

HCLSoftware

HCL DRYiCE MyCloud

Installation Guide
Version 10.8.1



The data contained in this document shall not be duplicated, used, or disclosed in whole or in part for any purpose. If a contract is awarded to chosen parties because of or in connection with the submission of this data, the client or prospective client shall have the right to duplicate, use, or disclose this data to the extent provided in the contract. This restriction does not limit the client's or prospective client's right to use the information contained in the data if it is obtained from another source without restriction. The data subject to this restriction is contained in all marked sheets.

HCL has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the HCL website at www.hcltechsw.com.

Copyright © 2024 HCL Technologies Limited.

Table of Contents

1	Preface.....	14
1.1	Intended Audience.....	14
1.2	About this Guide.....	14
1.3	Related Documents	14
1.4	Conventions	14
2	MyCloud Overview	16
2.1	MyCloud Features	16
2.2	MyCloud Component Overview	17
2.3	MyCloud Benefits	18
3	MyCloud Installation.....	20
4	MyCloud Environment Planning.....	21
4.1	Deployment Environment.....	21
4.2	Tiered Architecture of MyCloud	21
4.2.1	2- Tier Mode	21
4.2.2	3-Tier Mode	22
4.3	Hardware Configuration for MyCloud	22
4.3.1	Hardware Sizing for Minimal Deployment	23
4.3.2	Hardware Sizing for Small Environment (2 Tier non-HA)	23
4.3.3	Hardware Sizing for Small Environment (2 Tier HA)	24
4.3.4	Hardware Sizing for Medium Environment (3 Tier non-HA)	24
4.3.5	Hardware Sizing for Medium Environment (3 Tier HA)	25
4.3.6	Hardware Sizing for Large Environment (3 Tier non-HA)	26
4.3.7	Hardware Sizing for Large Environment (3 Tier HA)	26
5	MyCloud Environment Preparation.....	28
5.1	Pre-requisites to run the Installer	28
5.1.1	Installer.....	28
5.1.2	Enable Log on as Service.....	30
5.2	MyCloud Components Pre-requisites Installation.....	30
5.2.1	Installation of pre-requisites on Web Layer.....	31
5.2.2	Installation of Pre-requisites on App Layer	40
5.2.3	Installation of Pre-requisites on Database Layer	48
5.3	Deployment	49
5.3.1	MyCloud Web Layer Installation.....	50

5.3.2	MyCloud App Layer Installation.....	61
6	MyCloud Post Installation Task	71
6.1	Provide MyCloud License	71
6.1.1	Master Data changes	72
6.2	Change Certificate to CA Signed (Optional)	86
6.2.1	WebSite changes	89
6.2.2	WebAPI changes.....	89
6.2.3	Key Rotation changes	90
6.2.4	Middleware Component changes.....	90
6.3	Load Balancer Configuration (Optional)	105
6.3.1	Website changes	108
6.3.2	Web API changes.....	108
6.3.3	Middleware Component changes	108
6.3.4	Master Data changes	119
6.3.5	KRS Database String Encryption	121
6.4	Update Webapi URL (Not Able to Login into Portal)	122
6.5	Update Ldap/Saml Configuration for Admin	123
6.5.1	Update Admin Email and User Id	124
6.5.2	Configure LDAP Authentication	125
6.5.3	Configure SAML Authentication.....	126
6.5.4	Change Admin User Password (Form based Authentication Type)	127
6.6	Manage White Resource Lists	128
6.7	Rotate Encryption Key	131
6.7.1	Key Rotation	131
6.7.2	Key Rotation History	133
7	Support.....	134

Table of Figures

Figure 1 – MyCloud Installation Workflow Overview	28
Figure 2 – Installer	29
Figure 3 – Install Pre-requisites	29
Figure 4 – Install Python.....	30
Figure 5 – Install .Net Framework 4.8.....	31
Figure 6 – Install .Net Framework 4.8 (Cont.).....	32
Figure 7 – Enable IIS and add .Net Framework	32
Figure 8 – Add Roles and Features	33
Figure 9 – Enable IIS and Add .Net Framework (Cont.).....	33
Figure 10 – Enable IIS and Add .Net Framework (Cont.).....	34
Figure 11 – Enable IIS and Add .Net Framework (Cont.).....	34
Figure 12 – Enable IIS and Add .Net Framework (Cont.)	35
Figure 13 – Enable IIS and Add .Net Framework (Cont.)	35
Figure 14 – Enable IIS and Add .Net Framework (Cont.).....	36
Figure 15 – Enable IIS and Add .Net Framework (Cont.)	36
Figure 16 – Enable IIS and Add .Net Framework (Cont.).....	37
Figure 17 – Enable IIS and Add .Net Framework (Cont.).....	37
Figure 18 – Enable IIS and Add .Net Framework (Cont.)	38
Figure 19 – Enable IIS and Add .Net Framework (Cont.)	38
Figure 20 – Enable IIS and Add .Net Framework (Cont.)	39
Figure 21 – Installation Status	39
Figure 22 – Open IIS Manager.....	40
Figure 23 – Delete Default Website.....	40
Figure 24 – Install .Net Framework 4.8 Runtime	41
Figure 25 – Install .Net Framework 4.8 Runtime (Cont.).....	41
Figure 26 – Installing Messaging Queue.....	42
Figure 27 – Installing Messaging Queue (Cont.).....	42
Figure 28 – Installing Messaging Queue (Cont.)	43

Figure 29 – Installing Messaging Queue (Cont.)	43
Figure 30 – Installing Messaging Queue (Cont.)	44
Figure 31 – Installing Messaging Queue (Cont.)	44
Figure 32 – Installing Messaging Queue (Cont.)	45
Figure 33 – Installing Python	45
Figure 34 – Installing Python (Cont.)	46
Figure 35 – Installing Python (Cont.)	46
Figure 36 – Installing Python (Cont.)	47
Figure 37 – Installing Python (Cont.)	47
Figure 38 – Installing Python (Cont.)	48
Figure 39 – Database Properties	49
Figure 40 – Server Properties	49
Figure 41 – MyCloud Installer	50
Figure 42 – MyCloud – New Installation	51
Figure 43 – MyCloud – New Installation	51
Figure 44 – MyCloud – Upgrade Installation	52
Figure 45 – Web Component Selection	52
Figure 46 – Database Details	53
Figure 47 – Default Database Names	54
Figure 48 – Database Check Connection	54
Figure 49 – MyCloud Installer – Database Already Exist	55
Figure 50 – Server Configuration	55
Figure 51 – Prerequisite Checker	56
Figure 52 – Prerequisite Checker Information Assistance	56
Figure 53 – Prerequisite Checker (Cont.)	57
Figure 54 – Configure Admin Details	58
Figure 55 – Admin Details Information Assistance	58
Figure 56 – MyCloud Installation	59
Figure 57 – MyCloud Installation Progress	59
Figure 58 – MyCloud Installer – Success	60

Figure 59 – MyCloud Installer – Launch	60
Figure 60 – Rollback.....	61
Figure 61 – MyCloud Installer	61
Figure 62 – MyCloud Installer – New Installation.....	62
Figure 63 – MyCloud Installer – New Installation.....	62
Figure 64 – MyCloud Installer – Upgrade Installation.....	63
Figure 65 – App Layer – Service Component Setup.....	63
Figure 66 – Database Details.....	64
Figure 67 – MyCloud Default Database Names	65
Figure 68 – Database Details.....	65
Figure 69 – MyCloud Installer- Database Names	66
Figure 70 – Server Configuration	66
Figure 71 – Prerequisite Checker	67
Figure 72 – Prerequisite Checker Information Assistance	67
Figure 73 – Prerequisite Checker (Cont.)	68
Figure 74 – MyCloud Installation Details	68
Figure 75 – MyCloud Installer- Progress.....	69
Figure 76 – MyCloud Installer – Success	69
Figure 77 – MyCloud Installer – Setup Complete.....	70
Figure 78 – Rollback.....	70
Figure 79 – MyCloud Login	71
Figure 80 – MyCloud –Enter License Key	71
Figure 81 – MyCloud –Enter License Key	72
Figure 82 – Admin Home Page	72
Figure 83 – Manage Base Components	73
Figure 84 – Landing Page with selected Component URL Configuration	73
Figure 85 – Component URL Configuration	74
Figure 86 – Command Prompt as Administrator.....	74
Figure 87 – Run Command Window.....	75
Figure 88 – Windows Services Manager	75

Figure 89 – Windows Services Manager	76
Figure 90 – Windows Services Manager	77
Figure 91 – Service Host URL in Configuration File	78
Figure 92 – Run Command Windows.....	78
Figure 93 – Windows Certificate Console	79
Figure 94 – Windows Certificate Console with File Menu	79
Figure 95 – Add or Remove screen in Certificate Console.....	80
Figure 96 – Certificate snap-in Window.....	80
Figure 97 – Select Computer	81
Figure 98 – Add or Remove Snap-ins Window.....	81
Figure 99 – Personal Certificate Console.....	82
Figure 100 – Certificate Console with selected Certificate.....	82
Figure 101 – Copy Certificate	83
Figure 102 – Showing recently added Certificate	83
Figure 103 – Showing Recently Added Certificate.....	84
Figure 104 – Admin Landing Page	84
Figure 105 – Component URL Configuration	86
Figure 106 – Run window command.....	87
Figure 107 – Application Base Path Locator	87
Figure 108 – Run Command Window	87
Figure 109 – Service Properties Window.....	88
Figure 110 – Certificate Web.Config Certificate Name.....	89
Figure 111 – Certificate Web.Config Certificate Name	89
Figure 112 – Certificate Web.Config Certificate Name	90
Figure 113 – Certificate Web.Config Certificate name (Cont.)	90
Figure 114 – Web Config Certificate Name (Cont.).....	90
Figure 115 – Run Command Windows.....	91
Figure 116 – Windows Services Manager.....	91
Figure 117 – Stop Services	92
Figure 118 – Certificate Web.Config Certificate Name	92

Figure 119 – Certificate Web.Config Certificate Name	93
Figure 120 – Middleware AD Certificate Name	94
Figure 121 – Middleware AD Certificate Name	94
Figure 122 – Middleware Orchestrator Certificate Name	95
Figure 123 – Middleware Orchestrator Certificate Name	95
Figure 124 – Middleware Workflow Certificate Name	96
Figure 125 – Middleware WorkFlow Certificate Name	96
Figure 126 – Middleware SyncService Certificate Name	97
Figure 127 – Middleware SyncService Certificate Name	97
Figure 128 – Middleware ITSM Executor Certificate Name	98
Figure 129 – Middleware ITSM Executor Certificate Name	98
Figure 130 – Middleware Billing Certificate Name	99
Figure 131 – Middleware Billing Certificate Name	99
Figure 132 – Middleware Generic Service Certificate Name	100
Figure 133 – Middleware Generic service Certificate Name	100
Figure 134 – Middleware Monitor Certificate Name	101
Figure 135 – Middleware Monitor Certificate Name	101
Figure 136 – Middleware Performance Certificate Name	102
Figure 137 – Middleware Performance Certificate Name	102
Figure 138 – Middleware Cisco Intersight Certificate Name	103
Figure 139 – Run Command Windows	104
Figure 140 – Start Services	104
Figure 141 – Middleware Certificate Store Location	105
Figure 142 – Middleware Certificate Store Location (Cont.)	105
Figure 143 – Middleware Start Service IsSSLSelfSigned	105
Figure 144 – Run Command Window	106
Figure 145 – ApplicationBasePath Locator	106
Figure 146 – Run Command Window	106
Figure 147 – AD Service Properties	107
Figure 148 – Run Command Window	108

Figure 149 – Windows Service Manager	109
Figure 150 – Stop Below Service	109
Figure 151 – Load Balancer Listener Key Management Base Address	110
Figure 152 – Load Balancer AD Service Host.....	111
Figure 153 – Load Balancer Orchestrator Service Host URL	111
Figure 154 – Load Balancer Workflow Service Host URL.....	112
Figure 155 – Load Balancer SyncService Service Host URL.....	113
Figure 156 – Load Balancer ITSM Executor Service Host URL	113
Figure 157 – Load Balancer Billing Service Host URL	114
Figure 158 – Load Balancer GenericService Service Host URL.....	115
Figure 159 – Load Balancer Performance Service Host URL.....	116
Figure 160 – Load Balancer Performance Service Host URL.....	116
Figure 161 – Load Balancer Cisco Intersight Sync Service Host URL.....	117
Figure 162 – Run Command Window	118
Figure 163 – Start Services	118
Figure 164 – Landing Page	119
Figure 165 – Manage base Components.....	119
Figure 166 – Landing Page with selected Component URL Configuration	120
Figure 167 – Component URL Configuration.....	121
Figure 168 – Component URL Configuration	121
Figure 169 – Component URL Configuration	121
Figure 170 – KRS Login Screen.....	122
Figure 171 – Component URL Configuration in KRS.....	122
Figure 172 – KRS Login Screen.....	123
Figure 173 – Manage Admin User.....	123
Figure 174 – Edit Manage Admin User Details.....	124
Figure 175 – Successful Update message – Manage Admin User.....	125
Figure 176 – Manage Admin User – LDAP Configuration.....	125
Figure 177 – Manage Admin User – LDAP Configuration – Saved Successfully.....	126
Figure 178 – Manage Admin User – SAML Configuration	126

Figure 179 – Manage Admin User – SAML Configuration – Saved Successfully 127

Figure 180 – Manage Admin User – Form Based – Change Password..... 127

Figure 181 – Manage Admin User – Form Based – Change Password – Save Successfully 128

Figure 182 – KRS Login Screen..... 129

Figure 183 – Manage White Resource Lists..... 129

Figure 184 – Manage White Resource Lists (Cont.)..... 130

Figure 185 – Success Message..... 131

Figure 186 – Encryption Key Rotation 131

Figure 187 – Encryption Key Rotation – Confirmation Message 132

Figure 188 – Encryption Key Rotation – Request Successful Message..... 132

Figure 189 – Encryption Key Rotation History 133

Figure 190 – Encryption Key Rotation History 2 133

List of Tables

Table 1 – Conventions.....	15
Table 2 – MyCloud Component with their roles and responsibilities and pre-requisites.....	17
Table 3 – Components of MyCloud Installation	20
Table 4 – Deployment Environment	21
Table 5 – 2 Tier deployment mode	21
Table 6 – 3 Tier Mode	22
Table 7 – Hardware Sizing for Minimal Deployment	23
Table 8 – Hardware Sizing for Small Environment (2 Tier non-HA)	23
Table 9 – Hardware Sizing for Small Environment (2 Tier HA)	24
Table 10 – Hardware Sizing for Medium Environment (3 Tier non-HA)	24
Table 11 – Hardware Sizing for Medium Environment (3 Tier HA).....	25
Table 12 – Hardware Sizing for Large Environment (3 Tier non-HA).....	26
Table 13 – Hardware Sizing for Large Environment (3 Tier HA)	26
Table 14 – MyCloud Server Pre-requisites.....	28
Table 15 – Installer Files Description.....	29
Table 16 – Description of Certificate	30
Table 17 – MyCloud Component Prerequisites Installation	30
Table 18 – Database Setup	53
Table 19 – Database Setup	64
Table 20 – Edit Manage Admin User Details	124
Table 21 – Manage Admin User Details – LDAP Configuration	125
Table 22 – Manage Admin User Details – SAML Configuration	126
Table 23 – Manage Admin User Details –Change Password.....	128
Table 24 – Add White Resource.....	130

Document Revision History

This guide is updated with each release of the product or when necessary. This table provides the revision history of this Installation Guide.

Version Date	Description
May, 2020	Dryice MyCloud v9.2 Installation Guide
August, 2020	Dryice MyCloud v10.0 Installation Guide
November, 2020	Dryice MyCloud v10.1 Installation Guide
February, 2021	Dryice MyCloud v10.2 Installation Guide
April, 2021	Dryice MyCloud v10.4 Installation Guide
October, 2021	Dryice MyCloud v10.5 Installation Guide
September, 2022	Dryice MyCloud v10.6 Installation Guide
August, 2023	HCL_DRYiCE_MyCloud_10.7_Installation_Guide
May, 2024	HCL_DRYiCE_MyCloud_10.8_Installation_Guide
September, 2024	HCL_DRYiCE_MyCloud_10.8.1_Installation_Guide

1 Preface

This section provides information about the MyCloud Installation Guide and includes the following topics.

- [Intended Audience](#)
- [About This Guide](#)
- [Related Documents](#)
- [Conventions](#)

1.1 Intended Audience

This information is intended for Business administrators/IT administrators responsible for installing MyCloud and infrastructure administrators responsible for provisioning infrastructure required for installation of MyCloud.

1.2 About this Guide

This guide has instructions to install MyCloud. It includes the software & hardware pre-requisites, MyCloud components details and installation procedures for the product. This guide also provides references to other documents for detailed information and consists of the following major sections:

- [MyCloud Overview](#)
- [MyCloud Installation](#)
- [MyCloud Environment Planning](#)
- [MyCloud Environment Preparation](#)
- [Deployment](#)
- [MyCloud Post Installation Task](#)

1.3 Related Documents

The following documents can be referenced in addition to this guide for further information on MyCloud:

- MyCloud Introduction Guide
- MyCloud User Guide
- MyCloud Configuration Guide – Admin Module
- MyCloud Configuration Guide – Provider Module – Part 1
- MyCloud Configuration Guide – Provider Module – Part 2
- MyCloud Troubleshooting Guide
- MyCloud Developer Guide
- MyCloud API Guide
- MyCloud V3 API Guide

1.4 Conventions

The following typographic conventions are used in this document:

Table 1 – Conventions

Convention	Element
Boldface	Graphical user interface elements associated with an action, or terms defined in text or the glossary
Underlined blue face	Cross-reference and links
Courier New (Font)	Commands within a paragraph, URLs, code in examples, and paths including onscreen text and text input from users
Italic	Document titles, occasional emphasis, or glossary terms
Numbered lists	Steps in a procedure to be followed in a sequence
Bulleted lists	List of items that is not necessarily meant to be followed in a sequence

2 MyCloud Overview

DRYiCE MyCloud is a hybrid cloud management product that empowers organizations to optimally govern, provision, monitor, and manage cloud infrastructure. It combines data exploration and data visualization in an easy-to-use product that enables effective analysis and generates actionable insights for IaaS, PaaS resources and multi-machine blueprints. DRYiCE MyCloud's data-driven recommendations and advisories ensure continuous optimization of enterprise cloud environments across areas, including cost, performance, security, and utilization.

2.1 MyCloud Features

- **Self Service Catalog based Provisioning and Auto-decommissioning:**
Self Service Catalog based Provisioning & Auto-decommissioning– Provisioning of IaaS, PaaS, and multi-machine blueprints in a multi-cloud environment, through an intuitive self-service catalog and auto-decommissioning post a defined interval to avoid cost leakages.
- **Metering & Showback:**
Track utilization of resources across BUs, enabling transparency and visibility
- **Dynamic User interface:**
Flexibility to customize the service request form templates to capture configuration parameters while placing provisioning requests.
- **Dynamic Process Workflows:**
Enables automation of generic & custom tasks like installing agents, machine cloning etc. with support for parallel execution.
- **Script Library**
Create new or leverage out-of-the-box scripts in process workflows across environments.
- **Role Based Access Control:**
Manage user privileges based on their roles, eligibility, and policies.
- **Policy driven Orchestration:**
Be in control of your cloud orchestration ecosystem aligned to your organizational policies.
- **Rich Integration Ecosystem:**
Enables integration with industry leading third party tools through REST APIs and CLI
- **Enterprise-Grade Security:**
Ensure security of end-to-end cloud management and orchestration ecosystem through various mechanisms

2.2 MyCloud Component Overview

MyCloud has various service components, each playing a different role in multi cloud management. Each component has pre-requisites. Below table lists all the components, their roles and responsibilities and pre-requisites required for each component.

Table 2 – MyCloud Component with their roles and responsibilities and pre-requisites

Component Name	Description	Pre-Req's
MyCloud Portal	<p>It comprises two sub-components:</p> <ul style="list-style-type: none">• WEB UI: MYCLOUD WEB PORTAL• MYCLOUD API: REST API TO INTERACT WITH MYCLOUD <p>This component requires MyCloud database connectivity.</p>	IIS, MyCloud Certificate, .Net Framework 4.8
MyCloud KRS	<p>Key Rotation Service: To rotate encryption key on a periodic basis.</p> <p>This component requires MyCloud database connectivity.</p>	IIS, MyCloud Certificate, .Net Framework 4.8
Job Listener	<p>It helps in the execution of MyCloud jobs and interacting with different components internally.</p> <p>This is a window service.</p> <p>This component requires the MyCloud database connectivity.</p>	MyCloud Certificate, .Net Framework 4.8
Sync Service	<p>It is responsible for synchronization of the underlying infrastructure cloud resources. It supports vCenter, AWS, Azure RM, SCVMM 2012.</p> <p>This is a self-hosted WCF service.</p>	MyCloud Certificate, .Net Framework 4.8
Ad Sync Service	<p>It fetches AD group user data. This is a self-hosted WCF service.</p>	MyCloud Certificate, .Net Framework 4.8
Workflow Service	<p>It triggers MyCloud process workflow and notification service. This is a self-hosted WCF service. It requires MyCloud database connectivity.</p>	MyCloud Certificate, .Net Framework 4.8, MSMQ/Rabbit MQ
Orchestrator	<p>It helps in provisioning and automating other Tasks. This is a self-hosted WCF service.</p>	MyCloud Certificate, .Net Framework 4.8, PowerShell, Python 3.6

ITSM executor	It helps in interacting with ITSM tools. Currently, it only supports ServiceNow and Remedy. It is a self-hosted WCF service and requires MyCloud database connectivity.	MyCloud Certificate, .Net Framework 4.8
Generic Task Executor	It helps in Private Cloud Billing, Data Purging and Cost Models Activation. This is a self-hosted WCF service and requires MyCloud database connectivity.	MyCloud Certificate, .Net Framework 4.8
Billing Service	It enables Public Cloud Billing. This is a self-hosted WCF service and requires MyCloud database connectivity.	MyCloud Certificate, .Net Framework 4.8
Performance Service	It is responsible for metering and Public Cloud advisory data collection. This is a self-hosted WCF service.	MyCloud Certificate, .Net Framework 4.8
Health Monitor Service	It is responsible for monitoring the health of all the MyCloud Components. This is a self-hosted WCF Service.	MyCloud Certificate, .Net Framework 4.8
Database	MyCloud uses DB to store configuration and transactional data of request.	SQL Server 2016 Standard/Enterprise edition
Cisco Intersight Sync Service	It is responsible for syncing Cisco Intersight resources. This is a self-hosted WCF service.	MyCloud Certificate, .Net Framework 4.8

2.3 MyCloud Benefits

– Reduce Costs

- Higher cost savings through Process standardization & Automation
- Provide visibility of usage of virtual assets & cost obligations to key custodians
- Optimize virtual asset utilization to avoid cost leakages.

– Mitigate Risks

- Improve Performance, Fault Tolerance and Compliance of systems and services through proactive advisories.
- Transform the process from Human driven to Automation driven and eliminate human error from the equation.
- Mitigate security related risks based on system driven suggestions.

– Drive Efficiency

- Reduce VM provisioning cycle by up to 85%.
- Achieve up to 50% faster deployment of services through automation.

3 MyCloud Installation

The table below describes individual components and steps involved in MyCloud installation. Each of those are then detailed in the forthcoming sections.

Table 3 – Components of MyCloud Installation

Section Name	Description
MyCloud Environment Planning	Helps the organization to plan the scale of MyCloud deployment for their environment. It creates awareness among the users regarding its environments, architecture, and software and hardware requirements.
MyCloud Environment Preparation	It highlights the pre-requisites to run installer & components of MyCloud.
Pre-requisites to run the Installer	It highlights the pre-requisites to run the installer.
MyCloud Components Pre-requisites Installation	MyCloud has multiple components that are designated to perform multiple actions. The section highlights the pre-requisites to install the components.
MyCloud Web Layer Installation	The web layer is a part of MyCloud architecture that hosts the webserver. Further, the webserver hosts MyCloud web UI portal and MyCloud APIs.
MyCloud App Layer Installation	The app layer is a part of MyCloud architecture that hosts the application server. Further, the app server hosts the MyCloud components and Job Listener.

A complete installation of MyCloud comprises of Databases, Web Interface, and the services i.e., Orchestrator, Workflow, AD Sync etc.

4 MyCloud Environment Planning

This section describes how to plan for MyCloud deployment. It focusses on architecture, software, and hardware requirements.

4.1 Deployment Environment

The section highlights various MyCloud deployment environments to be selected based on the number of managed Virtual Machines (VMs).

Table 4 – Deployment Environment

Environment Type	Small	Medium	Large
No. of VMS managed	<1000	between 1000 and 3000	>3000
Data Retention	6 months	6 months	6 months

4.2 Tiered Architecture of MyCloud

MyCloud is installed in the following deployment modes:

4.2.1 2- Tier Mode

In this mode, all MyCloud components are installed on the following types of servers:

- **Web and App server**- It hosts all MyCloud components except the database.
- **Database server**- It hosts all MyCloud databases that include the Configuration data, Performance, and Billing.

Table 5 – 2 Tier deployment mode

Layer	MyCloud Service Component
Web and App	MyCloud Portal
	Job Listener
	Sync Service
	Ad Sync Service
	Workflow Service
	Orchestrator
	ITSM executor
	Generic Task Executor
	Billing Service
	Performance Service
	Health Monitor Service

	Cisco Intersight Sync Service
DB	Database

4.2.2 3-Tier Mode

MyCloud 3-Tier mode is different from 2-Tier mode as all the three components are segregated into individual layers, as shown below:

- **Web Server:** It hosts MyCloud web UI portal and MyCloud APIs. User login to the MyCloud portal using LDAP/SAML authentication.
- **App Server-** It hosts MyCloud Components & MyCloud Job Listener such as Orchestrator and Workflow Service.
- **Database Server-** Database server hosts MyCloud Configuration DB, Billing DB, and Performance DB.

The installer needs to be run on individual servers, i.e. **Application server**.

Table 6 – 3 Tier Mode

Layer	MyCloud Service Component
Web	MyCloud Portal
	MyCloud KRS
APP	Job Listener
	Sync Service
	Ad Sync Service
	Workflow Service
	Orchestrator
	ITSM executor
	Generic Task Executor
	Billing Service
	Performance Service
	Health Monitor Service
	Cisco Intersight Sync Service
DB	Database

4.3 Hardware Configuration for MyCloud

This section describes the hardware requirements based on the following parameters.

- No. of VMs to be managed.

- High Availability (HA) or Non-HA
- 2-Tier or 3 Tier

4.3.1 Hardware Sizing for Minimal Deployment

Table 7 – Hardware Sizing for Minimal Deployment

Server Name	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage (local)	Other Requirements	Remarks
Application + Web Server	1	Virtual	4 vCPU, 8 GB RAM	NA	50 GB	Operating System - Windows Server 2016, 64-bit	
Database Server	1	Virtual	4 vCPU, 12 GB RAM	Microsoft SQL Server 2016 - Standard Edition	150 GB	Operating System - Windows Server 2016, 64-bit	SQL_Latin1_General_CP1_CI_AS

4.3.2 Hardware Sizing for Small Environment (2 Tier non-HA)

Table 8 – Hardware Sizing for Small Environment (2 Tier non-HA)

Environment Type	Server Name	Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage (local)	Other Requirements	Remarks
Small	Application + Web Server	Web Tier	1	Virtual	4 vCPU, 8 GB RAM	NA	50GB	Operating System - Windows Server 2016, 64-bit	
		Application Tier							
	Database Server	Data Tier	1	Virtual	4 vCPU, 12 GB RAM	Microsoft SQL Server 2016 - Standard Edition	150 GB	Operating System - Windows Server 2016, 64-bit	SQL_Latin1_General_CP1_CI_AS

4.3.3 Hardware Sizing for Small Environment (2 Tier HA)

Table 9 – Hardware Sizing for Small Environment (2 Tier HA)

Environment Size	Server Name	Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage (local)	Shared Storage	Other Requirements	Remarks
Small	Application + Web Server	Web Tier	2	Virtual	4 vCPU, 8 GB RAM	NA	50 GB	20 GB	Operating System - Windows Server 2016, 64-bit	
		Application Tier								
	Database Server	Data Tier	2	Virtual	4 vCPU, 12 GB RAM	Microsoft SQL Server 2016 - Standard Edition	300 GB		Operating System - Windows Server 2016, 64-bit	SQL Cluster, Always On SQL_Latin1_General_CP1_CI_AS

4.3.4 Hardware Sizing for Medium Environment (3 Tier non-HA)

Table 10 – Hardware Sizing for Medium Environment (3 Tier non-HA)

Environment Size	Server Name	Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage (local)	Other Requirements	Remarks
Medium	Web Server	Web Tier	1	Virtual	4 vCPU, 12 GB RAM	NA	50 GB	Operating System - Windows Server 2016, 64-bit	

	Application Server	Application Tier	1	Virtual	4 vCPU, 12 GB RAM	NA	100 GB	Operating System - Windows Server 2016, 64-bit	
	Database Server	Data Tier	1	Virtual	4 vCPU, 16 GB RAM	Microsoft SQL Server 2016 - Standard Edition	300 GB	Operating System - Windows Server 2016, 64-bit	SQL_Latin1_General_CP1_CI_AS

4.3.5 Hardware Sizing for Medium Environment (3 Tier HA)

Table 11 – Hardware Sizing for Medium Environment (3 Tier HA)

Environment Size	Server Name	Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage (local)	Shared Storage	Other Requirements	Remarks
Medium	Web Server	Web Tier	2	Virtual	4 vCPU, 12 GB RAM	NA	50 GB	20 GB	Operating System - Windows Server 2016, 64-bit	
	Application Server	Application Tier	2	Virtual	4 vCPU, 12 GB RAM	NA	100 GB	20 GB	Operating System - Windows Server 2016, 64-bit	
	Database Server	Data Tier	2	Virtual	4 vCPU, 16 GB RAM	Microsoft SQL Server 2016 - Standard Edition	300 GB		Operating System - Windows Server 2016, 64-bit	SQL_Latin1_General_CP1_CI_AS

4.3.6 Hardware Sizing for Large Environment (3 Tier non-HA)

Table 12 – Hardware Sizing for Large Environment (3 Tier non-HA)

Environment	Server Name	Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage (local)	Other Requirements	Remarks
Large	Web Server	Web Tier	1	Virtual	4 vCPU, 16 GB RAM	NA	100 GB	Operating System - Windows Server 2016, 64-bit	
	Application Server	Application Tier	1	Virtual	4 vCPU, 16 GB RAM	NA	100 GB	Operating System - Windows Server 2016, 64-bit	
	Database Server	Data Tier	1	Virtual	8 vCPU, 32 GB RAM	Microsoft SQL Server 2016 - Standard Edition	500 GB	Operating System - Windows Server 2016, 64-bit	SQL_Latin1_General_CP1_CI_AS

4.3.7 Hardware Sizing for Large Environment (3 Tier HA)

Table 13 – Hardware Sizing for Large Environment (3 Tier HA)

Environment	Server Name	Tier	Server Count	Server Type	Hardware Configuration	Database Requirement	Storage (local)	Shared Storage	Other Requirements	Remarks
Large	Web Server	Web Tier	2	Virtual	4 vCPU, 16 GB RAM	NA	100 GB	50 GB	Operating System - Windows Server 2016, 64-bit	
	Application	Application	2	Virtual	4 vCPU, 16 GB RAM	NA	100 GB	50 GB	Operating System - Windows Server 2016, 64-bit	

	cation n Serv er	ation Tier		al	16 GB RAM				System - Windows Server 2016, 64- bit	
	Data base Serv er	Data Tier	2	Virtu al	8 vCPU, 32 GB RAM	Microso ft SQL Server 2016 - Standar d Edition	500		Operating System - Windows Server 2016, 64- bit	SQL_Latin1_ General_CP1 _CI_AS

5 MyCloud Environment Preparation

This section describes how to prepare the environment to perform the physical installation and configuration of MyCloud.

Before beginning the installation, identify the installation mode and prepare the environment accordingly.

The following figure gives an overview of MyCloud Installation Workflow.

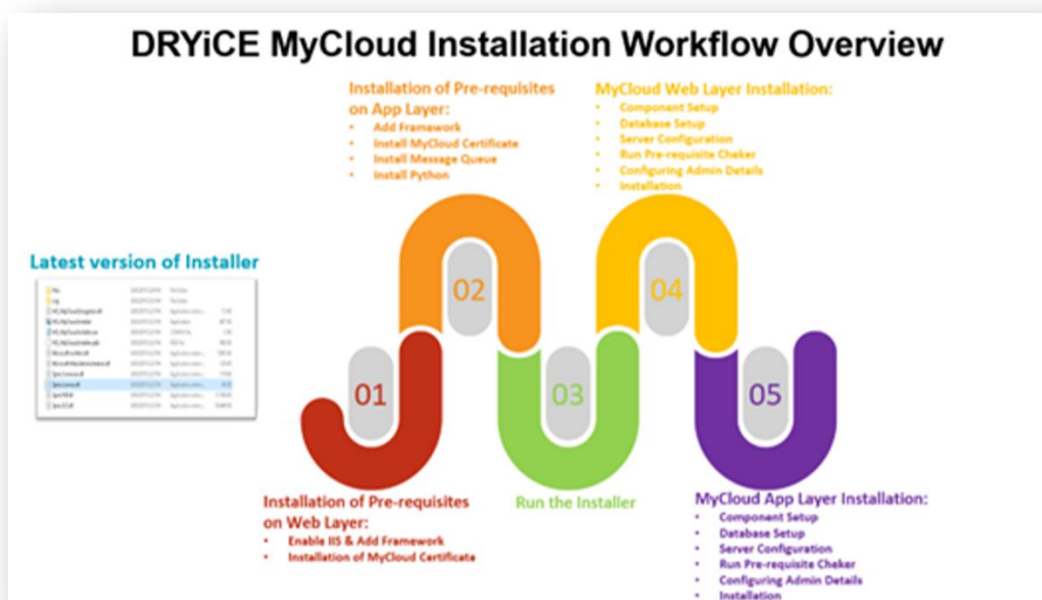


Figure 1 – MyCloud Installation Workflow Overview

5.1 Pre-requisites to run the Installer

Once the infrastructure resources are in place, identify the server on which the installer will run. Before executing the installer, the following software pre-requisites need to be in place on the server:

Table 14 – MyCloud Server Pre-requisites

Software	Version
Windows Version	Microsoft® Windows® Server 2016 Standard Edition or Windows Server 2016 Enterprise Edition Microsoft® Windows® Server 2016 Standard Edition, Windows Server 2016 Enterprise Edition or Microsoft® Windows® Server 2019 Edition
.Net Framework	.net framework 4.8
Licensed Software	SQL Server 2016/2019 Standard Edition

5.1.1 Installer

This section describes how to install the MyCloud components using installer on any server or standalone machine that can be further used for the deployment of MyCloud Web, Application, Database and its underlying components.

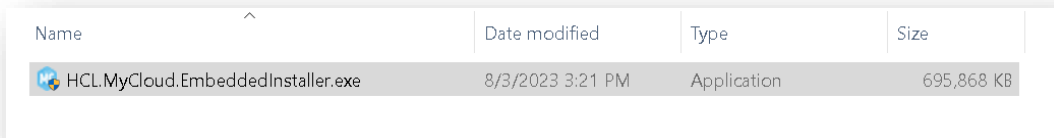
Get the latest version of the installer from the DRYiCE MyCloud Product Team or write to mycloud-product-supply@hcl.com.

MyCloud installer file includes a **Fully Executable Installer**.

This executable file enables the complete installation of MyCloud along with pre-requisite checker for all the servers.

MyCloud installation contains the following steps:

- [Pre-requisites to run the Installer](#).
- Run the installer.
- Installation of MyCloud using the **Installer**



Name	Date modified	Type	Size
HCL.MyCloud.EmbeddedInstaller.exe	8/3/2023 3:21 PM	Application	695,868 KB

Figure 2 – Installer

Refer the below table to understand some of the important fields mentioned in the above figure:

Table 15 – Installer Files Description

File Name	Description
Log	This folder contains a log created during the installation process. Initially folder will not be present, it will be generated once the installation is started.
HCL.MyCloud.EmbeddedInstaller	This is the executable file to install MyCloud

To Install the prerequisites, download the prerequisites folder from the same place where MyCloudInstaller is downloaded.

