** A full clone is an independent copy of a virtual machine that shares nothing with the parent virtual machine after the cloning operation. Ongoing operation of a full clone is entirely separate entity from the parent virtual machine.
2. **Linked Clone:** A linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner. This helps in conserving disk space and allows multiple virtual machines to use the same software installation.
   o **Linked Clones in HyWorks:** Linked cloning in HyWorks uses the following mechanism:
     1. When Linked Clones are initiated, HyWorks creates an exact replica or full clone of the Gold Image (Source VM).
     2. Then linked clone of Replica VMs are created.
     3. Having replica VM ensures that if gold image is modified in any manner, linked clones won’t get affected and if it requires to re-create all the linked cloned desktops then new replica VM can be deployed from gold image.
Please refer section [Functioning Support Provider vise](#) for linked and full clone support with different session providers.

❖ **Max Desktop Capacity**
The count of maximum number of Desktops to be created using Desktop Provisioning. The field accepts value from 1 to 1000, but this should be provided wisely as per requirement and available resources on the Dedicated Session Provider.

Once changes are committed HyWorks Controller will start creating the virtual machine as per provided number and in case Dedicated Session Provider is not having enough resources, provisioning will fail.

❖ **Desktop Creation Schedule**
This parameter defines the schedule of new VM creation; administrator can choose to provision new desktops in the following two schedules:

3. **Provision all Desktops now:** Proceeding in Desktop Pool wizard with schedule as **Provision all Desktop now** will create all desktops as per specified Max Desktop Capacity.

4. **On Demand:** Create desktops as per the demand arrives. While configuring Desktops on demand following two parameters are considered
   - **Count of Desktops to create now:** Defines how many desktops should be created first. E.g. if **Create Now Desktops** count is specified as 2, then at least 2 desktops will be created first as part of Desktop Provisioning.
   - **Count of spare Desktops to be provisioned:** Defines how many spare or extra desktops to be kept in Desktop Pool. E.g. **Count of spare Desktops to be provisioned** is 2, which means in this desktop pool at least 2 desktops will always be free and as soon as count of free desktop count goes to 1 it will start creating a new desktop to maintain the spare Desktop count.

Administrator can choose any of desktop creation schedule as per requirement.

❖ **Power on Desktop Post Provisioning**
Keeping the checkbox selected will power on the virtual machine after cloning is completed whereas unchecking this option will keep Desktop in powered off state after creation.

❖ **Enable DVM Reset**
Option to enable reset options for cloned VMs. If enabled, a restore point will be created of desktop VMs fresh state and if needed, DVMs or whole pool can be reverted to fresh state using **Reset** operation.

5. Not all providers support this option, please refer section [Functioning Support Provider vise](#) for detailed information on provider support. Providers which support Non-persistent VMs will also support option to reset DVMs

6. Enable DVM Reset will be default enabled for non-persistent desktops and is not modifiable.

❖ **Preserve MAC Address**
If deployment needs to preserve the last assigned MAC address, this configuration should be enabled. In use cases, where dynamic IP pools are limited, and same IP range should be utilized this setting can be very useful.

The feature or option currently works for VMware vCenter and Nutanix Hypervisors only.

❖ **Target Locations of Clones VMs**
Deployment Settings enables administrator to define target datastores and resource pools for the cloned desktops and replica VMs.
Deployment settings gets dynamically updated as per selected **Clone Type** option in following manner

a. For Linked Clone: Option to choose **Replica VM Deployment Settings**, gets enabled along with **Cloned VMs Deployment Settings**.

b. For Full Clone: Option for **Cloned VMs Deployment Settings** gets enabled.

Keeping the **Deployment Settings** option unchecked, will keep all configurations as default i.e. same configuration as gold image.

Considering that **Clone Type** is selected as **Linked Clone**, following configurations will be available:

- **Replica VM Deployment Settings**: The section can be used to change the location of the replica VM on dedicated session provider. To change configurations of replica VM, click on button **Change Location**.
  - Change Location
    Clicking on **Change Location** button will open **Available Datastores** dialog, which can be used to specify new location for the replica VM.
    Administrator can select the following two locations attributes by expanding the resource tree:
    - Resource Pool
    - Datastore
    In screenshot below, it is shown that datastore is changed to **datastore-181** and pool has been changed to **Migrated from 79**, which means the newly created desktops will be in **datastore-181** and under pool **Migrated from 79**.

- **Cloned VMs Deployment Settings**: Like replica VM deployment configurations, datastore and resource pool configurations of cloned VMs can also be modified. To modify the configurations of cloned VMs, click on button **Cloned VM Deployment Settings**.
  - This will start displaying the currently applied configurations for cloned VMs (set to Default, which means same as gold image)
  - Click on **Change Location** button to invoke **Available Datastores** dialog, follow steps mentioned in above section to change configurations of cloned VMs.

---

**Note:**

> ➢ Please note, Available Datastores dialog, displays all the available datastores and resource pools but it does not evaluate the feasibility of cloned VMs deployment on the target datastores or resource pool and administrator must choose these configurations carefully to avoid provisioning failure.

➢ As a thumb rule, the datastores and resource pools should be chosen in a manner they are able to read from replica image.

---

- **Deployment Settings Support for dedicated session providers**
  - **SCVMM Servers**: These advanced deployment settings are not supported with SCVMM servers configured as Dedicated Session Providers though shown as enabled. Clicking on Change location button with SCVMM server configured as Dedicated Session Provider will show the Available Data Stores dialog with error "no data centers found."
  - **Hyper-V Servers**: With Hyper-V Servers administrator will be able to change the Datastores up to available drives level and pool selection will not be available.
Changing the Datastore in case of Hyper-V servers will create a folder with name **Accops-Cloned-VMs** in the selected drive and will keep Desktops files in folder with the name of Desktop. As in the below screenshot where Datastore has been changed to D:\ drive, the newly created Desktops will be located at D:\Accops-Cloned-VMs\<Desktop Name>.

- **VMware vCenter Server:** As vCenter Servers presents two cases as per supported clone types and as per accessible ESXi servers.
  - **Linked Clones:** Option to move replica VM and cloned VMs are available. Please note the wizard will display the available Resource Pools and Datastores of all ESXi servers, but administrator should choose target locations carefully so that after completing the pool wizard provisioning does not fail.
  - **Full Clone:** In case of full clones with vCenter Server administrator will be able to change the Resource Pool or Datastore.

- **Nutanix:** Current version uses same configurations as gold master, though options can be shown to change storage pool.

### Customization Screen

Deployment screen ensures the deployment options which affects the new DVM configurations on Dedicated Session Provider E.g. Name of Desktop, Location, Power State, Count Etc. but the newly created Desktops may require some internal system level customizations which will be specific for specific Desktops e.g. computer name of all new Desktops must be different, locale etc.

For customizing such changes, customization screen can be used. On Customization screen administrator can opt to enable or disable customization.

Before moving to Customization process or available options, we must learn that few pre-requisites are met for customization to run successfully.

#### Disabling customization

Disabling the customization will create all Desktops as identical in terms of computer name, network settings, locate, product key. It can be a handy option if administrator is willing to customize new Desktops manually from Dedicated Session Provider or using any independent tool. To disable customization,

1. Keep **Customization needed** checkbox unselected and proceed to next screen

#### Enabling Customization

Administrator can opt to customize the new copies of the Desktops by selecting the checkbox **Customization needed** in **Customization** section of Desktop Pool (The screen will be enabled only when Desktop Provisioning is set to Dynamic). The following customizations in new clones are possible:

1. **Owner Name:** Owner name of the Desktop (Optional)
2. **Organization Name:** Organization name of the Desktop (Optional)
3. **Computer Name (Prefix):** Computer name of the Desktop. To keep each Desktop identical HyWorks Controller will append the provided computer name with hyphen and a unique number e.g. -XXXX new Desktops are provisioned and computer name is specified as 'ProVM' then computer name of 5 Desktops will be ProVM-0001, ProVM-0002 and so on.
a. Computer name (prefix) in customization cannot be more than 10 characters long. (* Mandatory field if customization is enabled)
b. HyWorks maintains same number for VM name and Computer name

4. **Local Username:** The new local user to be created on new Desktop. (Optional)

**Note:**
- If leaving Local Username field blank then, it should be making sure that at least one local admin (other than Administrator) user is already available on gold image, because post Sysprep administrator user gets disabled and could lead to configuration with no local administrator.

5. **Local Password:** Password to be set for new local user (* Mandatory field if local username is provided)

6. **Workgroup/Domain Configurations:**
   a. **Join a workgroup** is selected by default and requires entries in Workgroup textbox
   b. **Join a Domain:** If new Desktops need to be joined to existing Domain then this option can be selected while enable following fields:
      i. Domain Name: e.g. propalmsnetwork.com (* Mandatory if Join a domain combo box is selected)
      ii. Username: User with privileges to join a machine to domain e.g. domain admin user (* Mandatory if Join a domain combo box is selected)
      iii. Password and Confirm Domain Password: Password for domain admin user (* Mandatory if Join a domain combo box is selected)

7. **DNS Configurations:**
   a. **Preferred DNS:** Preferred DNS to be configured in network settings (Optional)
   b. **Alternate DNS:** Alternate DNS to be configured in network settings (Optional)

8. **AD Path:** Full OU path to which this computer should be registered. The provided domain username should have adequate rights to create objects in specified OU. (Optional)

9. **Select Locale:** For configuring local language of new Desktop

10. **OS Product Key:** Provide Volume product key, to be applied on new Desktop however if creating multiple VMs then this should be mass activation key or should be left blank for activating the OS later manually.

**Desktop Pool Management**

Administrator can use **Desktop Pools** section to:

- Add Desktop Pool
- Edit Desktop Pool
- Delete Desktop Pool
- Move desktops to maintenance mode
- Reset desktop pool (Non-persistent desktop pools or desktop pools deployed with **Enabled DVM Reset** option checked)

**Desktop Pool** wizard presents number of configurable properties in different screens of **Desktop Pool** wizard; we will try to understand different Desktop Pool concepts and associated fields in this section of document from Add Desktop Pool wizard.
Accops HyWorks v3.2 Administration

**Add Desktop Pool**
In previous section, different screens of desktop pool wizard, different types of configurations (Common/important) are already shared, in this section details will be provided as how different types of desktop pools can be added in HyWorks.

Following the classifications of desktop pools in section Desktop Pool Categorization, administrator can opt for following two types of desktop deliveries to end users:

1. Shared Hosted Desktop Deliveries
2. Dedicated Desktop Delivers

This section will include details for creating several types of desktop pools under these categories:

**Creating Desktop Pools of Several Types**
Administrator can proceed with Add Desktop Pool wizard to create following types of Desktop Pools in HyWorks deployments:

- **Using Existing Desktops (Desktop Provisioning type as None)**
  - Device Based
    - Using Dedicated Desktops from Dedicated Session Providers VMware/ vCenter Server, Microsoft Hyper-V/ SCVMM, Nutanix hypervisors
      - Floating
      - Personal
  - User Based
    - Using Dedicated Desktops from Dedicated Session Providers VMware/ vCenter Server, Microsoft Hyper-V/ SCVMM, Nutanix hypervisors
      - Floating
      - Personal

- **Using Dynamic Desktop Provisioning (Creating New Desktops with Desktop Pool)**
  - Device Based
    - Floating/ Personal
    - Linked Clone/ Full Clone
  - User Based
    - Floating/ Personal
    - Linked Clone/ Full Clone

Each type of pool can be a possible deployment scenario in different environment of different organizations. Administrator can simply choose the best fit case for the requirement and try creating a pool to fulfill it. In the below section of the document we will try to understand the process of creating several types of pools.

**Using Existing Desktops or Session Providers**
This section will cover creation of Desktop Pools using Desktops which are already present in the configured Dedicated Session Providers. Please note HyWorks Controller 2.1 supports Pooling of Dedicated Session Providers only, External Session Providers work without any pools. We will be covering use of External Session Provider Session Providers in a later section of document.

**Device Based – Personal Assignment Lifespan**
In any deployment, employees or professionals come to office premises, login to their respective desktops located at specific area and work from there.
Device based personally assigned pools replicate a similar environment where employee login from their respective devices and are provided with session of their dedicated desktops.

Pre-requisites

1. Appropriate Dedicated Session Provider (i.e. VMware/ vCenter Server or Microsoft Hyper-V/ SCVMM, Nutanix) is configured and reachable
2. Devices are registered with HyWorks Controller
3. Valid authentication server (Microsoft AD, Workgroup or Novell eDirectory) is configured - Required for validating the user credentials used for logon

**Desktop Pool Configurations in different screens**

<table>
<thead>
<tr>
<th>Screen Name</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>General Screen</td>
<td>Configuration Attribute</td>
<td>Name/Description</td>
<td>Entitlement Type</td>
<td>Desktop Virtualization Type</td>
<td>Select Session provider</td>
<td>Desktop Provisioning</td>
<td>Assignmen t Life Span</td>
</tr>
<tr>
<td>Expected Configuration</td>
<td>As Required</td>
<td>Device based</td>
<td>Persistent Virtual Desktop</td>
<td>As Required</td>
<td>None</td>
<td>Personal</td>
<td>As needed</td>
</tr>
<tr>
<td>Devices Screen</td>
<td>Configuration Attribute</td>
<td>Search, select and add devices as per requirement from the list of available registered devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expected Configuration</td>
<td>Search, select and add devices as per requirement from the list of available registered devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktop Assignment Screen</td>
<td>Configuration Attribute</td>
<td>As per requirement: 1. Auto assigned (if needed) or 2. Manually assign desktops to devices from desktop pool wizard or desktops screen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expected Configuration</td>
<td>Configure as per requirement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Pool creation is completed and user on logon with specific endpoints will get the configured desktops.

**Device Based - Floating Assignment Lifespan**

In above section, we have created a Device Based personally assigned Desktop Pool to keep the assignments forever.

However, there could be deployment requirements where the location of the user and thus device is fixed but it does not matter which desktop has been assigned to the device considering all desktops are having same configurations and same users log in from the devices. E.g. a hospital where user (doctors)
logs-in with a common username ‘doctor’ to access their desktop which does not have any local data rather work on a web-based application.

In such scenarios, a temporary Desktop Pool can be very handy. Follow the below steps to create a temporary Desktop Pool:

**Pre-requisites**
1. Appropriate Dedicated Session Provider (i.e. VMware/ vCenter Server or Microsoft Hyper-V/ SCVMM, Nutanix) is configured and reachable
2. Devices are registered with HyWorks Controller
3. Valid authentication server (Microsoft AD, Workgroup or Novell eDirectory) is configured - Required for validating the user credentials used for logon

**Desktop Pool Configurations in different screens**

<table>
<thead>
<tr>
<th>Screen Name</th>
<th>Configuration Attribute</th>
<th>Name/Description</th>
<th>Entitlement Type</th>
<th>Desktop Virtualization Type</th>
<th>Select Session provider</th>
<th>Desktop Provisioning</th>
<th>Assignment Life Span</th>
<th>Connect Profile</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Screen</td>
<td>Expected Configuration</td>
<td>As Required</td>
<td>Device based</td>
<td>Persistent Virtual Desktop</td>
<td>As Required</td>
<td>None</td>
<td>Floating on-login or on-connect</td>
<td>As needed</td>
<td></td>
</tr>
<tr>
<td>Desktops Screen</td>
<td></td>
<td>Search, select and add desktops as per requirement from selected dedicated session provider</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Devices Screen</td>
<td>Expected Configuration</td>
<td>Search, select and add devices as per requirement from the list of available registered devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktop Assignment Screen</td>
<td>Expected Configuration</td>
<td><strong>Auto assigned (Must)</strong></td>
<td>Note: Manual assignments in temporary pool are retained only until first login and are erased after logout</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advance Screen</td>
<td>Expected Configuration</td>
<td>Configure as per requirement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The pool creation is completed and user logging-in from the configured devices will be provided with appropriate Desktop session as per below examples:
User Based - Personal Assignment Lifespan

Consider a deployment scenario where a field employee used to visit different offices all the time and rather than carrying any hardware (Laptop etc.) with them to different offices due to security reasons but the employees need to connect to their desktops only.

In such scenario, a user based dedicated pool can be useful; where desktops are assigned to the users and irrespective of device, the session of same Desktop is provided to the user.

Below section will guide, how to create a user based personally assigned desktop pool.