1. Open the **Prerequisites** folder.



Figure 3 – Install Pre-requisites

2. To install any Prerequisite, Select respective folder (for e.g. Click **Python**).

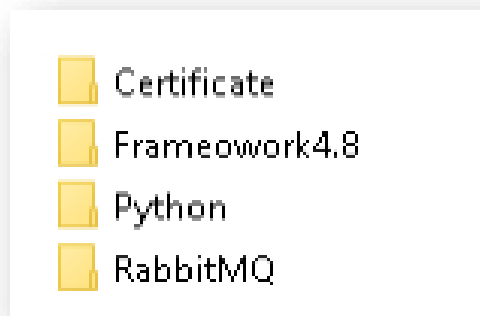


Figure 4 – Install Python

Refer the below table to understand the fields mentioned in the above figure:

Table 16 – Description of Certificate

File Name	Description
Certificate	This folder contains a MyCloud generated certificate that for inter-component communication
Framework4.8	This folder contains .net 4.8 runtime executable needed to be installed on MyCloud App and Web Servers
Python	This folder contains Python executable for windows
RabbitMQ	This folder contains RabbitMQ binaries.

For **Python** installation: Before running the installer, make sure that **Everyone** has the Write Permission on the Python folder.

Installation of Each Prerequisite installation procedure is detailed out in respective section below.

5.1.2 Enable Log on as Service

The user account/service account by which MyCloud services/components are run must have **Log on as Service** rights on both Web and App Servers.

- To check and enable the same (if not already enabled) follow the below Microsoft link:

<https://learn.microsoft.com/en-us/system-center/scsm/enable-service-log-on-sm?view=sc-sm-2022#enable-service-log-on-through-a-local-group-policy>

5.2 MyCloud Components Pre-requisites Installation

The following table lists the component-wise pre-requisites of MyCloud. It is important to install all the pre-requisites for the successful installation of MyCloud.

Table 17 – MyCloud Component Prerequisites Installation

Component Name	Microsoft .NET Framework 4.8	IIS	Certificate	Python/PowerShell	MSMQ/Rabbit MQ	DB
MyCloud Portal	Y	Y	Y	N	N	N
Job Listener	Y	N	Y	N	N	N

Sync Service	Y	N	Y	Y	N	N
Ad Sync Service	Y	N	Y	N	N	N
Workflow Service	Y	N	Y	N	Y	N
Orchestrator	Y	N	Y	Y	N	N
ITSM executor	Y	N	Y	N	N	N
Generic Task Executor	Y	N	Y	N	N	N
Billing Service	Y	N	Y	N	N	N
Performance Service	Y	N	Y	N	N	N
Health Monitor Service	Y	N	Y	N	N	N
Database	N	N	N	N	N	Y
Cisco Intersight Sync Service	Y	N	Y	N	N	N

5.2.1 Installation of pre-requisites on Web Layer

This section describes how to install the pre-requisites of **MyCloud Web Layer**. As stated in [Table 17 – MyCloud Component Prerequisites Installation](#), the web layer pre-requisites are **certificate**, **IIS** and **.Net Framework**.

5.2.1.1 Install .Net Framework 4.8 Runtime

1. Make sure the **MyCloudInstaller zip (provided by MyCloud Support Team)** is present on **Web** server.
2. Unzip the Installer **Zip** file.
3. Go to the .Net 4.8 setup file present in **Prerequisites** folder as shown below.

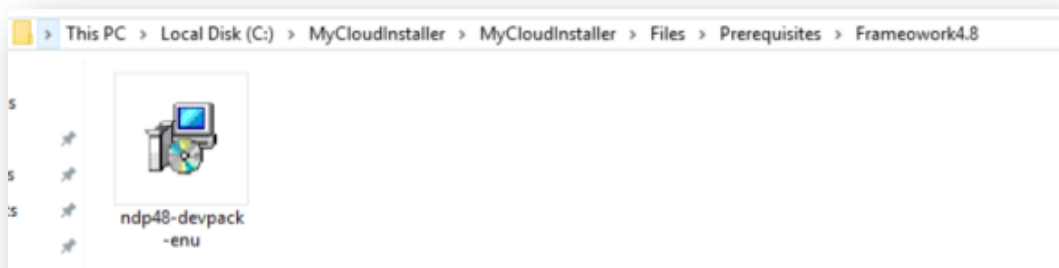


Figure 5 – Install .Net Framework 4.8

4. Install the .net 4.8 setup on the Web server.

5. On Successful installation, if the below message comes to restart the server, Restart the Web Server.
If System doesn't ask for Restart **close** the setup.

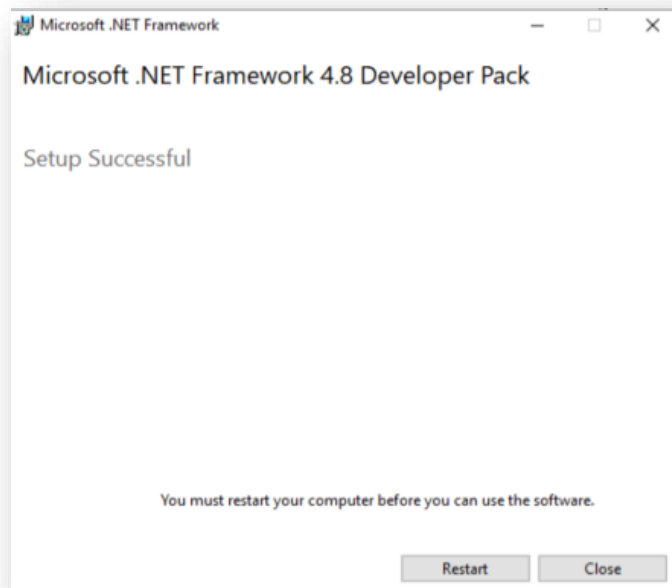


Figure 6 – Install .Net Framework 4.8 (Cont.)

5.2.1.2 Enable IIS and add .Net Framework

To enable IIS on MyCloud **Web Server**, login to the server and follow the below steps:

1. Press **Window + R** keys on keyboard to open RUN command window.
2. Type **ServerManager** and click **Ok**.

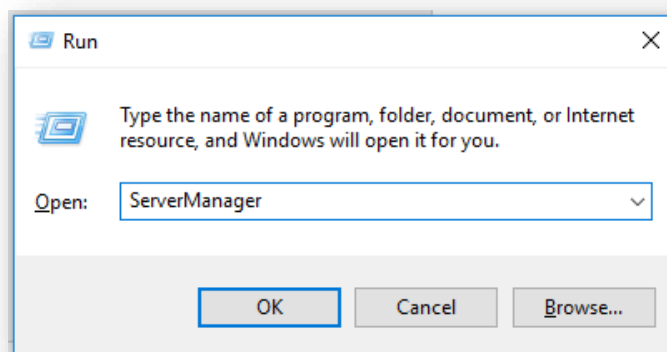


Figure 7 – Enable IIS and add .Net Framework

3. The Server Manager window appears.
4. Click on Add roles and features.

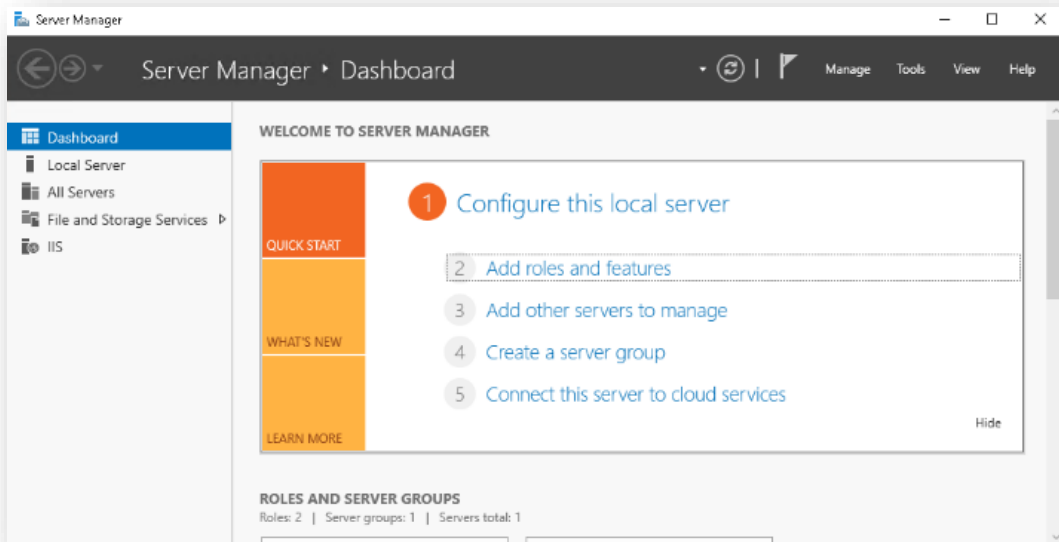


Figure 8 – Add Roles and Features

5. The Add roles and features wizard appears. By default, the option Before You Begin is selected in the left panel of the wizard.
6. Click **Next**.

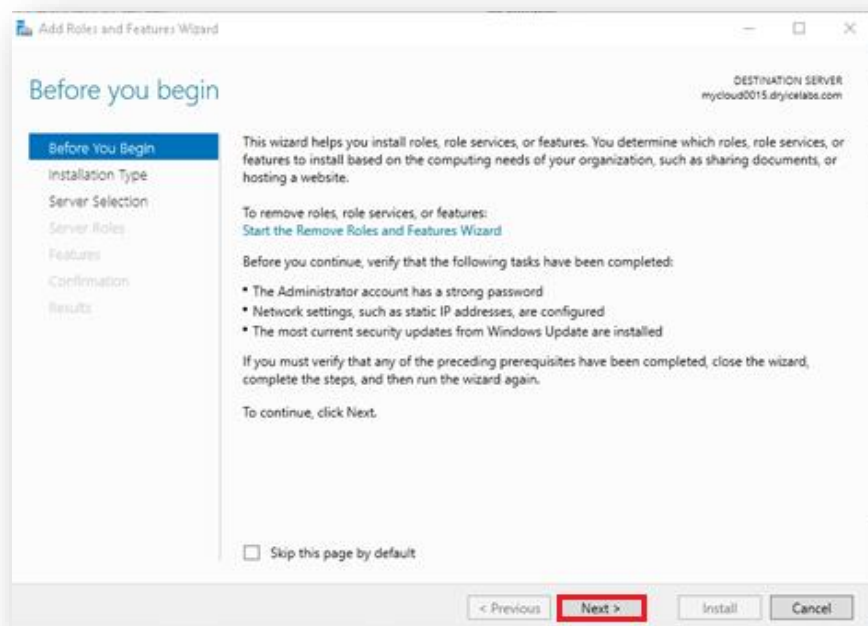


Figure 9 – Enable IIS and Add .Net Framework (Cont.)

7. The Installation Type option is auto selected. Enable Role-based or feature-based installation Radio button if not automatically enabled.
8. Click **Next**.

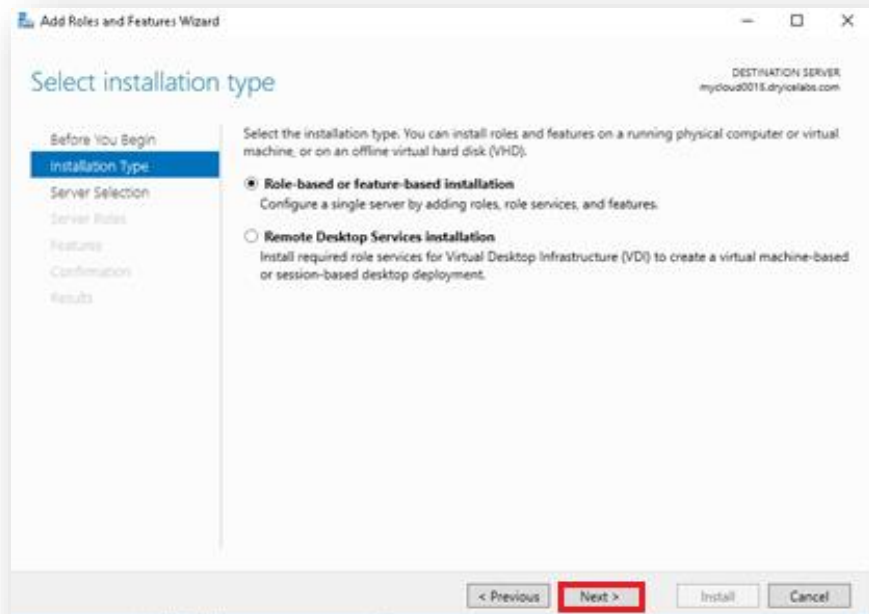


Figure 10 – Enable IIS and Add .Net Framework (Cont.)

9. The **Server Selection** option is auto selected.

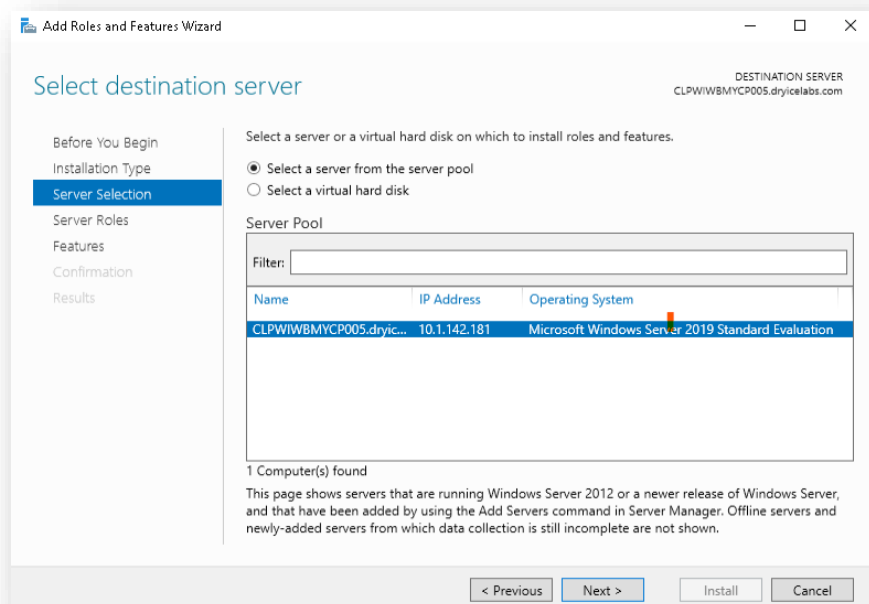


Figure 11 – Enable IIS and Add .Net Framework (Cont.)

10. Choose Select a server from the Server Pool option.
11. Select the Machine Name in the Server Pool if not automatically selected.
12. Click **Next**.

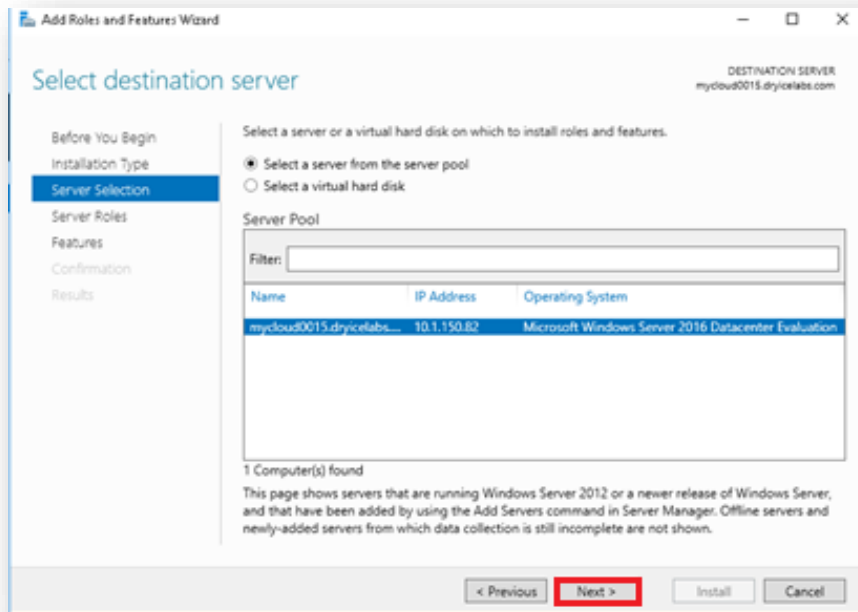


Figure 12 – Enable IIS and Add .Net Framework (Cont.)

13. The **Server Roles** Screen appears.
14. Enable IIS by selecting **Web Server (IIS)**.

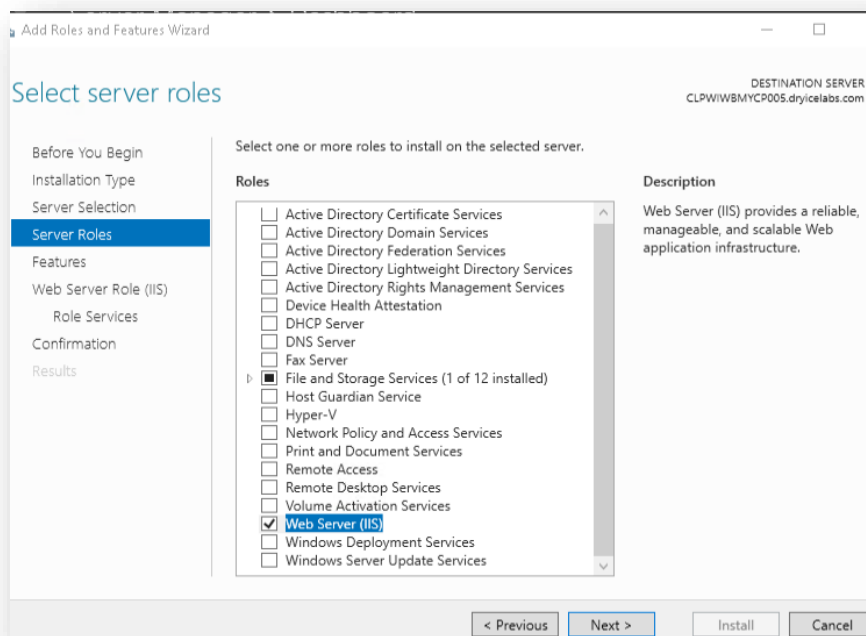


Figure 13 – Enable IIS and Add .Net Framework (Cont.)

15. Add Roles and Features Wizard appears, Click on Features.
16. Click Next.
17. Features screen gets enabled as below.

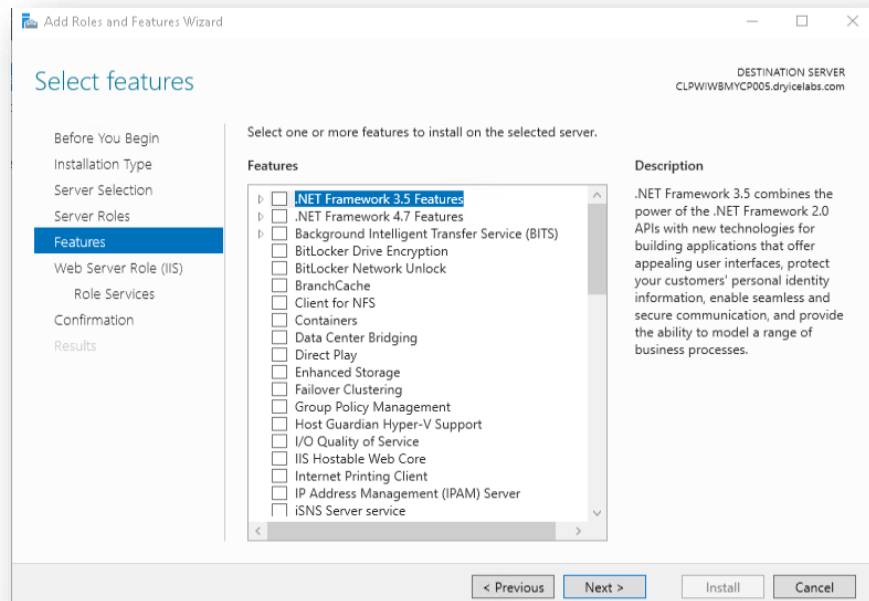


Figure 14 – Enable IIS and Add .Net Framework (Cont.)

18. Enable .Net Framework, ASP .Net Framework and WCF Services.

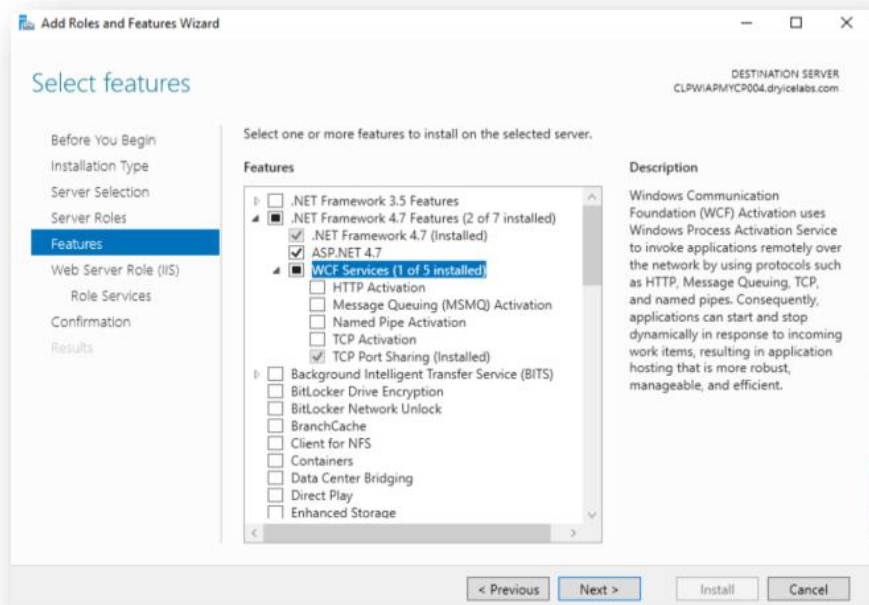


Figure 15 – Enable IIS and Add .Net Framework (Cont.)

19. Select All WCF Services as shown in below figure:

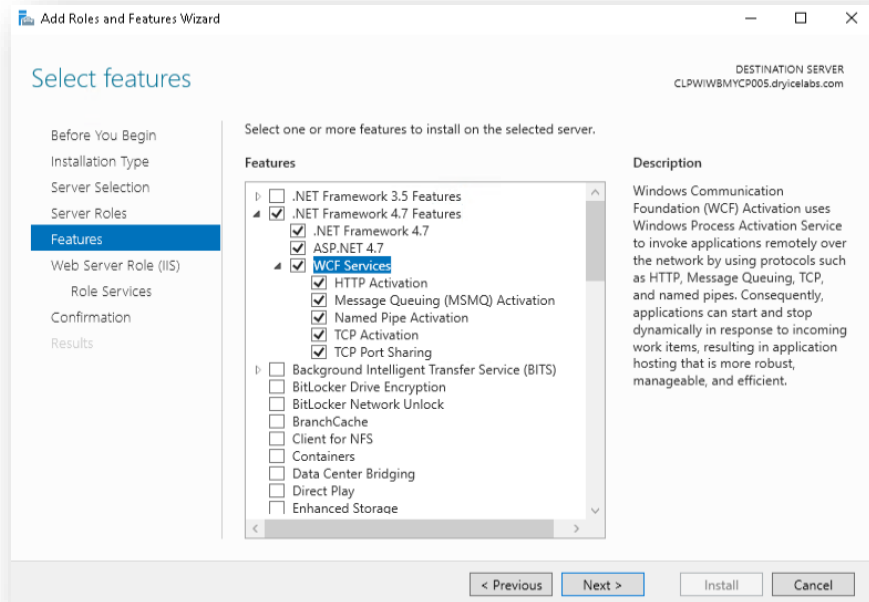


Figure 16 – Enable IIS and Add .Net Framework (Cont.)

20. Click **Next**, Web Server Role (IIS) screen appears.

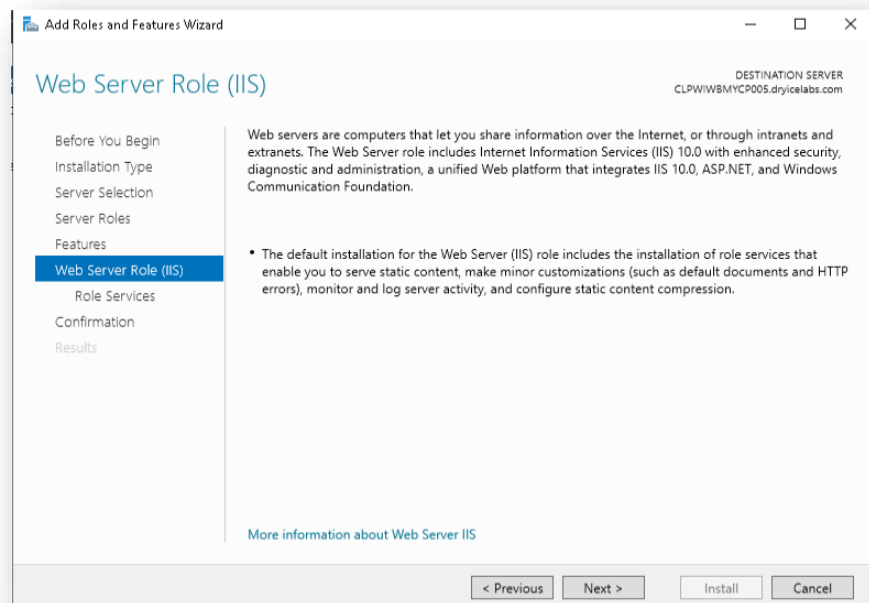


Figure 17 – Enable IIS and Add .Net Framework (Cont.)

21. Click Next to go to **"Role Services"**.

22. Under Web Server, Select **Services** as mentioned in below 2 screenshots.

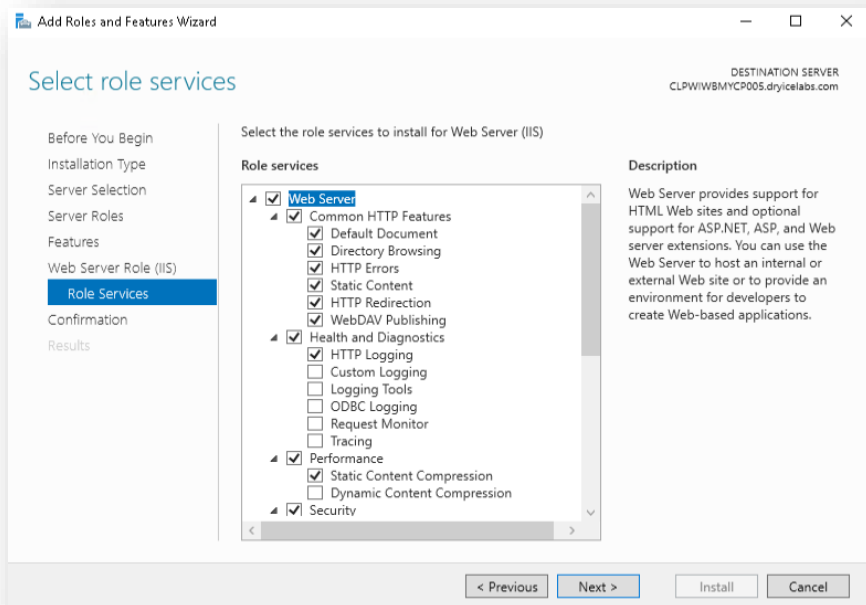


Figure 18 – Enable IIS and Add .Net Framework (Cont.)

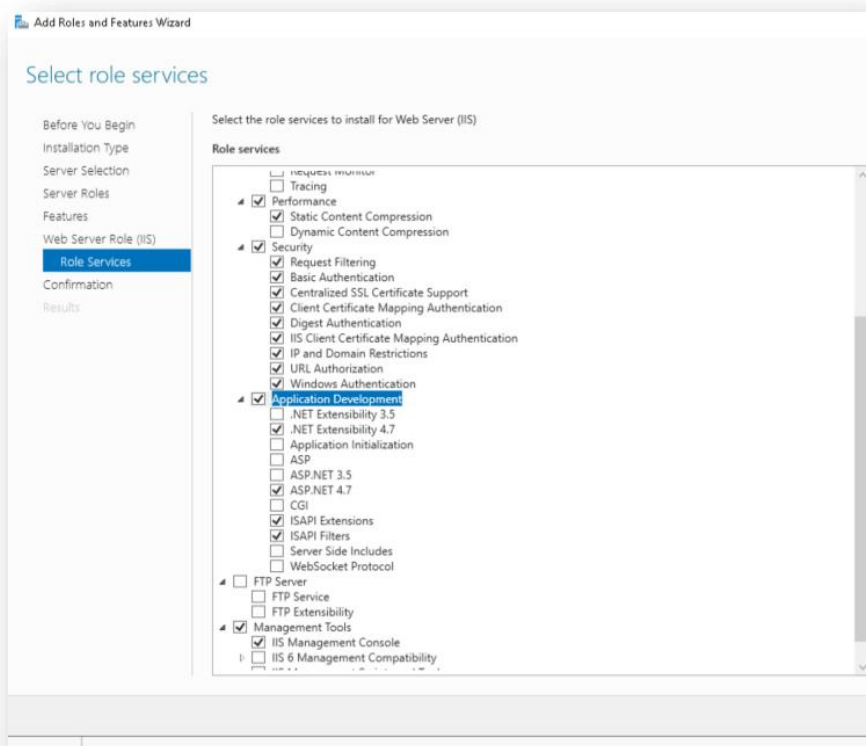


Figure 19 – Enable IIS and Add .Net Framework (Cont.)

23. Click **Next**

24. On Confirmation Screen, Click **Install**

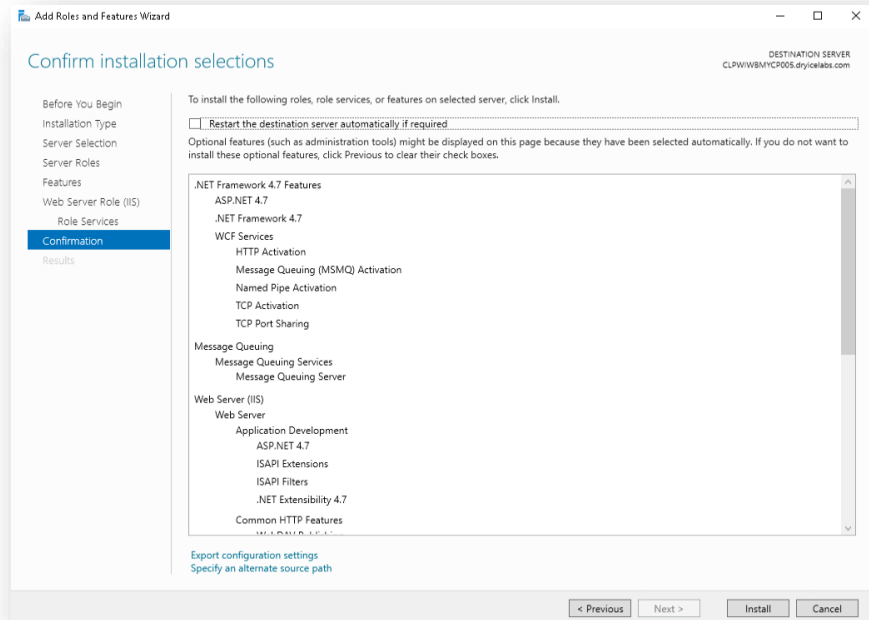


Figure 20 – Enable IIS and Add .Net Framework (Cont.)

Do not select the check box to **Restart Destination Server**.

The Installation progress screen shows the current installation status.

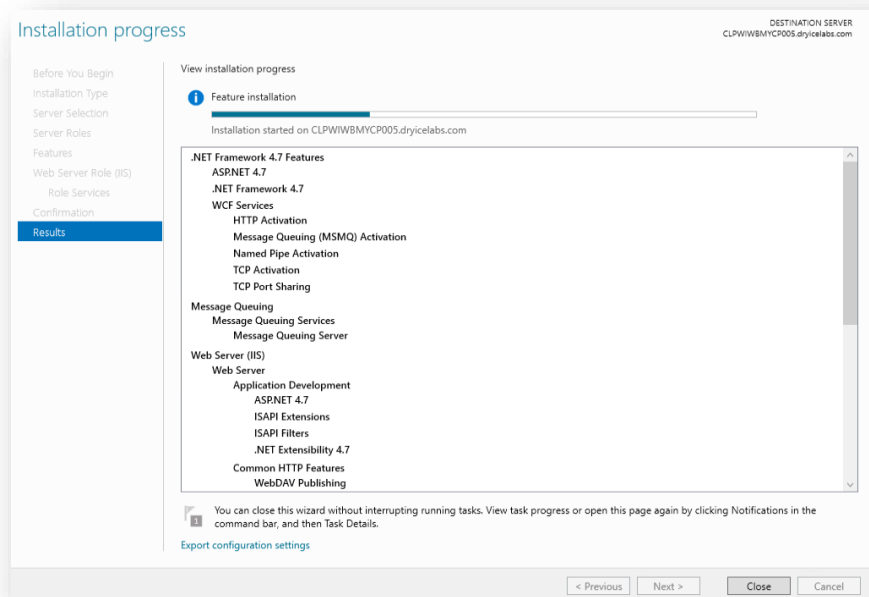


Figure 21 – Installation Status

25. Once the **IIS & .Net framework** are installed successfully, click on the **Close** button to exit the wizard.

A default website is configured on port '80' after the installation of IIS.
Please delete the website.

5.2.1.3 Delete Default Website on Port

1. Press **Window + R** keys on keyboard to open RUN command window.
2. Type **inetmgr** and click **Ok**.

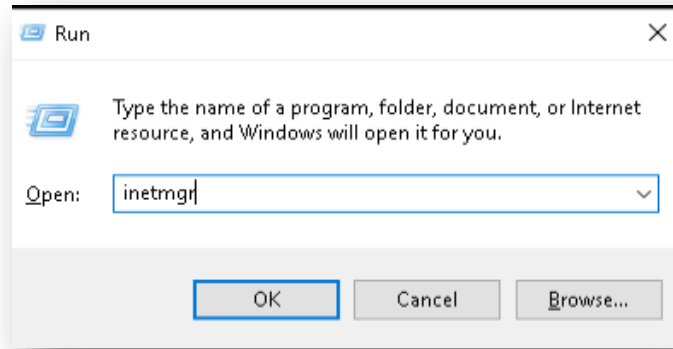


Figure 22 – Open IIS Manager

3. From **Connections** Menu on left panel, Click on **Web Server name**.
 - a. Expand and go to **Sites**, Expand **Sites** and delete Default Web Site (if exists) by clicking on **Remove** as shown in following figure:

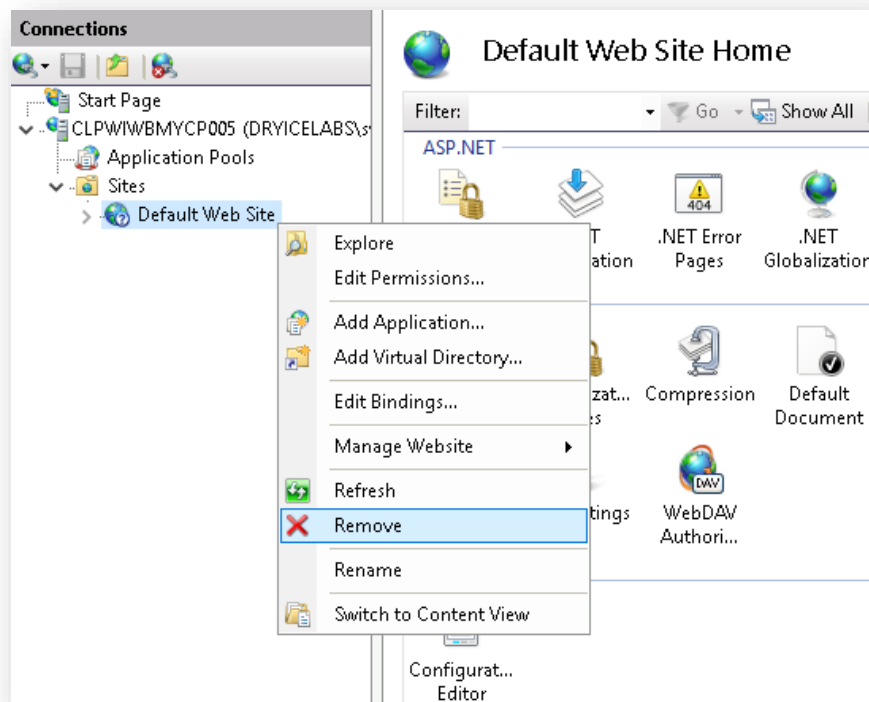


Figure 23 – Delete Default Website

5.2.2 Installation of Pre-requisites on App Layer

This section describes how to install the pre-requisites of **MyCloud App Layer**. As stated in [Table 17 – MyCloud Component Prerequisites Installation](#), the App layer pre-requisites are **Certificate**, **Messaging Queue**, **.Net Framework**, and **Python**.