Pre-requisites

1. Appropriate Dedicated Session Provider (i.e. VMware/ vCenter Server or Microsoft Hyper-V/ SCVMM or Nutanix) is configured and reachable
2. Valid authentication server (Microsoft AD, Workgroup or Novell eDirectory) is configured - Required for validating the user credentials used for logon
3. All required users exist on authentication server

Desktop Pool Configurations in different screens

<table>
<thead>
<tr>
<th>Screen Name</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Screen</td>
<td><strong>Expected Configuration</strong>&lt;br&gt;As Required</td>
</tr>
<tr>
<td>Desksops Screen</td>
<td><strong>Expected Configuration</strong>&lt;br&gt;Search, select and add desktops as per requirement from selected dedicated session provider</td>
</tr>
<tr>
<td>Users Screen</td>
<td><strong>Expected Configuration</strong>&lt;br&gt;Search, select and add users as per requirement from the list of available registered devices</td>
</tr>
<tr>
<td>Desktop Assignment Screen</td>
<td><strong>Expected Configuration</strong>&lt;br&gt;As per requirement: 1. Auto assigned (if needed) or 2. Manually assign desktops to users from desktop pool wizard or desktops screen</td>
</tr>
<tr>
<td>Advance Screen</td>
<td><strong>Expected Configuration</strong>&lt;br&gt;Configure as per requirement</td>
</tr>
</tbody>
</table>
User Based - Floating Assignment Lifespan

Consider a deployment scenario where field employees used to visit different offices all the time and rather than carrying any hardware (Laptop etc.) with them to different offices due to security reasons and the desktops need not to be specific to employee.

In such scenario, a user based dedicated pool can be useful; where Desktops are assigned to the users and irrespective of device, the session of different Desktop is provided to the user.

Below section will guide how to create a user based temporary assigned Desktop Pool.

Pre-requisites

1. Appropriate Dedicated Session Provider (i.e. VMware/ vCenter Server or Microsoft Hyper-V/ SCVMM) is configured and reachable
2. Valid authentication server (Microsoft AD, Workgroup or Novell eDirectory) is configured - Required for validating the user credentials used for logon
3. All required users exist on authentication server
4. Devices are registered with HyWorks Controller which will be used to login

Desktop pool configurations in different screens

<table>
<thead>
<tr>
<th>Screen Name</th>
<th>Configuration Attribute</th>
<th>Name/D Description</th>
<th>Entitlement Type</th>
<th>Desktop Virtualization Type</th>
<th>Select Session provider</th>
<th>Desktop Provisioning</th>
<th>Assignment Life Span</th>
<th>Connect Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Screen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Expected Configuration</td>
<td>As Required</td>
<td>User based</td>
<td>Persistent Virtual Desktop</td>
<td>As Required</td>
<td>None</td>
<td>Floating (On-login or On-connect)</td>
<td>As needed</td>
</tr>
<tr>
<td>Desksops Screen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration Attribute</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Expected Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Search, select and add desktops as per requirement from selected dedicated session provider</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users Screen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration Attribute</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Expected Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Search, select and add users as per requirement from the list of available registered devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktop Assignme nt Screen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration Attribute</td>
<td>Auto assigned (Must)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Expected Configuration</td>
<td>or</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Manually assign desktops to users from desktop pool wizard or desktops screen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advance Screen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration Attribute</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Expected Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure as per requirement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The pool creation is completed and user logging-in from the configured devices will be provided with appropriate Desktop session.
Using Dynamic Desktop Provisioning

In above section, we used existing desktops from selected dedicated session providers; now there could be a scenario where all new desktops need to be created. E.g. an institute where new Windows 7 Desktops with Java development environment for a whole new classroom: in such case administrator can prepare a gold image with Windows 7 operating system and then use dynamic Desktop provisioning to deploy new Desktops in HyWorks to fulfill requirements.

Now as we have understood the kind of deployments where dynamic Desktop provisioning might be required, let us move to section of creating several types of Desktop Pools which will use Desktop Provisioning in Desktop Pool wizard to deploy new Desktops.

As already explained in above sections that Desktop Provisioning will deploy all new Desktops with similar configurations by cloning (copying) the source VM and thus the Desktop assignment won’t be required as all the Desktops are same. Considering the above fact, the Desktop Assignment screen is not provided in Desktop Pools with dynamic Desktop Provisioning.

Below are few examples of creating several types of Desktop Pools, having Desktop Provisioning enabled:

Persistent Virtual Desktop: Device Based, Personal Assignment Lifespan, Dynamic Provisioning

As we have already understood the possible cases of provisioning new desktops, let us try to create a desktop pool, in which desktops will be provisioned with clone type a Linked Clones and desktops will be permanently assigned to devices.

We will also try to configure Desktop Creation Schedule in this section.

Pre-requisites

1. Appropriate Dedicated Session Provider i.e. vCenter Server is configured (Only vCenter Server supports Linked Clones)
2. vCenter Server has a source VM Ready for creating multiple linked clones of it
3. Devices are registered with HyWorks Controller
4. Valid authentication server (Microsoft AD, Workgroup or Novell eDirectory) is configured - Required for validating the user credentials used for logon

Desktop Pool configurations:

<table>
<thead>
<tr>
<th>Screen Name</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Screen</td>
<td>Configuration Attribute</td>
</tr>
<tr>
<td>Deployment Screen</td>
<td>Configuration Attribute</td>
</tr>
<tr>
<td>Expected Configuration</td>
<td>As Required</td>
</tr>
</tbody>
</table>

Accops Systems Private Limited 176
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Gold Image to be cloned</th>
<th>As needed</th>
<th>Linked Clone</th>
<th>On Demand Provision Now – # as needed</th>
<th>As needed</th>
<th>As needed</th>
<th>As needed</th>
</tr>
</thead>
</table>

### Customization

<table>
<thead>
<tr>
<th>Configuration Attribute</th>
<th>Configure as per requirement. Note: Customization requires some prerequisites in gold image machine, please check these configurations in respective section of this document.</th>
</tr>
</thead>
</table>

### Devices Screen

<table>
<thead>
<tr>
<th>Configuration Attribute</th>
<th>Search, select and add devices as per requirement.</th>
</tr>
</thead>
</table>

### Advance Screen

<table>
<thead>
<tr>
<th>Configuration Attribute</th>
<th>Configure as per requirement</th>
</tr>
</thead>
</table>

**Note:**

- As linked clones are supported with vCenter Server and Microsoft SCVMM only, hence selected dedicated session provider must be vCenter Server. If it is an ESXi, a Hyper-V, then **Linked Clone** option will not get enabled in **Deployment** Screen.
- **Desktop Assignment** screen will not appear in Dynamic Desktop Provisioning pool, as all the desktops are going to have same configurations and thus any desktop can be assigned to any client (device/ user)

**Details in Desktop Pools Tab of Deployed Dedicated Virtual Desktop Pool**

The pool creation is completed and now Desktop provisioning is started which can be first observed in **Desktop Pools** tab as highlighted in below screenshot: initially Desktop Pool status will be Cloning Desktops when Desktop Cloning is in progress and as soon as Desktop Cloning gets completed the status will be ready.

Another important thing to observe is that as per provided Desktop Creation Schedule only 2 Desktops have been created first.

**Details in Desktops Tab and Flow of Client Assignments to Clients**

Once the deployed dedicated desktop pool wizard is finished, **Desktops** tab can be used to see the provisioning progress as well understanding the **Desktop Creation** schedule.

1. **Desktop Provisioning Start:** New Desktops are cloned one by one and once the provisioning starts the Desktops to be created first will have following status:
a. The first Desktop for which cloning is started will be displayed as 'Creating Desktop'
b. Other Desktops to be provisioned later will be displayed with status 'Pending Desktop Creations'

2. **Desktop Provisioning - Create Now Completed**: Initially controller will create desktops equal to the count provided in field *No of Desktops to create now* in Desktop Creation schedule all the Desktops will be displayed with *Status as Powered On* (This does not mean that desktops are ready, there will be more processes in backend to complete the desktop provisioning)

3. **Customization Process**: Customization will happen in the following manner:
   a. Initially desktops will be marked with *Sysprep Info flag as Required* which means customization will be required on this Desktop. To see Desktops detailed status, click on it names in *Desktops VMs tab*; Desktop Detail dialog will be displayed with all the information about the Desktop
   b. HyWorks Controller will wait for new Desktops IP to be detected and once it's able to get the IP of new Desktop; it will try communicating with it.
   c. Once Communication establishes, Sysprep will be started on the new Desktop and flag SYSPREP Info will be marked as running suggesting that customization is in progress. New Desktop will get rebooted and will configure the customization as needed.
   d. Sysprep Info flag will be marked as Completed, which means Desktop customization is completed
   a. Desktop Agent status should now be Responding with Desktops DNS Name should display information which can help in identifying if Desktop has been customized correctly or not e.g. we configured Computer Name as DesktopLCWin7 and configured it domain accops.com so the DNS name of new Desktop after provisioning should be 'DesktopLCWin7-1.accops.local'.
   b. Now provisioning is completed for first set of desktops as per specified *Create Now Desktops* count, but the desktops assignment is remaining (Refer image below).
      i. Assignment will happen when a valid user from one of the configured device logs-in or when administrator manually assigns the device from Desktops tab.
      ii. Let us try to understand Auto Assignment and Desktop Creation Schedule process with an example:
         - We have provisioned Desktops as per below configurations: *Maximum Desktop Capacity* as 5, *Desktop Creation Schedule* as *On Demand*, where 2 *Desktops create now* and 2 Desktops to be kept in spare. The configured devices in Desktop Pools are Device-1, Device2....Device5.
         - In first step, as per above details also HyWorks Controller will create and customize 2 Desktops and will keep them unassigned say Desktop1 and Desktop2
         - Now as soon as a valid user from configured authentication server logs in from Device-1, HyWorks Controller will look for the ready Desktop and will assign the Desktop to Device-1. The assignment will also be remembered so if user from Device-1 logs in again same Desktop-1 will be presented.
         - Now as per configuration, HyWorks Controller must keep at least 2 Desktops in spare and once Desktop-1 is assigned to Device-1 which makes free Desktop count as 1 and now HyWorks Controller will start provisioning one more Desktop to keep spare Desktops as 2 (Refer image below)
Now if admin assigns or user logs in from Device-2, 2nd Desktop will be assigned to this device and HyWorks Controller will trigger creation of another Desktop which will be then provisioned and customized as per provided settings

a. The process of provisioning new Desktops will be continued until maximum Desktops capacity is reached which means HyWorks Controller has provisioned all 5 Desktops. Now login from Device-4 and Device-5 will be assigned with Desktop-4 and Desktop-5 but HyWorks Controller will not provision any new Desktop.

This now completes the Desktop Pool creation of

- Pool type Device based
- Assignment Type: Personal
- Dedicated Session Provider - vCenter Server/SCVMM Server
- Desktop Provisioning - Dynamic
- Clone Type - Linked Clone
- Desktop Creation Schedule: On Demand

Persistent Virtual Desktop: User Based, Floating Assignment, Dynamic Provisioning with Enabled DVM Reset

As we have already understood the possible cases of provisioning new desktops, let us try to create a desktop pool in which Desktops will be provisioned with clone type a Full Clones and desktops will be assigned to users.

We will also try to configure desktop creation schedule in this section.

Pre-requisites

- Appropriate Dedicated Session Provider i.e. VMware/ vCenter Server or Microsoft Hyper-V / SCVMM/Nutanix is configured (These Dedicated Session Providers support Full Clones)
  - Dedicated Session Provider has a source VM Ready for creating multiple linked clones of it
- Valid authentication server (Microsoft AD, Workgroup or Novell eDirectory) is configured - Required for validating the user credentials used for logon

Desktop pool configurations:

<table>
<thead>
<tr>
<th>Screen Name</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Screen</td>
<td>Expected Configuration Attribute Name/Description</td>
</tr>
<tr>
<td>User-based Floating Assigned Deployed Desktop Pool</td>
<td>As Required</td>
</tr>
</tbody>
</table>
Login and Assignment Flow

Let us try to understand user login and assignment process in case of Temporary user based provisioned pool.

1. We have provisioned total of 3 Desktops and all Desktops will be initially.
2. Once User-1 logs in from device-1, it will be assigned with either of 3 available Desktops say Desktop-1
3. If User-2 logs in with Desktop-1 already in session, User-2 will be assigned with Desktop-2 or Desktop-3 and if User-3 logs in with only Desktop-3 is remaining it will be provided with session of Desktop-3
4. If any other user logs in with all Desktops are already in use, user will be displayed appropriate error that no free Desktop is available.
5. Once users log out the session of respective Desktops, all the assignments will be removed
6. On next logon, again same process will be repeated where users will be assigned automatically as per availability and readiness of the desktops, but the old assignment will not be guaranteed.

This completes the Desktop Pool creation section which can be used to create several types of pools as per requirement. As explained above all provisioned Desktops will be available in Desktops tab and administrator can use Desktops tab for managing Desktops.

User Based - Floating Assignment, Dynamic Provisioning Non-persistent

As we have already understood the possible cases of provisioning new desktops, let us try to create non-persistent desktop pool with floating assignments for users.

Pre-requisites
- Appropriate Dedicated Session Provider i.e. VMware/ vCenter Server or Microsoft Hyper-V / SCVMM/Nutanix is configured (These Dedicated Session Providers support non-persistent desktops)
  - Dedicated Session Provider has a source VM Ready for creating multiple linked clones of it
- Valid authentication server (Microsoft AD, Workgroup or Novell eDirectory) is configured - Required for validating the user credentials used for logon

**Desktop pool configurations:**

<table>
<thead>
<tr>
<th>Screen Name</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Screen</td>
<td></td>
</tr>
<tr>
<td>Expected Configuration</td>
<td>Name/Description</td>
</tr>
<tr>
<td></td>
<td>As Required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deployment Screen</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected Configuration</td>
<td>Select a source VM</td>
</tr>
<tr>
<td></td>
<td>Gold Image to be cloned</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Customization</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Users Screen</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Advance Screen</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected Configuration</td>
<td>Power action when user logs-off</td>
</tr>
<tr>
<td></td>
<td>Shutdown/Power off/Restart (Choose as per need)</td>
</tr>
</tbody>
</table>

**Non-persistent Desktop Pool:**
A non-persistent desktop pool erases all changes done by a user in the session and thus a fresh VM is presented to user on next logon. How does it work:
1. HyWorks first deploys and customizes VMs as per deployment settings
2. Once VM is in ready (Fresh) state, HyWorks creates a restore point, which represents the fresh state
3. When user logs-in desktop is assigned to the user
4. On user logout, HyWorks revert the desktop to its fresh state using the restore point created.
   a. Restored VM will be kept in power state as per configuration done for Power Action when user log-off

Login and Connect to Assigned Desktop
The last step of Desktop deployment is user login from respective clients.

To verify if the pool is configured properly administrator can get users to login from appropriate devices to verify if only assigned Desktops is provided. Consider the examples below:

- Device based personally assigned pool with assignments are done manually as follows
  o Pool Configuration:
    ▪ Desktop-1 (Responding state) assigned to Device-1
    ▪ Desktop-2 (Responding state) assigned to Device-1
  o Login Process:
    ▪ Login from Device-1 with user credentials on successful authentication will configure Desktop-1 for remote access and will provide session on device-1
    ▪ In a same manner login from Device-2 will provide session of Desktop-2

- User based pool with floating auto assignment
  o Pool Configuration
    ▪ Users - User-1 and User-2 are configured as clients in pool
    ▪ Desktops - Desktop-1 and Desktop-2 are configured in pool and in responding state
  o Login Process:
    ▪ Login from any of registered device with user-1 credentials will provide session of any of Desktops i.e. Desktop-1 and Desktop-2. Assume session of Desktop-1 is provided to User-1
    ▪ Now if User-2 attempts to login when desktop session of Desktop-1 is running then session of Desktop-2 will be provided to User-2.
    ▪ Once desktop sessions are ended assignments will be removed and next logon from User-1 or User-2 credentials will randomly provide session of any of Desktops i.e. User-1 can be provided with session of Desktop-2 or Desktop-1.

Now administrator has successfully verified that the Desktop Pool is successfully configured, and users are able to connect to respective Desktops, administrator can happily work on other tasks when HyWorks Controller takes care of user access configuration and relevant tasks.

Note:
- Desktop Pool creation manages up to Desktop to Client (Devices/ Users) assignment level; the overall success of getting session depends on various other factors which must be addressed for successful HyWorks deployment. Few such factors are:
  o HyWorksTools especially HyWorks Desktop Agent installation on target Desktops: HyWorks Desktop Agent ensures RDP enabling for logged-in user and several other
  o Appropriate authentication server configuration and user credentials
Edit Desktop Pool

Edit Desktop Pool wizard presents different editable options to administrator according to the type of pool being modified.

In this section, details of pool editing process, modifiable options of several types of Desktop Pools will be provided.

How to Edit a Desktop Pool

To edit a pool, following steps should be followed:

1. Go to Desktop Pools page
2. Select the desktop pool needs modifications
3. Click on Edit button – It will open Edit Desktop Pool wizard
4. Update the configurations as per requirement in General, Desktops (for pools using existing desktops), Deployment/Customization (for pool using dynamic provisioning), Users/ Devices, Desktop Assignments (for pools using existing desktops) or Advance screens
5. On Summary screen, verify if updated information is displayed
6. Click on Finish button to complete pool edit process.

Editing Desktop Pools of Distinct Types

The section will describe modifying process of desktop pools of several types and the options which can be edited in Edit Desktop Pool wizard.

Editing Desktop Pool Having Existing Dedicated Desktops

Following configurations can be modified for desktop pools with existing desktops:

- General Configuration:
  - Name/ Description
  - Assignment Life Span
  - Connection Profiles

- Desktops:
  - Add More Desktops
  - Remove added Desktops

- Clients:
  - Add/ Remove Clients (Users/Devices)

- Change Assignments
  - Change Assignment Type from Manual to Auto-assignment or vice versa
  - Change mapping of desktops to clients
• Update Advance Options

*Editing Desktop Pool having Provisioned Dedicated Desktops*

In *Edit Desktop Pool* wizard, which are using **Dynamic** Desktop Provisioning to provision new desktops, presents following options to administrator:

1. **Stop Provisioning**
2. **Modifying other pool configurations:** Following editable options are available for desktop pool with dynamic desktop provisioning:
   - **General Information**
     - Name
     - Description
     - Assignment Life Span
     - Stop Provisioning (* Only when provisioning is in progress)
   - **Deployment Tab**
     - Recompose
     - Source VM
     - Desktop Name Prefix
     - Clone Type
     - Max Desktop Capacity
     - Desktop Creation Schedule
     - Power on Configuration
     - Advance Options
     - Without Recompose
     - Change Max Desktop Capacity
     - Power on Option
   - **Customization**
   - **Desktops**
     - Remove Provisioned Desktop from Pool
   - **Devices/ Users**
     - Add/ Remove new clients (Devices/ Users)
   - **Advance Options**

*Stop Provisioning*

Launching Edit Desktop Pool wizard, when desktop provisioning in progress; presents option to **Stop Provisioning**.

To stop provisioning following steps can be followed:

1. Go to **Desktop Pools** page
2. Select the Desktop Pool on which Desktop Provisioning is in progress (Can be identified by its Status in Desktop Pool—Status should be Cloning Desktops)
3. Click on **Edit** button – It will open *Edit Desktop Pool* wizard
4. Click on **Stop Provisioning** button
5. Confirm the action by clicking on Stop button on Confirm Action dialog
6. The Desktop Provisioning will be stopped:
   a. Any task of cloning will be completed and will not be cancelled
   b. HyWorks Controller will not provision any new Desktops
   c. Desktop Pools status will be changed to **Cloning Desktops Cancelled**

7. Appropriate Log entries will be created for the action
Recompose

As the term suggests, if administrator needs to re-provision all deployed desktop, recompose of provisioned desktop can be initiated by selecting **Recompose** checkbox and modifying all deployment options as allowed.

Recompose in HyWorks, allows administrator to re-provision all the desktops and at the same time keeps the assignment and other options intact for the desktop pool.

Recompose Candidates

Recompose should be done on the desktop pools where provisioning is completed. Recomposing desktop pools with provisioning in progress is not recommended and might leave some residual Desktops in respective dedicated Session Providers.

Recompose Mechanism for Distinct Types of Clones

8. **Linked Clone Provisioned Desktop Pool**
   
   On initiating Linked Cloned Provisioned Desktop Pool, following changes will be done:
   1. All linked cloned desktops will be deleted
   2. Replica Image will be deleted
   3. New replica image will be created from the specified gold image
   4. New desktops (linked cloned) will be provisioned
   
   i. The configurations of old desktops will be retained, and new desktops will have same configurations i.e. VM Name, Computer Name, client assignments etc.

9. **Full Clone Provisioned Desktop Pool**
   
   With desktop pool having full cloned provisioned desktops, following changes will be done:
   1. All provisioned desktops (full cloned) will be deleted
   2. New desktops (Full Cloned) will be provisioned
   
   i. The configurations of old desktops will be retained, and new desktops will have same configurations i.e. VM Name, Computer Name, client assignments etc.

Recompose – How To

Follow the below steps to recompose a provisioned desktop pool:

1. Select a desktop pool having provisioned desktops with all provisioning tasks are done
2. Modify general configurations (If needed)
3. On **Deployment** screen, select checkbox **Recompose**
4. Modify all the available options with recompose enabled. With Recompose enabled, only following configurations can be modified:
   
   a. **Deployment Configurations**:
      
      i. **Source VM**: Administrator can select any other gold image for provisioning
ii. Clone from Snapshot: If snapshot pointer to be changed, new snapshot or current state can be selected
iii. Desktop Name Prefix: Administrator can choose to change the Desktop Name Prefix
iv. Clone Type: If selected dedicated session provider is a vCenter Server/SCVMM then administrator will also have option to change the Clone Type
v. Power on Desktop Post Provisioning Configuration: If needed, power on configuration can be changed
vi. Deployment Settings: Administrator will also be able to modify the deployment settings for cloned desktops and replica image (only applicable if Clone Type is Linked Clone)

b. Customization Configurations:
   i. All configurations can be modified as needed

c. Other configurations:
   i. Modify as needed

5. Finish the Edit Desktop Pool wizard
6. All provisioned desktops will be deleted
7. HyWorks Controller will start provisioning new Desktops as per new deployment options

Recompose Example

Let us try to understand recompose process using an example.

1. Configuration: Desktop Pool-1 has been created using Dynamic Desktop Provisioning where 5 desktops were created (say Win7-Org-1 to Win7-Org-5)
   a. The provisioned desktops are in use and assigned to devices as shown in below image
2. Recompose is needed and in recompose the desktop pool has been modified to change desktop name as Recompose. Now the desktops will be recomposed with new name, but the assignments will be retained
3. Desktops VMs tab will display information on provisioning of new Desktops (refer screenshot above)
   a. Observe in screenshot that assignments are retained.

**Note:**

10. Initially Desktops VMs tab may display Desktops names with old names but eventually old Desktops will be deleted and new Desktops as per new deployment options will be created
11. Recompose, keeps the configurations of desktop pool same as before but the count cannot be modified, while recomposing the pool.
12. Recompose, in current version does not create desktops in sequential order

4. Appropriate Log entries will be displayed in Logs tab for all recompose tasks.
Other modifications in Provisioned Desktop Pool without Recompose

In **Edit Desktop Pool** wizard for desktop pool with provisioned desktops, administrator can also modify other deployment options without recomposing the desktop pool. Following options are editable in such desktop pools:

1. **Deployment Screen:** Only following configurations are editable in Deployment screen:
   - Max Desktop Capacity
   - Desktop Creation Schedule (If it was enabled while creating desktop pool)
   - Deployment Settings
2. All other screens provide editable options as specified in above sections.

The edit process remains same as specified in above section.

*Delete Desktop Pool*

Administrator can delete a Desktop Pool from HyWorks deployment using following steps:

1. Select Desktop Pool from **Desktop Pools** tab
2. Click on **Delete** button
3. Deleting options for provisioned desktop pools or desktop pools with existing desktops
   a. If it’s a provisioned desktop pool **Confirm Action** dialog will be displayed stating ‘Removing Desktop Pool will also remove all associated Desktops and client assignments’
      i. Keeping the option checked will delete all provisioned desktops from dedicated session provider
      ii. Unchecking the checkbox will delete the desktop pool and will leave the desktops on dedicated session provider
   b. For Desktop Pools (Using existing Desktops), the Confirm Action dialog, will not have any checkbox for deleting the desktops and thus confirming the pool deletion only deletes the desktop pool configuration from HyWorks Management Console
4. Click on **Delete** button on **Confirm Action** dialog
5. Desktop Pool will be deleted, and all associated Desktops will also be removed from **Desktops VMs** tab
Add to Maintenance
A desktop pool can be moved to maintenance mode to perform maintenance activities on it. In maintenance mode, desktop pool will be processed by HyWorks Controller, but users will not be able to access desktops from pool.

To enable maintenance mode in desktop pool:
1. Select desktop pool from list
2. Click on button Add to maintenance
3. On Confirm Action dialog box, click on OK button
4. Desktop pool will move to maintenance mode.

Reset Desktop Pool
For non-persistent desktop pools or deployed desktop pools which are enabled with DVM Reset option, administrator can reset all desktops in a desktop pool using Reset button.

To reset a desktop pool, follow below steps:
1. Select desktop pool from list
2. Click on button Reset
3. On Confirm Action dialog box, click on Reset button
4. All desktops in desktop pool will be reverted to respective restore point

Desktop Pools Page and Available Information
Once Desktop Pools are created by providing appropriate details in Add Desktop Pool wizard, Desktop Pools page is refreshed and displays following information of configured Desktop Pools using different columns.

- **Pool Name and Type:**
  - Desktop Pool Name and Entitlement Type as provided in General screen
- **Provider/Team Name and Type**
  - Name of session provider or session host team
  - Type of session provider
- **Desktop Provisioning and Connection Profile**
  - Desktop Provisioning configuration as Deployed for dynamic and None
  - Connection Profile if configured else None
- **Assignment Life Span/ DVM Persistence:**
  - Lifespan as Personal or On demand
  - DVM Persistence as Persistent or Non-persistent
- **Desktops Ready**
  - Total number of ready Desktops
  - Not applicable (NA) for Microsoft RDS Server Desktop Pools
- **Desktops in Use**
  - Desktops already assigned or being used in session
  - Not applicable (NA) for Microsoft RDS Server Desktop Pools
- **Free Desktops**
  - Unassigned Desktops in Pool, available for assignments and connection
- **Status**
  - Ready (Default fonts)
  - Ready in maintenance (Red Font)
  - Cloning Desktops (If provisioning is in progress)
• **Active**
  - If Desktop Pool is active or not

**Important Aspects of Desktop Delivery in HyWorks**

In this section we will try to learn some important aspects which can be used while deploying desktops:

**Provisioning and Customization Process in HyWorks**

Details about prerequisites for desktop customization and flow will be provided in this section:

**Desktop Customization Pre-requisites and Limitations**

1. The source VM must have VMware tools installed if selected Dedicated Session Provider is of type VMware/ vCenter Server
2. The source VM must have HyWorks Desktop Agent installed to initiate the customization
3. The source VM must be a fresh installed virtual machine in which customization is not run earlier. A single Desktop cannot be customized twice and thus if source VM is already customized once the clones i.e. new Desktops will not be able to run customization
4. The source VM should not be having expired product key as customization may get interrupted due to the activation notification thrown in between
5. The source VM should be configured with DHCP network settings as all clones will be created with same network settings and thus causing IP conflict and affecting HyWorks Controller to Desktop Agent communication
6. When joining cloned VMs to domain:
   - Specified credentials should have enough rights on the target OU (if specified) else on domain controller to create objects
   - Cloned VMs must be able to communicate with domain controller to move it to specified domain (specify DNS servers or DNS servers are provided from DHCP)

**Flow of events for desktop customization**

The Desktop Customization in HyWorks deployment is done using the following flow sequence:

1. Once all the customization attributes are properly configured and administrator committed the pool changes by completing the Desktop Pool wizard, HyWorks Controller will mark that the new Desktops will require customization. (This can be observed in Desktop Details dialog -> SYSPREP Info)
2. Source VM will be powered off and will be cloned multiple times as specified - New Desktops will be created as per provided deployment options
3. Desktops will be powered on automatically if configured or will require manual power on from administrator if **Power on Desktop Post Provisioning** is not enabled
4. After Desktops are powered on, HyWorks Controller will try to communicate with HyWorks Desktop Agent on each Desktop
   **Note:** This step requires that the source VM must have VMware tools and HyWorks Desktop Agent is installed
5. Till step# 4, new Desktops are exact replica of the source VM, Desktop details will display attribute **SYSPREP Info as Required**, which specifies that the new Desktop will require customization
6. Once HyWorks Controller can communicate with HyWorks Desktop Agent on new Desktops, it will share the customization details with each Desktop
7. Desktops will be rebooted and will run setup to customize the Desktop as per provided parameters (This step may take some time depending on the hardware, software resources and network settings)

8. Once the setup is completed, all new Desktops will be having a unique name, same local user with same password, joined with specified domain or workgroup, set with specified locale and activated with provided OS Product key.

The Desktop status will start displaying as Responding in Desktops VMs tab with Sysprep Info attribute showing as completed.

HyPrep and Sysprep for Desktop Customization
Latest HyWorks DVM Tools support following two methods of preparing cloned systems for usage in deployment:

5. Sysprep: Sysprep (System Preparation) prepares a Windows installation (Windows client and Windows Server) for imaging, allowing you to capture a customized installation. Sysprep removes PC-specific information from a Windows installation, "generalizing" the installation so it can be installed on different PCs.
   o Applicable for Windows systems only

6. Hyprep: Accops own system preparation tool with faster processing. Hyprep can be used for fast deployment.
   o Default for Linux systems
   o Can be used for Windows systems
   o Does not make any changes in security identifier
   o Requires object(Computer) creation and deletion privileges for user being used to join domain

How to use Hyprep
HyWorks Controller v3.2 does not provide option to use Hyprep from management console. Hyprep can be enabled on gold image using registry settings. To enable Hyprep:

1. Connect to gold image with user having administrator privileges
2. Open registry editor
3. Go to HKLM\SOFTWARE\Accops\DVMAgent
4. Change registry value of USEHYPREPTool to true
5. Now clones machine will be customized using Hyprep
6. Keeping it as false will continue to use Sysprep as default system preparation tool

HyWorks Fallback Model for Delivering Best Available VM to user
The logical fallback model best fits for desktop pools with floating assignment, where desktop assignments are removed on user logout and a new user is assigned with desktop as per availability.
Within desktop pool, a desktop may have following status:

7. [Priority# 1] Powered on, IP (Network) available, DVM Agent installed and responding
8. [Priority# 2] Powered on, IP (Network) available, DVM Agent not installed or not reachable
9. [Priority# 3] Powered on, IP (network) not available
10. [Priority# 4] Powered off or suspended

Considering the above priority model, HyWorks behavior in different use cases can be defined as below:
1. HyWorks checks desktop availability on above order only and provides desktop which is best fit for the user. E.g. if a pool is having 4 VMs with only one VM in powered-on state with IP and agent in reachable state, HyWorks will provide that desktop to user.

2. Another logic added to the above fallback model, where HyWorks will try to provide a fresh or not accessed VM to user unless all priority VMs are exhausted and every priority level works as a bucket for end-users. Consider following examples:
   a. A desktop pool with 3 VMs having agent responding, powered on state with IP, then if user-1 connects, VM-1 will be assigned to the user, if user-1 logs out and VM-1 is released (All VM-1,2 and 3 are available). If new user, user-2 requests desktops, then HyWorks will try to provide VM-2 or VM-3.
   b. If all VMs (VM-1,2 and 3) are currently in use and user-1 (accessing VM-1) logs out and releases VM-1. A new user, user-4 requests desktop access, then HyWorks will try to provide access of VM-1 only. Though it is most recently released but belong to the highest priority bucket.

**Network Ready Desktops**

In some cases, where users may use softwares affecting local networks as well (e.g. full tunnel VPN clients), then the respective machines may not remain usable after usage. Ideally in such situations, on user logout machine power policies should be set to reboot but still in some cases, HyWorks did not get notified and DVMs may remain unusable.

In such cases, the number of VMs available to end-user may keep on decreasing and thus it is important to assign only those VMs to users which are readily available.

To overcome such situations, HyWorks can be enabled to check reachability of all DVMs in a desktop pool to be reachable on specific network (RDP) port and only those VMs will be provided with access, which are found available on network.

Now in previous section, priority order is already defined which now will get changed as below:

11. Priority# 1] Powered on, IP (Network) available, DVM Agent installed and responding
12. [Priority# 2] Powered on, IP (Network) available, DVM Agent not installed or not reachable

Which means HyWorks will not provide access of any desktops which are not reachable and thus, avoiding any circumstances where user will be provided access of desktops which cannot be accessed.

**Provider Failsafe Policies**

As HyWorks has support to connect to hypervisor management layers (e.g. VMware vCenter servers, managing multiple ESXi servers, Microsoft SCVMM managing Hyper-V servers), it is possible that management servers are down though backend hypervisors and virtual machines hosted on those hypervisors are running fine on them.