5.2.2.1 Install .Net Framework 4.8 Runtime

1. Make sure the MyCloudInstaller zip (provided by MyCloud Support Team) is present on App server.
2. Unzip the Installer Zip file.

3. Go to the .Net 4.8 setup file present in **Prerequisites** folder as shown below.

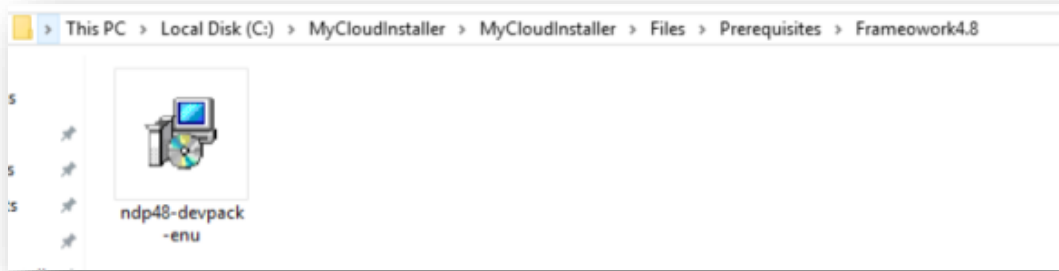


Figure 24 - Install .Net Framework 4.8 Runtime

4. Install the .net 4.8 setup on the App server.
5. On Successful installation if below message comes to restart the server, Restart the **App** Server. If System doesn't ask for Restart **close** the setup

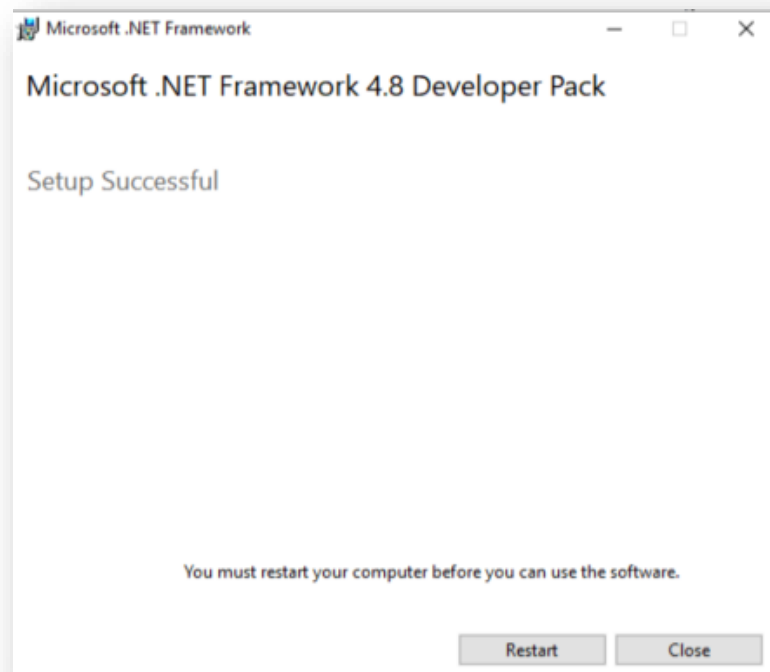


Figure 25 - Install .Net Framework 4.8 Runtime (Cont.)

5.2.2.2 Add .Net Framework

To add .Net framework, refer to [Enable IIS and Add .Net Framework](#) section.

5.2.2.3 Installing Messaging Queue

1. Press **Window + R** keys on the keyboard to open the **RUN** command window.
2. Type ServerManager and click **OK**.

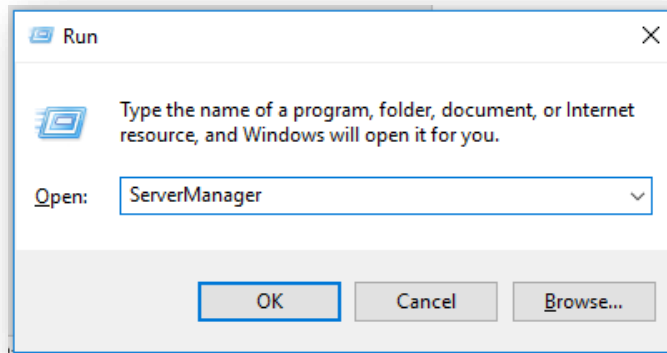


Figure 26 – Installing Messaging Queue

3. The Server Manager window appears.
4. Click on Add roles and features.

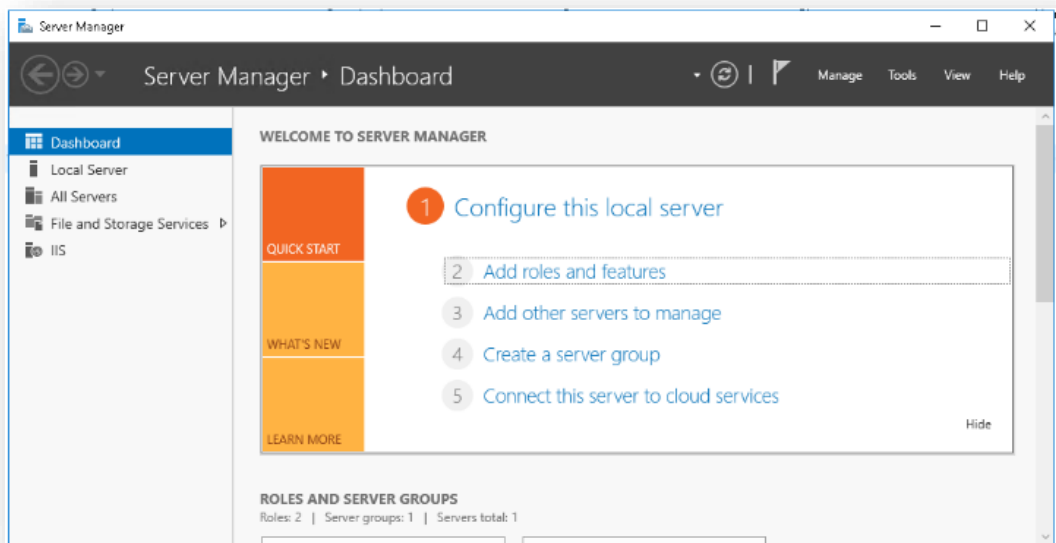


Figure 27 – Installing Messaging Queue (Cont.)

5. The Add roles and features wizard appears. By default, the Before you begin option is selected.
6. Click **Next**.

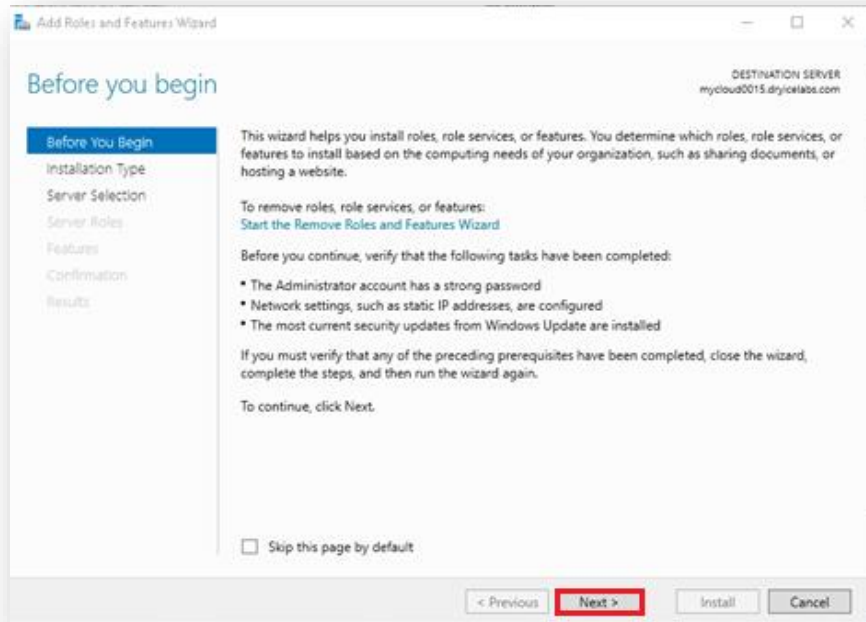


Figure 28 – Installing Messaging Queue (Cont.)

7. The Select installation Type page appears.
8. Select Role-based or feature-based installation and then click **Next**.

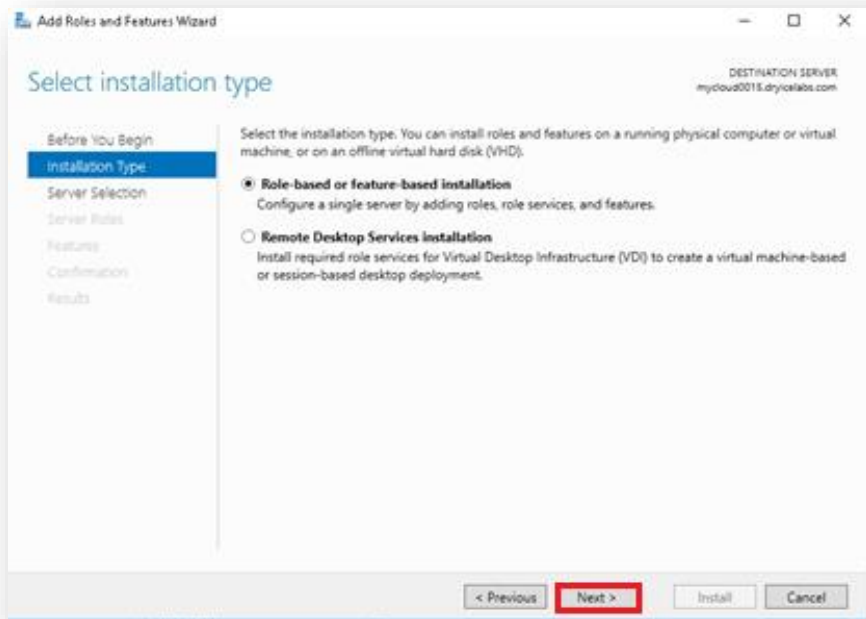


Figure 29 – Installing Messaging Queue (Cont.)

9. The Server Selection page appears.
10. Select the option Select a server from the server pool.
11. Select the **Machine Name** in the **Server Pool** field and then click **Next**.

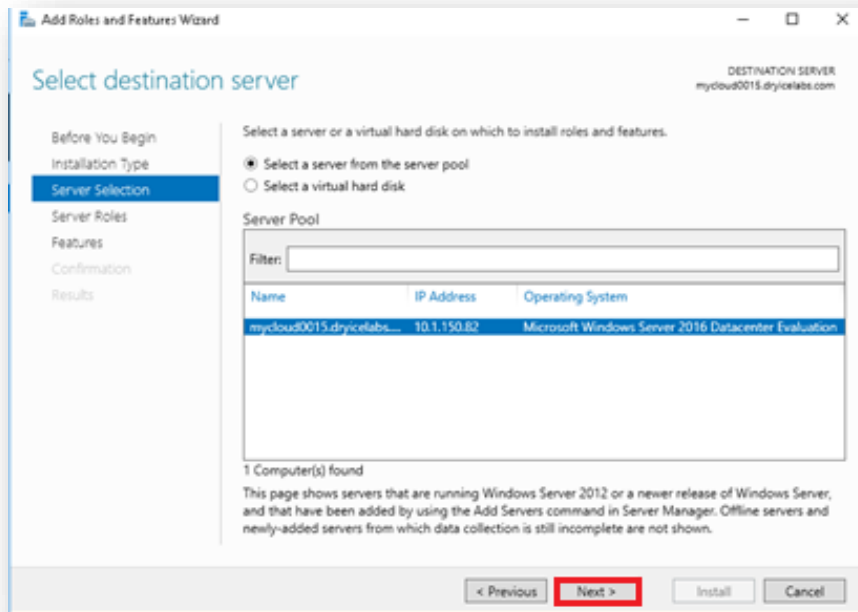


Figure 30 – Installing Messaging Queue (Cont.)

12. On **Features**, select **Message Queuing Server** (if not already selected) as shown in the following figure:

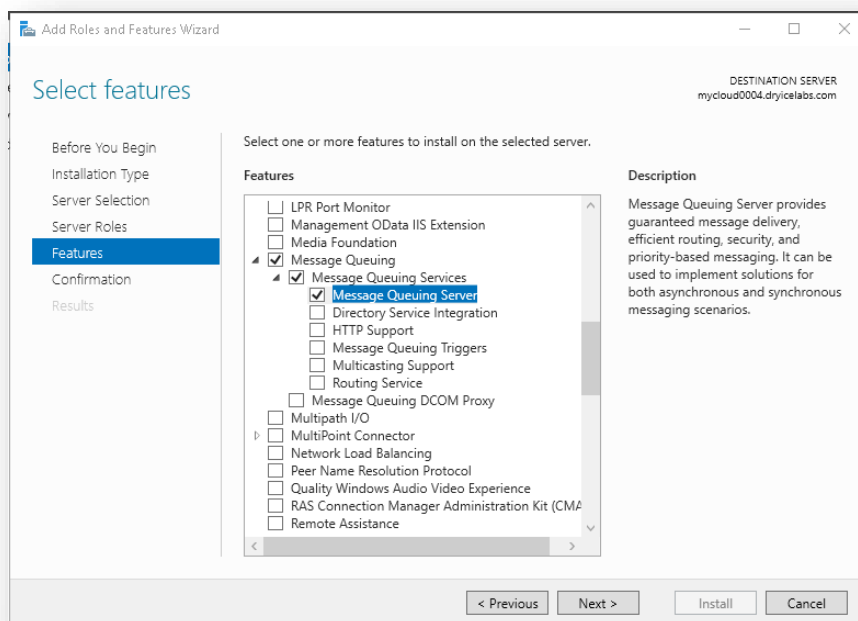


Figure 31 – Installing Messaging Queue (Cont.)

If Messaging Queue Server already showing as Installed, click on Cancel and close the wizard and skip below steps for Installing the same.

13. Click **Next**.
14. The Confirmation page appears.

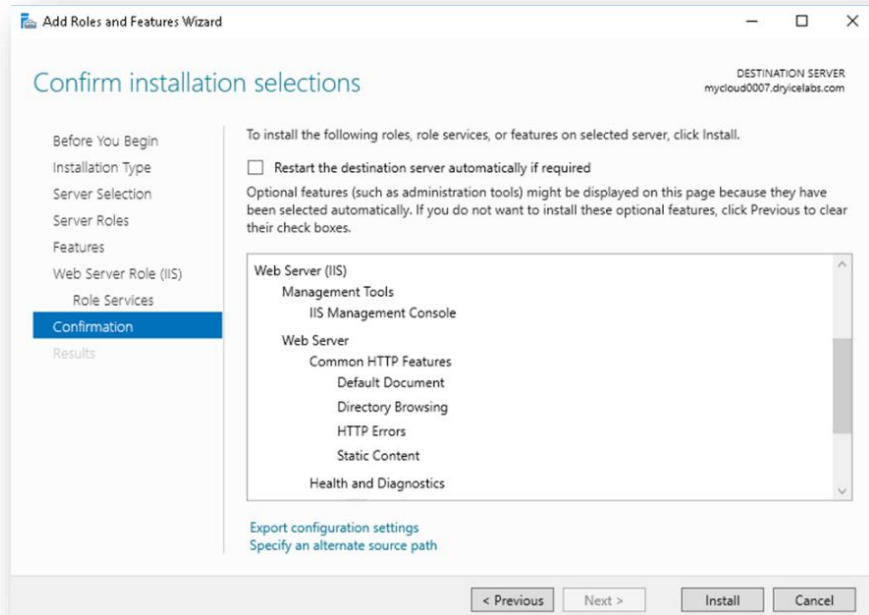


Figure 32 – Installing Messaging Queue (Cont.)

15. Click **Install**.

MyCloud supports **Microsoft Messaging Queue** and **RabbitMQ**. In this guide, we have considered **MSMQ** for installation. If the user wishes to use RabbitMQ, the user needs to do configuration changes against **Workflow Service** in **Manage Component Keys Section** using Admin login credentials. The user also needs to install RabbitMQ and configure stand-alone or in HA according to their architectural requirement.

16. Installation progress screen shows the installation status.

17. Once the Messaging Queue is installed, **Close** the Installation wizard and **Exit**.

5.2.2.4 Installing Python

Follow the steps below to install Python.

1. Go to the following location where Python setup file is available:
2. {drive where MyCloud installer exists} \MyCloudInstaller\Files\Prerequisites\Python\python-3.6.8-amd64.exe}.
3. Right-click on the setup file and click on **Run as administrator**.

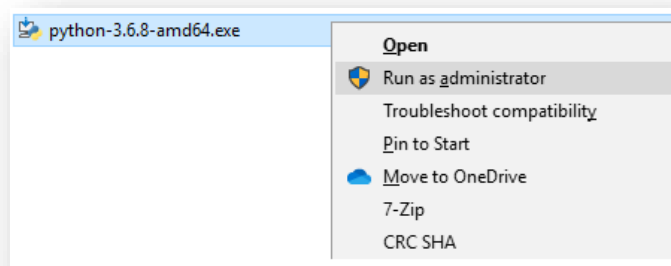


Figure 33 – Installing Python

4. The Python Setup wizard appears.

5. Click on Customize Installation.

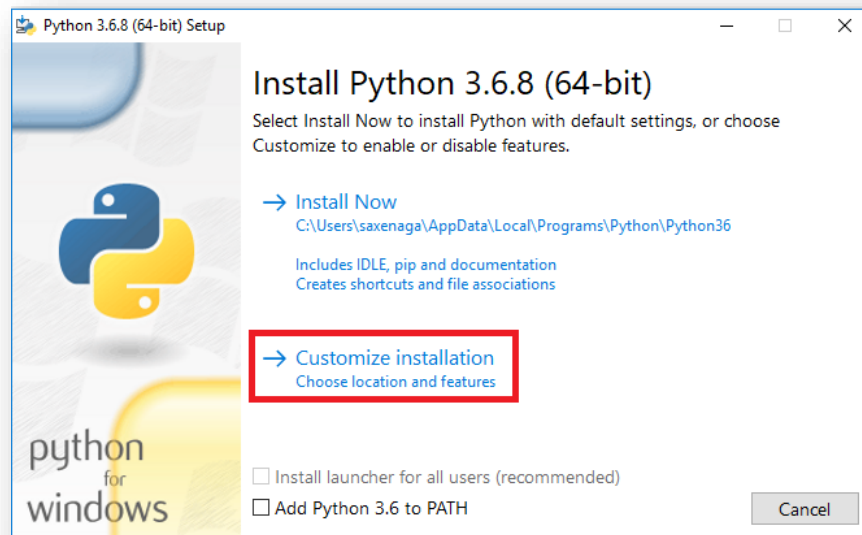


Figure 34 – Installing Python (Cont.)

6. The Optional Features screen appears.
7. Select options highlighted in red box below and Click **Next**.

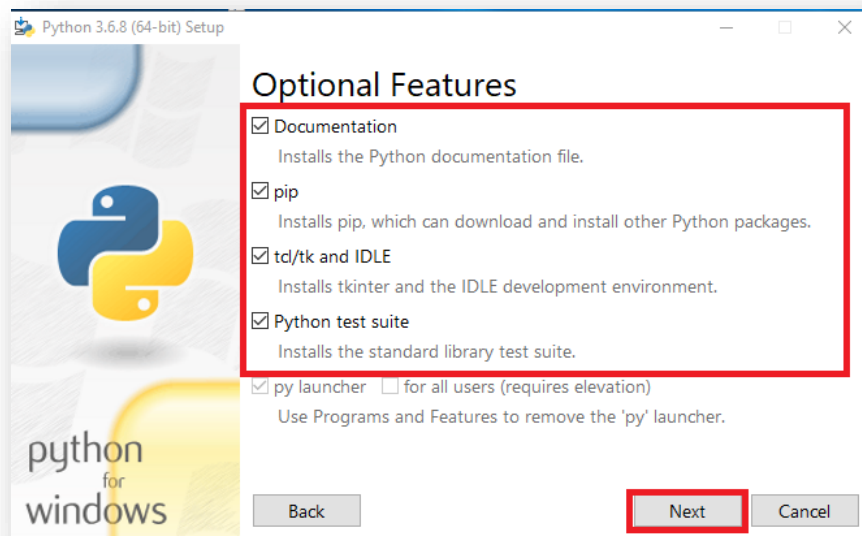


Figure 35 – Installing Python (Cont.)

8. The Advanced Options screen appears.
9. Select the check boxes as shown in the following figure and click Install.

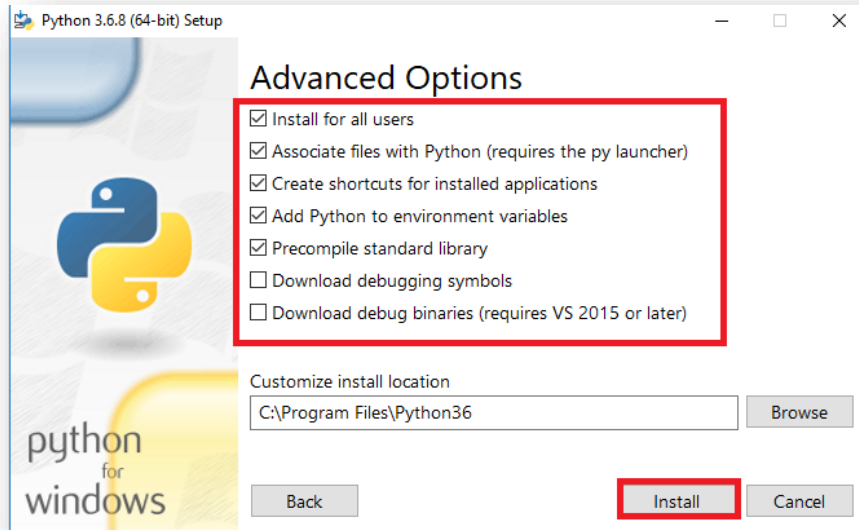


Figure 36 – Installing Python (Cont.)

Ensure Install for all users is checked.

10. Setup progress screen shows the current setup status.

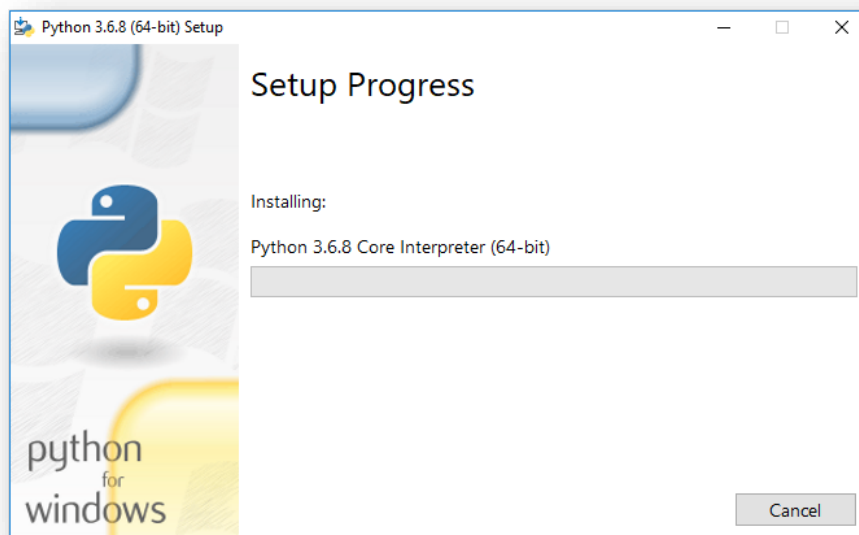


Figure 37 – Installing Python (Cont.)

11. After the completion of the setup process, the Setup was Successful message is displayed,

12. Click **Close** to close the installation wizard.



Figure 38 – Installing Python (Cont.)

Python version 3.6.8 and above is supported.

5.2.3 Installation of Pre-requisites on Database Layer

This section describes the pre-requisites of database.

1. SQL server version should be SQL server 2016(sp2), 2017 and 2019 edition.
2. Default SQL server and database collation is SQL_Latin1_General_CP1_CI_AS as shown in below.

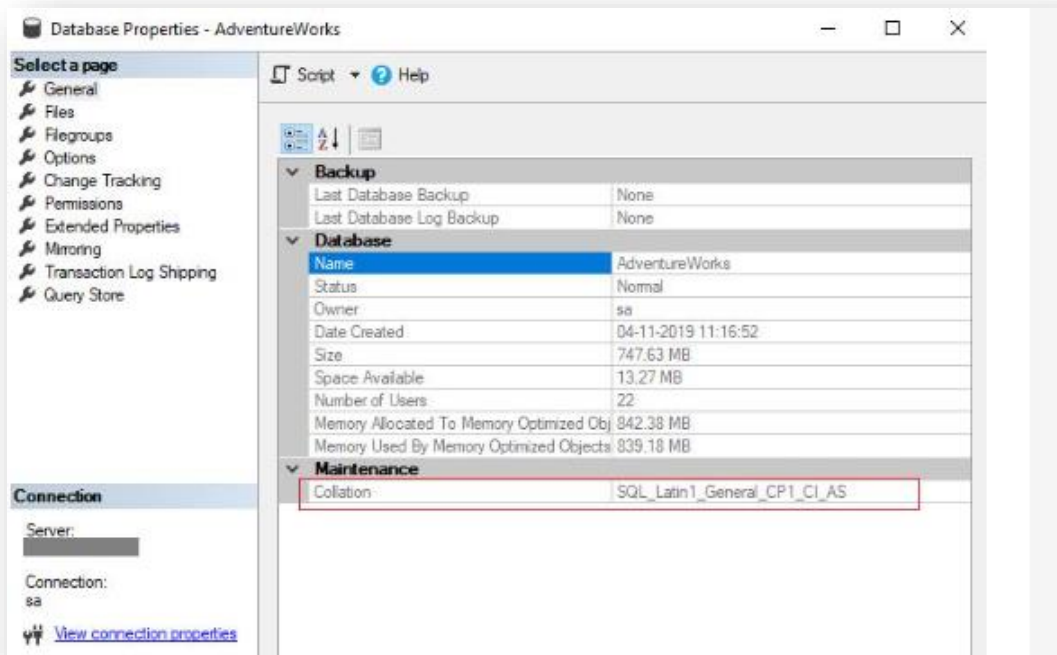


Figure 39 – Database Properties

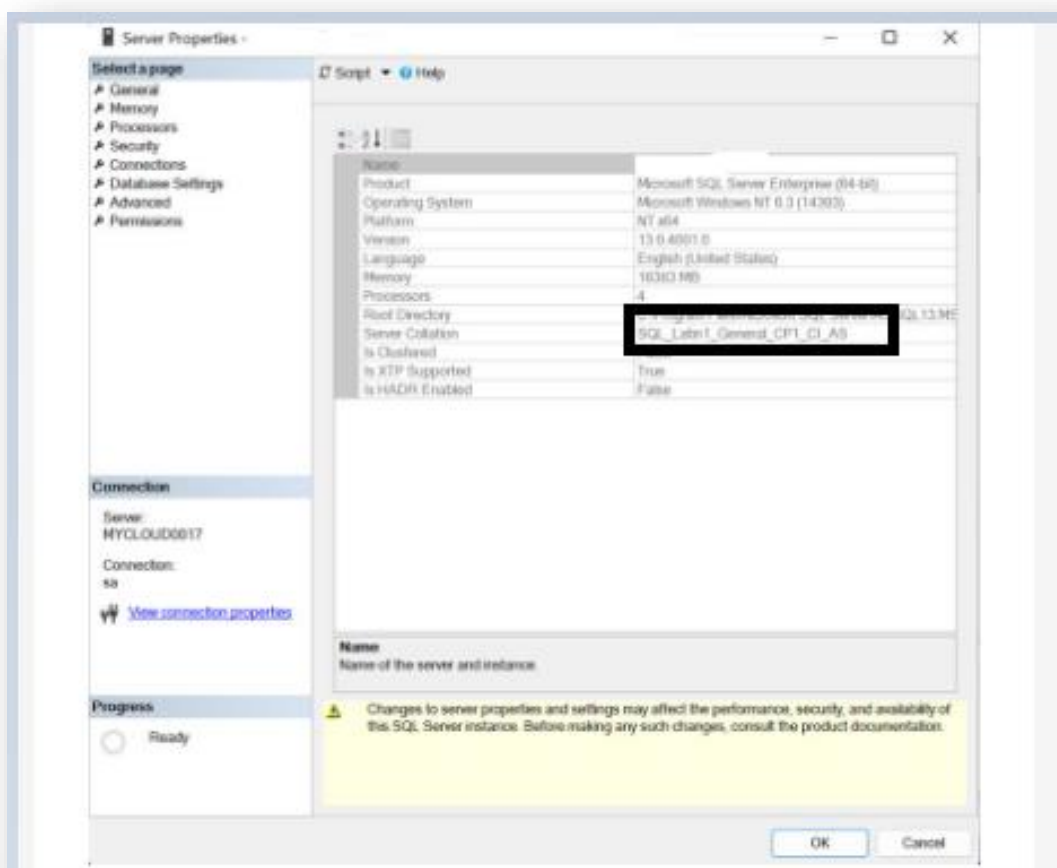


Figure 40 – Server Properties

5.3 Deployment

This section describes how to deploy MyCloud on required infrastructure. It includes the following steps:

- [MyCloud Web Layer Installation using the MyCloud installer](#)
- [MyCloud App Layer Installation using the MyCloud Installer](#)

5.3.1 MyCloud Web Layer Installation

Run the installer with Administrator permissions.

This section describes how to configure MyCloud Web Layer server.

MyCloud web layer has two components.

- MyCloud UI Portal
- Key Rotation Service (KRS)

5.3.1.1 Components Setup

To setup the Web components, follow the below steps:

1. Make sure the MyCloudInstaller zip (provided by MyCloud Support Team) is present on Web server.
2. Unzip the Installer **Zip** file.
3. Go to the unzipped MyCloudInstaller → MyCloudInstaller folder
4. Right-click on HCL.MyCloud.EmbeddedInstaller Application file and Run as Administrator


Name	Date modified	Type	Size
 HCL.MyCloud.EmbeddedInstaller.exe	8/3/2023 3:21 PM	Application	695,868 KB

Figure 41 – MyCloud Installer

5. Click on the start button to start the installation.

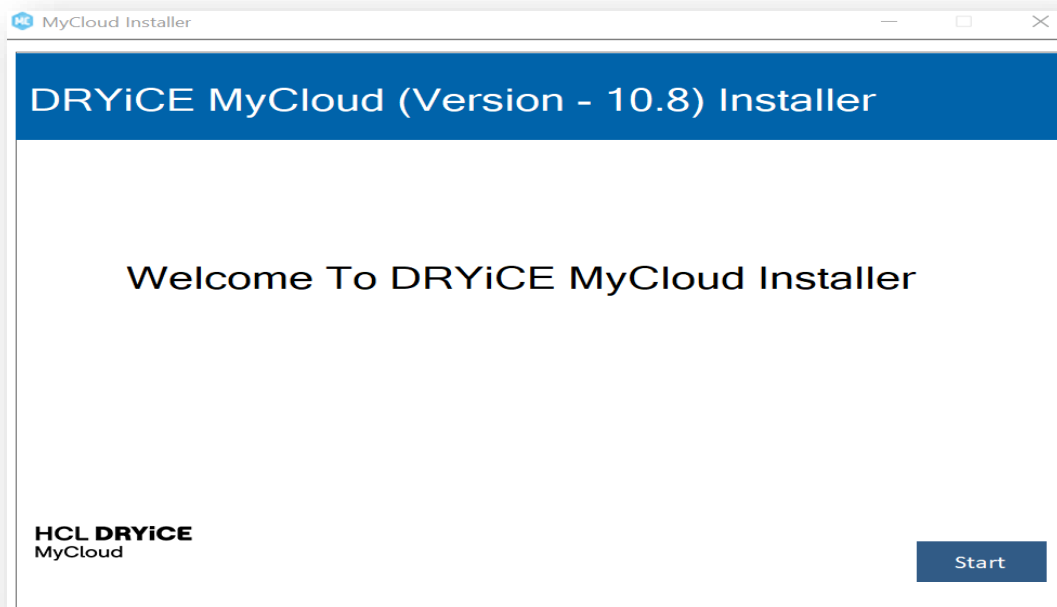


Figure 42 – MyCloud – New Installation

6. In case of fresh/new installation below screen will appear with the **"New installation"** radio checked.

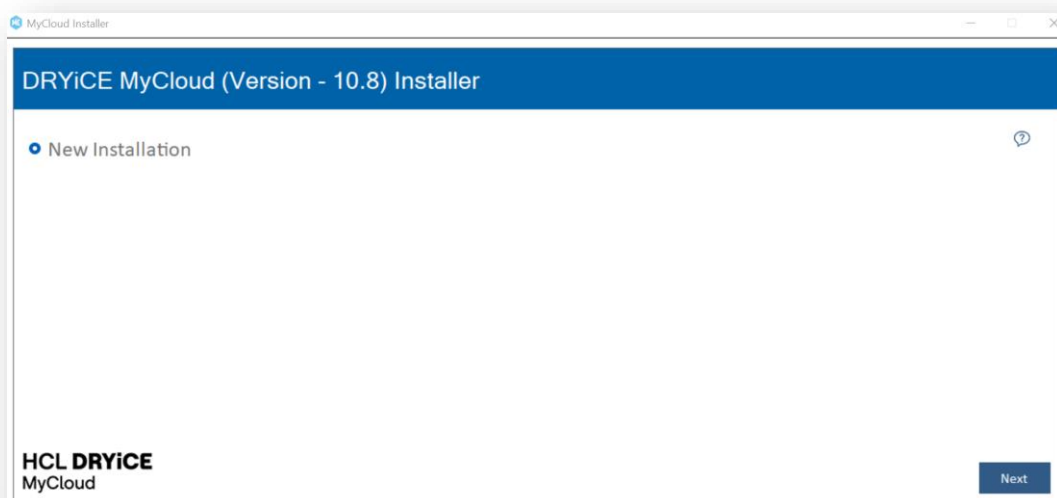


Figure 43 – MyCloud – New Installation

In case of Upgrade, below screen will appear for upgrade Installation

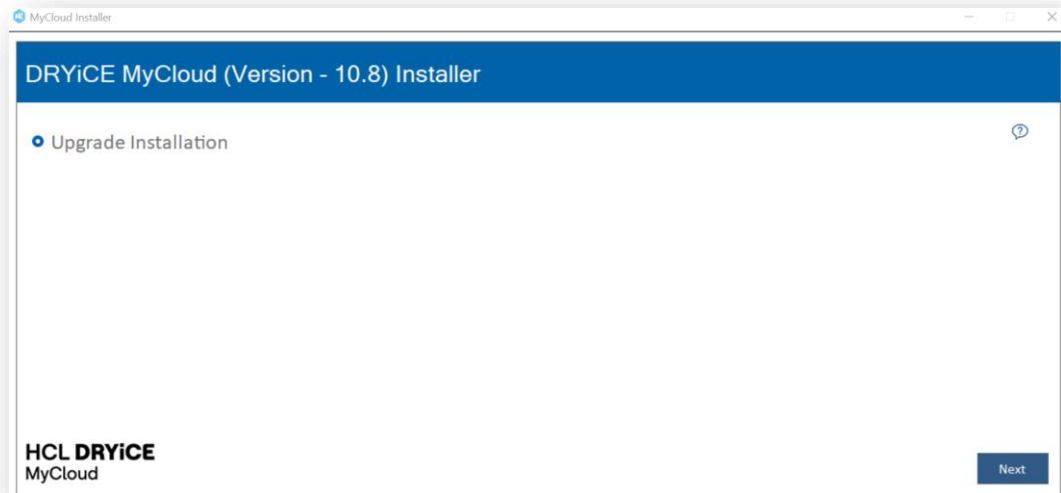


Figure 44 – MyCloud – Upgrade Installation

7. Click **Next**.
8. On the left navigation bar, Component Selection is auto selected.
9. As MyCloud **Web layer** is being configured, select the **Web Component**.