In such cases, HyWorks is configured to use cached values of DVMs power status, network status, and provide access to clients (wherever applicable).

The feature does not guarantee that all users will be provided error free access to assigned VMs, but it serves many users for whom assigned VMs are in deliverable mode.

Failsafe policies can be controlled from System -> Advanced Settings, following configurations are available:

1. Session provider failsafe policy: Suggesting if failsafe policy to be enabled or not. Default is true, suggesting by default failsafe policies are by default enabled.
2. Failsafe Policy Timeout (Min): Suggesting, for how long controller should continue to server sessions though provider is not reachable. Default is zero (0) means infinite.
What works and what fails with provider failure:

1. HyWorks will not be able to update desktop power status, IP address
2. Any desktops which is in running state and in connection ready state, will be given access
3. Any desktop which is in not running state or in not ready state, will be given access as per fallback model but connection may fail
4. Provisioning will not work
5. Any power operation initiated by HyWorks will not work
6. Non-persistent desktops will not be able to revert to fresh state on user logout
7. Adding new desktop pools or new desktops to existing desktop pools will be affected and not recommended.

One Desktop can used in only one desktop pool throughout HyWorks

A Desktop can be configured only in a single desktop pool in HyWorks deployment and thus Available Desktops dialog lists only virtual machines which are not yet configured in any of the Desktop Pools in the HyWorks Controller.

Therefore, if administrator is not able to see any specific virtual machine in Available Desktops dialog then either of the following conclusions can be made:

- It has been already configured in any existing Desktop Pool
- The Dedicated Session Provider cache does not have details of this Desktop (Can be resolved by refreshing the Available Desktops list as explained below).

DVM Details Duplication when Hypervisor and Management Server, both configured in HyWorks

As HyWorks supports desktop delivery from Microsoft Hyper-V as well as Microsoft SCVMM Server, in a similar manner it supports desktop delivery from ESXi servers as well as VMware vCenter Server as well. But if you configure a hypervisor and its management server both as a desktop provider, desktop VM details are duplicated and thus configuration may show some problems.

Reason: Every hypervisor keeps a unique Id for each VM and when a management server connects to hypervisor the same unique Id is used. This unique Id helps in maintaining identity of VMs even when their name or other attributes are same.

HyWorks also uses this unique Id to identify VM uniquely on desktop provider and at the same time it maintains its own unique Ids for each VM.

Consider a scenario:

1. VM on ESXi (Unique Id: EVM1) is added to HyWorks, HyWorks Id (HVM1)
2. vCenter Managing ESXi is also added (Which has VM Id same as ESXi)
3. vCenter is also added to HyWorks. So now if HyWorks will try to add one more VM as HVM2 pointing to same EVM1

Now for every VM operation, HyWorks will have duplicate Ids and may show failures.

Conclusion:

1. It is not recommended to add a Hypervisor and its managing server both in same deployment of HyWorks. It may cause failures. Some examples could be:
   a. ESXi server and vCenter Server
   b. Hyper-V and SCVMM Server
   c.
Monitoring Desktops

Desktops sub-section under Monitoring section lists all the dedicated desktops currently configured in any of the desktop pool in HyWorks.

Desktops sub-section also enables the administrator to perform various administrative tasks such as power operations, assignment modification etc.

Desktops VMs tab provides following information and actions to administrator:

- Viewing Desktop Information
- Power Operations
  - Power Off
  - Shutdown
  - Power On
  - Restart
  - Suspend
  - Resume
- Desktop Pool Related Operations
  - Remove from Pool
- Client Assignment Operations
  - Assign
  - Unassign

We will try to understand each operation in this section of document.

Viewing Desktop Information

All Desktops configured in created Desktop Pools are displayed in Desktops VMs tab. Following information is available in Desktops VMs tab:

- **OS**: Operating system of desktop VM. The information is fetched from session provider.
- **Desktop Name**: Name of DVM on session provider
- **IP Address and DNS Name**: IP Address and DNS Name of the Desktops as shared by Dedicated Session Provider.
  - VMware/ vCenter Server: Desktops must be installed in VMware Tools in order to get this information
  - For Powered off or Desktops whose IP and DNS information can be fetched will be displayed with NA
- **Pool Name and Type**: Desktop Pool Name and its type information in which this Desktop is configured. Pool type could be device based or user based.
- **Assigned Client and Type**:
  - Assigned Client: A desktop can be assigned to a user or client and it display the assigned client information accordingly, which can be username or device name
    - User
    - Device
  - Assignment Type: A desktop can be assigned permanently or temporarily to a client and the field will show possible values accordingly, which can be
    - Permanent
    - Temporary
- **Connection Status**: Reflects if session is connected or not, possible values can be
  - Connected
  - Not Connected
- **State**: DVM’s current Power State, which can have following values:
  - Powered Off; If the Desktop is in Powered off state
- **Powered On**: If Desktop is in Powered on State
- **Suspended**: If Desktop is in Suspended state
- **Not Synced**: This can be a temporary state shown when performing power operations e.g. Shutdown or when Dedicated Session Provider is gone unreachable etc.
- **Syncing**: The Desktop details are being synchronized with the dedicated session provider
- **Creating**

- **Network Ready**: Showing if desktop is configured for network ready status check or not and if configured and current status of connection readiness, possible values could be:
  - **Ready**
  - **Not ready**

- **Agent Status**: Displays the HyWorks Desktop Agent's status as
  - **Responding**: Means, HyWorks Desktop Agent is running, and HyWorks Controller can communicate with HyWorks Desktop Agent
  - **Not Responding**: Either HyWorks Desktop Agent is not running or some issues while establishing connection with HyWorks Desktop Agent
    - When Agent status is in **Not Responding** state then mouse hover on Agent Status will also displays the details status with possible cause of the status.
  - **Not available**: DVMs in powered-off or suspended state.

This is how different columns in **Desktops VMs tab** provide valuable information about the Desktops. Administrator can also click on Desktop Name (Works as a link) to open Desktop Detail dialog which displays above and some additional information of selected desktop.

**Desktop Details Dialog**

To open Desktop Details dialog, click on Desktop Name in **Desktops VMs tab**.

Desktop Details dialog provides following details of selected Desktop:

- **Basic Info**:
  - **Desktop Name**: Name of the Desktop
  - **DNS Name**: DNS Name as gathered from Dedicated Session Provider
  - **OS Name**: Operating system on DVM
  - **OS Version**: Version of operating system on DVM
  - **Assigned Client Name**: Device Name or Username assigned to this Desktop
  - **Desktop Status**: Current Power State of Desktop
  - **Connection Status**: If connected or not.
  - **Pool Name**: The name of Desktop Pool to which this Desktop belongs
  - **Networks**: Network configuration of Desktop as collected from Session Provider
    - **IP Address**: IP Address
  - **Enable DVM Reset**: If reset is enabled on DVM during deployment or not
  - **Restore Point Statue**: Name of restore point if DVM Reset is enabled, else values could be required or not required.
  - **VM Path**: Full path of VM location

- **Agent Info**: For displaying details information regarding HyWorks Desktop Agent on selected Desktop
  - **Status**: Responding or Not Responding
  - **Message**: Detailed status of Desktop e.g. if Desktop Agent Status is responding then message will be Desktop is Ready and if it's not responding then relevant message suggesting why the agent is not responding
  - **Version**: HyWorks DVM Tools version
  - **Installed On**: Date on which HyWorksTools was installed
Accops HyWorks v3.2 Administration

- Info Last Updated On: Date and time information when Desktop Information was last updated
- Desktop Agent Info: Version: Version of HyWorks Desktop Agent
- Eltima Info: Version number of Eltima software installed on Desktop or shown as not installed if not installed
- SEP Info: Version number of SEP software on Desktop or shown as not installed if not installed
- Sysprep Info: Status flag of Sysprep, possible values can be
  - Required: Suggesting customization was done on the Desktop during provisioning and is required but not yet run
  - Running: Customization is in progress
  - Completed: Customization is completed
  - Not Required: Customization was not enabled while provisioning and thus customization won’t be run, when Desktop will be powered on
  - Unknown: When selected Desktop is not a provisioned one and is an existing VM from dedicated session provider

- Hypervisor Tool Info: Displaying information of Hypervisor tools on selected Desktop. E.g. in case of Desktop is coming from VMware then following information can be displayed
  - Version: Some number as 9354
  - Status: As shared by Dedicated Session Provider E.g. Running(Current)

Administrator can use the above details to verify if Desktop is ready for user access.

Desktop Management Operations

In Desktop VMs tab, administrators will be able to perform multiple power, pool, assignment operations on registered DVMs. This section will provide detailed information about these actions:

Power Operations

Administrator can perform following power operations on selected Desktop. The power operations will be enabled or disabled as per current power state of the Desktops:

- **Desktop is in powered Off state:** Following power operation will be enabled:
  - Power On
  - Saved state (On Hyper-V only)

- **Desktop is already in powered on state:** Following power operation will be enabled:
  - Power Off
  - Shutdown
  - Restart
  - Suspend

- **Desktop is in suspended state:** Following power operation will be enabled:
  - Resume

Performing Power Operation

To perform any power operation on Desktop:

1. Select the Desktop in Desktops page
2. Based on its current power state appropriate power operations will be displayed (e.g. Desktop is in Power on State and thus Power Off, Shutdown, Reboot and Suspend buttons will be displayed)
3. Click on button as per required power operations e.g. Suspend
4. Click on OK button on Confirm Action dialog box (if displayed, based on the initiated operation) to continue performing operation
5. Power operation will be initiated by HyWorks Controller and will be forwarded to Dedicated Session Provider, meanwhile wait dialog will be displayed
   a. Please wait until the operation is completed; the dialog will be dismissed automatically
   Or
   b. Click on OK button to dismiss the dialog, the task will be completed, and desktop’s status will be updated automatically.
6. Once initiated operation is successfully executed, Desktop status will be updated in **Desktops VMs tab**

Above example considers the Desktop power state as Powered On, other operations Resume, Restart, Shutdown, power off can also be performed using same steps.

**Important Note for Desktop Power Operations**

HyWorks Controller communicates with Dedicated Session Provider for updated Desktop status, but this is periodic and sometimes there might be some mismatch between desktop VM’s power state in HyWorks Controller and Desktop’s actual power state in Dedicated Session Provider and in similar cases, performing power operation may fail.

**Desktop Pool Related Operations**

Desktops can be removed from HyWorks Configuration and from its respective desktop pool from Desktop section, by following the below steps:

1. Select the Desktop in Desktops page
2. Click on **Remove from Pool** button
3. **Confirm action** dialog will be displayed, where an option to delete DVM will be displayed,
   a. **Delete the desktop from session provider also?** Select this check box if DVM is no longer required and should be deleted

   **Note:**
   ➢ The action is irreversible and deleted VM cannot be restored. Administrator should choose this option only when they are sure about deletion of DVM from provider.

4. Desktop will be removed from **Desktops VMs tab** and respective Desktop Pool.

**Client Assignment Operations**

Like Power Options, appropriate Assignment Options will be enabled or disabled, e.g.

- Desktop is in assigned state: Following options should be enabled
  o Assign: To re-assign the Desktop to any other client
  o Unassign: To remove current client assignment from Desktop
- Desktop is in unassigned state: Following options will be available
  o Assign: To assign a client to this Desktop

**Unassign Client from a Desktop**

Unassigning a client from selected Desktop will only removes the association of client and Desktops, which means the Desktop is now will be available for assignment to any other client.
Unassign option will be available when administrator selects any Desktop which is currently assigned to a client.

**Unassign in Manual Assignment Pool**
In a Desktop Pool, where Auto Assignment was not checked and manual assignment was done, then Unassigning will
- Remove the association of Desktop and the client
- Desktop will be available
- Desktop will not be assigned automatically to any other client as it was a manually assigned pool
- Logon from the client, which was unassigned from Desktop, will be displayed with error No Desktop is assigned to this client

**Note:**
- Unassign operation does not remove client entry from desktop pool. Thus, if any specific client must be removed, then it should be done from Edit Desktop Pool wizard

**Unassign in Auto Assignment Pool**
In a Desktop Pool, where Auto Assignment was checked and
- Remove the association of Desktop and the client
- Desktop will be available
- Desktop will be assigned automatically to any other or this client on very next logon

**Note:**
- As explained above, Unassigning a Desktop in Auto Assignment pool, makes Desktop available for all the clients in Desktop Pool and thus
  - If a Desktop is being unassigned when session is in progress will make it available for some other client. The session will not be affected
  - If some other client logs on, then the current user session might be disconnected

**Assign Client to a Desktop**
Administrator can perform Desktop Assignment from *Desktops VMs tab* and it can be done to already assign Desktop or an unassigned Desktop.
Assigning a client to Desktop not only assigns the client to Desktop but also adds the client in to the pool configuration.
Client can be a user or device and as per the pool type appropriate dialog will be displayed i.e.
- **Device Based Pool:** Selecting the Desktop which belongs to a device-based pool and clicking on Assign button will display, Desktop Assignment dialog listing devices to be assigned
- **User Based Pool:** Selecting the Desktop which belongs to a User based pool and clicking on Assign button will display, Desktop Assignment dialog listing users to be assigned

**Assignment Process**
Follow the below steps to perform assignment on *Desktops VMs tab*:
1. Select a Desktop from *Desktops VMs tab*
2. Click on Assign button
3. Select a desired client (Device or User as per Pool Type) from list of clients displayed in Desktop Assignment dialog (As shown in above screenshots)

4. Click on Assign button
   a. If the selected client is already assigned to any other Desktop in the pool then Confirm Action dialog will be displayed, click on OK button to continue
   b. If selected client is not yet assigned with any Desktop in the pool, then no such dialog will be presented, and Desktop Assignment dialog will be dismissed, and selected desktop will now be shown as assigned to selected client (Device or User as per Pool Type)

Impact of assignment on several types of pools

1. **Case #1: Unassigned client to unassigned Desktop**
   a. **Floating pool**
      Though temporary assignment pools require auto assignment to be enabled but administrator can also do one-time assignment of Desktops to any device. This assignment will work only for the next logon from the client and will be removed on session disconnect.
      As the client was not assigned to any Desktop, thus client will be connected to this assigned Desktop on next logon.

   b. **Permanent pool**
      In permanent pools if the client was not assigned to any Desktop earlier and then it is assigned to any free Desktop then the assignment will be permanent and from next logon, session of newly assigned Desktop will be provided to the client.

2. **Case #2: Unassigned client to already assigned Desktop**
   In case if the Desktop is currently assigned with a client then assigning it with new client will remove the current assignment and new client will be assigned.
   If any session is in progress from old client, then the session will not be disconnected however on logon from new client this session will be notified and disconnected or may get disconnected directly.

3. **Case# 3: An assigned client to unassigned Desktop**
   In case if the selected client (say Client-1) is already assigned to any other Desktop (Say Desktop-1) and now it is being selected to be assigned to new Desktop (Say Desktop-2 unassigned) then existing assignment of Desktop-1 to Client-1 will be removed and only one assignment that is Client-1 to Desktop-2 will be made.
   Thus, on next logon from Client-1 will be given session of Desktop-2.

4. **Case #4: An assigned client to already assigned Desktop**
   In case if the selected client (say Client-1) is already assigned to any other Desktop (Say Desktop-1) and now it is being selected to be assigned to new Desktop (Say Desktop-2 assigned to Client-2) then existing assignments of Desktop-1 to Client-1 and Desktop-2 to Client-2 will be removed and only one assignment that is Client-1 to Desktop-2 will be made.
   Thus, on next logon from Client-1 will be given session of Desktop-2; whereas next logon from Client-2 will be displayed with error ‘No Desktop is assigned to this client’.

**Reset Desktop**
Desktop VMs which are deployed in Non-persistent desktop pool or deployed in desktop pool with option Enable DVM Reset, have specific restore point of fresh state. Administrator can reset desktop VM from Desktop VMs tab.
Option to reset will be displayed for those desktops only, which are deployed in HyWorks with **Enable DVM Reset** option enabled. To reset a desktop, follow the below step:

1. Search and select desktop from list of DVMs
2. Observe button to reset is shown
3. Click on button **Reset**
4. Confirm reset operation by clicking on **Ok** button shown on **Confirm Action** dialog
5. Desktop will be reset to its fresh state

**Refresh Desktop**
If anytime a desktop VM power state, IP or other aspects are not synced or not showing latest information, administrator can initiate refresh operation.

Refresh operation performs following tasks:

1. Get the latest details of power state, IP or DNS name of desktop VM
2. Initiate agent communication to check agent status
3. Updates desktop VM information as per refresh operation result.