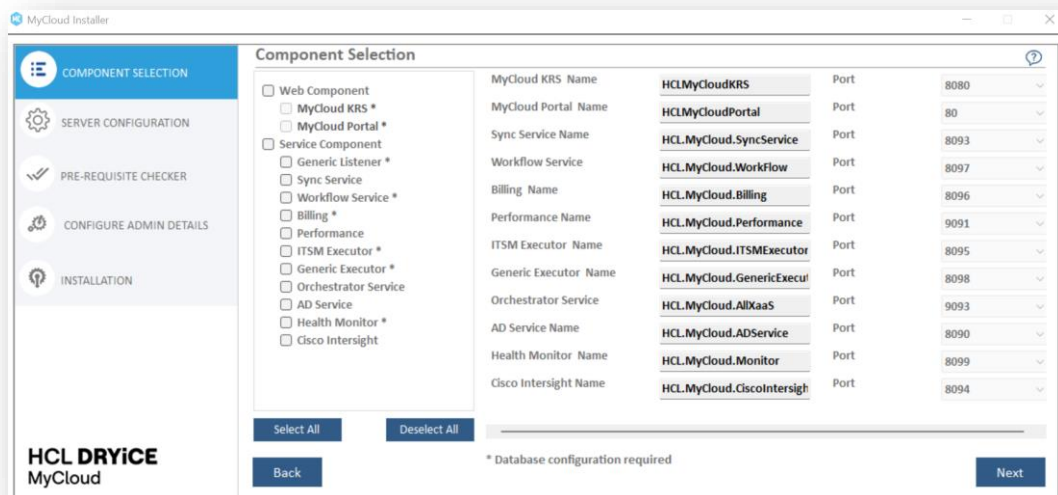


Figure 45 – Web Component Selection

In case of UPGRADE, Web Components which are already installed are auto selected

10. Select the **Port** against both selected web component and leave them as it for default.
 - MyCloud KRS – port 8080 (default)
 - MyCloud Portal – port 80 (default)
11. Click **Next** to go to Database **Setup**.

5.3.1.2 Database Setup

MyCloud Installer uses database screen to capture details which are required to connect to the **Database Server** and create required databases. Following are the steps:

1. After **Web Components** are selected, On clicking **Next**, User is redirected to **Database Details** screen. The **Database Details** pane appears as below:

Figure 46 - Database Details

Refer the below table to understand the fields mentioned in the above figure:

Table 18 - Database Setup

Field Name	Description
Database Details	This pane captures details of the database like server name, authentication type, username, password, that are being used for database creation.
Server HostName/IP	Field to input database server hostname or IP address.
Database Instance Name	Field to input database server instance. This is Optional field.
Authentication	Authentication type to be used to connect to the database server/instance. options are windows authentication or SQL Server authentication .
UserName and Password	<p>These credentials are used to login to the database server to authenticate & establish the connection.</p> <p>These fields cannot be overridden if authentication type is windows authentication.</p> <p>If authentication type is SQL Server Authentication, then username and password are mandatory and need to be provided.</p>
Check Connection	Upon clicking the option, it validates whether connection (between Web layer and Database) has been established successfully or not.

2. Enter the Database Server **Hostname** or **IP Address**.
3. Enter Database Instance Name. (**Optional**)

4. Select **Authentication**. Database configuration is done with the following authentication:

- Windows Authentication
- SQL Server Authentication

If Authentication is "SQL Server Authentication ", Enter the login credentials i.e., the **Username and Password** for getting access to the database server.

By default, MyCloud installer will create the databases with the **default database names** as shown in figure below:

The screenshot shows the 'Database Details' configuration window. On the left is a sidebar with navigation options: COMPONENT SELECTION, DATABASE DETAILS (selected), SERVER CONFIGURATION, PRE-REQUISITE CHECKER, CONFIGURE ADMIN DETAILS, and INSTALLATION. The main area contains the following fields:

- Server HostName/IP: 10.1.30.62
- Database Instance Name: Enter DB Instance.
- Authentication: Windows Authentication (dropdown)
- User Name: DRYICELABS/svc-mycl-admin
- Password: (empty field)
- Database Name: A list with three items: MyCloudDB, MyCloudBillingDB, and MyCloudPerformanceDB. This entire section is enclosed in a red rectangular box.

Figure 47 – Default Database Names

While doing MyCloud UPGRADE make sure the database name is same as it was provided during installation.

5. Click **Check** Connection to check the connection to the respective server.

This screenshot shows the 'Database Details' window after a connection check. The configuration is as follows:

- Server HostName/IP: 10.1.160.25
- Database Instance Name: Enter DB Instance.
- Authentication: SQL Server Authentication (dropdown)
- User Name: sa
- Password: (masked with asterisks)
- Database Name: A list with three items: MyCloudDB, MyCloudBillingDB, and MyCloudPerformanceDB. Each item has the word 'New' in green text to its right.

A green button labeled 'Connection Success' is located below the database names. At the bottom of the window are 'Back' and 'Next' buttons, and the HCL DRYICE MyCloud logo is in the bottom left corner.

Figure 48 – Database Check Connection

Above Screenshot shows that Database Names has been Changed from Config file as per step 6 above.

During Installation If database names already exist on the database server as shown in below figure, change the database name as mentioned in step 7 above.

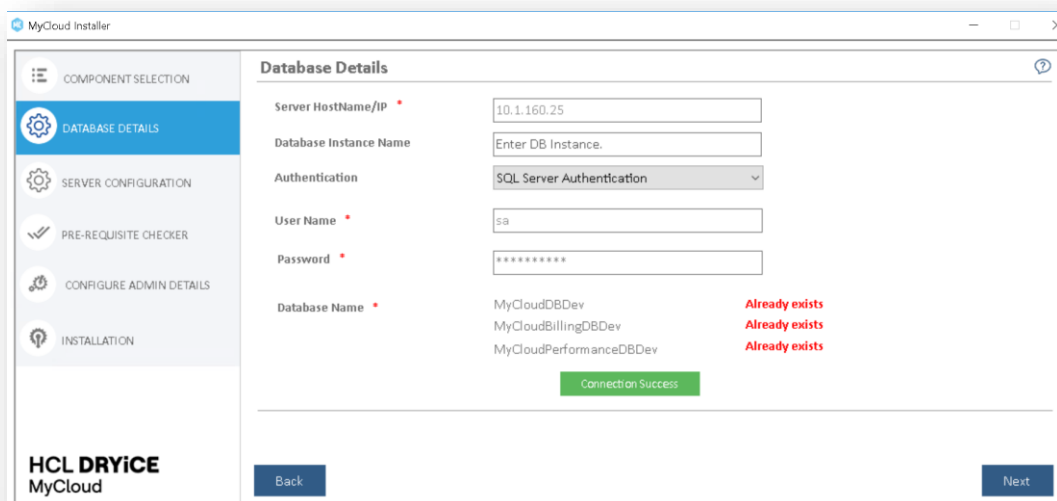


Figure 49 – MyCloud Installer – Database Already Exist

6. Click Next to go to Server Configuration page.

5.3.1.3 Server Configuration

In this section, details of MyCloud Web Server using the installer is being captured.

1. IP Address/Host Name is auto populated.
2. Enter the Account Type (Domain Administrator or Local Administrator).
3. Provide the Domain
4. Enter the UserName to access the Web server.
5. Enter the Password for the web server.
6. Click on **Check User Validity** button.

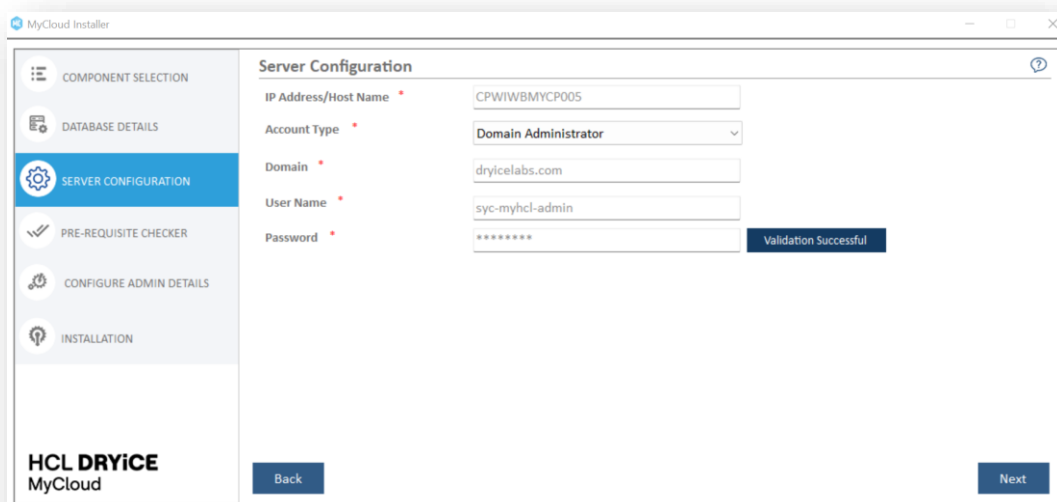


Figure 50 – Server Configuration

7. If Validation Success message appears, Click Next.

8. The Prerequisite Checker screen appears.

All the fields marked with asterisk (*) are mandatory.

5.3.1.4 Run Prerequisite Checker

This section describes how to run the prerequisite checker to verify that the installation pre-requisites have been installed.

The **Prerequisite Checker** screen lists the configurations that are mandatory for the components selected on previous screen.

Prerequisite Checker always runs as part of Setup.

1. Click **Run** to start the pre-requisite checker against components selected for installation on the web server.

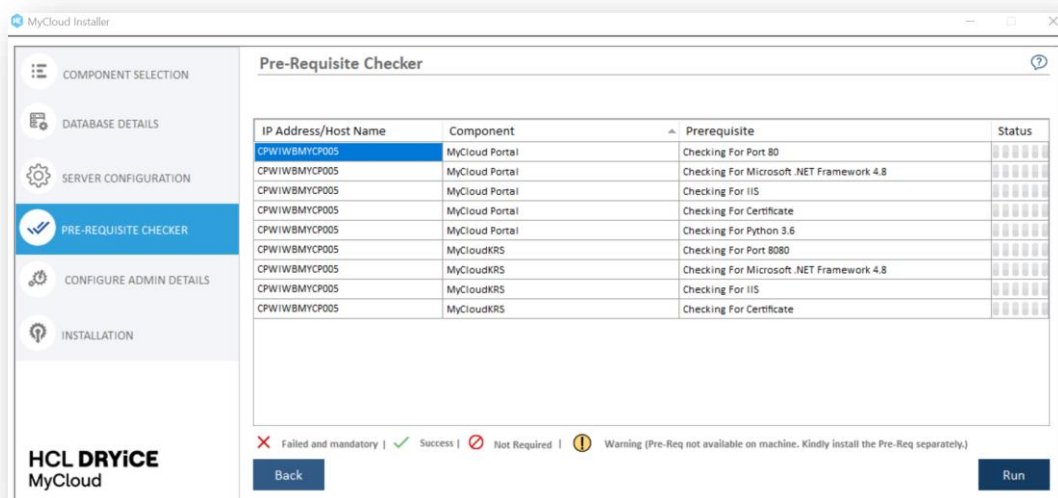


Figure 51 - Prerequisite Checker

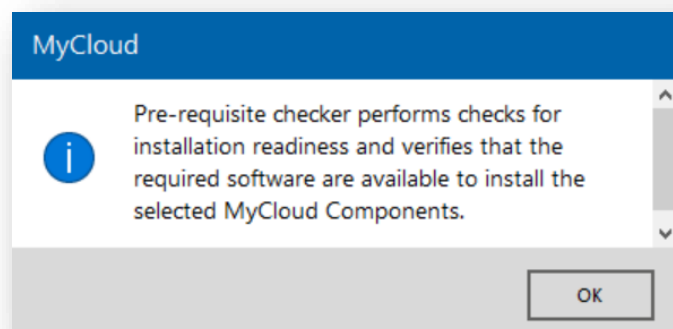


Figure 52 - Prerequisite Checker Information Assistance

The **Prerequisite Checker** identifies the existing host, component, list of relevant pre-requisites and performs the check for installation readiness. If any pre-requisite is missing, it gets listed under the **Status** field as (X). If any pre-requisite is not required, it gets listed under the **Status** field as (no) means **Not Required**. Pre-requisites which show as **Warning** can be ignored.

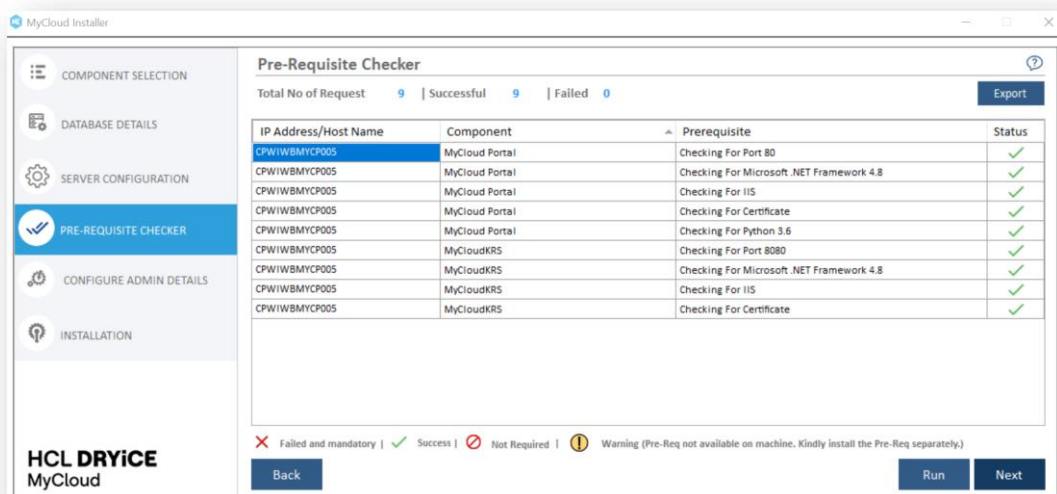


Figure 53 – Prerequisite Checker (Cont.)

2. If all the checks succeed, the **Next** button is enabled, click **Next** to proceed.

If any of the mandatory checks fails, the **Next** button is disabled.

3. On completion of these steps, click **Next** and configure the **admin Details**.

All the fields marked with asterisk (*) are mandatory.

5.3.1.5 Configuring Admin Details

Configure Admin Details Section comes only during the New Installation, and this does not appear during MyCloud UPGRADE.

This section will capture details of an admin user with full access to MyCloud to add admins, manage settings and perform governance actions.

To add the admin details, follow the below steps:

1. On the Configure **Admin Details** screen, enter the **Administrator Name**, **Administrator Email**, **Password**, and **Confirm Password**. These credentials are used to access MyCloud Web portal for configuration.

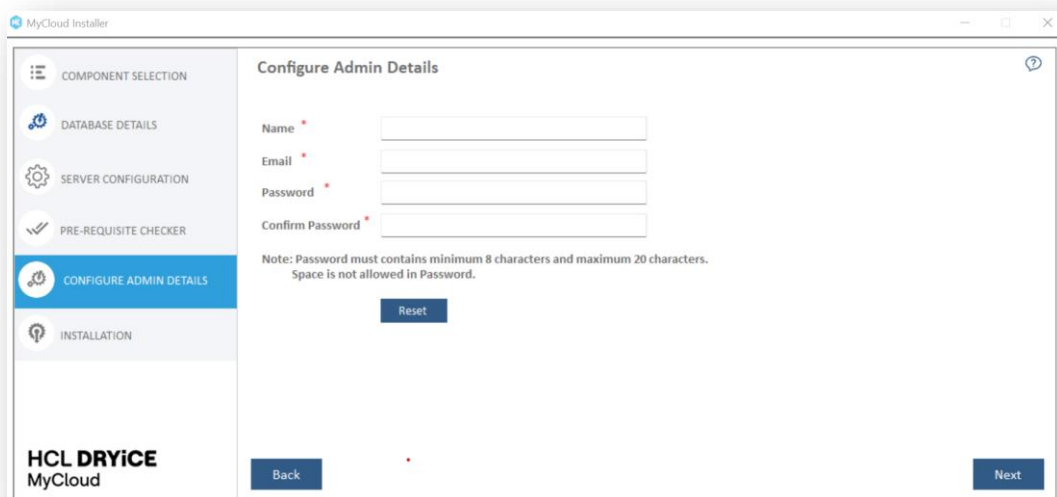


Figure 54 – Configure Admin Details

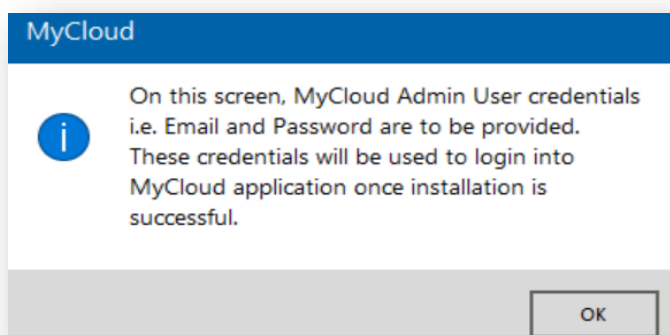


Figure 55- Admin Details Information Assistance

2. Click **Next**.

5.3.1.6 Installation

This section lists down all the configurations as entered (server and component wise). Review the details and verify that the responses provided are correct.

1. Verify the Details which were provided and click on **Run** to start the Web Components installation.

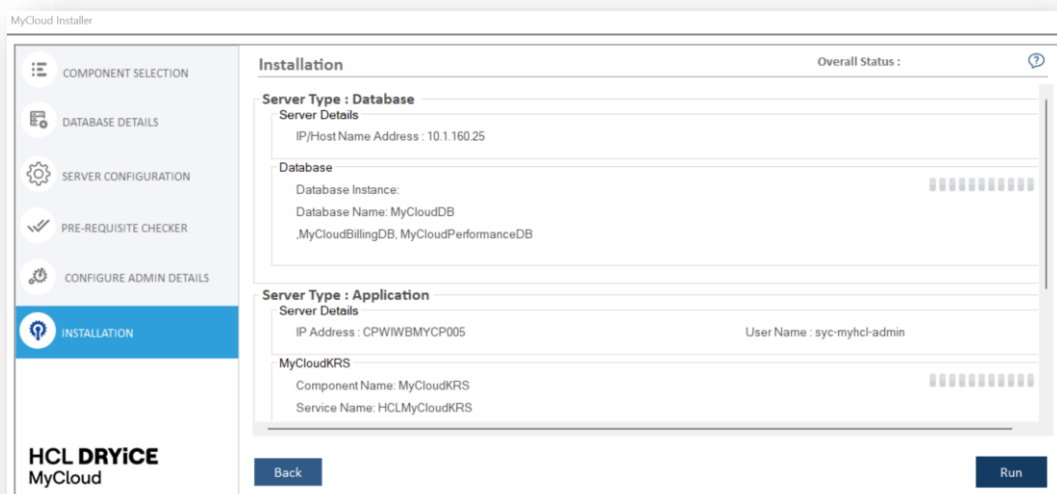


Figure 56 – MyCloud Installation

2. Installation progress can be seen as shown below.

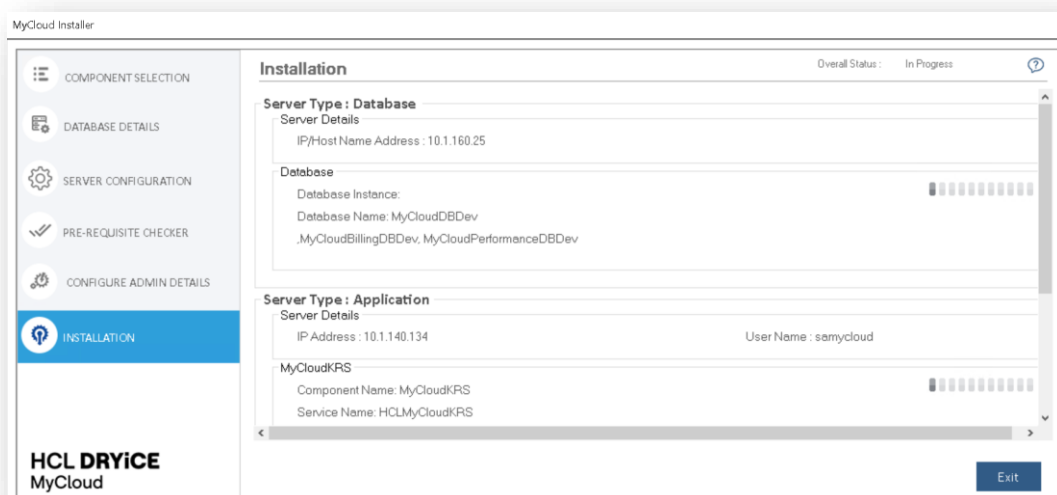


Figure 57 – MyCloud Installation Progress

3. On successful installation of web components, below screen will appear with **Launch Application** Button.

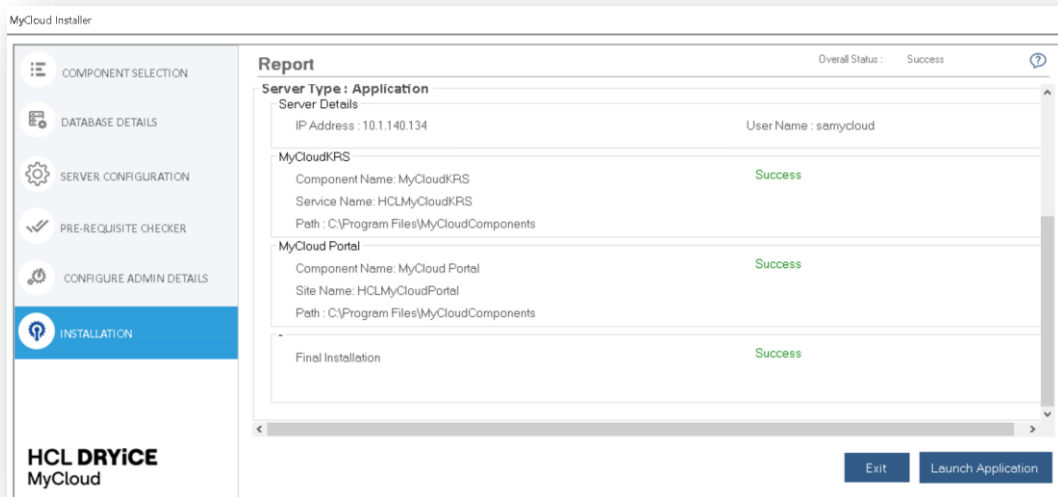


Figure 58 – MyCloud Installer – Success

- Click on **Launch Application** to launch the MyCloud Web portal.

MyCloud takes some time to configure the website, below screen will appear, click on OK.

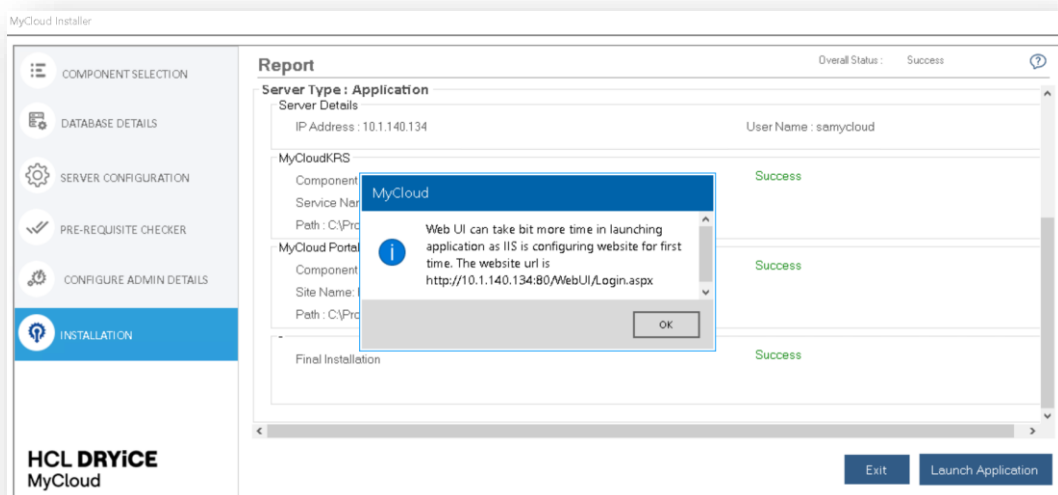


Figure 59 – MyCloud Installer – Launch

- Click **OK**.
- Copy the URL in your notepad for future reference and open the portal in browser.

In case of any failure the error is displayed in Red on the screen and it's advisable to reach out to MyCloud-Product-Supp@hcl.com for further help.

5.3.1.7 Rollback

This section describes the rollback functionality. Rollback is only applicable to installed components in the case of a new installation. Rollback does not delete or remove the database as it is only applicable to installed components.

For a New Installation, if installation fails for any reason, then the Rollback option gets enabled and clicking it removes the installed component.

During the installation of components and DB for the first time, if the DB is created successfully and if any component installation fails, the Rollback button gets enabled.

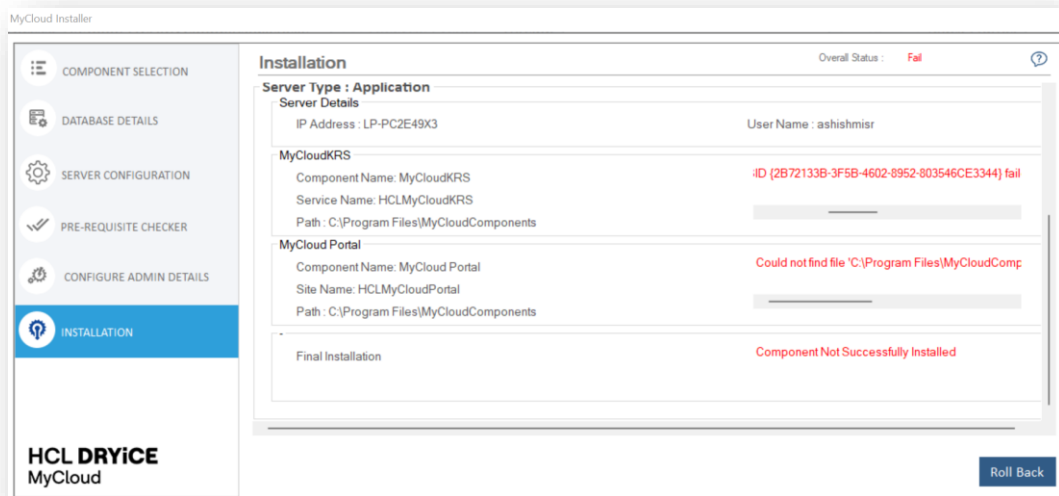


Figure 60 – Rollback

When Rollback action is performed, all selected components get rolled back except DB. So, there is no impact on DB while performing Rollback.

5.3.2 MyCloud App Layer Installation

Run the installer with Administrator permissions.

This section describes how to configure **MyCloud App Layer server**.

5.3.2.1 Components Setup

To setup the App Layer components, follow the below steps:

1. Copy the **MyCloudInstaller** zip (provided by MyCloud Support Team) to **App** server.
2. Unzip the Installer **Zip** file.
3. Go to the unzipped MyCloudInstaller → MyCloudInstaller folder.
4. Right-click on **HCL.MyCloud.EmbeddedInstaller** Application file and Run as **Administrator**

Name	Date modified	Type	Size
HCL.MyCloud.EmbeddedInstaller.exe	8/3/2023 3:21 PM	Application	695,868 KB

Figure 61 – MyCloud Installer

5. Click on **Start** button to start the installation.

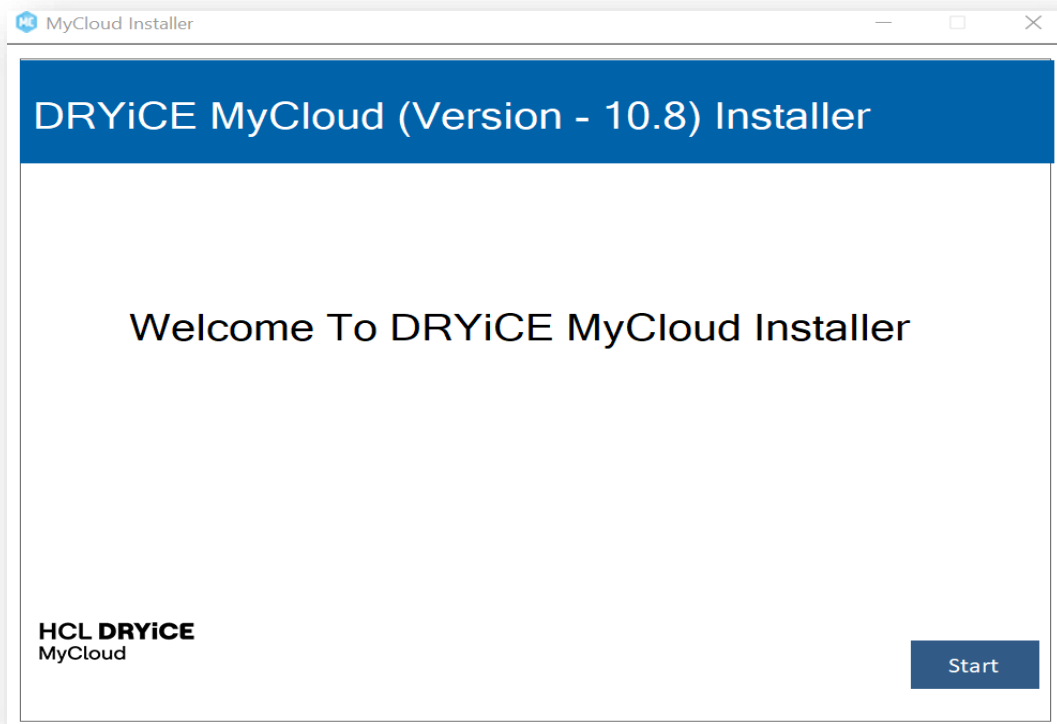


Figure 62 – MyCloud Installer – New Installation

6. In case of fresh/new installation below screen will appear with the **"New installation"** radio checked.

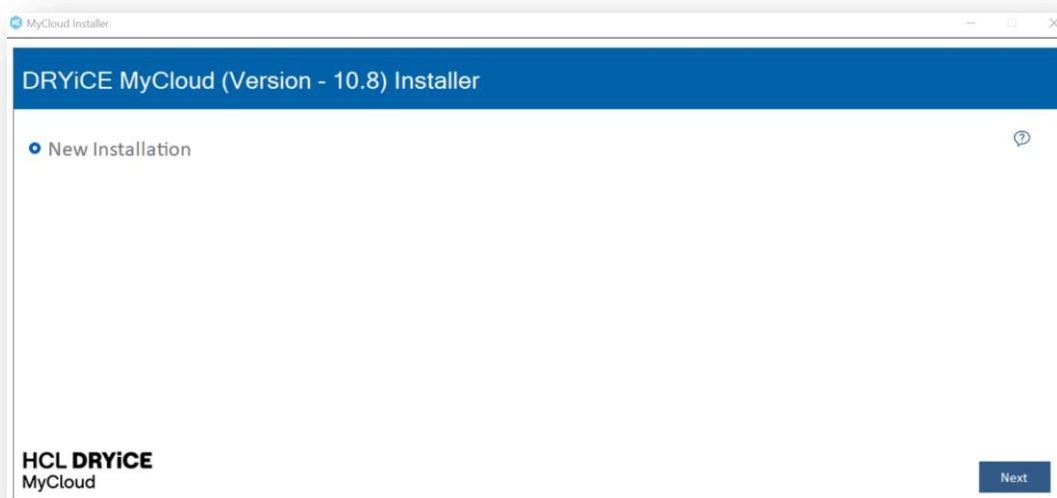


Figure 63 – MyCloud Installer – New Installation

In case of Upgrade, the screen below will appear for upgrade Installation.

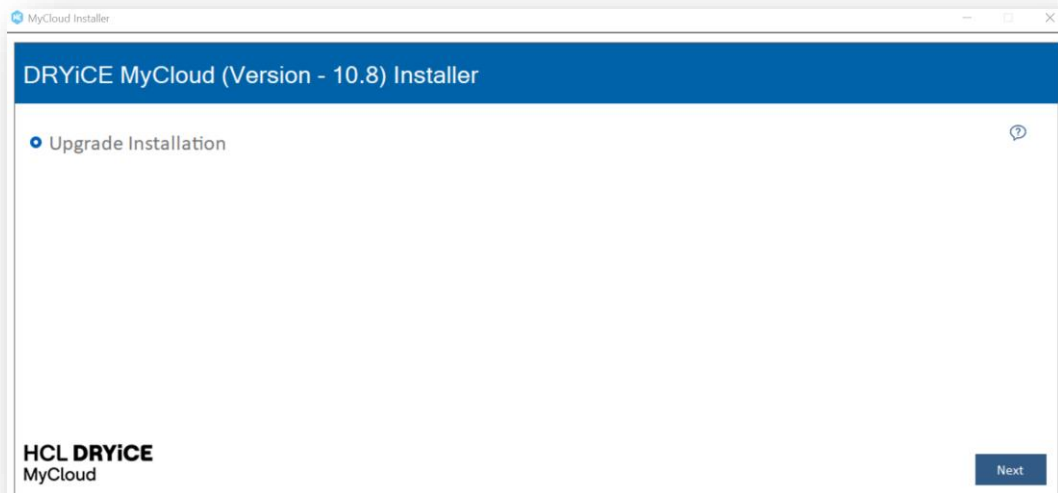


Figure 64 – MyCloud Installer – Upgrade Installation

7. Click **Next**
8. On the left navigation bar, click Component **Selection**.
9. The **Component Selection** pane comes prepopulated with the components.
10. As **MyCloud App layer** is being configured, select the **Service Component**.

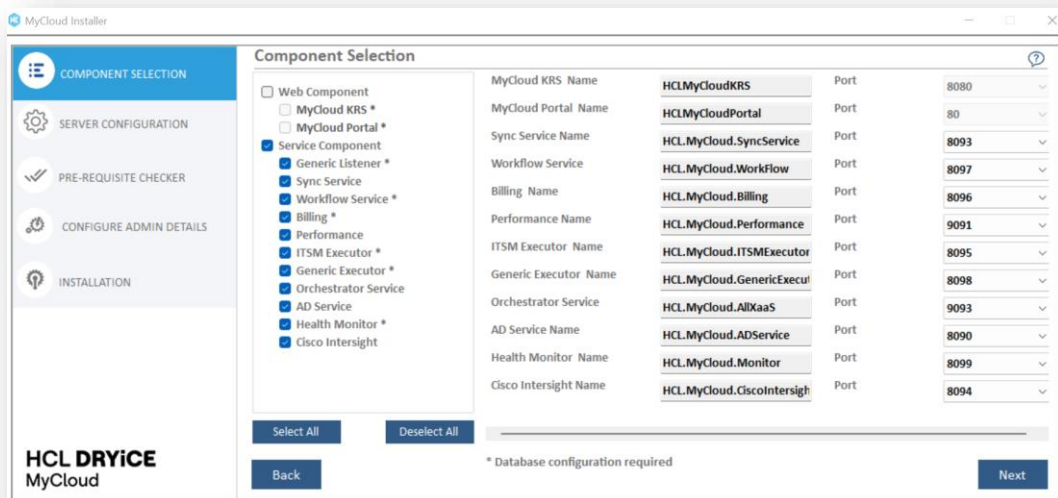


Figure 65 – App Layer - Service Component Setup

In case of **UPGRADE**, **Service Components** are auto selected.

11. Select the **Port** against both selected **Service Component** and leave them as it with default.
12. Click **Next** to go to **Database Setup**.

5.3.2.2 Database Setup

MyCloud Installer uses database screen to capture details which are required to connect to the **Database Server** and create required databases. Following are the steps:

1. After **Service Components** are selected, On clicking **Next**, User is redirected to **Database Details** screen.
2. The **Database Details** pane appears as below:

Figure 66 - Database Details

Refer the below table to understand the fields mentioned in the above figure:

Table 19 – Database Setup

Field Name	Description
Database Details	This panel captures details of the database like server name, authentication type, username, password, that are being used for database creation.
Server HostName/IP	Field to input database server hostname or IP address.
Database Instance Name	Field to input database server instance. This is Optional field.
Authentication	Authentication type to be used to connect to the database server/instance. options are windows authentication or SQL Server authentication .
UserName and Password	<p>These credentials are used to login to the database server to authenticate & establish the connection.</p> <p>These fields cannot be overridden if authentication type is windows authentication.</p> <p>If authentication type is SQL Server Authentication, then username and password are mandatory and need to be provided.</p>
Check Connection	Upon clicking the option, it validates whether connection (between Web layer and Database) has been established successfully or not.

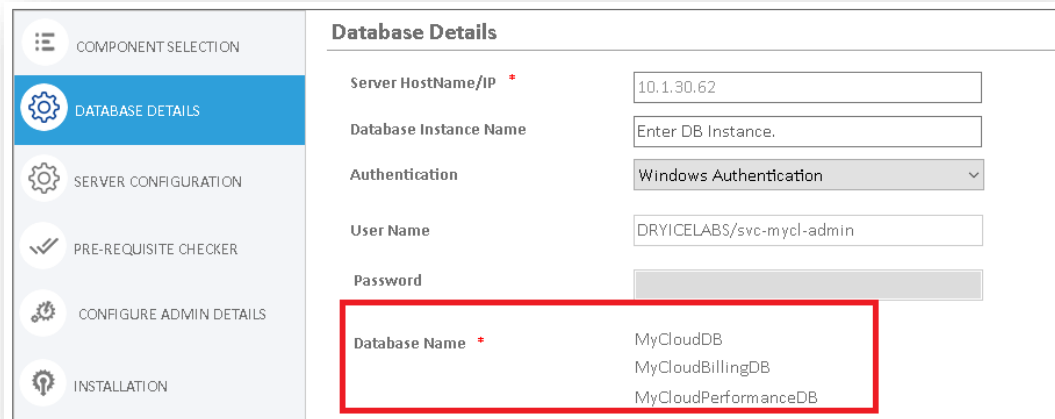
3. Enter the Database Server **Hostname** or **IP Address**.
4. Enter Database Instance Name. (**Optional**)

5. Select **Authentication**. Database configuration is done with the following authentication:

- Windows Authentication
- SQL Server Authentication

If Authentication is "SQL Server Authentication ", Enter the login credentials i.e., the **Username and Password** for getting access to the database server.

6. By default, MyCloud installer will populate the database with the default database names as shown in figure below:



The screenshot shows the 'Database Details' configuration window in the MyCloud installer. On the left is a sidebar with navigation options: COMPONENT SELECTION, DATABASE DETAILS (selected), SERVER CONFIGURATION, PRE-REQUISITE CHECKER, CONFIGURE ADMIN DETAILS, and INSTALLATION. The main area contains the following fields:

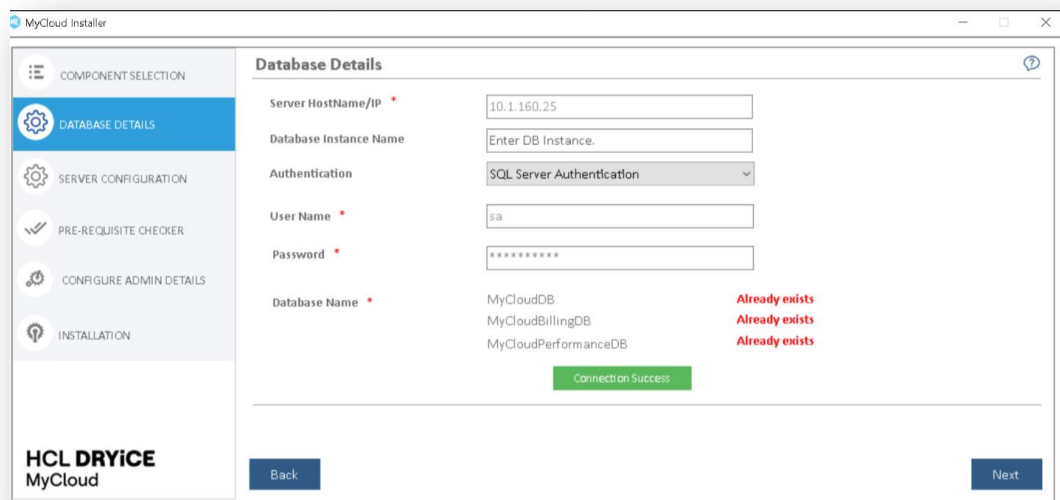
- Server HostName/IP: 10.1.30.62
- Database Instance Name: Enter DB Instance.
- Authentication: Windows Authentication (dropdown)
- User Name: DRYICELABS/svc-mycl-admin
- Password: (empty)
- Database Name: A list containing MyCloudDB, MyCloudBillingDB, and MyCloudPerformanceDB. This section is highlighted with a red rectangular box.

Figure 67 – MyCloud Default Database Names

While doing MyCloud UPGRADE make sure the database name is same as it was provided during installation.

Make sure the database names provided during App layer database setup are same as provided during installation for Web Components (Section 5.3.1.2)

7. Click **Check Connection** to check the connection to the respective server.



This screenshot shows the 'Database Details' window after a connection check. The configuration is as follows:

- Server HostName/IP: 10.1.160.25
- Database Instance Name: Enter DB Instance.
- Authentication: SQL Server Authentication (dropdown)
- User Name: sa
- Password: (masked with asterisks)
- Database Name: MyCloudDB, MyCloudBillingDB, MyCloudPerformanceDB. To the right of each name is the text 'Already exists' in red.

Below the database names is a green button labeled 'Connection Success'. At the bottom of the window, there is a logo for 'HCL DRYICE MyCloud' and two buttons: 'Back' and 'Next'.

Figure 68 – Database Details

All the fields marked with asterisk (*) are mandatory.

During Installation of App Layer on App Server, Since Web layer is already installed on Web Server with the same database names below highlighted in red will appear.

Figure 69 – MyCloud Installer- Database Names

8. Click **Next** to go to Server Configuration page.

5.3.2.3 Server Configuration

In this section, details of MyCloud App Server using the installer is being captured.

1. IP Address/Host Name is auto populated.
2. Enter the Account Type (Domain Administrator or Local Administrator).
3. Provide the Domain
4. Enter the UserName to access the Web server.
5. Enter the Password for the web server.
6. Click on Check User Validity button.

Figure 70 – Server Configuration

7. Select Messaging Queue as MSMQ (if not already selected)

8. Click **Next**.
9. The Prerequisite Checker screen appears.

All the fields marked with asterisk (*) are mandatory.

5.3.2.4 Run Prerequisite Checker

This section describes how to run the prerequisite checker to verify that the installation pre-requisites have been installed.

The **Prerequisite Checker** screen lists the configurations those are mandatory for the components selected on previous screen.

Prerequisite Checker always runs as part of Setup.

1. Click **Run** to start the pre-requisite checker.

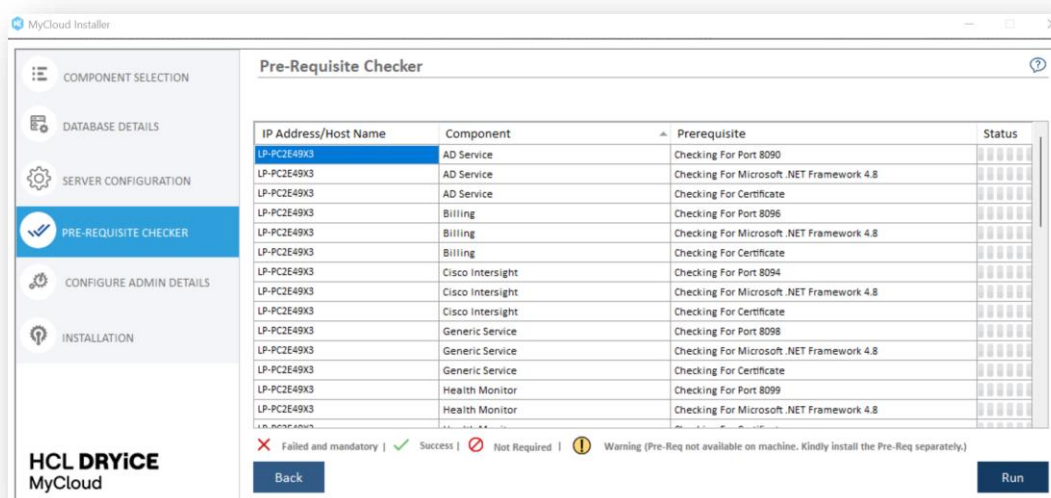


Figure 71 - Prerequisite Checker

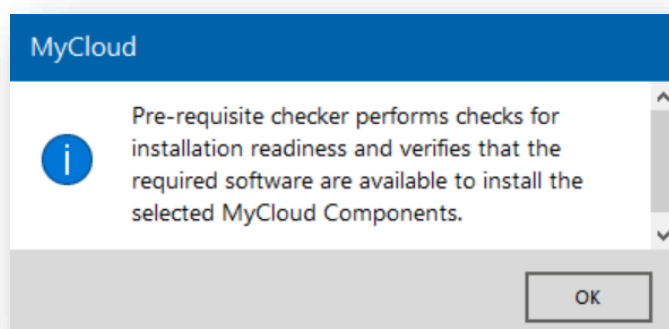


Figure 72 - Prerequisite Checker Information Assistance

The **Prerequisite Checker** identifies the existing host, component, list of relevant pre-requisites and performs the check for installation readiness. If any pre-requisite is missing, it gets listed under the **Status** field as (X). If any pre-requisite is not required, it gets listed under the **Status** field as (⊘) means **Not Required**. Pre-requisites which show as **Warning** can be ignored.

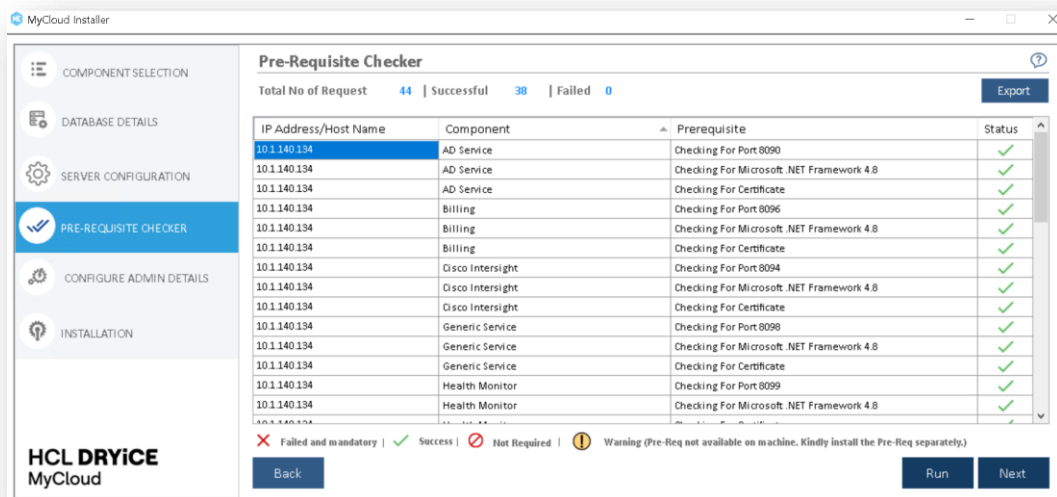


Figure 73 – Prerequisite Checker (Cont.)

2. If all the checks succeed, the **Next** button is enabled, click **Next** to proceed.

If any of the mandatory checks fails, the **Next** button is disabled.

3. On completion of these steps, click **Next**.

5.3.2.5 Installation

This section lists down all the configurations as entered (server and component wise). Review the details and verify that the responses provided are correct.

1. Verify the Details which were provided and click on **Run** to start the App Layer Service Components installation.

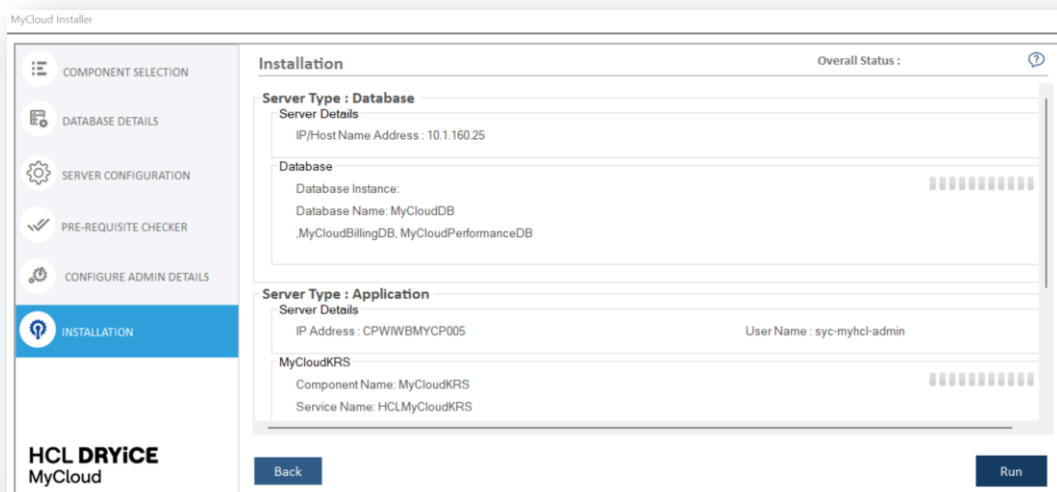


Figure 74 – MyCloud Installation Details

2. Installation progress can be seen as shown below.

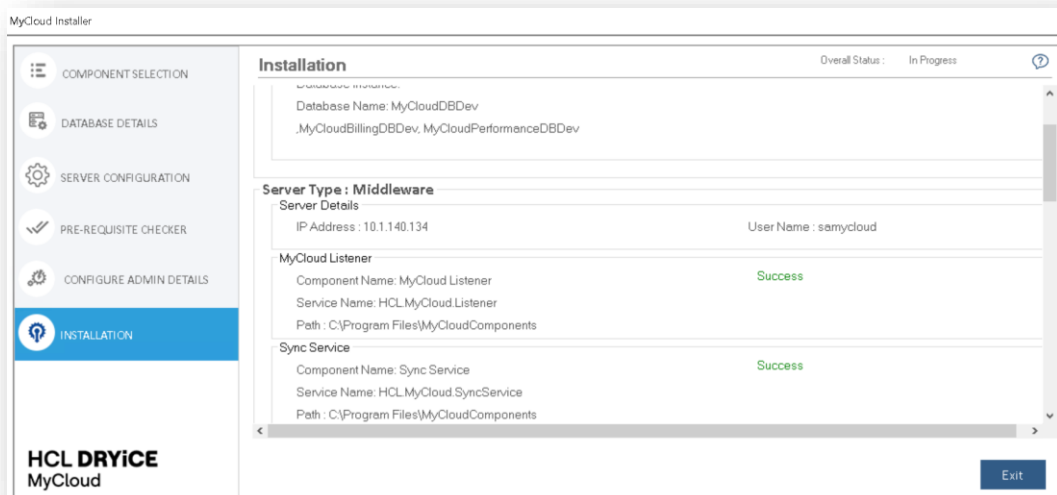


Figure 75 – MyCloud Installer- Progress

- On successful installation of web components, below screen will appear.

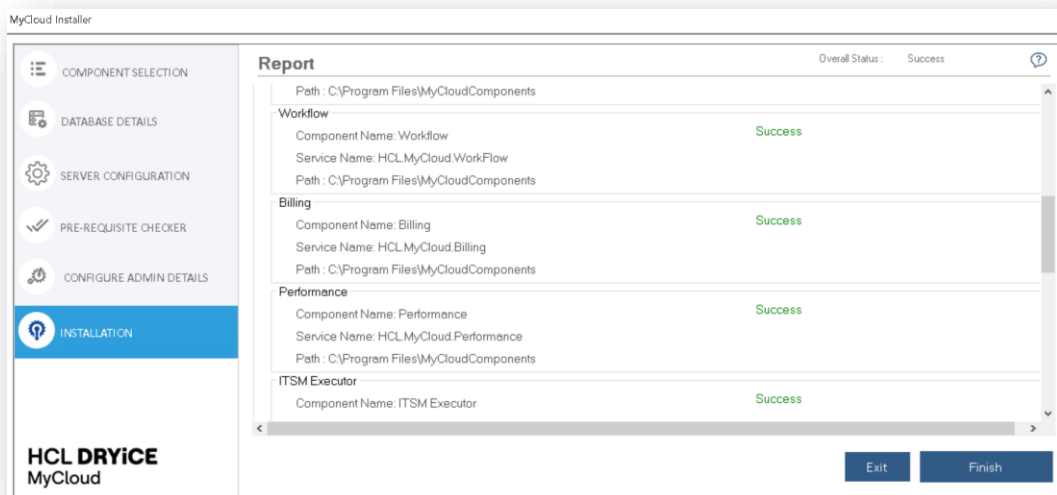


Figure 76 – MyCloud Installer – Success

- Click **Finish** and below popup message will display with “**Setup Completed**”. Click **OK**

Also, in case of Upgrade/Fresh Installation, KMS URL will be updated in config file. First this URL will be fetched from DB and will be updated. If does not exist, the default URL will be updated.

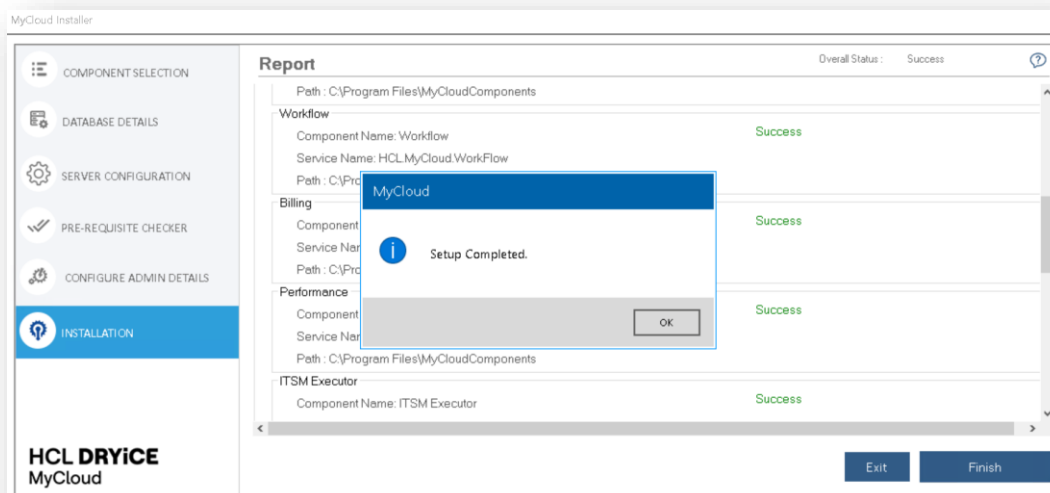


Figure 77 – MyCloud Installer – Setup Complete

If the Installation fails, go to Rollback.

5.3.2.6 Rollback

This section describes the rollback functionality. Rollback is only applicable to installed components in the case of a new installation. Rollback does not delete or remove the database as it is only applicable to installed components.

For a New Installation, if installation fails for any reason, then the Rollback option gets enabled and clicking it removes the installed component.

During the installation of components and DB for the first time, if the DB is created successfully and if any component installation fails, the Rollback button gets enabled.

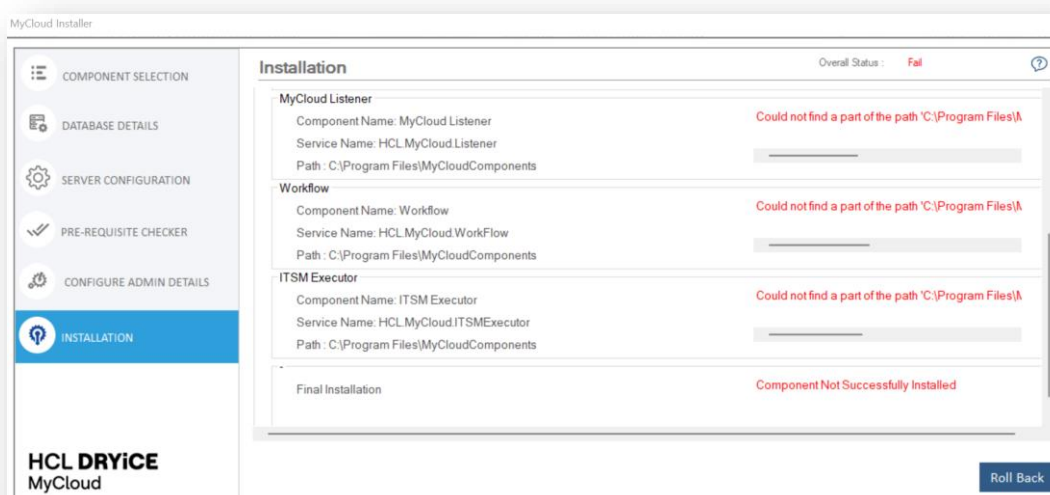


Figure 78 – Rollback

When Rollback action is performed, all selected components get rolled back except DB. So, there is no impact on DB while performing Rollback.

6 MyCloud Post Installation Task

Once MyCloud is installed and configured as per default settings, the admin user can change the product configurations to add another layer of security. It can be done by making the following configuration changes:

6.1 Provide MyCloud License

1. Launch MyCloud Web by providing MyCloud Web URL in supported browser.
2. Enter MyCloud Admin email id.

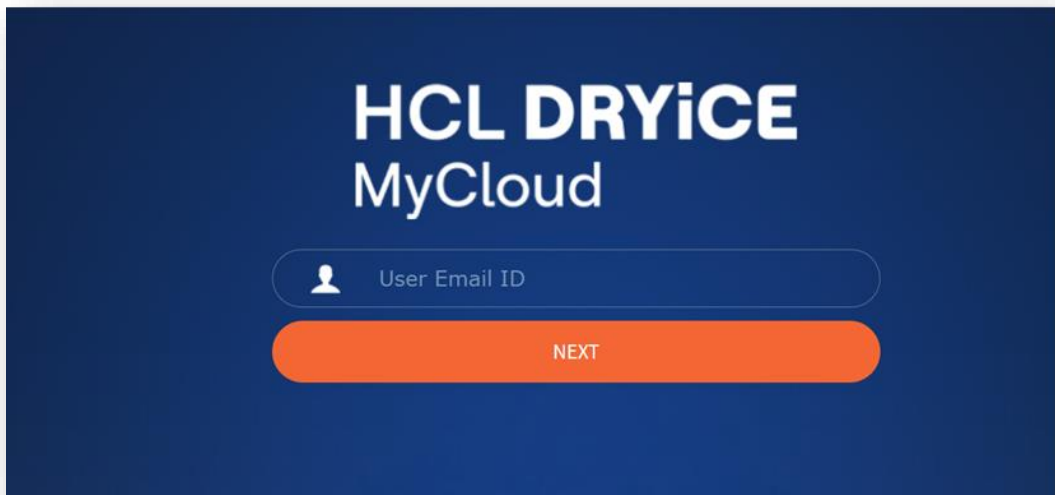


Figure 79 – MyCloud Login

3. Click **Next**
4. Message will appear mentioning license key is expired or not available.

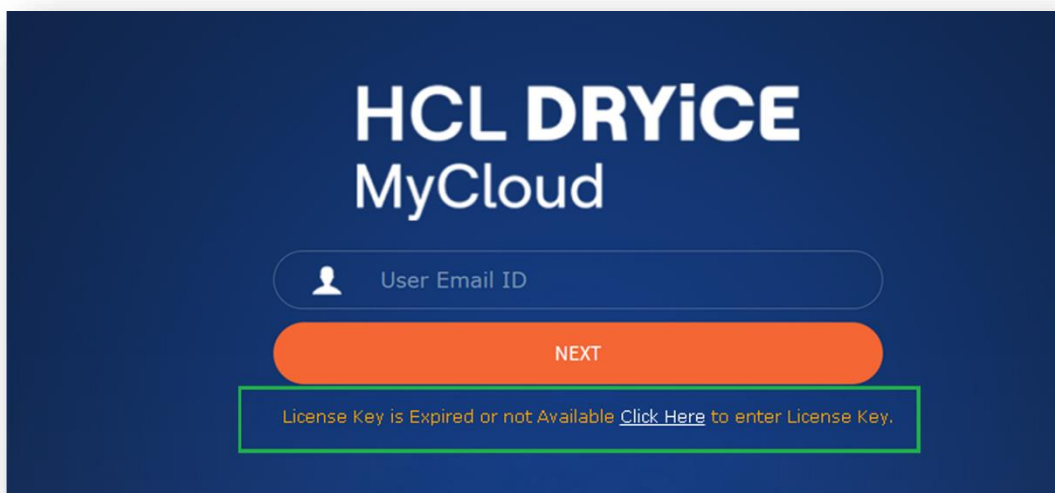
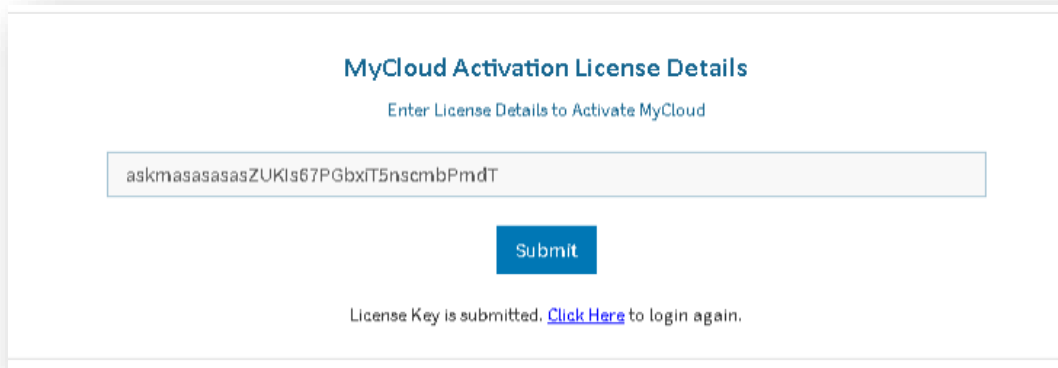


Figure 80 – MyCloud -Enter License Key

5. Click on **Click Here** to enter the license Key.
6. Enter the License Key and click **Submit** button.



MyCloud Activation License Details

Enter License Details to Activate MyCloud

askmasasasasZUKIs67PGbxIT5nscmbPmdT

License Key is submitted. [Click Here](#) to login again.

Figure 81 – MyCloud -Enter License Key

Contact to administrator to get license key.

7. Click on “**Click Here**” to login again.
8. Provide the MyCloud Admin email id and Password and check if login is successful.

6.1.1 Master Data changes

1. Login into MyCloud Portal with http protocol URL.
<<http://{webserverhostname}/WebUI/Login.aspx>>.
2. Change webserver hostname in the URL with actual webserver hostname.
3. After the login, user is redirected to the landing page. Navigate to **Master→ Manage Base Components Keys** as shown in [Figure 82 – Admin Home Page](#).

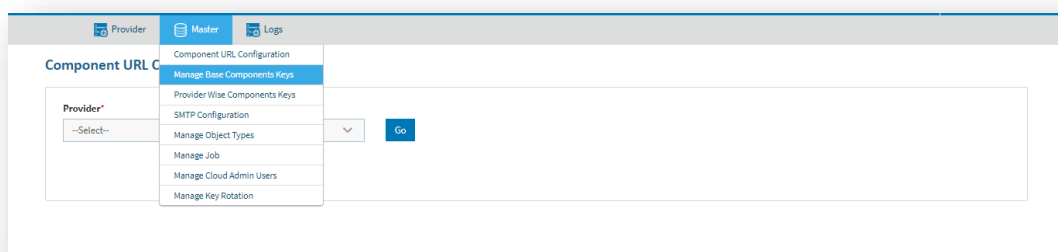


Figure 82 – Admin Home Page

4. User will be redirected to the **Manage Base Component** page, as shown in [Figure 83 – Manage Base Components](#).
5. Select **Website Service (WEBSITE)** in the Component Name dropdown and click on **Go** button.
6. Change the Key value for the following Key Name(s):
 - *JsURL* from <http://XX.X.XXX.XX:443/WebUI/JS> to <https://XX.X.XXX.XX/WebUI/JS>
 - *SiteURL* from <http://XX.X.XXX.XX:443/WebUI> to <https://XX.X.XXX.XX/WebUI>

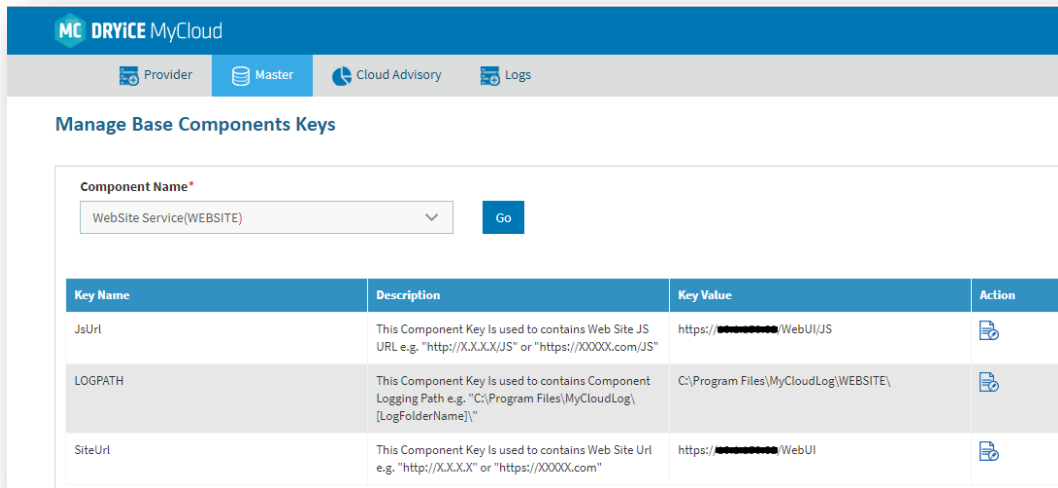


Figure 83 – Manage Base Components

7. Navigate to **Master** → **Component URL Configuration**.

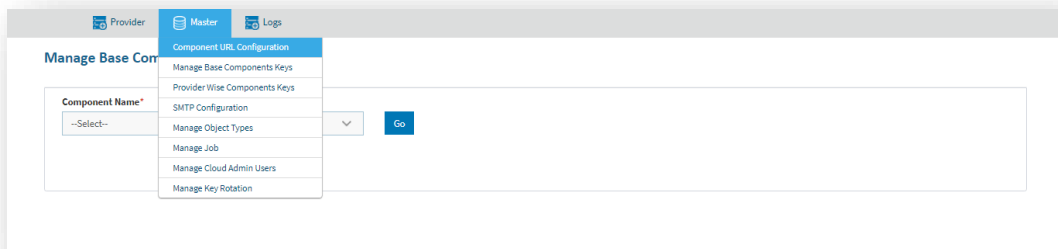


Figure 84 – Landing Page with selected Component URL Configuration

8. Select **Base** in the **Provider** dropdown and click on **Go** button.
9. Change the URL for the following Component Name(s):
 - Web API from http://XX.X.XXX.XX:443/WebAPI to https://XX.X.XXX.XX/WebAPI
 - Key Management Services (Rotation Key) from http://XX.X.XXX.XX:80/KMS to https://XX.X.XXX.XX:8443/KMS.
10. To test Middleware Components, click **Test URL**.

If Test URL for Web API gets failed, Copy the WebAPI URL and open in browser and click Advanced and proceed. After this test the WebAPI URL again for success.

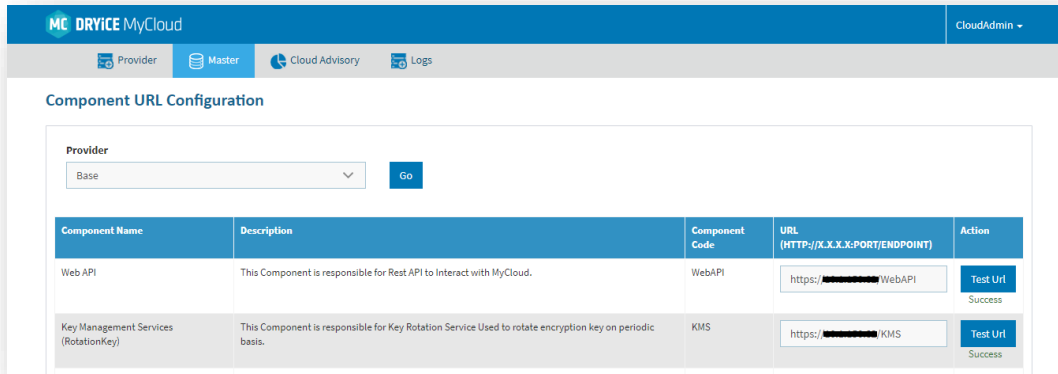


Figure 85 – Component URL Configuration

11. Restart the IIS. Steps are as follows:
12. Open Command Prompt by clicking on Start on windows task bar → Type cmd → right-click on the Command Prompt → select **Run as administrator**.

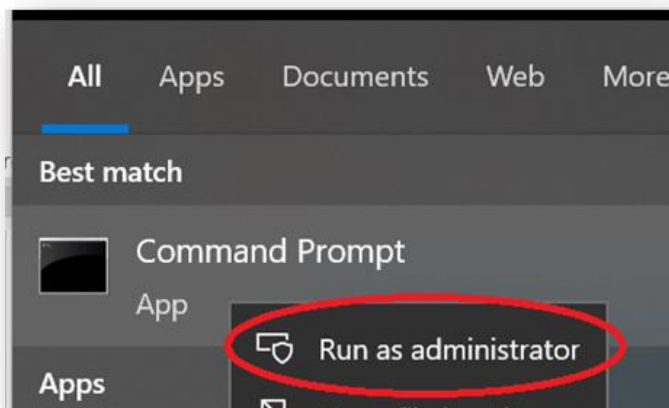


Figure 86 – Command Prompt as Administrator

13. Run Command: **"IISRESET"**
14. Now Close the browser and open the webapplication with HTTPS URL.

6.1.1.1 Stop All Services

1. Stop all the Services and find services file location. This step must be performed on the server where the middleware components/App Layer are installed.
2. Press **Window + R** keys to open run window, then type **services.msc** and click **OK**.