Follow below steps to refresh a desktop:

1. Search and select desktop from list of DVMs
2. Click on button **Refresh**
3. Desktop status will be refreshed

**Upgrade DVM Agent**
Administrator can upgrade DVM agent for specific desktop from **Desktop VMs** tab.

**File Location for Upgrading DVM Agent**
For pushing upgrade, HyWorks must have appropriate version file placed in appropriate directory, below are the details of placing Windows and Linux DVM Tools:

❖ **Windows DVM Tools:**

1. Place latest HyWorks DVM Tools for Windows in following directory:
   
   C:\Program Files (x86)\Accops\HyWorks\HyWorksUpgradeService\Updates\Windows

2. HyWorks will automatically pick the version from setup and will update details.
3. Respective desktops can be upgraded as described below.

❖ **Linux DVM Tools:**

1. Place latest HyWorks DVM Tools for Linux in following directory:
   
   C:\Program Files (x86)\Accops\HyWorks\HyWorksUpgradeService\Updates\Firmware

2. Update information of DVM Tools in following file:
   
   C:\Program Files (x86)\Accops\HyWorks\HyWorksUpgradeService\Updates\Linux\info.inf

   Following information must be passed:
   a. FileName=<Name of file placed in step#1> e.g. FileName=HyWorksDvmTools_Linux_merged_3.2.2.24.tgz
   b. Version=<Version of placed DVM tools> e.g. Version=3.2.2.24
3. Save the file.
4. HyWorks will read latest DVM Tools version information and desktops running lower versions can be upgraded accordingly. Upgrade process is defined below
To upgrade DVM agent, follow below steps:

1. Search and select desktop from list of DVMs
2. Click on button **Upgrade Agent**, based on current running tool version, following options will be displayed:
   a. DVMs running lower version:
      i. Option to upgrade components:
         1. HyWorks Desktop Agent
         2. HyWorks Built-in USB Redirection Driver
         3. HyWorks Printing Module (Session Server Extensions)
         4. HyWorks USB Cleaner
            a. Option to reboot DVM
      ii. Select appropriate options and click on **Upgrade** button
      iii. Upgrade will be initiated and respective DVM will get upgraded with latest version
   b. DVMs running greater version
      i. Upgrade is not possible
      ii. Appropriate message should be displayed, stating that the version running on DVM is already higher and cannot be upgraded.
   c. DVMs running same version: This can be treated as
      i. Option to upgrade components:
         1. HyWorks Desktop Agent
         2. HyWorks Built-in USB Redirection Driver
         3. HyWorks Printing Module (Session Server Extensions)
         4. HyWorks USB Cleaner
            a. Option to reboot DVM
      ii. Select appropriate options and click on **Upgrade** button
      iii. Upgrade will be initiated and respective DVM will get upgraded with latest version
External Session Delivery in HyWorks (TSE and Pano)

Though HyWorks itself works to deliver desktops from configured session providers, it also supports legacy application and shared hosted desktop delivery software TSE and dedicated desktop delivery software Pano as external session providers.

It is recommended to replace these legacy softwares with latest HyWorks but to maintain support for customers, HyWorks still supports desktop deliveries from these systems.
External Session Provider Configuration and Desktop Delivery

Following two types of external session providers are supported:

- Propalms TSE: for serving shared hosted desktop from Microsoft RDS Servers installed with Propalms TSE
- Pano Controller: For serving dedicated desktops from Pano Controller.

This section will provide information on adding external session providers.

Add Pano Controller as External Session Provider

1. Go to Server – Session Providers section
2. Click on Add button to invoke Add Session Provider wizard
3. Select Category as External Session Provider
4. Select Type as Pano Controller
5. Provider a logical name in Name field
6. In the Host Address text box provide IP or hostname of the Pano Controller address (e.g. 192.168.1.2 or PanoCtrl1.propalmsnetwork.com)
7. Select Extra Authentication checkbox to enable user authentication with HyWorks Controller (Not selecting this option will pass-on the user details to Pano Controller and password management won’t be possible). Refer section Extra Authentication for detailed information of this feature.
8. Specify if you want to make this Session Provider Active. Un-checking the option will make the Session Provider inactive and this Session Provider will be ignored when desktops are retrieved.
9. Click on Test Connection button to check connection with the specified Pano Controller server, on successful connection appropriate status message will be displayed
10. Click on Add button to continue adding the Pano Controller
11. Session Provider will be added, and HyWorks Controller will start connecting with configured Pano Controller, please note the Desktop Count will be displayed as NA because of Pano Controller being an External Session Provider where its Desktop management is done by its own management console.

Getting Desktops from Pano Controller

Desktop Pools using external session providers are not supported and users are always authenticated on configured Pano controller.

If user is having appropriate desktop assignment on Pano Controller, then its desktop session will be returned.

Note:

➢ Having mixed configurations of External Session Provider and Shared/ Dedicated Session Provider in single HyWorks deployment, may cause slow login as users are always authenticated twice, first at HyWorks Controller and second at External Session Provider.

Add TSE as External Session Provider

Go to Server – Session Providers section

1. Click on Add button to invoke Add Session Provider wizard
2. Select Category as External Session Provider
3. Select **Type** as TSE
4. Provider a logical name in **Name** field
5. In the Host Address text box provide IP or hostname of the TSE address (e.g. 192.168.1.2 or ProTSE.propalmsnetwork.com).

**Note:**
- **TSE Web Service** must be installed on respective TSE Server to configure it as Session Provider in HyWorks deployment.

6. Provide appropriate Domain information in Domain text box. The Domain field is optional however if this information is not provided then users will be required to provide domain information during logon. Therefore, for simple login it’s recommended to provide appropriate domain information.
3. Specify if you want to make this Session Provider Active. Un-checking the option will make the Session Provider inactive and this Session Provider will be ignored when desktops are retrieved.
4. Select **Extra Authentication** checkbox to enable user authentication with HyWorks Controller (Not selecting this option will pass-on the user details to TSE and password management won’t be possible). Refer section **Extra Authentication** for detailed information of this feature.
5. Select the checkbox **Add Secondary Session Provider**, if it’s needed to configure secondary Session Provider to support provider failover (This will enable **Secondary Provider Address and Domain** fields in Create New Session Provider tab)
   i. Provide appropriate IP or hostname for secondary TSE Server
   ii. Provide Domain information in Domain field
   iii. Refer section **Session Provider Failover Support** for detailed instructions
6. Click on **Test Connection** button to check connection with the specified TSE server, on successful connection appropriate status message will be displayed, click on
7. Session Provider will be added, and HyWorks Controller will start connecting with configured TSE Server, please note the **Desktop Count** will be displayed as NA because of TSE being an External Session Provider where its desktop or application management is done by its own management console.

**Getting Desktops from TSE Server**

Desktop Pools using external session providers are not supported and users are always authenticated on configured TSE Server.

If user is having appropriate desktop assignment on TSE Server, on client login controller will communicate with TSE server to get the assigned desktop settings and then forward the same information to the client with appending its connection profile.

Now client can connect to assign desktop using connection settings provided by the controller.

**Additional Configurations for External Session Providers**

In HyWorks v3.0 following features are available using Session Provider Configurations:
1. Session Provider Failover Support
2. Extra Authentication for Third Party Connection Broker

More detailed information about these features (configurations) will be provided below.
**Session Provider Failover Support**

HyWorks v3.0 supports configuring secondary provider in the Session Provider dialog to support high availability during the failure of one Session Provider.

**Supported Session Providers**

Provider Failover or secondary Session Provider is available for following types of Session Providers:

- In **External Session Provider** category
  - TSE

**Secondary Provider Configuration for TSE**

This section will guide you configuring secondary provider.

1. In Add Session Provider wizard:
   a. Select **Category** as External Session Provider
   b. Select **Type** as TSE
   c. In Name text box provide any logical name
   d. In the **Host Address** text box provide IP or hostname of the TSE Server address (e.g. 192.168.1.2 or TSE1.propalmsnetwork.com)
   e. Provide appropriate Domain information in Domain text box. The Domain field is optional however if this information is not provided then users will be required to provide domain information during logon. Therefore, for simple login it’s recommended to provide appropriate domain information.
   f. Select **Extra Authentication** checkbox to enable user authentication with HyWorks Controller (Not selecting this option will pass-on the user details to TSE and password management won’t be possible)
   g. Specify if you want to make this Session Provider **Active**. Un-checking the option will make the Session Provider inactive and this Session Provider will be ignored when desktops are retrieved.
   h. Select the checkbox **Add Secondary Session Provider** (This will enable **Secondary Provider Address** and **Domain** fields in Create New Session Provider tab)
      i. Provide appropriate IP or hostname for secondary TSE Server
      ii. Provide appropriate domain information for secondary TSE Server

2. Click on **Test Connection** button to check connection with the specified TSE server
   a. On successful connection to both the hosts appropriate status message with green background will be displayed and **Add** button will remain enabled
   b. If Primary server is down appropriate error will be displayed and **Add** button will be disabled
   c. If Primary server is reachable and secondary server is not reachable, then error will be displayed but **Add** button will be enabled.

2. Click on **Add** button

3. Session Provider will be added, and HyWorks Controller will start connecting with configured TSE servers.

4. TSE Servers are now configured to support failover. Refer section **Session Provider Failover Support** to understand the functioning of this feature.

**Provider Failover Mechanism**

Objective of the feature provider failover is to ensure that users will be continued to provide session even when one of the Session Provider is not available.
With two Session Providers (TSE or RDS) configured with secondary Session Provider, following few cases can occur:

1. **Both Session Providers Available**
   With both Session Providers available, HyWorks Controller will be providing sessions from Primary server only.

2. **Both Up and Secondary Goes Down**
   HyWorks Controller will serve connection from primary server.

3. **Both Up and Primary goes Down**
   Primary TSE server will not be used, and HyWorks Controller will start providing sessions from secondary server.

4. **Primary gets Up and Secondary Goes Down**
   HyWorks Controller will automatically start using Primary server to server sessions.

5. **Both server goes down and One comes up**
   HyWorks Controller will start using whichever server comes up to serve the desktops.

6. **Primary goes Down and gets Up again (Use Primary)**
   When Primary server will be down, HyWorks Controller will start using secondary server and if primary server gets up again then HyWorks Controller won’t start using it automatically until secondary goes down or administrator manually makes it primary.
   In this case button **Use Primary** is shown against the primary TSE server, clicking on this button will make HyWorks Controller to start using Primary TSE Server for providing next sessions.

### Extra Authentication

HyWorks v3.0 supports authentication for External Session Providers. Users logging-in from HyWorks Clients will be first authenticated with authentication server configured in HyWorks and then will be forwarded to respective Session Provider for getting the assigned desktop information.

This feature enables the user password management on HyWorks Client login screen itself, which serves the following purpose:

- Enabling users to change password in case of password expiry or first logo
- Notifying users with appropriate errors when
  - User account is disabled
  - User account is locked
  - User account is expired

### How to Enable Extra Authentication

Extra Authentication can be enabled from **Add / Edit Session Provider** wizard by selecting the checkbox **Extra Authentication**.

Extra Authentication feature is supported for following Session Providers of category **External Session Provider**:

- Pano Controller
- TSE

For enabling **Extra Authentication**, appropriate (Same as external provider's authentication server) must be configured in HyWorks Controller else user login will start failing with error no authentication server found.
Accops HyWorks v3.2 Administration

Connection Profiles

Connection Profiles in HyWorks can be used to define following two important aspects of user, application or desktop session:

1. Defining remote session performance, resource redirection, appearance configurations
2. Defining session timeouts

Connection Profiles can be managed from HyWorks Controller Management Console – Workspace – Connection Profile section.

Connection Profile Types

- **Default Profile**: This is a system generated non-removable but editable profile that will be assigned to devices by default, which means all the newly registered devices and devices with no profile will be assigned with default profile.
- **Admin Created Profiles**: Removable and editable profiles. Admin can create a new profile by clicking on Add button in Connection Profiles section.

Connection Profile Attributes

A connection profile has the following sections:

- **Basic Settings**: Only for identification of connection profiles.
  - Profile Name: Logical name of connection profile
  - Description: Logical description of connection profile

- **Experience**: Defining the user experience of remote session. All configurations are applied to remote session. To enable or disable user experience related features for remote session. Following settings will be enabled or disabled in remote session using Experience section settings
  - Connection Type: Custom\LAN\Modem\Broadband\Detect Automatically. Based on components chosen for connection type following attributes can come as auto-selected, which administrator will be able to modify.
    - **Visual Styles**: To enable or disable desktop themes
    - **Font Smoothing**: Configure smooth fonts in remote session
    - **Desktop Background**: To allow desktop wallpaper configuration
    - **Desktop Composition**: Enable or disable desktop composition in remote session
    - **Menu and Windows Animation**: To allow animated display
    - **Show Window Contents While Dragging**: Show contents while dragging the window
  - Persistent Bitmap Caching: To allow bitmap caching during remote session
  - **Automatic reconnect the session**: Configure if sessions should attempt to reconnect automatically if disconnected due to network issues or similar problems

Selecting specific **Connection Type** also enables or disables relevant experience attributes as listed in table below:

<table>
<thead>
<tr>
<th>Connection Type</th>
<th>Default Selected Features</th>
<th>Default Deselected Features</th>
<th>Selection Possible</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Default Deselected Features</td>
<td>Selection Possible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default Deselected Features</td>
<td>Selection Possible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default Deselected Features</td>
<td>Selection Possible</td>
</tr>
</tbody>
</table>

Accops Systems Private Limited 206
### Display Configuration

These configurations also apply to remote session.

- **Color**: Defines the color depth for the remote session
- **Monitor**: For configuring multi-monitor configuration. Available options are **Native**, **Multiple Display** and **Extended Display**.
  - With HyDesk/Linux devices, this configuration must be kept to **Native** and multi-monitor configuration should be done from Device Settings.
  - For Windows Clients this setting can be used along with advanced options for setting up appropriate display settings for end-users.
- **Display connection bar**: (Applicable for Windows Clients only) On enabling, desktop sessions will be shown with connection bar and user can minimize or maximize desktop.

**Note:**
- The Multimonitor settings on devices should always be done from Device Settings only. See [Device Settings](#) section for more details on Multimonitor settings for devices.

### Local Resources

Applies to remote session, for redirection of local resources and multimedia configurations

- **Multimedia**:
  - **Audio Mode**:
    - Redirect to this endpoint (Enable redirection to client)
      - Audio Quality: High/ Medium/ Dynamic (As matching the server-side configuration)

**Note:**
- Limiting the quality of audio playback can improve connection performance, particularly over slow links and thus should be wisely configured as per requirement.
• Do not redirect: Stop Audio redirection
• Play on remote computer
  ▪ **Microphone:**
    • Redirect to this endpoint: Enable redirection to client
    • Do not record
  ▪ **Enable Video Redirection:** Not required with RDP8/RDP10 protocols on HyDesk devices.
  
  o **Local Drives and Resources:** Enabling redirection of local drives and resources to the endpoints
    ▪ **Drives:** For redirecting client-side drives to remote session. Applies to Windows Clients and HyLite. Following options are available:
      • Redirect all
      • Specific Drive (Specify the drives to be shared)
    
    The settings are not applicable for HY2000, HY3000, HY4000 or TS3020 HyDesk devices. Additional command lines can be specified to redirect drives on Linux client platforms.
    ▪ **Clipboard:** Enable clipboard support in remote session. Applies to Windows Clients and HyLite
    ▪ **Printers:** Enable printer redirection. Applies to Windows Clients and HyLite
    ▪ **Smart Card/Ports/Plug n Play devices:** Redirection of the Smart Card, Ports or Plug n Play devices, applies to windows clients only.
  
  o **Redirect All USB Drives:** Applies to HyDesk devices only, for controlling USB redirection using Built-in or Enhanced USB Redirection driver. Driver selection can be configured from Management Console -> Endpoints -> Device/Group or Default Settings
  
  o **Redirect Multi-Touch Device:** Applies to HyDesk devices only, for enabling multi-touch device redirection.
    It is important to know that redirection of Multi-Touch device may require additional device drivers to be installed on client (HyWorks Clients) and server (Desktop to be connected)
  
  o **Allow RDP Plugins:** This configuration is supported only on Windows Clients, for enabling/disabling session server extensions-based features e.g. HyPrint, File transfer

• **Advanced Settings:** Advanced configuration options for remote session.
  
  o **Enable Console:** To provide console access to the user. Should be kept disabled until required to give console access to user.