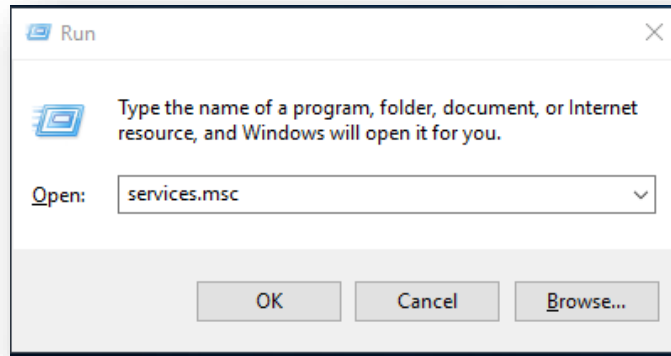


Figure 87 – Run Command Window

3. User will be redirected to the **Windows Service Manager**.

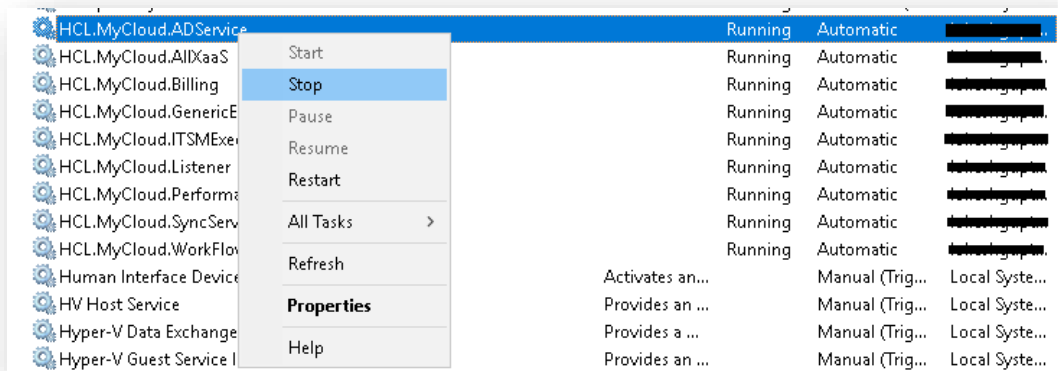


Figure 88 – Windows Services Manager

4. Stop the below mentioned services. Each of these services is responsible for a component in MyCloud. Select the service, then right-click and select **Stop**.
 - HCL.MyCloud.ADServices
 - HCL.MyCloud.AllXaaS
 - HCL.MyCloud.Billing
 - HCL.MyCloud.GenericExecutor
 - HCL.MyCloud.ITSMExecutor
 - HCL.MyCloud.Listener
 - HCL.MyCloud.Performance
 - HCL.MyCloud.SyncService
 - HCL.MyCloud.WorkFlow
 - HCL.MyCloud.Monitor
 - HCL.MyCloud.CiscoIntersightSyncService

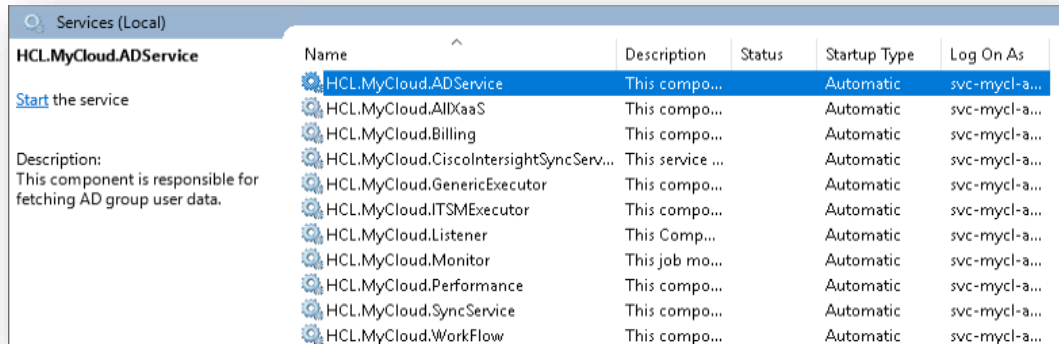


Figure 89 – Windows Services Manager

- After stopping all the services, the next step is to find out the Middleware Components file location.

6.1.1.2 Path To Executable Services

Once the user has stopped all the services mentioned above, next step is to find the **PathToExecutable** of the deployed service(s).

- Open Services.msc from run.
- Select the service (HCL.MyCloud.ADSERVICE), right-click and select Properties.
- This will open the properties window for that service as shown in [Figure 90](#).
- Locate the "**Path to Executable**" section in this window.
- Copy the path and save it in a notepad or a document for future reference.
- Similarly, copy and save the path to executable for all the services mentioned above in section 6.2.2.1.

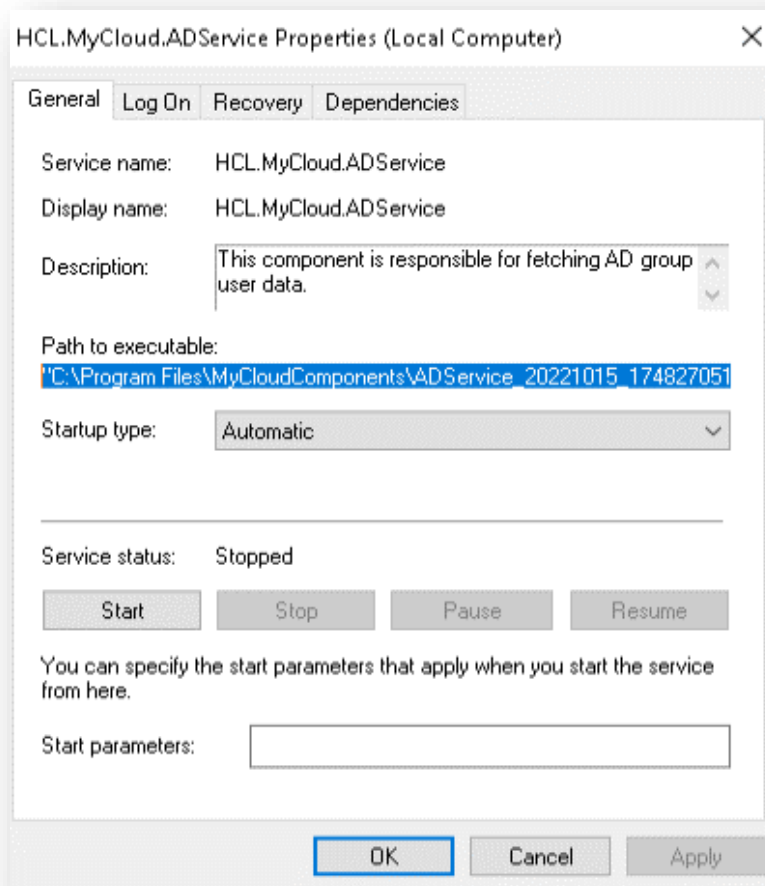


Figure 90 – Windows Services Manager

6.1.1.3 Find Port Number

1. Find the Port Number on which services are running.
2. Go to PathToExecutable.
3. For example:
"C:\ProgramFiles\MyCloudComponents\ADSservice_XXXXXXXX_XXXXXXXX"
4. Open the respective service config file (exe.config):

Files names for reference is given below:

- HCL.MyCloud.Service.AD.exe.config
- HCL.CloudBilling.DataCollector.Service.Host.exe.config
- HCL.MyCloud.CiscoIntersightSyncService.Host.exe.config
- HCL.MyCloud.Generic.Host.exe.config
- HCL.MyCloud.Monitor.Host.exe
- HCL.MyCloud.Snow.Host.exe
- HCL.MyCloud.AllXaaS.Host.exe
- HCL.CloudPerformance.DataCollector.Service.Host.exe
- HCL.MyCloud.SyncJobService.Host.exe
- HCL.MyCloud.WorkflowEngine.exe

5. Now find the **ServiceHostURL** key

```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 91 – Service Host URL in Configuration File

6. Copy the **Port** as shown in the above figure and save it in a notepad or a document for future reference.
7. In a similar way, copy and save the ports for all the services.

6.1.1.4 Certificate changes

During installation (New/Upgrde), all certificates will be installed automatically.

Make sure MyCloud Certificate is present in the **personal** folder of **Window Certificate** console and if not present then copy the certificate.

1. Press **Window + R** keys to open the run command window.
2. Now type "**mmc**" and click **OK**.
3. The Certificate Console will open.

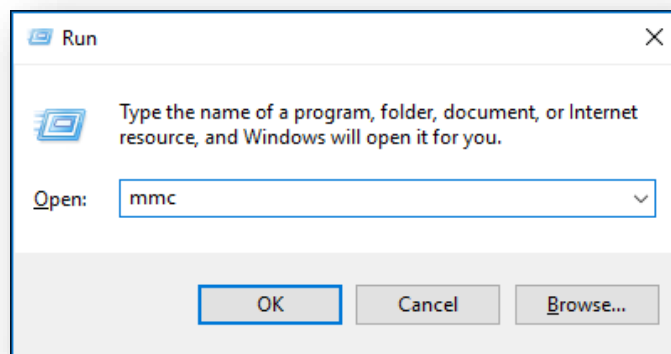


Figure 92 – Run Command Windows

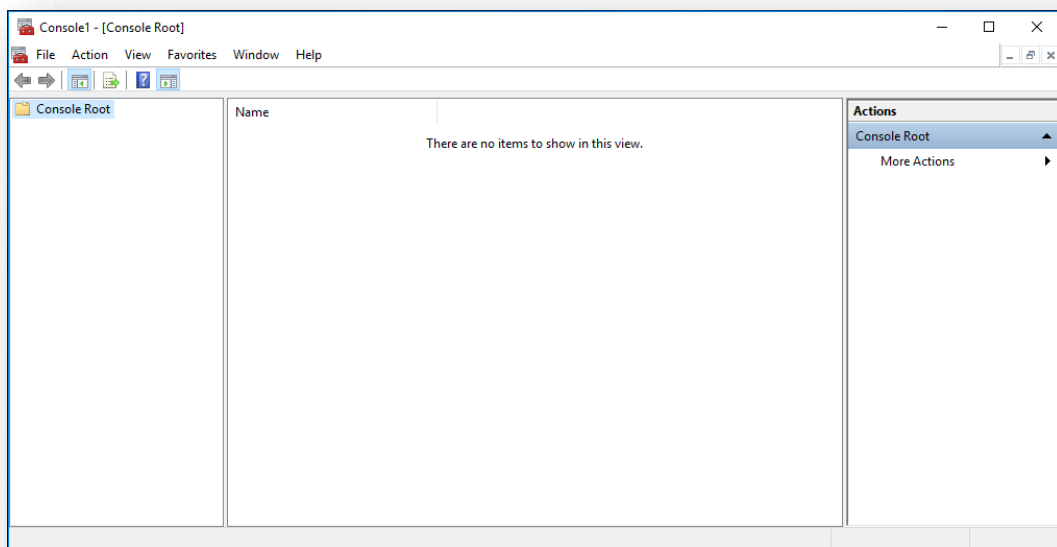


Figure 93 – Windows Certificate Console

4. On the console window, in the top menu, click **File** → **Add/Remove Snap-in**

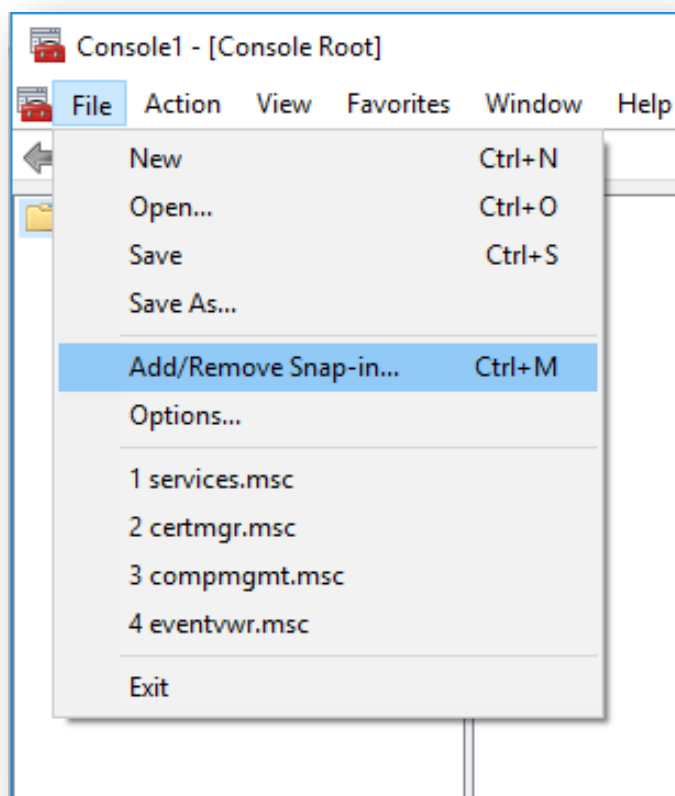


Figure 94 – Windows Certificate Console with File Menu

5. In the **Add or Remove Snap-ins** window, in the **Available snap-ins** pane (left side), select **Certificates**, then click on **Add** button.

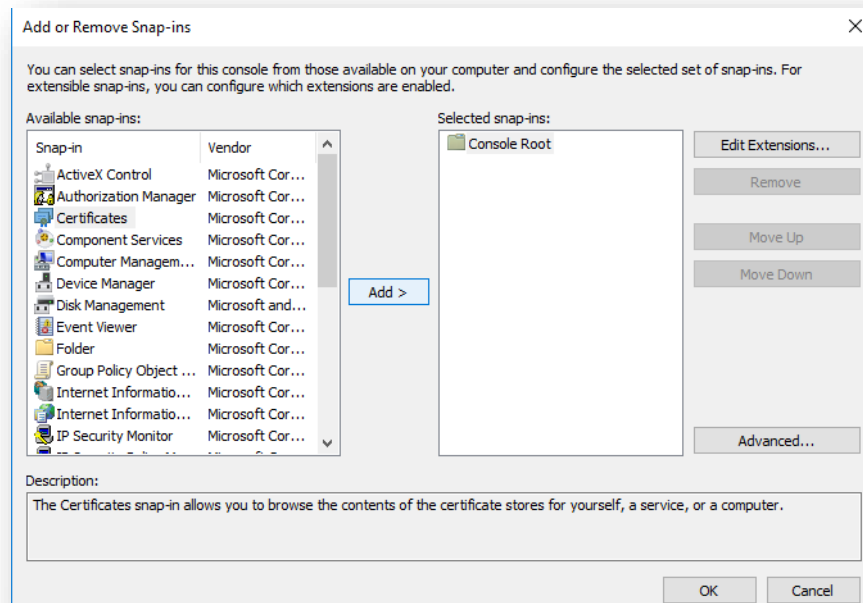


Figure 95 – Add or Remove screen in Certificate Console

6. In the Certificate snap-in window, select Computer account and then click Next.

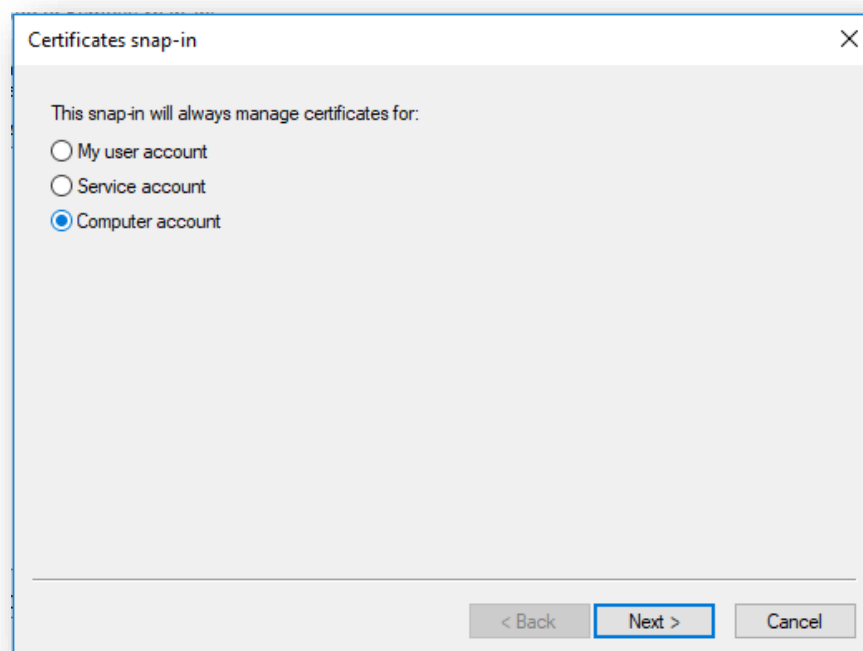


Figure 96 – Certificate snap-in Window

7. In the **Select Computer** window, select **Local computer** and then click **Finish**.

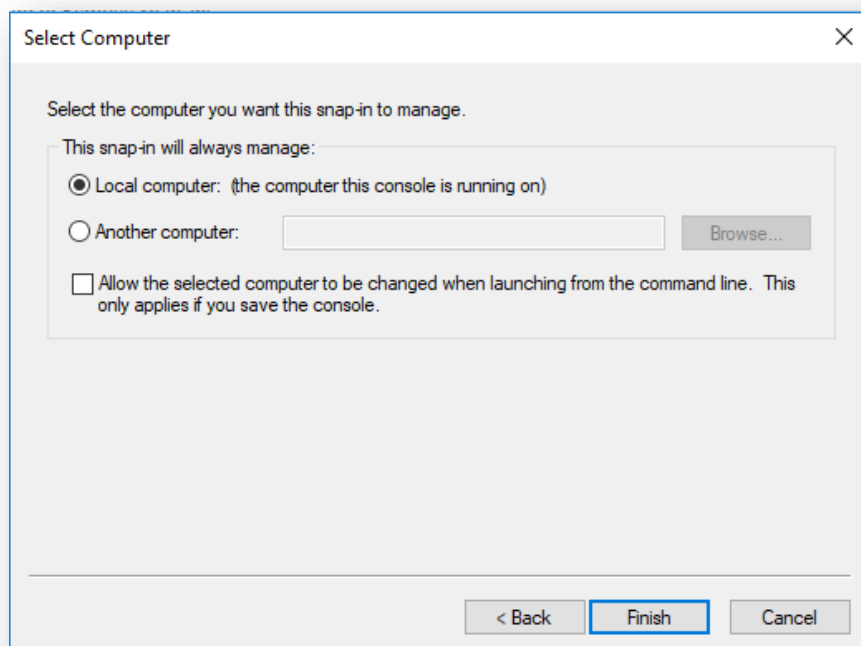


Figure 97 – Select Computer

8. In the **Add or Remove Snap-ins** window, click **OK** as shown in below figure.

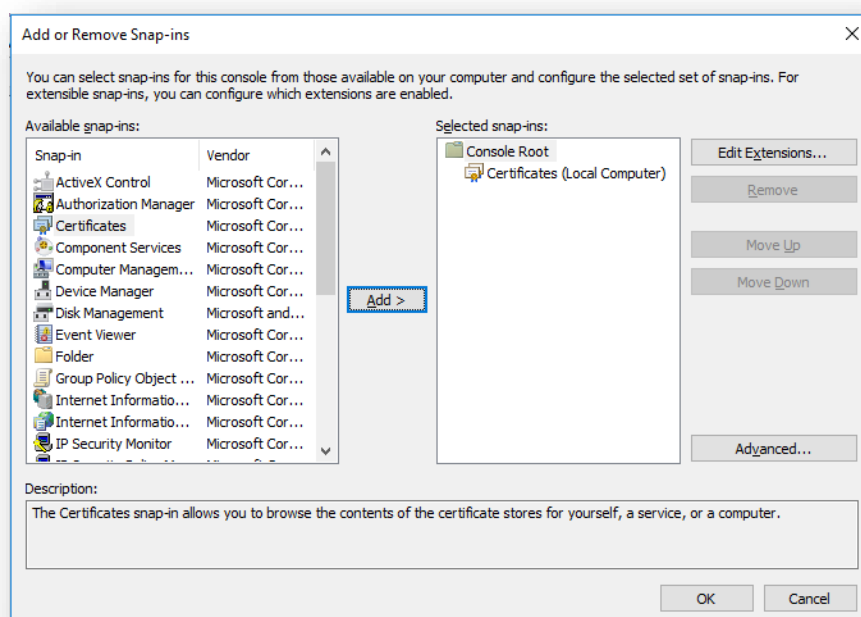


Figure 98 – Add or Remove Snap-ins Window

9. Navigate to the certificate console window, as mentioned in step 3. In the **Console Root** pane expand **Certificates (Local Computer)**, **Personal** folder and then select the **Certificate** folder. Check if it contains "**HclTech.MyCloud.App**" certificate as shown below:

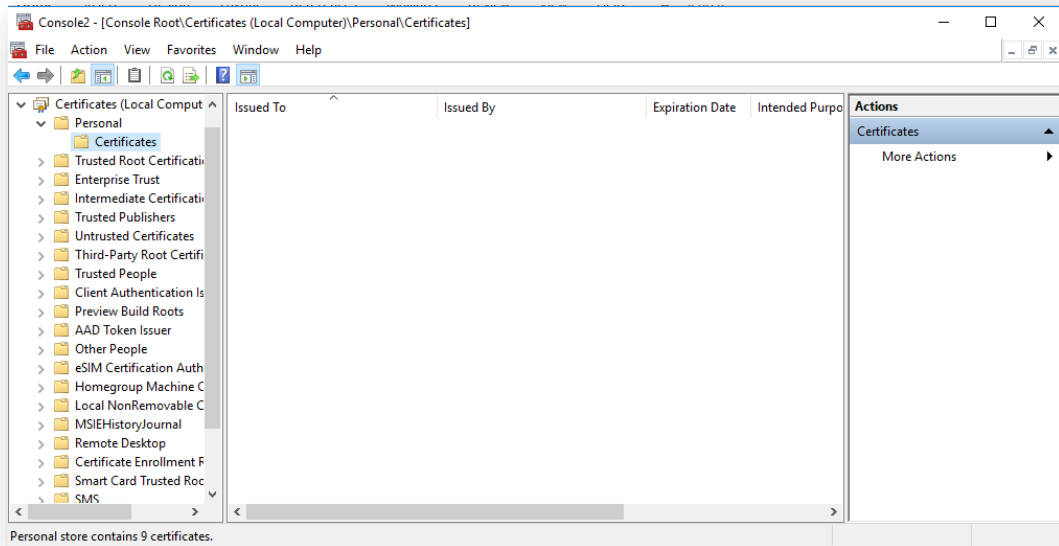


Figure 99 – Personal Certificate Console

10. If the Certificate is not present, follow the below steps.
 - a. In the Console window, under the Console Root pane (left side), expand Certificates (Local Computer), expand the Trusted People folder, click **Certificates** and then right-click "**HclTech.MyCloud.App**" certificate and select Copy as shown in below figure.

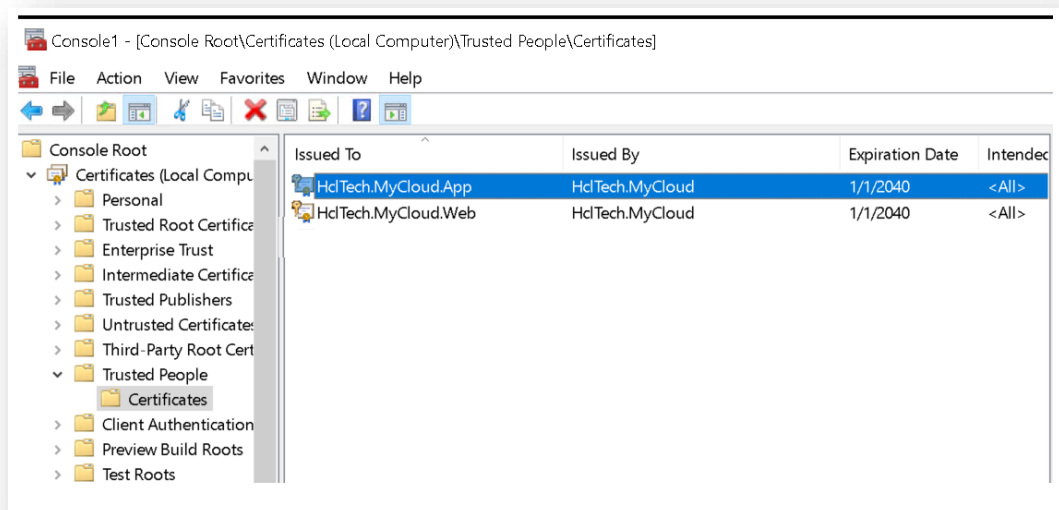


Figure 100 – Certificate Console with selected Certificate

- b. Now right-click on **Personal folder** in the left Console Root window, then click on **Paste** as shown below.

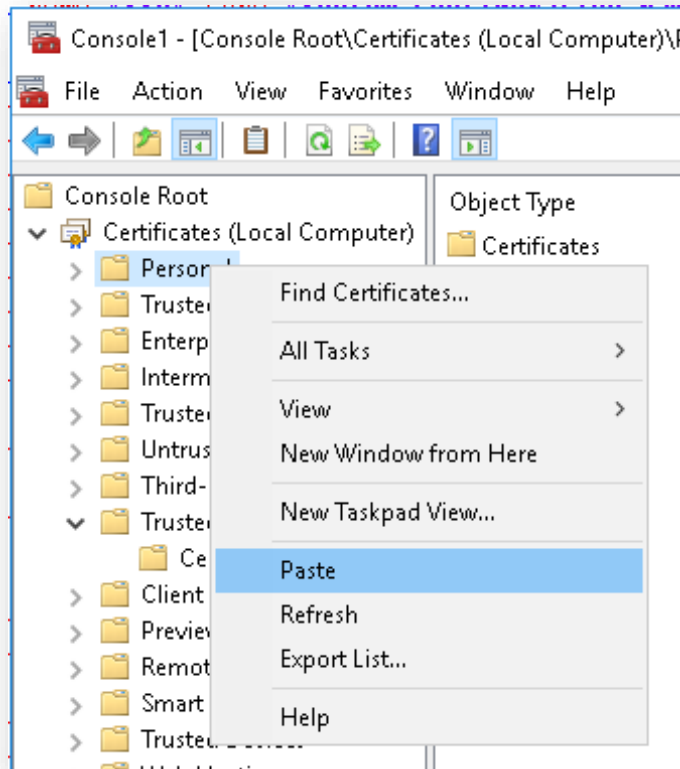


Figure 101 – Copy Certificate

- c. Now expand **Personal** folder and click on **Certificate** folder, now it will show the recently pasted certificate in the main window.

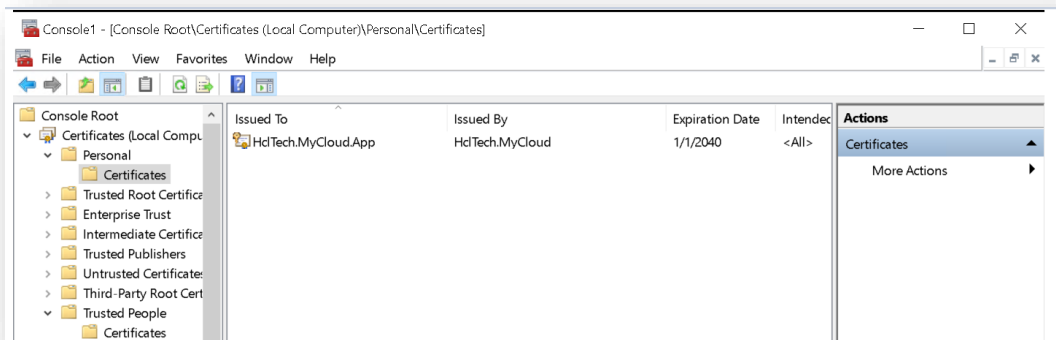


Figure 102 – Showing recently added Certificate

- d. Double click on the recently pasted certificate. Certificate Properties window will open.
- e. Click on the **Details** tab and scroll down to field **Thumbprint**.
- f. Copy the thumbprint value. The value is used as "certhash" in below commands.

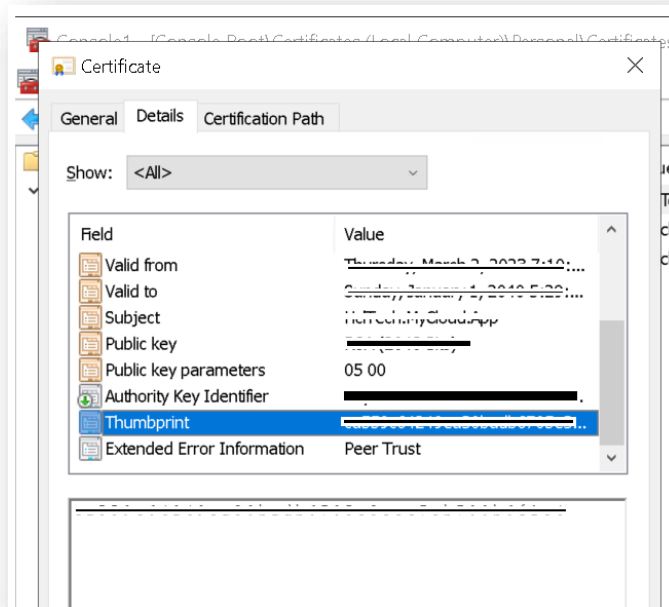


Figure 103 – Showing Recently Added Certificate

6.1.1.4.1 Master Data changes

1. Login the website with **MyCloud Admin account**.
2. Go to **Master** and then click **Component URL Configuration**.

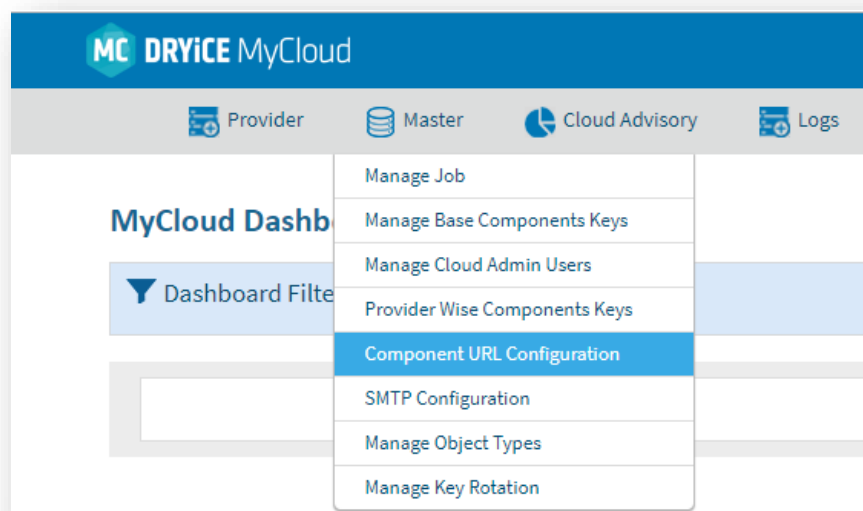


Figure 104 – Admin Landing Page

3. Select **Base** in the **Provider** drop down and click on **Go** button.
4. Change the URL for the following Component Name(s) as shown in [Figure 105 – Component URL Configuration](#).
 - Workflow Service
 - from `http://<ip>:<port>/WorkflowService` to `https://<ip>:<port>/WorkflowService`
 - Data Collector Billing and Advisory

- from http://<ip>:<port>/DataCollector to https://<ip>:<port>/DataCollector
 - ServiceNow Executer
 - from http://<ip>:<port>/SnowService to https://<ip>:<port>/SnowService
 - Generic Service
 - from http://<ip>:<port>/GenericService to **Error! Hyperlink reference not valid.**
 - Application Health Monitoring
 - from http://<ip>:<port>/ MonitorService to https://<ip>:<port>/ MonitorService
5. Click on **Test URL** against each service and check for success.
 6. Click **Update**.

Kindly update the Provider level Components URLs after creating new Provider(s).

Follow Below steps only if you have created provider, if not created, ignore the below steps as of now. However. After creating Provider, MyCloud admin must configure the below configuration.

1. Select **Provider** in the Provider drop down and click on **Go** button.
2. Change the **URL** for the following Component Name(s):
 - Platform Data Sync
 - from http://<ip>:<port>/SyncService to https://<ip>:<port>/SyncService
 - Performance Data Sync
 - from http://<ip>:<port>/PerformanceDataCollector to https://<ip>:<port>/PerformanceDataCollector
 - Orchestrator Services
 - from http://<ip>:<port>/OrchestratorService to https://<ip>:<port>/OrchestratorService
 - Active Directory
 - from http://<ip>:<port>/ADService to https://<ip>:<port>/ADService.
 - Cisco Intersight Sync
 - From http://<ip>:<port>/CiscoSyncService to https://<Hostname/IP>:<port>/CiscoSyncService.

Kindly update the Provider level Components URLs after creating new Provider(s).

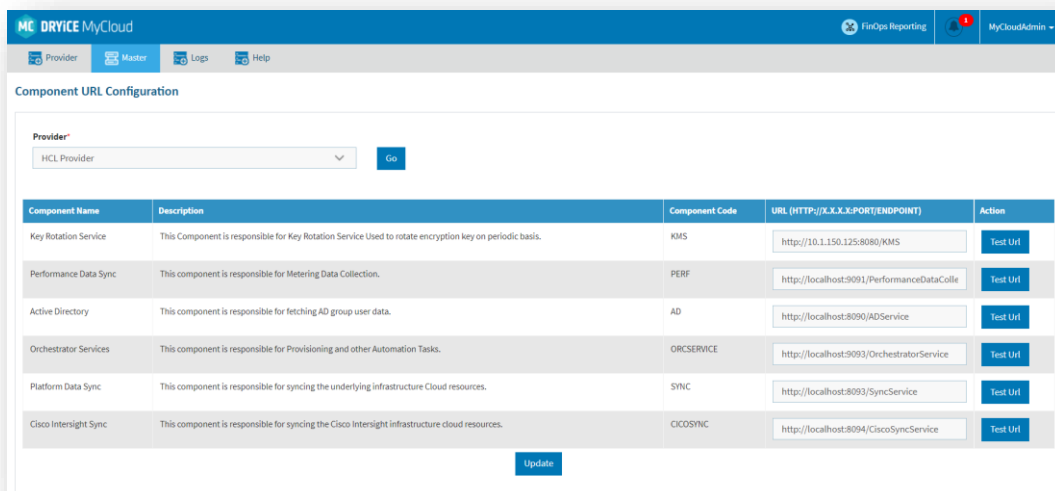


Figure 105 – Component URL Configuration

6.2 Change Certificate to CA Signed (Optional)

This section describes the steps to use Certificate provided by the customer instead of MyCloud Default certificate. The same certificate can be used for HTTP(S) communication between components.

1. MyCloud application has server wise certificates. Below are the details of default certificates installed by MyCloud Installer:
 - **Web Server Certificates**
 - HclTech.Mycloud.Web – Private (.pfx)
 - HclTech.MyCloud.App – Public (.cer)
 - **App Server Certificates**
 - HclTech.Mycloud.Web – Public (.cer)
 - HclTech.MyCloud.App – Private (.pfx)
2. Next step is to find Website, Web API and Key Rotation Service, ApplicationBasePath.
3. Follow the steps mentioned below to do that:
 - a. Press **Window + R** keys to open run command window.
 - b. Now type "inetmgr" and click OK.
 - c. The IIS Console will open.

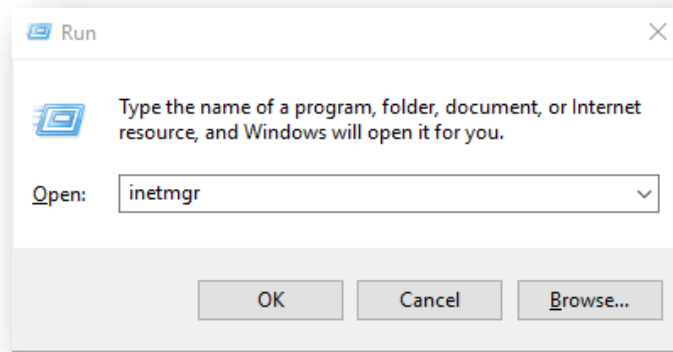


Figure 106 – Run window command

- d. Now expand the Server Name node → Sites node using the connections section and right-click on the HCLMyCloudPortal node and click on Explore.
- e. This will locate the ApplicationBasePath for Website, WebAPI and Key Rotation Service as highlighted in Figure 107 – Application Base Path Locator.

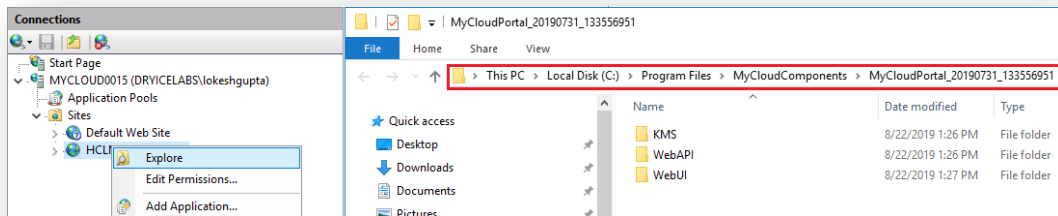


Figure 107 – Application Base Path Locator

4. Copy the base path and save for future reference.
5. The next step is to find the path of the Middleware component configuration files. The steps are mentioned below:
 - a. Find the PathToExecutable of the service(s).
 - b. Press **Window + R** keys to open **RUN** window.
 - c. Type services.msc and click **Ok**.

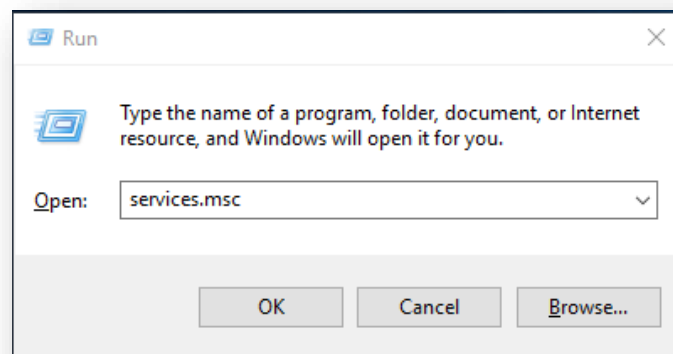


Figure 108 – Run Command Window

- d. For the below mentioned services: (Select the service, then right-click, then select Properties and save the highlighted Path to Executable as shown in [Figure 107 – Application Base Path Locator](#) for future steps).
- HCL.MyCloud.ADSERVICE
 - HCL.MyCloud.AllXaaS
 - HCL.MyCloud.Billing
 - HCL.MyCloud.GenericExecutor
 - HCL.MyCloud.ITSMExecutor
 - HCL.MyCloud.Listener
 - HCL.MyCloud.Performance
 - HCL.MyCloud.SyncService
 - HCL.MyCloud.WorkFlow
 - HCL.MyCloud.Monitor
 - HCL.MyCloud.CiscoIntersightSyncService

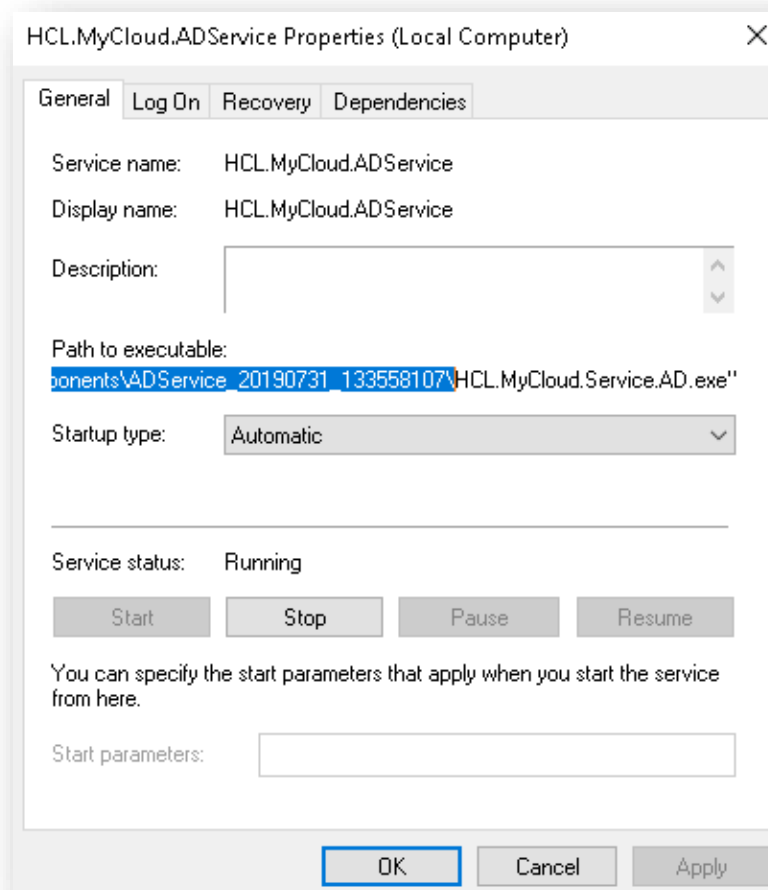


Figure 109 – Service Properties Window

6. Copy the string as highlighted in [Figure 109 – Service Properties Window](#) and save it in a notepad or a document for future reference.
7. In a similar way, copy and save the path to executable for all the services mentioned above.

8. Once the configuration path is saved then the next step is to make the website, Web API, and middleware component changes.
9. Let us begin with website, Web API and key rotation changes. These steps must be performed on the server where the website is installed. This information can be obtained from the administrator or by dropping an email to MyCloud-Product-Supp@hcl.com.

6.2.1 WebSite changes

6.2.1.1 Web.config changes

1. Go to ApplicationBasePath of WebUI.

2. **For example:**

"C:\ProgramFiles\MyCloudComponents\MyCloudPortal_XXXXXXXX_XXXXXXXX\ WebUI"

- Update DNS Certificate name in System.serviceModel.clients as mentioned below

For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End

"HclTech.MyCloud.Web" to Private Certificate Name of Web Server.

For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Public Certificate Name of App Server.