**Note:**

➢ Accessing remote session with this flag enabled using non-admin user could result in session connection failure.

  o **Remote FX:** To enable Remote FX support in remote session which could help in improved remote session performance. Howsoever only enabling Remote FX in connection profile, don’t work and it also requires hardware and software level changes on the remote server to make it work.
o **Enable Graphics Acceleration**: Enabling graphics acceleration can help in getting improved graphical and video performance. But the following facts should be remembered while using this remote session enhancement feature
  ▪ **This attribute is applicable for only HyDesk Hy2000, Hy3000 and HY4000**
  ▪ With RDP7 protocol, the option does not have any impact and thus can be kept disabled.
  ▪ With RDP8 protocol, this option can be enabled to have better graphics but if target desktop is having RDP10 i.e. Windows 10 or Windows 2016 session may freeze on access.
  ▪ Best graphical performance could be achieved with RDP10 protocol on HyDesk device and graphics acceleration option enabled including session of RDP10 windows machines.

o **Enable Progressive GFX**: To enable progressive GFX in remote session.

o **Enable Compression**: For enabling compression of remote session data.

- **Protocol Security**: Protocol Security section in Connection profile determines the security protocol to be used while connecting to remote server. Improper configuration of security protocol may lead to connection failure and thus should be configured cautiously. Following configurations are possible:
  o **Auto**: Automatically choose the best security settings as per capabilities negotiated between client (HyWorks Clients) and server (target Desktop to be connected)
  o **Force (Enabled)**:
    ▪ Enable RDP: Uses RDP security settings forcefully and may fail if server is using NLA or TLS level settings
    ▪ Enable NLA: Pushes NLA level security settings from client side
    ▪ Enable TLS: Uses TLS security settings from client side for remote connection
  o **Force (Disabled)**:
    ▪ Enable RDP: Un-checking this will ignore RDP for remote connection and will use NLA or TLS, whereas selecting this option will specify RDP security settings as well for remote connection.
    ▪ Enable NLA: Deselecting this will ignore NLA for remote connection and will use RDP or TLS
    ▪ Enable TLS: Deselecting this will ignore RDP for remote connection and will use RDP or NLA
  o **Enable CredSSP**: For supporting Credential Security Support Provider. For NLA enabled SHDs or app delivery, this can be kept enabled.

- **Session Timeouts**: Session timeouts in connection profiles apply to following two types of sessions:
  1. Remote sessions on Session Host Server or Desktops
  2. User sessions on HyWorks Controller as well.

More information about applying session timeouts will be explained later in this section. Following configurations are available in Session Timeouts section:

  o **On Client - Disconnect**: Defining how the client disconnect should be interpreted on controller, following decisions can be made:
    ▪ **Disconnect the user session**: Keeping the associated sessions in disconnected mode
    ▪ **Logout the user session**: Completely logging-out the user session along with associated sessions.
Enable User Inactivity Monitoring: To enable/ disable user inactivity monitoring
  ▪ Make User Session Idle In: Time in minutes after which inactive (session with no user activity) will be marked as idle
  ▪ Expire Idle Session In: Time in minutes after which idle sessions will be removed as per the configured On Expire settings.
  ▪ On Expire: Determines if sessions should be disconnected or logged out on expire
    • Disconnect the user session
    • Logout the user session

Set Max Session Timeout: To enable only limited time remote session.
  ▪ Force Terminate User Session In: Time in minutes after which user session will be forcefully terminated
  ▪ On Exceeding Max Session Timeout: Determines, if sessions should be disconnected or logged out on expire
    • Disconnect the user session
    • Logout the user session

Logoff Disconnected Session After: Time in minutes after which disconnected sessions will be logged-out from controller or session host server.

Application Access Settings: Important configurations defines the remote session appearance and access methods. Following configurations are available:
  ▪ Application Launch Mode: Decides how the applications will be launched
    ▪ Remote App: Remote applications will appear like native applications and all applications will run in single remote sessions on session host server.
    ▪ Shell: Applications are launched in separate windows shell, which means every application session will be launched in different remote session and will lead to multiple license consumption for single user.
  ▪ Session Experience Option: Defines the launching experience of the remote session. Applies to windows clients only, following options are available:
    ▪ Always Seamless: Sessions will be launched in seamless mode and until the session is connected completely, HyWorks custom dialog and progress bar will be displayed
    ▪ Non-Seamless on Error: HyWorks custom dialog and progress bar will be displayed, until any error occurs. On error, the Seamless window will disappear.
    ▪ Never Seamless: Remote desktop window will be displayed always to handle any unknown prompts or error. This opens another parent application window.

Additional Settings: Any other custom attributes can be defined using additional settings section. Additional command line option for different protocols can be defined here. Additional command line options can be specified for following protocols:
  ▪ RDP 7.0 (Linux): Use this section for Linux based clients running with RDP10 or RDP8 protocols. Example -k 0x00000407, -a 32
  ▪ RDP 8.0 (Linux): Use this section for Linux based clients running with RDP10 or RDP8 protocols. Example: /floatbar
  ▪ RDP (Windows): Use this section for Windows based clients. Example connection type:i:7
  ▪ Generic RDP: As per format supported by client using generic RDP (HyLite).
Note:
➢ Additional command line options are very useful. But with Linux Clients the invalid command line attributes can result in session failures as well.

In above section, information about all the attributes of Connection Profile has been given. The later section of document will detail about creating, modifying and deleting connection profiles.

Connection Profile Management Options

Connection Profiles tab in Workspace section allows administrator to perform following management options:

Create a New Connection Profile
To create a new Connection Profile, follow the below steps:
1. Go to Connection Profile section
2. Clicking on the +Add button to open the form for new connection profile.
3. In Add Connection Profile wizard, provide all mandatory information and enable or disable all required settings in different sections
4. Once all configurations are done, click Add Profile button to complete the operation.
5. The new profile will be added and displayed in Connection Profiles section.
6. Administrator can assign the new profile to devices from Device Settings dialog or using button Assign Profile in Endpoints tab

Edit Connection Profile
1. Go to Connection Profiles section in HyWorks Controller Management Console
2. Select the connection profile and click on Edit button
3. All fields are editable - update the required configurations and click on Update button.

Delete Connection Profile
1. Go to Connection Profiles section in HyWorks Controller Management Console
2. Select the connection profile and click on Delete button
3. Confirm the action by clicking on Delete button on Confirm Action dialog. The profile will be deleted.
4. Connection Profile will be deleted and will be removed from Connection Profile section in Setup tab

Note:
➢ Default Profile cannot be deleted.
➢ On deletion, connection profile with any existing references will display appropriate error and will not get deleted until all the references are deleted completely.

Connection Profile Assignment and Fallback Model in HyWorks
In HyWorks v3.0, a connection profile can be assigned to multiple objects to have maximum granularity while providing application or desktop sessions to the clients. Following objects can be assigned with connection profile in respective sections:
1. **Endpoints:**
   a. Default Settings: To all devices using default settings
   b. Group Settings: To a group of devices using Group settings
   c. Device Settings: To individual devices using Device Settings

2. **Entitlements:**
   a. Users: To assign devices to different users, assignment can be done from Entitlements -> Users section
   b. User Groups: To assign connection profile to a group of users, Entitlements -> Groups section can be used
   c. OUs: To assign connection profile to an OU, Entitlements -> OUs section can be used
   d. Pools: User based shared hosted desktop pools can be assigned with specific connection profiles from Entitlements -> Pools section.

3. **Desktop Pools:** To use any specific connection profile for a desktop pool, connection profile can be assigned to a desktop pool as well. Desktop pools can be assigned with connection profile from Add/Edit Desktop Pool wizard.

4. **Applications:** Applications can also be assigned with specific connection profile while being added or being modified in Add Application or Edit Application wizard respectively.

---

**Connection Profile Fallback Model**

Connection Profile fallback model in HyWorks defines, the priority order in which connection profile can be applied.

Connection profiles are used to define two types of attributes for a session:

1. **Session timeouts**
2. **Connection parameters**

Session timeouts are derived from connection profile applied to user, whereas connection attributes for application or desktop sessions are derived from connection profile applied to application session or desktop session.

Connection Profile priorities are calculated in the following manner based on the type of client from where user is logging-in:

Connection profile are used in following priority order:

<table>
<thead>
<tr>
<th>User Session</th>
<th>Application Session</th>
<th>Desktop Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned to User</td>
<td>Assigned to Application</td>
<td>Assigned to Desktop Pool</td>
</tr>
<tr>
<td>Assigned to Group</td>
<td>Assigned to User</td>
<td>Assigned to User</td>
</tr>
<tr>
<td>Assigned to OU</td>
<td>Assigned to Group</td>
<td>Assigned to User Group</td>
</tr>
<tr>
<td>Assigned to Device (*Only when desktop client is being used to login)</td>
<td>Assigned to OU</td>
<td>Assigned to OU</td>
</tr>
<tr>
<td>Assigned to Device Group (*Only when desktop client is being used to login)</td>
<td>Assigned to Device (*Only when desktop client is being used to login)</td>
<td>Assigned to Device Group (*Only when desktop client is being used to access)</td>
</tr>
<tr>
<td>Organization Default Settings (For HyLite based logon)</td>
<td>Assigned to Device Group (*Only when desktop client is being used to login)</td>
<td>Assigned to Device Group (*Only when desktop client is being used to login)</td>
</tr>
</tbody>
</table>
Organization Default Settings (For HyLite based access) | Organization Default Connection Profile (For HyLite based access)  
--- | ---  

Let us try to understand this priority order using an example:
User-1 is member of group-2 and both are path of OU-3. User-1 is assigned with an application app-4 and desktop pool-5 and the connection profiles are assigned in following manner:

1. User-1 -> Profile-1  
2. Group-2 -> Profile-2  
3. OU-3 -> Profile-3  
4. App-4 -> Profile-4  
5. Pool-5 -> Profile-5

**Connection Profile Assignments and Precedence:**
The connection profiles will be assigned to

1. The user session and all remote session timeouts will be managed though connection profile assigned to user i.e. Profile-1 (as User is having highest priority), which means if profile-1 is having idle timeout as 5 minutes, then user sessions and remote sessions will be marked idle on inactivity of 5 minutes, though other connection profiles have some other timeouts defined for them.  
2. While accessing the application app-4, the applied connection profile on remote session will be Profile-4 as application is having higher precedence over user, but this won’t change the user session connection profile which is already using Profile-1 and the session timeouts for app session will be used from the profile assigned to user session.

**Note:**
- Connection Profile assigned to application takes precedence while setting up the remote session only when
  1. When Shell mode is enabled, the connection setting assigned to the application is used. If no connection is assigned to the application, then the connection profile assigned to the user will be used.  
  2. In RemoteApp mode, the application session is the first from that session host server, else the remote app will use the connection profile being assigned to first application.
- Now if the user accesses the desktop from the assigned pool, remote session environment will be decided by the user assigned connection profile (having the high precedence over pool) and the session timeouts for the remote session will also be defined from user assigned connection profile.

**Connection Profile Assignment in Conflicting Situations**
In following cases, conflicting situation occurs where the user is being assigned with two connection profiles.
1. In case user is member of two groups and both groups are assigned with different connection profiles

**Applied Connection Profile:** In such cases, controller randomly selects the connection profiles and assigns it to the user.
Sessions - Monitoring Logged-in Users/VDI/ Application Sessions

Sessions section in Management Console - Monitoring can be used to monitor user sessions, VDI sessions and application sessions.

User Sessions
Section Monitoring - Sessions - User Sessions
As soon as any user logs in from HyWorks client or User Workspace portal or HyLite, user session is created and can be tracked in User Sessions section.
User Sessions section provides a list view of all user sessions, providing following information:

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Username</td>
<td>Displays the username of the logged in user</td>
</tr>
<tr>
<td>2</td>
<td>Endpoint Type</td>
<td>Type of Endpoint (HyDesk/ HyLite)</td>
</tr>
<tr>
<td>3</td>
<td>Device Name</td>
<td>Displays the name of the device, if user has logged in from HyDesk or HyWorks Client</td>
</tr>
<tr>
<td>4</td>
<td>IP Address</td>
<td>IP address of the machine from where the user has logged-in. In case of HyLite, this will be IP address of HySecure Gateway</td>
</tr>
<tr>
<td>5</td>
<td>Connection Profile</td>
<td>Connection profile applicable for this user session</td>
</tr>
<tr>
<td>6</td>
<td>Application Sessions</td>
<td>Count of application sessions</td>
</tr>
<tr>
<td>7</td>
<td>Virtual Desktop Sessions</td>
<td>Shown with tick (✓) mark if user is having any running full desktop session and shown with cross (X) mark if no desktop session is running</td>
</tr>
<tr>
<td>8</td>
<td>Status</td>
<td>Status of User session, which could be Active/Idle/Disconnected</td>
</tr>
</tbody>
</table>

Remove User Sessions
Selecting a single/multiple session, enables the administrator to remove the user sessions.
Use session removal presents following options to the administrator in Confirm Action dialog:

1. Logoff all active sessions:
   a. Select this check box to completely wipeout the user session along with all associate application and desktop sessions
   b. Keeping this as unchecked will only disconnect the user and associated application and desktop session
2. Show wait message: On selecting this option
   a. **Message:** Text area control will be displayed, which can be used to show a custom message to the user, while removing the session
   b. **Time:** Wait time, after which the session will be removed

Steps to Remove User Session(s):
To remove user sessions, follow the below steps:

1. Go to Monitoring – Sessions – User Sessions
2. Select single or multiple user sessions
3. Click on button **Remove Session(s)**

4. In **Confirm Action** dialog, select available options as per requirement
   a. Logoff all active sessions:
      i. Select this check box to completely wipeout the user session along with all associate application and desktop sessions
      ii. Keeping this as unchecked will only disconnect the user and associated application and desktop session
   b. Show wait message: On selecting this option
      i. **Message:** Text area control will be displayed, which can be used to show a custom message to the user, while removing the session
      ii. **Time:** Wait time, after which the session will be removed

5. Click on **Remove** button.
6. Sessions will be removed/disconnected as per selected options.

**User Sessions Removal Cases**

User sessions are the topmost container listing the currently logged-in user sessions and displaying all the Application and Desktop Sessions running for that user. Removing a user. User session will have following behavior:

1. Controller provides the option to remove one or more user session
2. User sessions can be completely removed or disconnected
3. Sessions can be removed with message and timer also, but it depends on availability of
   a. RDP Extensions Client Module
   b. RDP Extensions Server Module

**1. Disconnecting the User Session**

a. All associated desktop or application sessions will also get disconnected
b. Application sessions running in Shell mode won’t be able to reconnect
c. SHD and Application Sessions in Remote App Mode can be reconnected before the user session is expired

**2. Logging Off All Active Sessions:**

a. Removing a user session with option checked to log off all active sessions will also remove (logout)
   i. All Provider Sessions of that user (Logout)
   ii. All VDI Sessions of that user (Logout)

b. User Session Removal will require session agent to be available to execute all the tasks

c. User session disconnection timer gets updated on controller when client notified back about disconnection

**VDI Sessions**

VDI Session section displays the list of all desktop sessions (dedicated/ shared hosted desktops). Administrator can remove any specific VDI session by clicking on **Remove Sessions** button.
The VDI sessions tab provides the following information in tabular format:

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Username</td>
<td>Displays the username of the logged in user</td>
</tr>
<tr>
<td>2</td>
<td>Device Name</td>
<td>Displays the name of the device, if user has logged in from HyDesk or HyWorks Client</td>
</tr>
<tr>
<td>3</td>
<td>IP Address</td>
<td>IP address of the machine from where the user has logged-in. In case of HyLite, this will be IP address of HySecure Gateway</td>
</tr>
<tr>
<td>4</td>
<td>Session Id</td>
<td>Remote Session Id on Session Host Server</td>
</tr>
<tr>
<td>5</td>
<td>Pool Name</td>
<td>Name of the desktop pool from where sessions are coming</td>
</tr>
<tr>
<td>6</td>
<td>Desktop Name</td>
<td>Name of accessed desktop VM. In case of SHD this will display session host server name</td>
</tr>
<tr>
<td>7</td>
<td>Desktop IP Address</td>
<td>IP Address of the desktop connected by desktop</td>
</tr>
<tr>
<td>8</td>
<td>Status</td>
<td>Status of the desktop session (Connected/Disconnected)</td>
</tr>
<tr>
<td>9</td>
<td>Remote Control</td>
<td>Option to take remote control of connected session. Applicable for SHD sessions only.</td>
</tr>
</tbody>
</table>

Remove VDI Session

1. Go to Monitoring – Sessions – VDI Sessions
2. Select any VDI session by clicking on respective checkbox
3. Click on button **Remove Session(s)**
4. Confirm the action in displayed dialog box
5. Selected VDI Sessions will be logged out.

Behavioral Facts of SHD and Desktop VM Sessions

**Dedicated Desktop VMs Sessions**

1. No option to select between disconnect and logout
2. No option to send message to client
3. Default VDI Session Removal Behavior: Disconnect the sessions (Unsaved user data will not be lost until session expires)
4. Removing Session When Session Host Agent is not available: Session will be removed with success message, but warning will be logged in logs
   a. On HyLite: Session can run infinitely as client does not sync the sessions (App/Desktop)
   b. On HyWorks Client: Sessions will be disconnected on next heartbeat sync

**Shared Hosted Desktop Sessions**

1. No option to select between disconnect and logout
2. No option to send message to client
3. Default VDI Session Removal Behavior: Logout the RDS session (Unsaved user data will be lost)
4. Removing Session When Desktop Agent is not available: Session will be removed with success message, but warning will be logged in logs
a. On HyLite: Session can run infinitely as client does not sync the sessions (App/Desktop)
b. On HyWorks Client: Sessions will be disconnected on next heartbeat sync

**App Sessions**
App Sessions are comprised of Provider Sessions and Application Sessions. Provider sessions are the container for all application sessions running under same RDS session.

**Application Sessions**
Any independent application accessed using HyWorks Client or HyLite will be logged in HyWorks Controller Management console and will be termed as App session. All applications being delivered to users are tracked using unique App Session Ids. Following behavior of the app session is available:

1. Some applications e.g. Internet Explorer (x86) invokes another process of 64bit Internet explorer and then exits. -> In this case HyWorks Session host may try to get track of Child application, but if it fails to get the details of Child process then it will lose the track of app session and when the entry will be shown as “0” -> Zero app sessions.
   a. But provider session (Please see next section) will be kept alive as some child process is running -> In this case the reconnection won’t be possible.
2. Closing application session does not provide any option to disconnect or logout. It will simply close the selected application
3. In case of same apps is launched multiple times, no identification mechanism is available for uniquely identifying any app
4. While closing the application session, administrator can choose to send a custom message with timer
   a. HyWorks Client: Message will be displayed, and application will remain active for provided time
   b. HyLite: No message will be displayed but application will be closed as per the provided time
   c. Dependency for Custom Message: RDP Extensions
5. Remove App Sessions when Session Host Agent is not available: Removing App session when Session Host Agent is not available
   a. HyWorks/HyLite: App session removal will be failed, and an error entry will be created followed by appropriate warning entries

**Provider Session**
RDS session (WTS Session), under which multiple application sessions run, is termed as Provider session. The provider session can have following behavior:

1. A single provider session can have one or multiple application sessions
2. For the applications whose control is lost (which invokes child processes and gets itself killed later.), will have no application session entry and will not be shown under the provider session.
3. Provider session will have unique WTS Id associated with it.
4. Selecting a provider session, enables the terminate Process(s) button which can be used to **completely logout** the specific RDS session
5. Multiple Provider sessions can be removed together, and it will also logout all the associated App sessions
Session Provider Management

The term **Session Providers** refer to the servers which can provide remote sessions to end users. Based on the types of desktops being served by servers, they can be kept into various categories:

Session Provider Categorization

Session Providers are kept into following three distinct categories:

- Shared Session Host
- Dedicated Session Provider
- External Session Provider

❖ **Shared Session Host**

Please refer section [Shared Session Host Management](#) for detailed information on management of shared session hosts in HyWorks,

❖ **Dedicated Session Provider**

Please refer section [Dedicated Session Provider Management](#) for detailed information on management of dedicated session providers in HyWorks.

❖ **External Session Providers**

Session Providers which have independent management capabilities and thus all the user assignments are done from their respective management console are kept under External Session Provider.

For such Session Providers HyWorks Controller only works as a mediator to pass on the login information and getting the information of assigned desktop.

Following two types of External Session Providers are supported:

- Pano Controller
- TSE

**Pano Controller**

The Pano System enables organizations to centralize desktop computing inside the data center rather than having it scattered across user’s desktops. Pano Controller currently supports the following windows virtual desktops:

- Windows 7
- Windows 8
- Windows 8.1

**Supported Pano Controller Version**: Version 6.0.1

**Propalms TSE**

TSE (Terminal Server Edition) is an application-delivery management program that works within the network-centric, server-based computing paradigm. TSE as an external session provider in HyWorks can be used to provide shared hosted desktops from following two Microsoft RDS Servers running module TSE App Server:

- Windows 2008 R2
- Windows 2012 R2

**Supported TSE Versions**: Version 7 with **Web Service**
Please refer section External Session Delivery in HyWorks (TSE and Pano) for detailed instruction on configuration and management of external session providers.

**Note:**
- In case of External Session Providers, desktop assignments are done through their independent management console.
  For details about installation, management and configuration of Pano Controller or TSE, please visit [http://www.accops.com](http://www.accops.com).
System
System section in HyWorks is for configuring system (HyWorks controller system) related settings. These configurations are very critical and thus available to only super administrators only.

System section consists of following important subsections: License, Backup Restore, SMTP Configuration, Virtual Profiles, Service Path, Service Config, and Advance Config.

Available configurations in each of these sections will be explained in this section.

License
For license management of HyWorks deployments. Go to section Licensing in HyWorks for detailed information.

HyWorks Backup Configuration
HyWorks Controller Management -> System -> Backup Restore section can be used to back up HyWorks database. All detailed information can be found in section HyWorks Controller Database Backup and Restore.

SMTP Configuration
SMTP configurations for HyLabs notifications or sending database over email can be done from Management Console -> System -> SMTP Config section. Detailed information is available in section SMTP Configuration for Email Notifications.

Virtual Profiles
Virtual Profiles sub-section under Section can be used for configuring Virtual IP profiles to be assigned to applications for per-program IP virtualization.

By default, Virtual Profile section, contains a default virtualization profile, which is read-only by default and have Network Virtualization disabled.

Following administrative tasks can be performed:
- Add Virtualization Profile
- Edit Virtualization Profile
- Delete Virtualization Profile

Add Virtual Profile
1. Go to System – Virtual Profiles section
2. Click on Add button
3. In Add Virtualization Profile wizard
   a. Provide appropriate Name for new Virtualization Profile
   b. Select Enable Network Virtualization
4. Click on Save button to save the details
5. Virtualization Profile will be saved and can now be assigned to applications for network virtualization
Edit Virtual Profile
1. Go to System – Virtual Profiles section
2. Select listed virtual profile
3. Click on Edit button
4. In Edit Virtualization Profile wizard
   a. Provide appropriate Name for new Virtualization Profile
   b. Select or Unselect Enable Network Virtualization
5. Click on Save button to save the changes.

Delete Virtual Profile
1. Select listed virtual profile
2. Click on Delete button
3. Confirm Action dialog box will be displayed, confirm the action
4. Virtual Profile will be deleted and will not be displayed in Virtual Profiles list

Note:
➢ If selected virtual profile is in use by any application, then deletion of profile will fail with appropriate error.

Service Path
Service Path sub-section in System can be used to point HyWorks Controller Management Console to connect to HyWorks Controller service.

Default Service Path
By default, Service Path section displays the currently configured HyWorks Controller service path:

<table>
<thead>
<tr>
<th>HyWorks Controller Service Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Localhost</td>
</tr>
<tr>
<td>Enter Service Path</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Change Service Path
If it is required to point HyWorks Controller Management console to some other HyWorks Controller Service, then following steps can be followed:
1. Go to System – Service Path section
2. Uncheck option Localhost, if it is checked
3. Provide path of HyWorks Controller service with port number e.g. https://<hostname> or IP of Controller service>: <portnumber>
4. Click on Update button
5. Current session will be logged out and administrator will be redirected to login page requiring administrator credentials for new HyWorks service.

Note:
➢ While configuring HyWorks Controller Service path, if the management console fails to connect to new controller service then it will automatically reset to the last saved HyWorks Controller Service Path.

Service Config
Service Config sub-section in System section can be used to configure some important configurable settings of HyWorks Controller. Following configurable settings are available:

➢ Discovery Settings
  o Stop/Start HyWorks Controller Broadcasting
  o Edit (Configure Broadcasting Interval)
➢ RDP Proxy Server Settings
  o Stop/Start RDP Proxy Server
  o Edit (Configure RDP Proxy Server Port and VM RDP Port)

Discovery Settings
Discovery setting defines the discovery mechanism of the HyWorks Controller by HyWorks Clients. The default configuration of devices/ endpoints is to detect HyWorks Controller automatically though administrator can still configure HyWorks Controller on devices manually by providing appropriate IP/Hostname and Port information.

Mechanism:
For detecting HyWorks Controller automatically, HyWorks Controller broadcasts its information on the network for port 39003 and devices keep on listening for broadcasts on port 39003. Once the broadcast is received by devices, they start communicating with HyWorks Controller.

This is an ideal deployment scenario where devices can communicate with HyWorks Controller directly and broadcasts are not blocked. However, in case of 'connection over internet' or 'with firewall in between', the HyWorks Controller should be configured manually, and broadcasting mechanism cannot be used.

Discovery Settings in System – Service Config section enables administrator to stop/start HyWorks Controller broadcasting if it's not in use or configure broadcasting duration.

Default Configuration
By default, discovery settings are stopped, and broadcasting is not enabled. However, administrator can start the broadcasting (if needed).

Start Broadcasting
1. Go to System – Service Config section – Discovery Settings
2. By Default, Broadcasting is stopped in HyWorks Controller
3. Click on Start button to start broadcasting
4. Settings will be saved, and controller broadcasting will get started as per configurations

**Stop Broadcasting**
If broadcasting is started, then it can be stopped using same process as used to Start the broadcasting:

1. Go to System – Service Config section – Discovery Settings
2. Click on **Stop** button will be displayed if it’s already started
3. Settings will be saved, and controller broadcasting will get stopped as per configurations

**Edit Discovery settings**

1. Go to System – Service Config section – Discovery Settings
2. Click on **Edit** button to **Edit Discovery Settings** dialog
   a. Provide appropriate entries for **Broadcasting Interval** field in seconds
3. Click on **Apply** button to apply the settings
4. New broadcasting interval will come into effect

**RDP Proxy Server Settings**
RDP Proxy Server in HyWorks Controller provides mechanism to connect to desktops or applications over the internet where devices do not have direct access to desktops but could connect to HyWorks Controller using its public IP.

Following RDP Proxy Server Settings could be configured from HyWorks Controller Configuration section:

**Stop/Start RDP Proxy Server**

1. Go to System – Service Config – RDP Proxy Server Settings section
2. By Default, ‘**RDP Proxy Server**’ is started with HyWorks Controller
3. Click on **Stop** button to stop RDP Proxy Server
   a. Proxy server will be stopped and sessions using HyWorks Controller proxy will not work
4. Click on **Start** button to start RDP Proxy Server if stopped
   a. Proxy server will be started, and users will be able to connect to assigned applications or desktops using Controller Proxy

**Edit RDP Proxy Server Settings**

1. Go System – Service Config - RDP Proxy Server Settings section
2. Click on **Edit** button to open RDP Proxy Server Settings wizard
3. Provide appropriate entries in RDP Proxy Server Port (if Proxy Server must be started on some other port)
4. Provide appropriate entries in VM RDP Port (If VMs RDP Port is different than current)
5. Click on **Apply** button to apply new RDP Proxy Server settings
6. RDP Proxy server will be stopped and started with new configured settings

**Advance Config**
Advance Config sub-section under System is very critical system level configurations and should not be configured until advised by Accops team.

The configurations are currently not defined for normal user but being redefined with user-friendly names.
Example of available configurations are:

1. Heartbeat Interval: Configuration decides what should be the default heartbeat interval for registered endpoints. Should not be modified to have very low value as it could affect system performance.
2. DBlog_MAXRecords: Maximum number of DB records to be kept in HyWorks Controller. After reaching the log limit, HyWorks Controller starts rotating the logs. Default value is now 500000.

Modifying Advance Configurations

To modify advance configurations, follow the below steps:

1. Login into HyWorks Management Console using Super-Administrator credentials (Advance Configurations are available to super-administrators only)
2. Go to System – Advance Config section
3. By default, all configurations are shown in disabled mode
4. Click on Edit button, displayed against the field to be modified e.g. Heartbeat Interval
5. Provide new configurations as per instructions in the description column
6. Click on Update button to apply the settings

Note:
- Few settings will require HyWorks Controller Service to be restarted. Please contact Accops Support Team before modifying any of advance configurations.
- All advance configurations can affect HyWorks functioning as well HyWorks performance and thus should not be modified directly. Accops Support team should be contacted for changing Advance Configurational Changes.

Few Example Configurations & Usage

This section will cover some example configurations which can be used to set some important performance or functional aspects.

But this is important to be configured with the help of Accops support team for best results and avoiding failures.

**Setting Endpoints Heartbeat Interval**

**Configuration name: Heartbeat Interval**

**Default Value:** 40

**Usage:** All endpoints use this interval to communicate with HyWorks Controller, also any relevant configurations on endpoints can be set using this heartbeat interval.

In large deployments with too many desktop clients, the heartbeat interval can be increased to improve performance overhead of processing heartbeats from too many endpoints.

Note: Increasing heartbeat interval causes longer gaps in communication with endpoints and thus any settings changed on controller will take effect as per configured interval.

**In Session HyDesk Heartbeat Timeout Multiplier**

**Configuration:** In Session HyDesk Heartbeat Timeout Multiplier
**Default Value: 3**

**Description/Usage:** With user-logged-in heartbeats are also usage this configuration to increase default heartbeat time, which means if a device with no user logged-on sends heartbeat in 40 seconds, the same device with user logged-on will send heartbeat in 40*3 (Consider multiplier is set as 3) = 120 seconds.

---

**Disable HyDesk Activity Monitoring**

**Configuration:** Disable HyDesk Activity Monitoring

**Default value:** True

**Description/Usage:** By default, endpoints sends timer details if any user activities are there or not, but in cases where user has logged-in, active on desktop but not accessing any desktops/applications. In such cases HyWorks usage this flag to determine if information sent by endpoints about user being active should be considered or not.

It should be kept as true as HyWorks will then ignore user activeness details by client with no desktops or apps accessed.

---

**Enable Win Alternate Shell**

**Configuration:** Enable Win Alternate Shell

**Default Value:** True

**Description/Usage:** Defines the windows shared hosted desktops access mechanism. If end-users are switching in between different types of clients e.g. HyLite, Windows or Linux based clients, then keeping the flag as True, makes sure that same shared hosted desktop session will be reconnected.

**Note:** The configuration is not supported by v3.1 or lower version of Windows endpoints.

---

**AD group Retrieval type**

**Configuration:** AD Group Retrieval Type

**Default Value:** 3

**Description/Usage:** Determines which functions should be used to fetch user groups from configured active directory authentication server.

In some cases when administrator may change group membership in AD very frequently, then 3 group retrieval may not fetch changed membership details and thus can be switched to type 4.

Type 4 group retrieval mechanism does not provide default built-in groups e.g. domain users, domain admin groups details and thus any entitlements using these groups may fail.

**Note:** Group retrieval type must be considered very carefully and should be kept as default unless advised and explained by Accops team.

---

**Force RemoteApp Conversion**

**Configuration:** Force RemoteApp Conversion

**Default Value:** True

**Description/Usage:** Forcefully converting application access mode to Shell for MAC Client with Accops RDP being used as access protocol. The forceful conversion will take place when access mode in defined connection profile is RemoteApp.

Shell mode access mechanism provides better performance, but RemoteApp mode provides seamless access experience and thus configuration has to be changed as per requirement.
User Authorization Control
Configuration: User Authorization Control
Default Value: True
Description/Usage: If true HyWorks fetches user’s group and OU information from configured active directory authentication server. Disabling it will cause entitlements not working done using user groups or OUs.
Can be disabled in deployments where major performance or slowness is observed due to group fetching from active directory authentication server, but the deployment must use only user based entitlements. Recommended to keep it as true only.

User Authentication Control
Configuration: User Authentication Control
Default Value: True
Description/Usage: Authenticating user with configured authentication server. Recommended to keep it as true. But in workgroup environments where user password may be different on front-end HySecure server and HyWorks, authentication can be kept as false as user will get authenticated via HySecure but will get authentication failure in HyWorks because of use of different authentication server.
Note: Keeping it as false, will make HyWorks to allow logon of users without authentication.

Show VM Name
Configuration: Show VM Name
Default Value: False
Description/Usage: By default, on user logon, HyWorks provides the name of desktop pool to access. But in cases where users should be shown actual VM Name, this flag can be enabled.
No functional impact but enabling may reveal actual VM Name to end-users.