```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract="
HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract="
HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
</client>
```

Figure 110 – Certificate Web.Config Certificate Name

6.2.2 WebAPI changes

6.2.2.1 Web. Config changes

1. Go to ApplicationBasePath of WebAPI.

2. **For example:**

"C:\ProgramFiles\MyCloudComponents\MyCloudPortal_XXXXXXXX_XXXXXXXX\ WebAPI"

3. Update the following keys in the web.config files:

- **CertificateName** key value from HCL.MyCloud.Web to Web Server Private Certificate name XXXX.

```
<add key="CertificateName" value="HclTech.MyCloud.Web" />
```

Figure 111 – Certificate Web.Config Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below

For KMS Connectivity - Change the dns value under KMS_WSHttpBinding_End

"HclTech.MyCloud.Web" to Private Certificate Name of Web Server.

For Service Connectivity - Change the dns value "HclTech.MyCloud.App" to Public Certificate Name of App Server.

```
<client>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
    "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
    "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
</client>
```

Figure 112 – Certificate Web.Config Certificate Name

6.2.3 Key Rotation changes

6.2.3.1 Web.config changes

1. Go to ApplicationBasePath as of WebAPI.
2. For example:
"C:\ProgramFiles\MyCloudComponents\MyCloudPortal_XXXXXXXX_XXXXXXXX\KMS"
3. Update the following keys in the web.config files:
 - **CertificateName** key value from HCL.MyCloud.Web to Web Server Private Certificate name XXXX.

```
<add key="CertificateName" value="HclTech.MyCloud.Web" />
```

Figure 113 – Certificate Web.Config Certificate name (Cont.)

- Certificate Name in Behaviour of system.serviceModel, Change the HclTech.Mycloud.Web to Private Certificate Name of the App Server.

```
</system.web>
<system.serviceModel>
  <services>
  <bindings>
  <behaviors>
    <serviceBehaviors>
      <behavior name="">
        <serviceMetadata httpGetEnabled="true" httpsGetEnabled="true"
        <serviceDebug includeExceptionDetailInFaults="false" />
        <serviceCredentials>
          <clientCertificate>
            <authentication certificateValidationMode="PeerTrust" />
          </clientCertificate>
          <serviceCertificate findValue="HclTech.MyCloud.Web" storeLoca
            "FindBySubjectName" />
          </serviceCredentials>
        </behavior>
      </serviceBehaviors>
    </behaviors>
  </bindings>
  </services>
</system.serviceModel>
```

Figure 114 – Web Config Certificate Name (Cont.)

6.2.4 Middleware Component changes

Middleware components are part of App Server. Thus, we need to Update the following certificate:

- **Public Web Certificate** (.cer)
- **Private App Certificate** (.pfx)

Stop all the Services and find out the services file location. The step must be performed on the server where the middleware components have been installed. This information can be obtained from the administrator or by dropping an email to MyCloud-Product-Supp@hcl.com.

1. Press **Window + R** keys to open **RUN** window.
2. Type **services.msc** and click **OK**.

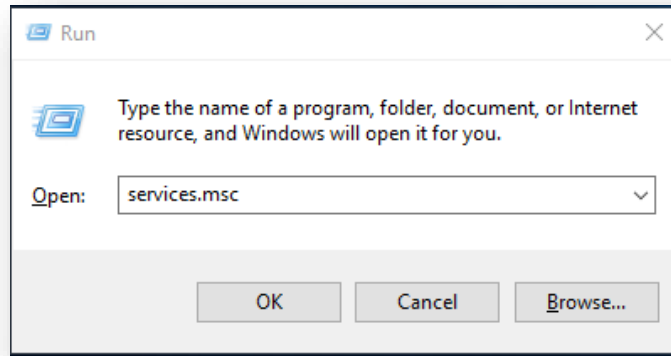


Figure 115 – Run Command Windows

3. User will be redirected to the **Windows Service Manager**.

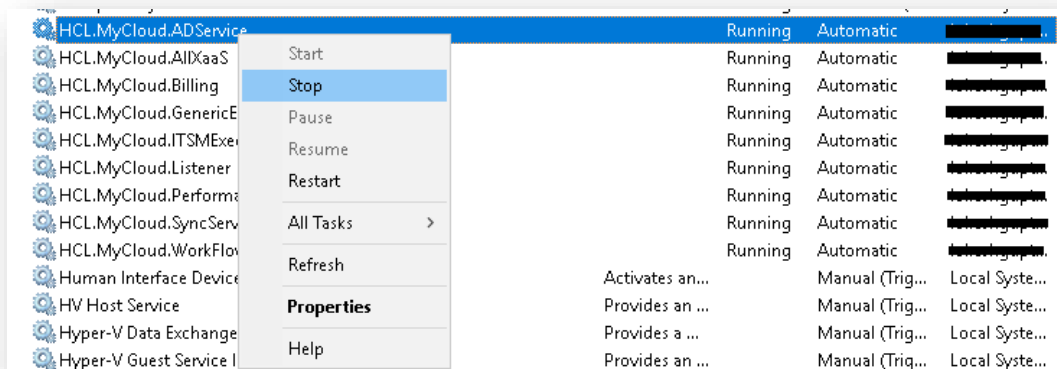


Figure 116 – Windows Services Manager

4. Stop the below mentioned services. Each of these services is responsible for a component in MyCloud. Select the service, right click on it and select **Stop**.
 - HCL.MyCloud.ADServices
 - HCL.MyCloud.AllXaaS
 - HCL.MyCloud.Billing
 - HCL.MyCloud.GenericExecutor
 - HCL.MyCloud.ITSMExecutor
 - HCL.MyCloud.Listener
 - HCL.MyCloud.Performance

- HCL.MyCloud.SyncService
- HCL.MyCloud.WorkFlow
- HCL.MyCloud.Monitor
- HCL.MyCloud.CiscoIntersightSyncService

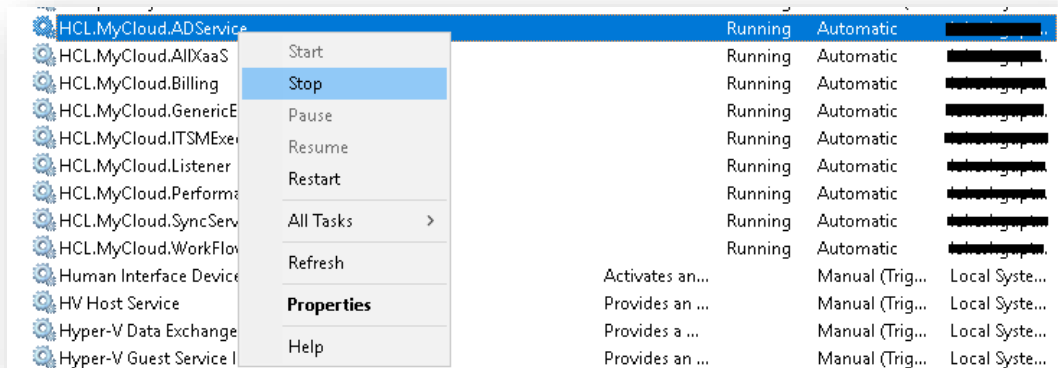


Figure 117 – Stop Services

5. After stopping all the services, perform the configuration changes in the Middleware components.

6.2.4.1 Listener Component Changes

This component is responsible for execution of MyCloud Jobs and Interacting with different components internally and is a self-hosted WCF service that requires MyCloud database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.Listener.
2. **For example:**
 "C:\ProgramFiles\MyCloudComponents\MyCloudListener_XXXXXXXX_XXXXXXXX\"
3. Open HCL.MyCloud.Listener.Service.Host.exe.config and change the following keys:
 - Update **CertificateName** key value from HclTech.MyCloud.Web to **Private Certificate of APP ServerXXXX**.

```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 118 – Certificate Web.Config Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below
For KMS Connectivity – Change the dns value under KMS_WSHttpBinding_End
 "HclTech.MyCloud.Web" to Public Certificate Name of Web Server.
For Service Connectivity – Change the dns value "HclTech.MyCloud.App" to Private
 Certificate Name of App Server.

```

<identity>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
"HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
"HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
</identity>

```

Figure 119 – Certificate Web.Config Certificate Name

4. In Listener, we also need to add some configuration mentioned below:

- <add key="KRSRetryCount" value="1"/>
 <!--KRS Retry | Default Values KRSRetryCount=1 and KRSRetrySleepTime (MS) = 2000 -->
 When Listener component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
- <add key="KRSRetrySleepTime" value="2000"/>
 When Listener component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.
- <add key="MaxDBConnectionRetryCount" value="100"/>
 This Key defines the Max number of tries to be made to successfully establish a connection between the Listener component and database. Once the Maximum retry has been achieved and successful database connection has not been established then Listener Service will be marked as Stop. Default value of **MaxDBConnectionRetryCount** is 100 and user can change its value from the application config file of the component.

In case of an upgrade or fresh installation, the KMS URL will also be updated in the config file of the listener on the app server. The installer will first check the database to retrieve the URL and in case of no value in DB, system will set it to the default value.

6.2.4.2 AD Changes

This component is responsible for fetching AD group user data. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.ADSERVICE.
2. **For example:**
 "C:\ProgramFiles\MyCloudComponents\ADService_XXXXXXXX_XXXXXXXX\"
3. Open **HCL.MyCloud.Service.AD.exe.config** and change the following keys:
 - Update **CertificateName** key value from HclTech.MyCloud.Web to **Private Certificate of APP ServerXXXX**.

```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 120 – Middleware AD Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below
For KMS Connectivity – Change the dns value under KMS_WSHttpBinding_End
"HclTech.MyCloud.Web" to Public Certificate Name of Web Server.
For Service Connectivity – Change the dns value "HclTech.MyCloud.App" to Private
Certificate Name of App Server.

```
<clients>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
    "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
    "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
</clients>
```

Figure 121 – Middleware AD Certificate Name

4. In AD Service component, we also need to add some configuration key which are mentioned below:
 - <add key="KRSRetryCount" value="1"/>
When AD Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - <add key="KRSRetrySleepTime" value="2000"/>
When AD Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.4.3 Orchestrator Changes

This component is responsible for Provisioning and other Automation Tasks. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.AllXaaS.
2. **For example:**
"C:\ProgramFiles\MyCloudComponents\Orchestrator_XXXXXXXX_XXXXXXXX\"
3. Open **HCL.MyCloud.AllXaaS.Host.exe.config** and change the following keys:
 - Update **CertificateName** key value from HclTech.MyCloud.Web to **Private Certificate of APP ServerXXXX**.

```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 122 – Middleware Orchestrator Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below
For KMS Connectivity – Change the dns value under KMS_WSHttpBinding_End
"HclTech.MyCloud.Web" to Public Certificate Name of Web Server.
For Service Connectivity – Change the dns value "HclTech.MyCloud.App" to Private
Certificate Name of App Server.

```
<clients>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
    "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
    "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
</clients>
```

Figure 123 – Middleware Orchestrator Certificate Name

4. In Orchestrator component, we also need to add some configuration key which are mentioned below:
 - <add key="KRSRetryCount" value="1"/>
 - When Orchestrator component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - <add key="KRSRetrySleepTime" value="2000"/>
 - When Orchestrator component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.4.4 WorkFlow Changes

This component is responsible for triggering MyCloud Process workflow and notification service. This is a self-hosted WCF service. This component requires MyCloud database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.WorkFlow.
2. **For example:**
"C:\ProgramFiles\MyCloudComponents\WorkFlow_XXXXXXXX_XXXXXXXXX\"
3. Open **HCL.MyCloud.WorkflowEngine.exe.config** and change the following keys:
 - Update **CertificateName** key value from HclTech.MyCloud.Web to **Private Certificate of APP ServerXXXX**.

```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 124 – Middleware Workflow Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below
For KMS Connectivity – Change the dns value under KMS_WSHttpBinding_End
"HclTech.MyCloud.Web" to Public Certificate Name of Web Server.
For Service Connectivity – Change the dns value "HclTech.MyCloud.App" to Private
Certificate Name of App Server.

```
<clients>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
    "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
    "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
</clients>
```

Figure 125 – Middleware WorkFlow Certificate Name

4. In Worflow component, we also need to add some configuration key which are mentioned below:
 - <add key="KRSRetryCount" value="1"/>
 - When Worflow component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - <add key="KRSRetrySleepTime" value="2000"/>
 - When Worflow component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.4.5 SyncService Changes

This component is responsible for syncing the underlying infrastructure Cloud resources. It supports vCenter, AWS, AzureRM, SCVMM 2012. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.SyncService.
2. **For example,**
"C:\ProgramFiles\MyCloudComponents\SyncService_XXXXXXXX_XXXXXXXXXX\")
3. Open **HCL.MyCloud.SyncJobService.Host.exe.config** and change the following keys:
 - Update **CertificateName** key value from HclTech.MyCloud.Web to **Private Certificate of APP ServerXXXX**.

```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 126 – Middleware SyncService Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below
For KMS Connectivity – Change the dns value under KMS_WSHttpBinding_End
"HclTech.MyCloud.Web" to Public Certificate Name of Web Server.
For Service Connectivity – Change the dns value "HclTech.MyCloud.App" to Private
Certificate Name of App Server.

```
<clients>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
    "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
    "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
</clients>
```

Figure 127 – Middleware SyncService Certificate Name

4. In Sync Service component, we also need to add some configuration key which are mentioned below:
 - <add key="KRSRetryCount" value="1"/>
 - When Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - <add key="KRSRetrySleepTime" value="2000"/>
 - When Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.4.6 ITSM Executor Changes

This component is responsible for ITSM Tools Interaction. Currently this supports ServiceNow and Remedy. This is a self-hosted WCF service. This component requires MyCloud database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.ITSMExecutor.
2. For example,
3. "C:\ProgramFiles\MyCloudComponents\ITSMExecutor_XXXXXXXX_XXXXXXXXXX\"
4. Open **HCL.MyCloud.Snow.Host.exe.config** and change the following keys:
 - Update **CertificateName** key value from HclTech.MyCloud.Web to **Private Certificate of APP ServerXXXX**.

```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 128 – Middleware ITSM Executor Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below
For KMS Connectivity – Change the dns value under KMS_WSHttpBinding_End
"HclTech.MyCloud.Web" to Public Certificate Name of Web Server.
For Service Connectivity – Change the dns value "HclTech.MyCloud.App" to Private
Certificate Name of App Server.

```
<?xml version="1.0"?>
<endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
"HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
  <identity>
    <dns value="HclTech.MyCloud.Web" />
  </identity>
</endpoint>
<endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
"HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
  <identity>
    <dns value="HclTech.MyCloud.App" />
  </identity>
</endpoint>
```

Figure 129 – Middleware ITSM Executor Certificate Name

5. In ITSM Executer component, we also need to add some configuration key which are mentioned below:
 - <add key="KRSRetryCount" value="1"/>
 - When ITSM Executer component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - <add key="KRSRetrySleepTime" value="2000"/>
 - When ITSM Executer component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.4.7 Billing Changes

This component is responsible for Public Cloud billing. This is a self-hosted WCF service. This component requires MyCloud database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.Billing.
2. **For example,**
"C:\ProgramFiles\MyCloudComponents\Billing_XXXXXXXX_XXXXXXXX\")
3. Open HCL.CloudBilling.DataCollector.Service.Host.exe.config and change the following keys:
 - Update **CertificateName** key value from HclTech.MyCloud.Web to **Private Certificate of APP ServerXXXX**.

```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 130 – Middleware Billing Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below
For KMS Connectivity – Change the dns value under KMS_WSHttpBinding_End
"HclTech.MyCloud.Web" to Public Certificate Name of Web Server.
For Service Connectivity – Change the dns value "HclTech.MyCloud.App" to Private
Certificate Name of App Server.

```
<clients>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
    "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
    "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
</clients>
```

Figure 131 – Middleware Billing Certificate Name

4. In Billing component, we also need to add some configuration key which are mentioned below:
 - <add key="KRSRetryCount" value="1"/>
 - When Billing component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - <add key="KRSRetrySleepTime" value="2000"/>
 - When Billing component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.4.8 Generic Service Changes

This component is responsible for Private Cloud billing, Data Purging and Cost Models Activation. This is a self-hosted WCF service. This component requires MyCloud database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.GenericExecutor.
2. For example,
3. "C:\ProgramFiles\MyCloudComponents\GenericService_XXXXXXXX_XXXXXXXXXX\")
4. Open **HCL.MyCloud.Generic.Host.exe.config** and change the following keys:
 - Update **CertificateName** key value from HclTech.MyCloud.Web to **Private Certificate of APP ServerXXXX**.

```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 132 – Middleware Generic Service Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below
For KMS Connectivity – Change the dns value under KMS_WSHttpBinding_End
"HclTech.MyCloud.Web" to Public Certificate Name of Web Server.
For Service Connectivity – Change the dns value "HclTech.MyCloud.App" to Private
Certificate Name of App Server.

```
<clients>
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
    "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.Web" />
    </identity>
  </endpoint>
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
    "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
    <identity>
      <dns value="HclTech.MyCloud.App" />
    </identity>
  </endpoint>
</clients>
```

Figure 133 – Middleware Generic service Certificate Name

5. In Generic Service component, we also need to add some configuration key which are mentioned below:
 - <add key="KRSRetryCount" value="1"/>
When Generic Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - <add key="KRSRetrySleepTime" value="2000"/>
When Generic Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.4.9 Health Monitor Changes

This component is responsible for monitoring the health of MyCloud Components. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.Monitor.
2. For example,
3. "C:\ProgramFiles\MyCloudComponents\HealthMonitor_XXXXXXXX_XXXXXXXX\"
4. Open **HCL.MyCloud.Monitor.Host.exe.config** and change the following keys:
 - Update **CertificateName** key value from HclTech.MyCloud.Web to **Private Certificate of APP ServerXXXX**.

```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 134 – Middleware Monitor Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below
For KMS Connectivity – Change the dns value under KMS_WSHttpBinding_End
"HclTech.MyCloud.Web" to Public Certificate Name of Web Server.
For Service Connectivity – Change the dns value "HclTech.MyCloud.App" to Private
Certificate Name of App Server.

```
<clients>  
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=  
    "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">  
    <identity>  
      <dns value="HclTech.MyCloud.Web" />  
    </identity>  
  </endpoint>  
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=  
    "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">  
    <identity>  
      <dns value="HclTech.MyCloud.App" />  
    </identity>  
  </endpoint>  
</clients>
```

Figure 135 – Middleware Monitor Certificate Name

5. In Health Monitor component, we also need to add some configuration key which are mentioned below:
 - <add key="KRSRetryCount" value="1"/>
When Health Monitor component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - <add key="KRSRetrySleepTime" value="2000"/>
When Health Monitor component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.4.10 Performance Changes

This component is responsible for Metering and Public Cloud Advisory Data Collection. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.Performance.
2. **For example,**
"C:\ProgramFiles\MyCloudComponents\Performance_XXXXXXXX_XXXXXXXX\"
3. Open HCL.CloudPerformance.DataCollector.Service.Host.exe.config and change the following keys:
 - Update **CertificateName** key value from HclTech.MyCloud.Web to **Private Certificate of APP ServerXXXX**.

```
<add key="CertificateName" value="HclTech.MyCloud.App" />
```

Figure 136 – Middleware Performance Certificate Name

- Update DNS Certificate name in System.serviceModel.clients as mentioned below
For KMS Connectivity – Change the dns value under KMS_WSHttpBinding_End
"HclTech.MyCloud.Web" to Public Certificate Name of Web Server.
For Service Connectivity – Change the dns value "HclTech.MyCloud.App" to Private
Certificate Name of App Server.

```
<clients>  
  <endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=  
    "HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">  
    <identity>  
      <dns value="HclTech.MyCloud.Web" />  
    </identity>  
  </endpoint>  
  <endpoint address="https://localhost:8081/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=  
    "HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">  
    <identity>  
      <dns value="HclTech.MyCloud.App" />  
    </identity>  
  </endpoint>  
</clients>
```

Figure 137 – Middleware Performance Certificate Name

4. In Performance component, we also need to add some configuration key which are mentioned below:
 - <add key="KRSRetryCount" value="1"/>
When Performance component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - <add key="KRSRetrySleepTime" value="2000"/>
When Performance component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.4.11 Cisco Intersight Sync Service Changes

This component is responsible to sync organizations, Operating System Files, Physical Summary, Profile Templates, SCUtility Distributable, Server Profile, Device Registration, Organization, Array, Host, Host Group, Host Lun, Volume, Targets, Virtualization (Cluster, Cluster Storage, Data Store, Data Center, Distributed Network, Distributed Switch, Folder, Host, Instance, Resource Group, Template, VCenter), Workflow. This is a self-hosted WCF service.

1. Go to PathToExecutable of HCL.MyCloud.
2. For example:
 - Update DNS Certificate name in System.serviceModel.clients as mentioned below

For KMS Connectivity – Change the dns value under KMS_WSHttpBinding_End
"HclTech.MyCloud.Web" to Public Certificate Name of Web Server.

For Service Connectivity – Change the dns value "HclTech.MyCloud.App" to Private
Certificate Name of App Server.

```
<!--
-->
<endpoint address="https://localhost:8080/Service1" binding="wsHttpBinding" bindingConfiguration="KMS_WSHttpBinding" contract=
"HCL.MyCloud.Encryption.IKeyManagement" name="KMS_WSHttpBinding_Endpoint">
  <identity>
    <dns value="HclTech.MyCloud.Web" />
  </identity>
</endpoint>
<endpoint address="https://localhost:8080/Services" binding="wsHttpBinding" bindingConfiguration="Service_WSHttpBinding" contract=
"HCL.MyCloud.JobServiceContract.IJobService" name="Service_WSHttpBinding_Endpoint">
  <identity>
    <dns value="HclTech.MyCloud.App" />
  </identity>
</endpoint>
```

Figure 138 – Middleware Cisco Intersight Certificate Name

3. In Cisco Intersight Sync Service component, we also need to add some configuration key which are mentioned below:

- <add key="KRSRetryCount" value="1"/>

When Cisco Intersight Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of KRSRetryCount is 1 and user can change its value from the application config file of the component.

- <add key="KRSRetrySleepTime" value="2000"/>

When Cisco Intersight Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of KRSRetrySleepTime is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.2.4.12 Start all the Services

Once the changes are made, each of these services must be started again. Follow the steps mentioned below to do that:

1. Press **Window + R** keys to open **RUN** window.
2. Type **services.msc** and click **OK**.

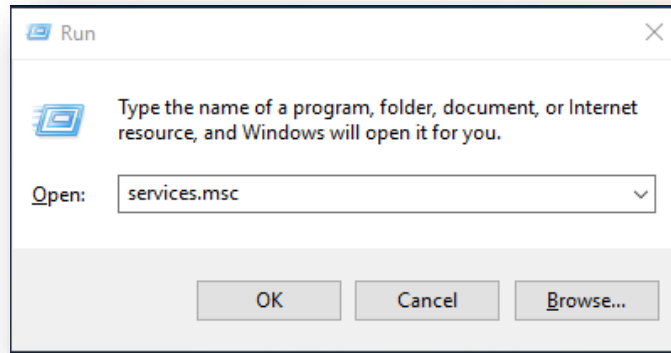


Figure 139 – Run Command Windows

3. Start the below mentioned services: (Select the service, right-click on it, and select **Start**.)

- HCL.MyCloud.ADSERVICE
- HCL.MyCloud.AllXaaS
- HCL.MyCloud.Billing
- HCL.MyCloud.GenericExecutor
- HCL.MyCloud.ITSMExecutor
- HCL.MyCloud.Performance
- HCL.MyCloud.SyncService
- HCL.MyCloud.Listener
- HCL.MyCloud.Monitor
- HCL.MyCloud.CiscoIntersightSyncService

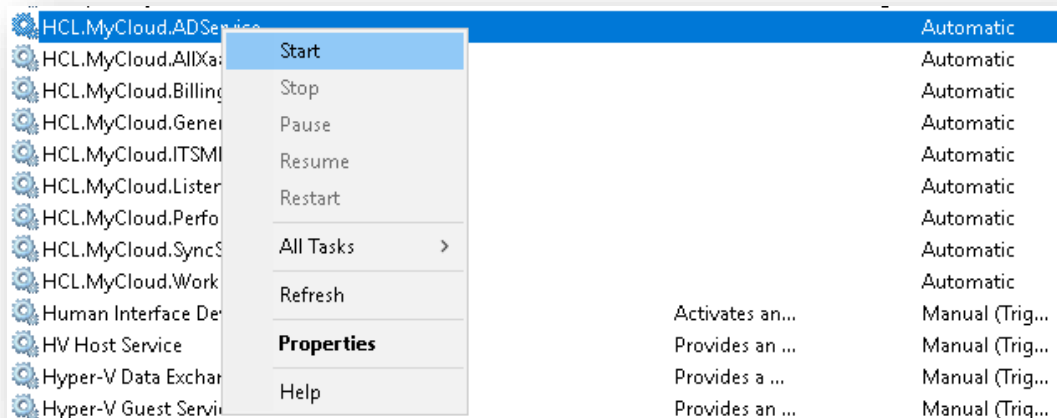


Figure 140 – Start Services

If the certificate location is changed, then repeat all the steps from section **Error! Reference source not found**. and change the below mentioned properties accordingly:

- **CertificateStoreLocation** key value from "2" to one of the following options:
 - 1 for CurrentUser
 - 2 for LocalMachine

```
<add key="CertificateStoreLocation" value="2" />
```

Figure 141 – Middleware Certificate Store Location

- **CertificateStoreName** key value from "7" to one of the following options:
 - 1 for AddressBook
 - 2 for AuthRoot
 - 3 for CertificateAuthority
 - 4 for Disallowed
 - 5 for My
 - 6 for Root
 - 7 for TrustedPeople
 - 8 for TrustedPublisher

```
<add key="CertificateStoreName" value="7" />
```

Figure 142 – Middleware Certificate Store Location (Cont.)

- **IsSSLSelfSigned** key value from "N" to "Y"

```
<add key="IsSSLSelfSigned" value="Y" />
```

Figure 143 – Middleware Start Service IsSSLSelfSigned

Once all the configuration is done in all the components, MyCloud components will start using the custom Certificate configuration.

6.3 Load Balancer Configuration (Optional)

If High Availability is required for MyCloud, then the website has to be configured with the Load Balancer.

Follow the steps mentioned below to do that.

1. Find Website, WebAPI and Key Rotation Service ApplicationBasePath.
2. Press **Window + R** keys to open RUN command window.
 - a. Now type inetmgr and click OK.
 - b. The IIS Console will open.

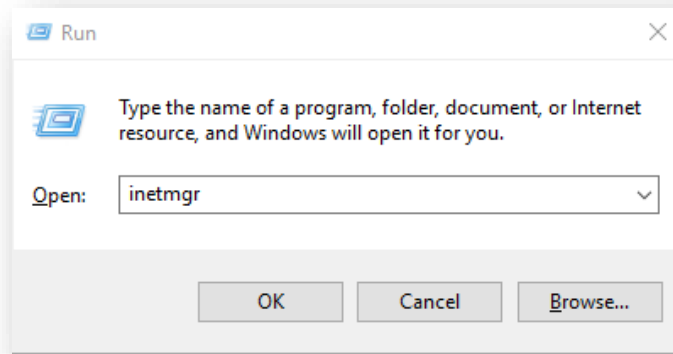


Figure 144 – Run Command Window

- c. Now expand the Server Name node → Sites node using the Connections section. Right-click on the HCLMyCloudPortal Node and click on Explore.
- d. This will locate the ApplicationBasePath for Website and Web API as highlighted in [Figure 145 – ApplicationBasePath Locator](#).

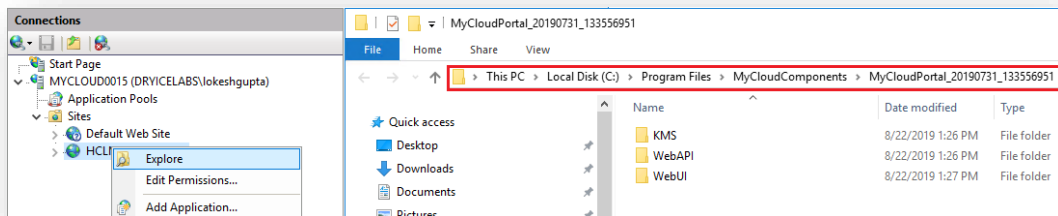


Figure 145 – ApplicationBasePath Locator

3. Copy the base path and save for future reference.
4. The next step is to find the path of the Middleware component configuration files. The steps are mentioned below:
5. Find the PathToExecutable of HCL.MyCloud.Listener service.
 - a. Press **Window + R** keys to open RUN window, then type services.msc and click OK.

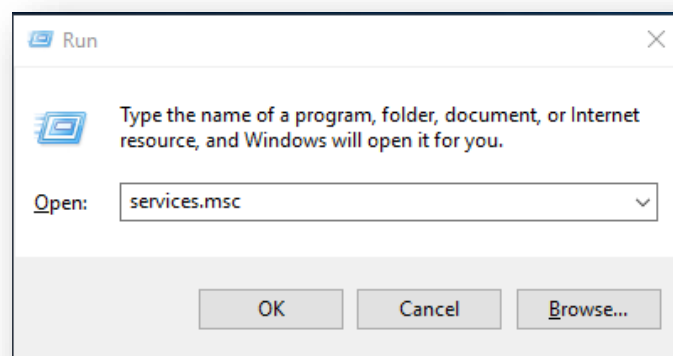


Figure 146 – Run Command Window

- b. For the below mentioned services: (Select the service, right-click to select Properties and save the highlighted Path to executable as shown in the following screenshot).
 - HCL.MyCloud.ADSERVICE

- HCL.MyCloud.AllXaaS
- HCL.MyCloud.Billing
- HCL.MyCloud.GenericExecutor
- HCL.MyCloud.ITSMExecutor
- HCL.MyCloud.Listener
- HCL.MyCloud.Performance
- HCL.MyCloud.SyncService
- HCL.MyCloud.WorkFlow
- HCL.MyCloud.Monitor
- HCL.MyCloud.CiscoIntersightSyncService

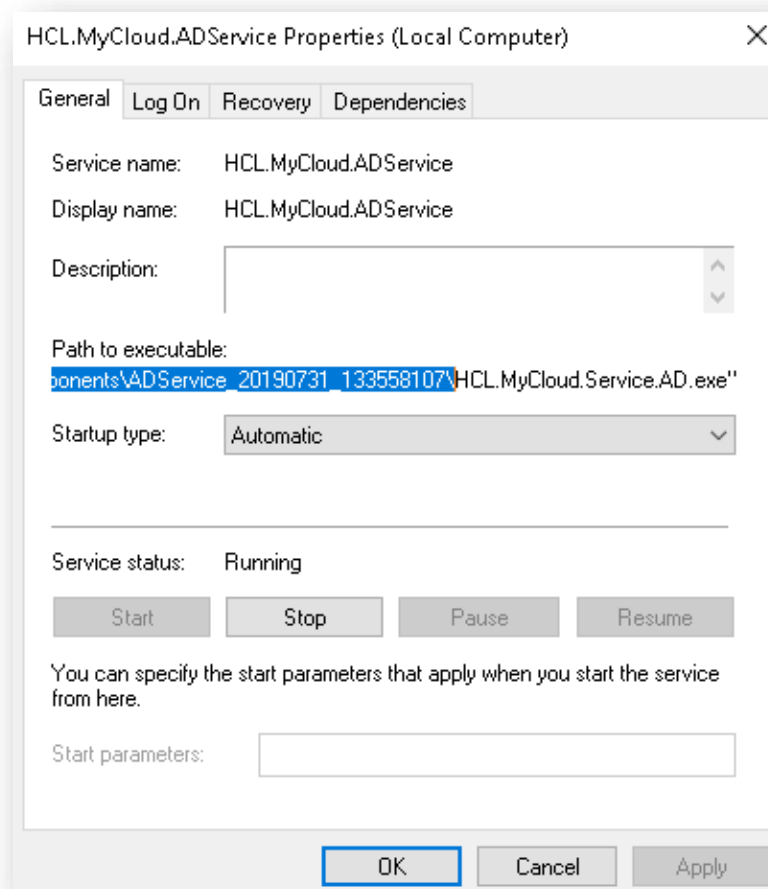


Figure 147 – AD Service Properties

- c. Copy the string as highlighted in [Figure 109 – Service Properties Window](#) and save it in a notepad or a document for future reference.
 - d. Also, copy and save the path to executable for all the services mentioned above.
6. Once the configuration path is saved then the next step is to make the website, Web API and middleware component changes.
 7. Let us begin with website and Web API. These steps must be performed on the server where the website has been installed. This information can be obtained from the administrator who has run the installer or by dropping an email to MyCloud-Product-Supp@hcl.com.