Session Provider Failsafe Policy
Configuration: Session Provider Failsafe policy
Default Value: True
Recommended Value: True
Description/Usage: Providing desktop VMs’ session even when session provider is not responding using cached information of DVMs power and network information.
Applicable for dedicated session providers only. Please note, if session provider gets reachable again, HyWorks will automatically start using latest information to provide connection details by refreshing information in HyWorks.

Failsafe Policy Timeout(min)
Configuration: Failsafe Policy Timeout
Default Value: 0=Infinite
Recommended Value: 0
**Description/ Usage:** Timeouts after which HyWorks will stop giving session from unreachable session providers. Default value is zero but if cached values are not correct or have started causing issues then this can be configured to some numeric values.

**Syslog Config**

HyWorks Controller servers can be configured to send logs to external syslog server. HyWorks Controller Management Console -> System -> Syslog config section can be used to send data to syslog server. The configurations are important if logs must be archived for a longer duration.

To configure syslog server on HyWorks Controller, follow below steps:

**Configuring Syslog Server in HyWorks Controller for Archiving**

**Prerequisites**

1. External syslog server is installed, running and accessible from HyWorks Controller Server
2. External syslog server is configured in UDP mode

**Process to Configure External Syslog Server**

For configuring Syslog server in HyWorks, follow the below steps:

1. Login into HyWorks Controller Management Console using appropriate credentials
2. Go to **System – Syslog Config** page
3. Syslog Configuration page will be displayed, provide appropriate entries for
   a. Identity: Text field for uniquely identifying the Controller logs on Syslog
   b. Remote Address: Syslog Server IP or Hostname
   c. Remote Port: Port on which syslog server is configured to receive logs
   d. Enable Syslog: To be selected to send logs to configured syslog server.
4. Once all details are correctly set then click on **Update** button
5. Syslog server configuration is successfully done and now HyWorks Controller will start sending logs to configured Syslog server.
Logging and Analysis in HyWorks
Logs are very important information in understanding and analyzing user, administrator or system activities and thus can be referred to troubleshoot any issues in system.

- The flow of operations in HyWorks
- Monitoring the changes being done and identifying the source of change
- Cause of any failures

Logs section in HyWorks Controller Management console provides the view to view these logs. In this section of HyWorks administrator, all HyWorks Controller logging information will be shared.

Log Database
HyWorks log database is set during installation and supports following two types of log databases:

1. **Microsoft SQL Server:** Same instance as HyWorks controller or preferably on another instance, log database can be set. In that case HyWorks will create a log database with name provided during installation and will write all logs in database created on SQL server.
   - HyWorks also going to read the logs from configured instance for showing on HyWorks Controller Management Console -> Logs page.
   - Location of database: On configured Microsoft SQL Server instance\Data folder.

2. **Embedded:** (Microsoft SQL Server CE), a file-based database. Not recommended. HyWorks keeps the logs file in .sdf format at following default location:
   
   ```
   C:\Program Files (x86)\Accops\HyWorks\Service\Logs
   ```

   ❖ Additional Logging:

   1. **Log Text Files:** HyWorks as a standard process writes data on configured Log database but also writes logs in text files.
      - All latest logs are written into EDCController.txt file and on reaching 50 MB size it archives it with name `EDCController.txt.1`
      - HyWorks keeps only 5 such files and deleted the oldest one while creating new one.
      - These log files can be referred when HyWorks controller management console is also not working and thus logs can be viewed.

   2. **Sending logs to external syslog server:** To send HyWorks Controller logs to external syslog server, Syslog server configuration can be done from HyWorks Management Console -> System -> Syslog config section. Refer section [Syslog Config](#) for detailed information.

Viewing Logs on HyWorks Management Console
The following operations are available in **Logs** tab:

Information in Logs tab
The following information is displayed in Logs tab:

- Log time: The time on which log has been generated or the activity has been performed
- Source: The source of action e.g. few logs are created when a client sends some requests to controller, then logs will be generated, and source will be shown as device IP. In a similar manner
if a log is generated because of a request received from session host server, source will be session host server.

- **Type**: The log type e.g. info, error, warning
- **Username**: User who is initiating the operation (Administrator, user or system)
- **Message**: Brief message of the log
- **Details**: Details of the log message (if any)

### Filter Logs

Following filters are available for

- **Filter by Log Type**
  
  Administrator can filter logs based on its type by clicking on respective buttons i.e.
  
  - **All**: Display all logs
  - **Error**: Show Error logs only
  - **Warning**: Show Warning logs
  - **Info**: Display Info logs only

- **Filter by Date**
  
  - To see logs filter by date, select appropriate **To** and **From** dates
  - Click on **Go** button to view logs filtered by date

### Search Logs

1. Providing appropriate search string in ‘Search’ text box and pressing **Enter** key will display the search results matching search criteria.

2. If any specific string with spaces must be searched, search text can be provided in double quotes e.g. for searching an IP address following search text can be used **“192.168.1.100”**

### Download Logs

Administrator will also be able to download the logs using following steps:

1. Go to Logs page
2. Click on **Download Logs** button.
3. The **Download Logs** dialog will be shown provides following options:
   
   a. Specifying specific date range: Admin will be able to specify start and end date to get logs of specific date range only.
   
   b. File format: The format in which user wishes to download the log file
      
      - **CSV**
      - **TXT**

4. Select appropriate date range and file format - Click on **Get Logs** button to retrieve the specified logs.
5. HyWorks Controller will process the logs and will enable **Download Log File** button in **Download Logs** dialog
6. Click on button **Download Log File** button to download the log file.

![Download Logs dialog](image)

7. Log file will be downloaded in zipped format, containing logs in CSV or TXT format as specified

**Log Archiving**

HyWorks does not archive old logs and it deletes older logs once it reaches the thresholds. The threshold for log is set in System -> Advance config section.

**Increasing Maximum Number of Records to be kept**

By default, HyWorks keeps maximum of 500000 records in its log database and it will delete older logs once it reaches to set threshold.

Though it is recommended to keep a syslog server for log archiving, the number can still be changed as per requirement and below steps can be followed to change number of logs to kept in HyWorks log database.

1. Log-into HyWorks Controller Management Console using super administrator account.
2. Go to System -> Advance Config page
3. Locate the setting **DBlog_MAXRecords** and click on **Edit** button
4. Update the value as per requirement e.g. 100000
5. Click on button **Update**, displayed on top and bottom of the **Advance Config** section
6. New settings are saved and now Controller will keep maximum of 100000 records in default embedded log db.

Advanced Log Configurations
All latest HyWorks Controller setup, displays option to configure SQL Server as log database but if any deployment is running older version of HyWorks Controller which does not support to set SQL Server for log database, below sub-section can be used:

Using SQL Server for HyWorks Logs

Note:
➢ This is manual process requires **HyWorks Controller Service restart** and should be done under the supervision of Accops Support Team
➢ Necessary backups of configuration files should be taken for faster restoring if any problematic effects are observed
➢ Configurations are required on both Controller servers if HyWorks cluster is configured

Recommended:
➢ It is recommended to install another SQL Instance for logging. Configure HyWorks Controller database and logging both on same instance could lead to performance degradation.

Configuration Steps to Change the Logs Server

Pre-requisites:
- Another instance of SQL Server must be created for logging. To create another database instance, run the SQL installer again and follow the installation process.

Configuration Process:
1. Open Microsoft SQL Server Management Studio and Connect using appropriate administrator credentials to the newly created SQL Server instance to be configured as Log server
2. Open a new SQL query and paste the following queries to create a new logs DB

```
CREATE DATABASE LOGDB
GO
```

3. Now new database is created, run the following query to create appropriate tables in LOGDB

```
USE LOGDB
GO

CREATE TABLE [Log] (
    [LogId] bigint IDENTITY (1,1) NOT NULL,
    [Date] datetime NOT NULL,
    [Level] nvarchar(100) NOT NULL,
    [Logger] nvarchar(100) NOT NULL
)
```
4. SQL Server is ready to be configured in HyWorks Controller.
5. Connect to HyWorks Controller Server system using remote desktop connection or console session (if in HA, first connect to secondary HyWorks Controller server)
6. Go to HyWorks Controller Installation location (default installation path is mentioned below)
   
   C:\Program Files (x86)\Accops\HyWorks\Service

7. Locate the configuration file EDC.Service.exe.config
8. Copy the file and paste it at some safe location for backup
9. Download the EncryptDecryptAppConfigFile tool (Please ask the Accops support team for the download link)
10. Copy the tool on HyWorks Controller Server installation folder, default installation path is
    
    C:\Program Files (x86)\Accops\HyWorks\Service

11. Run the tool with admin privileges and browse the EDC.Service.exe file and click on button Decrypt Config

    Default Location is C:\Program Files (x86)\Accops\HyWorks\Service\EDC.Service.exe

12. It will decrypt the EDC.Service.exe.config file for next operation
13. Open the EDC.Service.exe.config with WordPad
14. In ConnectionStrings section, locate the connection strings for LogsDBContext which should be like the below screenshot

```
<add name="LogDBContext" connectionString="Data Source=<ServerAddress or FQDN>\sqlexpress,1433;Initial Catalog=LOGDB;User ID=sa;Password=password@123;Encrypt=False;Min
```

15. Replace it with the following Connection String

```
<add name="LogDBContext" connectionString="Data Source=<ServerAddress or FQDN>\sqlexpress,1433;Initial Catalog=LOGDB;User ID=sa;Password=password@123;Encrypt=False;Min`
a. Please note the highlighted sections should be changed as per SQL Server instance configurations, the configurations are
   i. SQL Server Address
   ii. SQL Server Instance Name
   iii. SQL Server Static Port to be used
   iv. User Id: to be used to connect to SQL Server
   v. Password: User password

16. Save the file
17. Run the tool with admin privileges and browse the EDC.Service.exe file and click on button Encrypt Config

Default Location is C:\Program Files (x86)\Accops\HyWorks\Service\EDC.Service.exe

18. Open Services (Open Run Prompt, type Services.msc and press Enter)
19. Locate and select Accops HyWorks Controller Service and click on Restart link
20. Accops HyWorks Controller Service will get restarted and will now start sending the logs to configured SQL Server
21. Perform couple of activities on HyWorks Controller Management Console, go to Logs section and verify if appropriate logs entries are being created

**Note:**
➢ Old logs will not be moved to the new SQL Server but will remain in previous embedded logsdb, the location of the file is:

C:\Program Files (x86)\Accops\HyWorks\Service\Logs

**Alternate way of Configuring Syslog Server**

Like above section, where HyWorks Controller server was not having option during installation to change log database to SQL Server, but the same configurations can be done externally, syslog server configurations were also not supported in older version. To configure syslog server externally following steps can be followed:

1. Connect to HyWorks Controller Server system using remote desktop connection or console session (if in HA, first connect to secondary HyWorks Controller server)
2. Go to HyWorks Controller Installation location (default installation path is mentioned below)

C:\Program Files (x86)\Accops\HyWorks\Service
3. Locate the configuration file log4net.config
4. Update syslog server IP and port in log4net.config
   • In log4net.config find appender with name "RemoteSyslogAppender" (See screenshot below for reference)
   • Set Syslog Server’s IP address and Port as per highlighted section below in

```xml
<appender name="RemoteSyslogAppender" type="log4net.Appender.RemoteSyslogAppender">
```
5. Enable Syslog Appender: In the log4net.config file, at the bottom, in root section -> Add following Appender xml node in <root>

```xml
<appender-ref ref="RemoteSyslogAppender" />
<root>
  <level value="INFO" />
  <appender-ref ref="UdpAppender"/>
  <appender-ref ref="RemoteSyslogAppender"/>
</root>
```

6. Save the log4net.config file
7. Open Services (Open Run Prompt, type Services.msc and press Enter)
8. Locate and select Accops HyWorks Controller Service and click on Restart link
9. Accops HyWorks Controller Service will get restarted and will now start sending the logs to configured syslog Server

**Note:**
- The configuration is tested with CentOS based rsyslog server. If any issues are observed after configuration, please contact Accops Support team.
- It requires UDP based syslog server, as the controller supports only UDP based communication with syslog server.
Help and Download Links of Important Modules

The Help page contains:

- Links for detailed help documents (see list below) for installation, administration and quick deployment of HyWorks Controller
  a. Accops HyWorks Controller Quick Start Guide
  b. Accops HyWorks Controller Admin Guide
  c. Accops HyWorks Controller Install Guide

- Link for Accops Support Center
  a. Visit Accops Support Center

- Links to download support tools embedded with HyWorks Controller
  a. HyWorks DVM Tools
  b. Accops Upgrade Server
  c. Hyper-V Connector
HyWorks Sizing

The table below provides the information on appropriate sizing of HyWorks. The sizing is based on the performance of various components of HyWorks e.g. Login time, device operations, Management Console performance etc.

<table>
<thead>
<tr>
<th>Concurrent Users</th>
<th>Server Resources</th>
<th>Database Configuration</th>
<th>Additional Server</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>100-250</td>
<td>4 CPUs/ 4 GB RAM</td>
<td>SQL Express Edition</td>
<td>Secondary controller for high availability</td>
<td></td>
</tr>
<tr>
<td>250-1000</td>
<td>8 CPUs/ 8 GB RAM</td>
<td>SQL Express edition (SQL Standard or Enterprise edition can also be used)</td>
<td>Secondary controller for high availability</td>
<td></td>
</tr>
<tr>
<td>1000-2000</td>
<td>8 CPUs/ 8 GB RAM</td>
<td>SQL Standard or Enterprise edition</td>
<td>Secondary controller for high availability</td>
<td></td>
</tr>
<tr>
<td>2000+</td>
<td>16 CPUs/ 16 GB RAM</td>
<td>SQL Standard or Enterprise edition</td>
<td>Secondary controller for high availability</td>
<td>HyWorks v3.3 (General release is pending) with active-active clustering should be preferred.</td>
</tr>
</tbody>
</table>

Note:

- Minimum recommended configuration is 4GB RAM/ 4 vCPUs.
- Changing the heartbeat interval for HyWorks Controller v2.5 with embedded database cannot be done easily and will require 3rd party soft wares.
- Increasing heartbeat value will directly affect the time required to update the device settings as it takes at least 1 heartbeat for the devices to update the settings as provided by HyWorks Controller.
Appendix

How to reset HyWorks Super-Administrator Credentials

Administrator credentials can be reset using following two methods:

1. Using Installation wizard in Maintenance (Repair) mode
2. From HyWorks Controller Management Console

Super-admin Password is lost

Using Installation Wizard in Maintenance Mode

If HyWorks Controller installation is invoked on the windows server machine, already installed with same version of HyWorks Controller then installation is run in maintenance mode which provides the option of repairing existing installation.

HyWorks Controller repair option can also be used to reset the administrator credentials in the following situations:

1. Administrator does not remember the username or password and thus cannot change the password from management console
2. Administrator is willing to reset the username also along with password
3. Administrator is willing to change the login mechanism i.e. changing to active directory-based configuration to local user configuration or vice versa

To reset the administrator credentials using HyWorks Controller Repair wizard, Follow the below steps:

• Access the server where HyWorks Controller Service is installed
• Re-run the same HyWorks Controller setup, which was used to install HyWorks Controller Service on the server
• The setup will run in Maintenance mode – Choose option Repair to proceed
• Proceed with default options until asked for new Administrator credentials
• Provide new administrator credentials and complete the HyWorks Controller repair setup
• The password for HyWorks Controller Service will reset with provided credentials
• Reload the HyWorks Controller Management console to attempt login using new credentials

Changing Password from Management Console

If it is required to change the password of current local administrator user only, then administrator can simply use management console.

To change the password of administrator user from management console, follow the below steps:

1. Access HyWorks Controller Management console on any supported browser
2. Login into HyWorks Controller using existing administrator credentials
3. Administrator will be navigated to Dashboard
4. On Top Right Corner, Welcome message for currently logged in user is displayed
5. Click on Username to view available options
6. Click on option Change Password
7. In Change Password dialog, provide appropriate details (Old Password, New Password and Confirm Password) and click on Save button
8. Password will get changed and current session will be logged out
9. Administrator can now log-in using new password
Now we have already learned about accessing and login to HyWorks Controller management console, later in the document HyWorks Management from HyWorks Controller management console will be explained in detail.

Note:

➢ Change Password feature works for local HyWorks Controller administrator user only and is not applicable for active directory users configured as HyWorks Controller administrator
Reference Documents

Please refer to following other documents related to Accops HyWorks

- Accops HyWorks Controller Installation Guide
- Accops HyWorks Quick Start Guide
- HyWorks Hyper-V Connector Installation Guide
Support
Contact Accops Support team [support.accops.com](support.accops.com) for any assistance or queries.
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’ s 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.