6.3.1 Website changes

6.3.1.1 Web

We are keeping session in SQL Server but in case we need to change the default session timeout, we can change timeout property mentioned below:

- `<sessionState mode="SQLServer" allowCustomSqlDatabase="true" partitionResolverType="ConnectionStringResolver" regenerateExpiredSessionId="true" compressionEnabled="true" useHostingIdentity="true" timeout="40"/>`

6.3.2 Web API changes

6.3.2.1 Web. Config changes

6.3.3 Middleware Component changes

1. Stop all the Services and find the services file location where they have been installed by default. This step must be performed on the server where the middleware components have been installed. This information can be obtained from the administrator or by dropping an email to MyCloud-Product-Supp@hcl.com.
2. Press **Window + R** keys to open the **RUN** window.
3. Type **services.msc** and click **OK**.

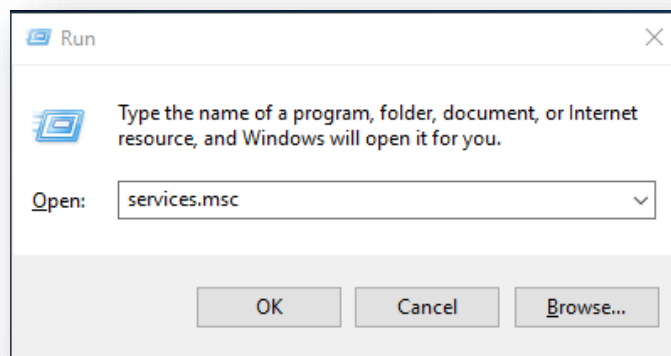


Figure 148 – Run Command Window

4. User will be redirected to the **Windows Service Manager**.

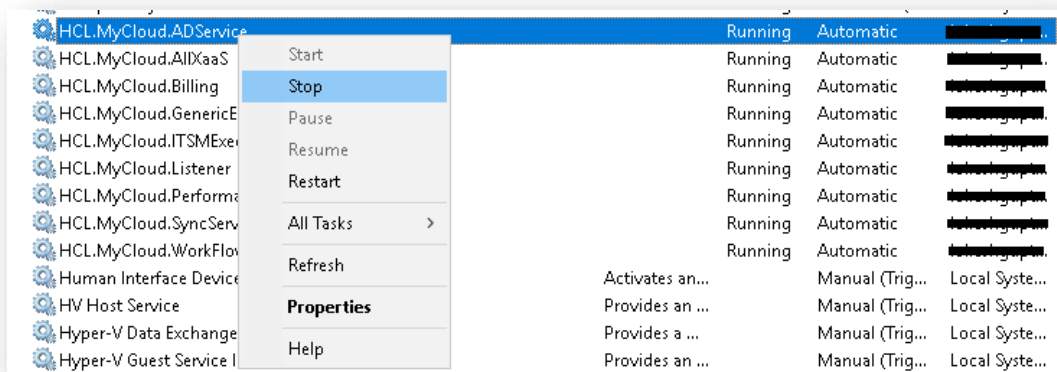


Figure 149 – Windows Service Manager

5. Stop the below mentioned services: (Select the service, **right click** on it, and select **Stop**)

- HCL.MyCloud.ADServices
- HCL.MyCloud.AIXaaS
- HCL.MyCloud.Billing
- HCL.MyCloud.GenericExecutor
- HCL.MyCloud.ITSMEExecutor
- HCL.MyCloud.Listener
- HCL.MyCloud.Performance
- HCL.MyCloud.SyncService
- HCL.MyCloud.WorkFlow
- HCL.MyCloud.Monitor
- HCL.MyCloud.CiscoIntersightSyncService

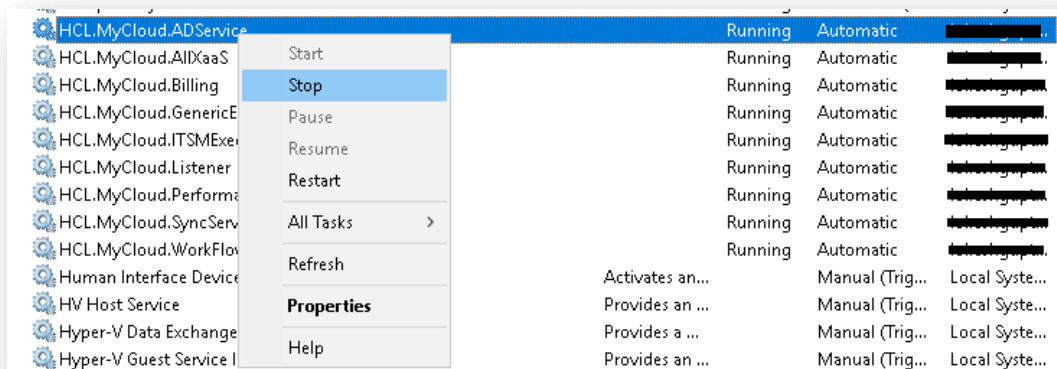


Figure 150 – Stop Below Service

6. Once a user has stopped all the services, perform the configuration changes in the Middleware components.

6.3.3.1 Listener Component Changes

This Component is responsible for execution of MyCloud Jobs and Interacting with different components internally. This is a window service. This component requires MyCloud database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.Listener.
2. **For example,**
"C:\ProgramFiles\MyCloudComponents\MyCloudListener_XXXXXXXX_XXXXXXXX\"
3. Open **HCL.MyCloud.Listener.Service.Host.exe.config** and change the following keys:
 - Update *KeyManagementBaseAddress* key value from `http://<ip>:<port>/KMS` or `https://<ip>:<port>/KMS` to `http://<LBIP>:<port>/KMS` or `https://<LBIP>:<port>/KMS`

```
<add key="KeyManagementBaseAddress" value="http://XX.XX.XX.XXX:XXXX/KMS" />
```

Figure 151 – Load Balancer Listener Key Management Base Address

4. In Listener, we also need to add some configuration key which are mentioned below:
 - `<!--KRS Retry | Default Values KRSRetryCount=1 and KRSRetrySleepTime (MS) = 2000 -->`
 - `<add key="KRSRetryCount" value="1"/>`
 - When Listener component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - `<add key="KRSRetrySleepTime" value="2000"/>`
When Listener component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.
 - `<add key="MaxDBConnectionRetryCount" value="100"/>`
This Key defines the Max number of tries to be made to successfully establish a connection between the Listener component and database. Once the Maximum retry has been achieved and successful database connection has not been established then Listener Service will be marked as Stop. Default value of **MaxDBConnectionRetryCount** is 100 and user can change its value from the application config file of the component.

In case of an upgrade or fresh installation, the KMS URL will also be updated in the config file of the listener on the app server. The installer will first check the database to retrieve the URL and in case of no value in DB, system will set it to the default value.

6.3.3.2 AD Changes

This component is responsible for fetching AD group user data. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.ADSERVICE.

2. For example,

"C:\Program Files\MyCloudComponents\ADService_XXXXXXXX_XXXXXXXX\"

3. Open **HCL.MyCloud.Service.AD.exe.config** and change the following keys:

- **ServiceHostURL** key value from `http://<ip>:<port>` or `https://<ip>:<port>` to `http://<LBIP>:<port>` or `https://<LBIP>:<port>`

```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 152 – Load Balancer AD Service Host

4. In AD Service component, we also need to add some configuration key which are mentioned below:

- `<add key="KRSRetryCount" value="1"/>`

When AD Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.

- `<add key="KRSRetrySleepTime" value="2000"/>`

When AD Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.3.3 Orchestrator Changes

This component is responsible for Provisioning and other Automation Tasks. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.AllXaaS.

2. For example,

"C:\ProgramFiles\MyCloudComponents\Orchestrator_XXXXXXXX_XXXXXXXX\"

3. Open **HCL.MyCloud.AllXaaS.Host.exe.config** and change the following keys:

- **ServiceHostURL** key value from `http://<ip>:<port>` or `https://<ip>:<port>` to `http://<LBIP>:<port>` or `https://<LBIP>:<port>`

```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 153 – Load Balancer Orchestrator Service Host URL

4. In Orchestrator Service component, we also need to add some configuration key which are mentioned below:

- `<add key="KRSRetryCount" value="1"/>`

When Orchestrator component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.

- `<add key="KRSRetrySleepTime" value="2000"/>`

When Orchestrator component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.3.4 WorkFlow Changes

This component is responsible to trigger MyCloud Process workflow and notification service. This is a self-hosted WCF service. This component requires MyCloud database connectivity.

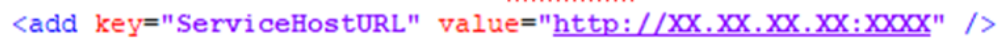
1. Go to **PathToExecutable** of HCL.MyCloud.WorkFlow.

2. **For example:**

"C:\ProgramFiles\MyCloudComponents\WorkFlow_XXXXXXXX_XXXXXXXXX\"

3. Open **HCL.MyCloud.WorkflowEngine.exe.config** and change the following keys:

- Update **ServiceHostURL** key value from `http://<ip>:<port>` or `https://<ip>:<port>` to `http://<LBIP>:<port>` or `https://<LBIP>:<port>`



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 154 – Load Balancer Workflow Service Host URL

4. In Workflow Service component, we also need to add some configuration key which are mentioned below:

- `<add key="KRSRetryCount" value="1"/>`

When Workflow component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.

- `<add key="KRSRetrySleepTime" value="2000"/>`

When Workflow component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.3.5 SyncService Changes

This component is responsible for syncing the underlying infrastructure Cloud resources. It supports vCenter, AWS, AzureRM, SCVMM 2012. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.SyncService.
2. **For example:**
"C:\ProgramFiles\MyCloudComponents\SyncService_XXXXXXXX_XXXXXXXX\"
3. Open **HCL.MyCloud.SyncJobService.Host.exe.config** and change the following keys:
 - Update **ServiceHostURL** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>

```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 155 – Load Balancer SyncService Service Host URL

4. In Sync Service component, we also need to add some configuration key which are mentioned below:
 - <add key="KRSRetryCount" value="1"/>
When Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - <add key="KRSRetrySleepTime" value="2000"/>
When Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.3.6 ITSM Executor Changes

This component is responsible for ITSM Tools Interaction. Currently this supports ServiceNow and Remedy. This is a self-hosted WCF service. This component requires MyCloud database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.ITSMExecutor.
2. **For example:**
"C:\ProgramFiles\MyCloudComponents\ITSMExecutor_XXXXXXXX_XXXXXXXX\"
3. Open **HCL.MyCloud.Snow.Host.exe.config** and change the following keys:
 - Update **ServiceHostURL** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>

```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 156 – Load Balancer ITSM Executor Service Host URL

4. In ITSM Executer component, we also need to add some configuration key which are mentioned below:

- `<add key="KRSRetryCount" value="1"/>`

When ITSM Executer component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.

- `<add key="KRSRetrySleepTime" value="2000"/>`

When ITSM Executer component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.3.7 Billing Changes

This component is responsible for Public Cloud billing. This is a self-hosted WCF service. This component requires MyCloud database connectivity.

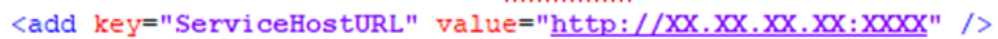
1. Go to **PathToExecutable** of HCL.MyCloud.Billing.

2. **For example:**

"C:\ProgramFiles\MyCloudComponents\Billing_XXXXXXXX_XXXXXXXX\"

3. Open HCL.CloudBilling.DataCollector.Service.Host.exe.config and change the following keys:

- Update **ServiceHostURL** key value from `http://<ip>:<port>` or `https://<ip>:<port>` to `http://<LBIP>:<port>` or `https://<LBIP>:<port>`



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 157 – Load Balancer Billing Service Host URL

4. In Billing component, we also need to add some configuration key which are mentioned below:

- `<add key="KRSRetryCount" value="1"/>`

When Billing component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.

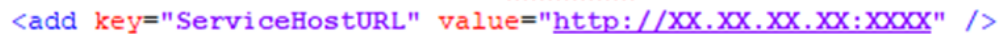
- `<add key="KRSRetrySleepTime" value="2000"/>`

When Billing component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.3.8 GenericService Changes

This component is responsible for Private Cloud billing, Data Purging and Cost Models Activation. This is a self-hosted WCF service. This component requires MyCloud database connectivity.

1. Go to **PathToExecutable** of HCL.MyCloud.GenericExecutor.
2. **For example:**
"C:\ProgramFiles\MyCloudComponents\GenericService_XXXXXXXX_XXXXXXXXXX\"
3. Open **HCL.MyCloud.Generic.Host.exe.config** and change the following keys:
 - Update **ServiceHostURL** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 158 – Load Balancer GenericService Service Host URL

4. In Generic Service component, we also need to add some configuration key which are mentioned below:
 - `<add key="KRSRetryCount" value="1"/>`
When Generic Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.
 - `<add key="KRSRetrySleepTime" value="2000"/>`
When Generic Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.3.9 HealthMonitor Changes

This component is responsible for Monitoring the health of MyCloud Components. This is a self-hosted WCF service.

1. Go to **PathToExecutable** of HCL.MyCloud.Monitor.
2. **For example:**
"C:\ProgramFiles\MyCloudComponents\HealthMonitor_XXXXXXXX_XXXXXXXXXX\"
3. Open **HCL.MyCloud.Monitor.Host.exe.config** and change the following keys:
 - Update **ServiceHostURL** key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or https://<LBIP>:<port>

```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 159 – Load Balancer Performance Service Host URL

4. In Health Monitor component, we also need to add some configuration key which are mentioned below:

- `<add key="KRSRetryCount" value="1"/>`

When Health Monitor component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.

- `<add key="KRSRetrySleepTime" value="2000"/>`

When Health Monitor component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.3.10 Performance Changes

This component is responsible for Metering and Public Cloud Advisory Data Collection. This is a self-hosted WCF service.

1. Go to PathToExecutable of HCL.MyCloud.Performance.
2. **For example,**
"C:\ProgramFiles\MyCloudComponents\Performance_XXXXXXXX_XXXXXXXX\"
3. Open HCL.CloudPerformance.DataCollector.Service.Host.exe.config and change the following keys:
 - Update **ServiceHostURL** key value from `http://<ip>:<port>` or `https://<ip>:<port>` to `http://<LBIP>:<port>` or `https://<LBIP>:<port>`

```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 160 – Load Balancer Performance Service Host URL

4. In Performance component, we also need to add some configuration key which are mentioned below:

- `<add key="KRSRetryCount" value="1"/>`

When Performance component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of **KRSRetryCount** is 1 and user can change its value from the application config file of the component.

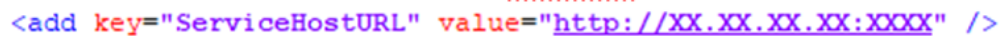
- `<add key="KRSRetrySleepTime" value="2000"/>`

When Performance component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of **KRSRetrySleepTime** is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.3.11 Cisco Intersight Sync Service Changes

This component is responsible to sync organizations, Operating System Files, Physical Summary, Profile Templates, SCUtility Distributable, Server Profile, Device Registration, Organization, Array, Host, Host Group, Host Lun, Volume, Targets, Virtualization (Cluster, Cluster Storage, Data Store, Data Center, Distributed Network, Distributed Switch, Folder, Host, Instance, Resource Group, Template, VCenter), Workflow. This is a self-hosted WCF service.

1. Go to PathToExecutable of HCL.MyCloud.CiscoIntersightSyncService.
2. **For example,**
"C:\ProgramFiles\MyCloudComponents\CiscoIntersightSyncService_XXXXXXXX_XXXXXXXX\"
3. Open HCL.MyCloud.CiscoIntersightSyncService.Host.exe.config and change the following keys:
 - Update ServiceHostURL key value from http://<ip>:<port> or https://<ip>:<port> to http://<LBIP>:<port> or **Error! Hyperlink reference not valid.**



```
<add key="ServiceHostURL" value="http://XX.XX.XX.XX:XXXX" />
```

Figure 161 – Load Balancer Cisco Intersight Sync Service Host URL

4. In Cisco Intersight Sync Service component, we also need to add some configuration key which are mentioned below:
 - `<add key="KRSRetryCount" value="1"/>`
When Cisco Intersight Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines how many times component will retry to get the connection string from the KRS. Default value of KRSRetryCount is 1 and user can change its value from the application config file of the component.
 - `<add key="KRSRetrySleepTime" value="2000"/>`
When Cisco Intersight Sync Service component gets the connection string from KRS service but somehow it gets failed. So, this key defines the interval in which the component will retry to get the connection string from the KRS. Default value of KRSRetrySleepTime is (2000 = 2 sec) and user can change its value from the application config file of the component.

6.3.3.12 Start All the Services

Once the changes are made, each of these services needs to be restarted. Follow the steps mentioned below to do that:

1. Press **Window + R** keys to open **RUN** window.
2. Type **services.msc** and click **OK**.

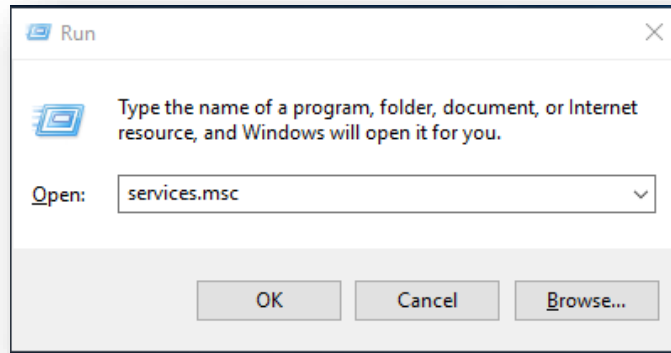


Figure 162 – Run Command Window

3. Start the below mentioned services: (Select the service, right-click on it, and select **Start**)

- HCL.MyCloud.ADSERVICE
- HCL.MyCloud.AIXaaS
- HCL.MyCloud.Billing
- HCL.MyCloud.GenericExecutor
- HCL.MyCloud.ITSMExecutor
- HCL.MyCloud.Performance
- HCL.MyCloud.SyncService
- HCL.MyCloud.Listener
- HCL.MyCloud.Monitor
- HCL.MyCloud.CiscoIntersightSyncService

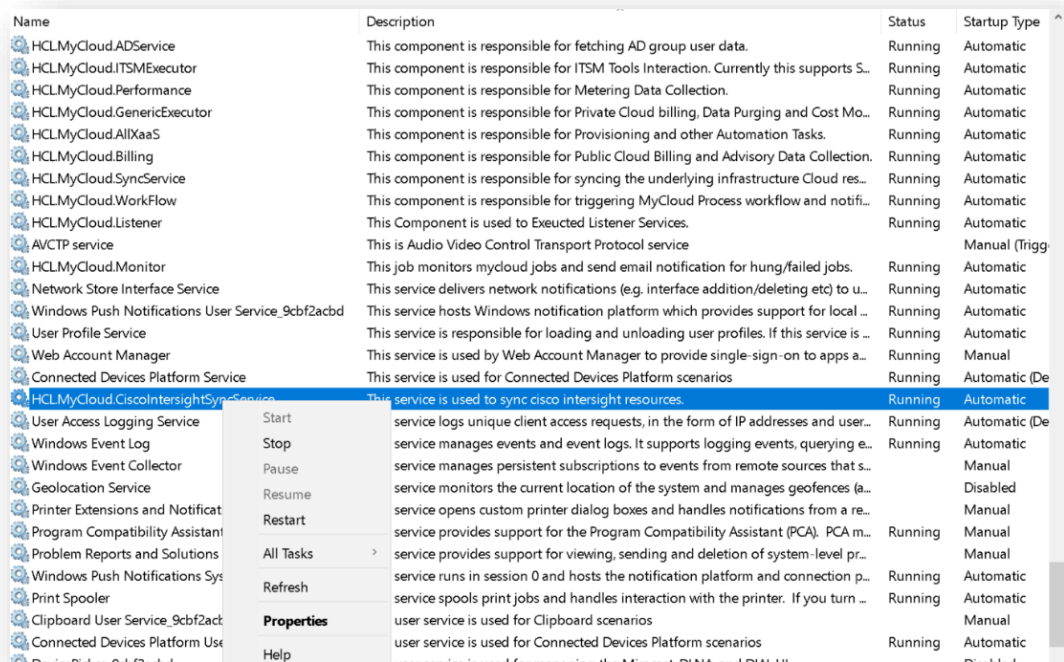


Figure 163 – Start Services

6.3.4 Master Data changes

These changes can be made after the user logs into MyCloud portal. In order to do that, the user must have the admin credentials. If user doesn't have the credentials, please contact MyCloud Admin or drop an email to MyCloud-Product-Supp@hcl.com.

After login, user will be redirected to the landing page as shown in [Figure 164 – Landing Page](#). To make the changes, user needs to follow the below steps:

1. **Go to Master** → Manage Base Components Keys.

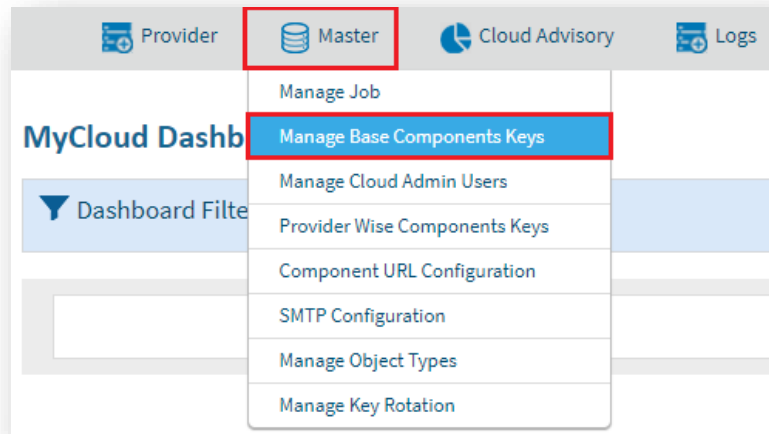


Figure 164 – Landing Page

2. User will be redirected to the **Manage Base Component** page.
3. Select **Website Service (WEBSITE)** in the **Component Name** dropdown and click on **Go** button.
4. Change the Key value for the following Key Name(s):
 - **JsURL** from `http://<ip>:<port>/WebUI/JS` to `https://<LBIP>:<port>/WebUI/JS`
 - **SiteURL** from `http://<ip>:<port>/WebUI` to `https://<LBIP>:<port>/WebUI`

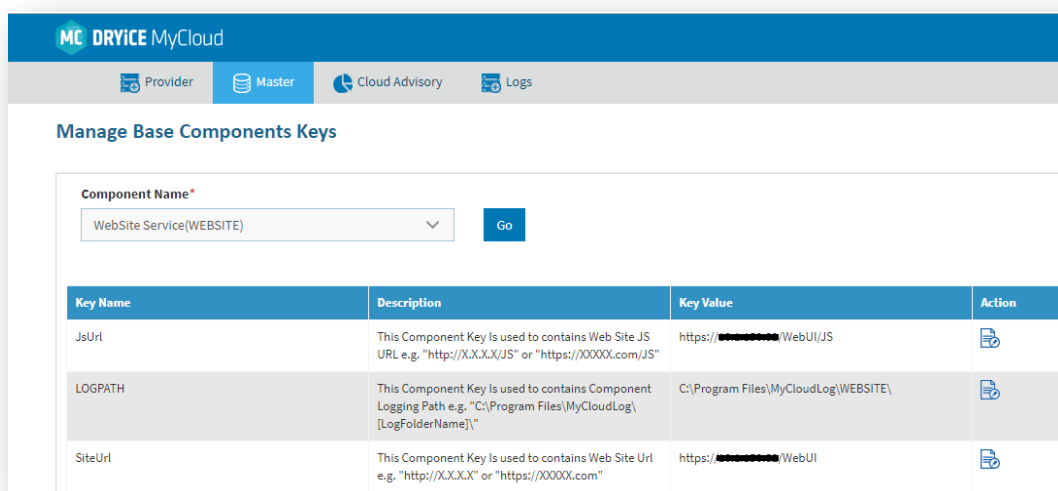


Figure 165 – Manage base Components

5. Go to **Master** and then click **Component URL Configuration**.

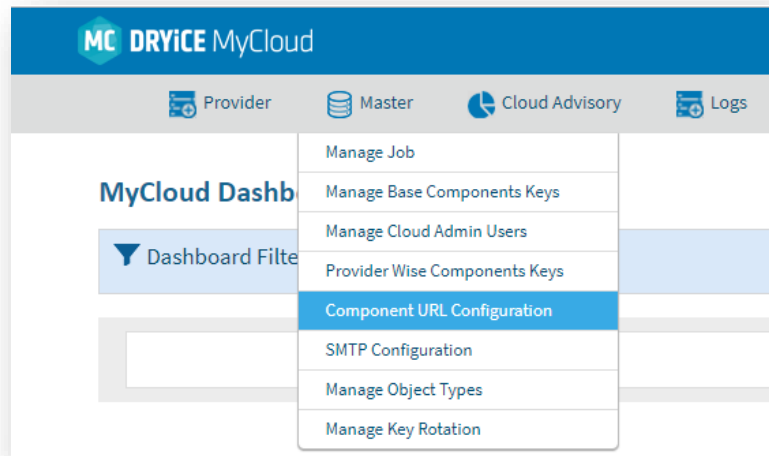


Figure 166 – Landing Page with selected Component URL Configuration

6. Select **Base** in the **Provider** dropdown and click on **Go** button.
7. Change the **URL** for the following Component Name(s):
 - **Workflow Service** from `http://<ip>:<port>/WorkflowService` to `https://<LBIP>:<port>/WorkflowService`
 - **Data Collector Billing and Advisory** from `http://<ip>:<port>/DataCollector` to `https://<LBIP>:<port>/DataCollector`
 - **ServiceNow Executer** from `http://<ip>:<port>/SnowService` to `https://<LBIP>:<port>/SnowService`
 - **Generic Service** from `http://<ip>:<port>/GenericService` to `https://<LBIP>:<port>/GenericService`
8. Select **{Provider}** in the **Provider** dropdown and click on **Go** button.
9. Change the URL for the following Component Name(s):
 - **Platform Data Sync** from `http://<ip>:<port>/SyncService` to `https://<LBIP>:<port>/SyncService`
 - **Performance Data Sync** from `http://<ip>:<port>/PerformanceDataCollector` to `https://<LBIP>:<port>/PerformanceDataCollector`
 - **Orchestrator Services** from `http://<ip>:<port>/OrchestratorService` to `https://<LBIP>:<port>/OrchestratorService`
 - **Active Directory** from `http://<ip>:<port>/ADService` to **Error! Hyperlink reference not valid.**
 - **Cisco Intersight Sync** from `http://<ip>:<port>/CiscoSyncService` to <https://<LBIP>:<port>/CiscoSyncService>

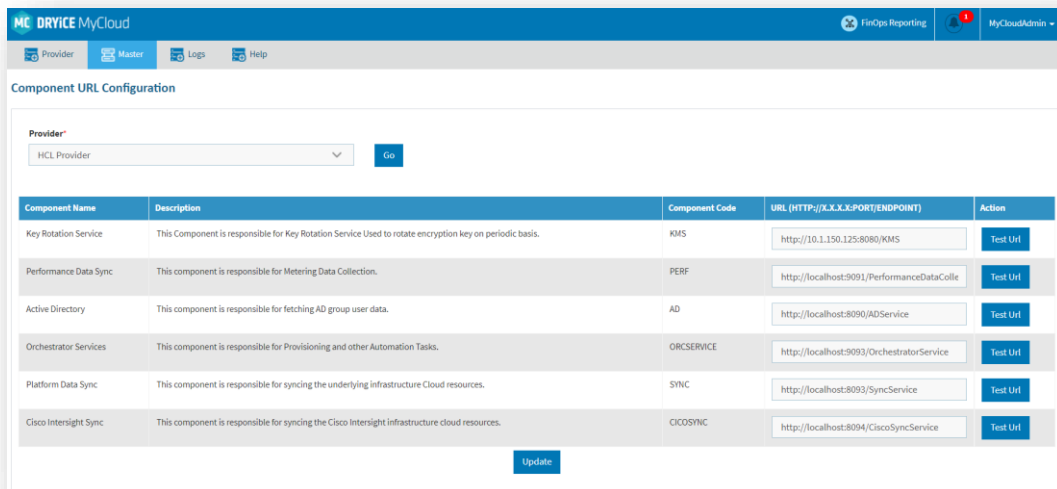


Figure 167 – Component URL Configuration

6.3.5 KRS Database String Encryption

1. Open Internet Manager.
2. Select **HCL.MyCloudKRS**.
3. Right click and Explore to the web.config under **KMS** folder.

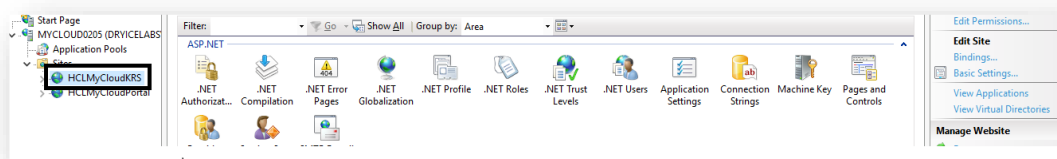


Figure 168 – Component URL Configuration

4. Open Web.Config.
5. By default, "EncryptedConnectionString" key is set to false. In case to use encrypted DB string, update key to True.

```
<appSettings>
  <add key="aspnet:UseTaskFriendlySynchronizationContext" value="true" />
  <add key="KeyRotationComponentCode" value="WebSite" />
  <add key="EncryptedConnectionString" value="false" />
  <!--<add key="MyCloud.Web.ConfigDB" value="OQvESS05WqZljGX59kgUH0igrfCmcuRBdEfXyP6s/ePK2mp1ZcGLzKrk1xFto/S0Ym9TsCu2IRMf
  <add key="MyCloud.Web.ConfigDB" value="server=10.1.160.19;database=MyCloudDBV101;User id=admin;Password=d5I111t2C1h9;M
  <add key="CertificateName" value="Hcl.MyCloud" />
  <add key="CertificateStoreLocation" value="2" />
  <!--CurrentUser = 1, LocalMachine = 2-->
  <add key="CertificateStoreName" value="7" />
  <!--AddressBook = 1, AuthRoot = 2, CertificateAuthority = 3, Disallowed = 4, My = 5, Root = 6, TrustedPeople = 7, Trus
  <add key="EncryptionSalt" value="560A18CD-6346-4CF0-A2E8-671F986B9EA9" />
```

Figure 169 – Component URL Configuration

This marks the completion of MyCloud Installation.

6.4 Update Webapi URL (Not Able to Login into Portal)

This section will provide the details, how to change the WebAPI URL, if admin user is not able to login into the application. To do that, the user must have the Service Account used as Application pool identity to run KRS Service. If user doesn't have the credentials, please contact MyCloud Admin or drop an email to MyCloud-Product-Supp@hcl.com.

To make the changes, user needs to follow the below steps:

1. Open **KRS** portal.

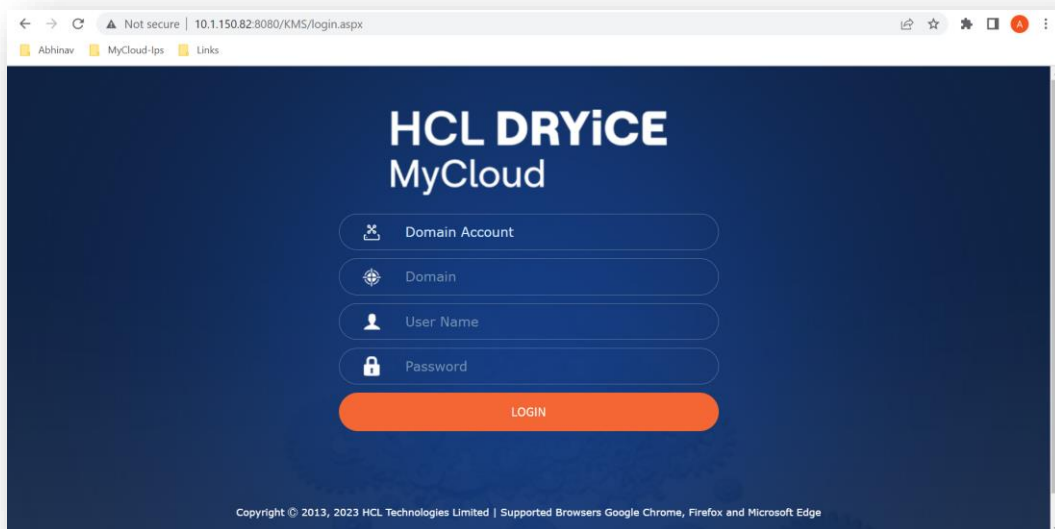


Figure 170 – KRS Login Screen

2. Login credentials of KRS portal are the same which were entered on the Server Configuration page of the Installer. For more details refer [Figure 50 – Server Configuration](#) Or in simpler terms, the Service Account used as Application pool identity to run KRS Service.
3. On successfully login, navigate to “**URL Configuration**” under Configurations menu.

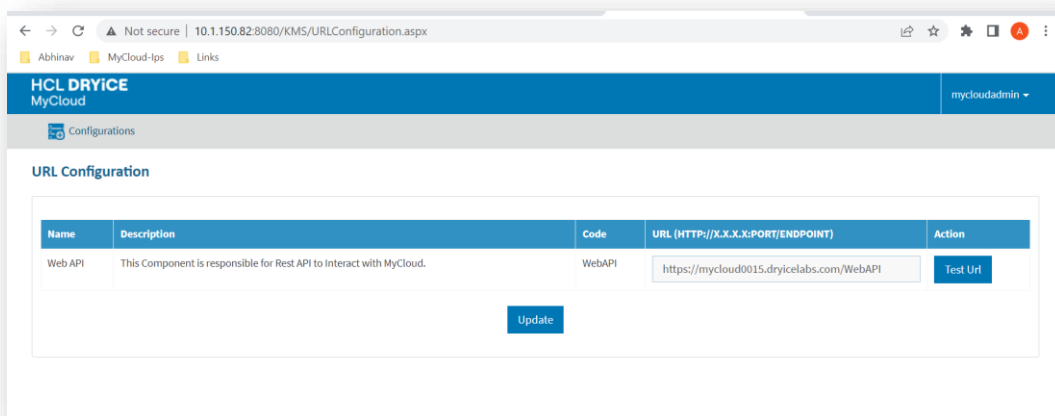


Figure 171 – Component URL Configuration in KRS

4. Now user can update the URL of WebAPI. User can also perform the Test URL connectivity.
5. Click on Update button to update the URL.

6.5 Update Ldap/Saml Configuration for Admin

This section will provide the details, how configuration LDAP and SAML for admin users. In order to do that, the user must have the Service Account used as Application pool identity to run KRS Service. If user doesn't have the credentials, please contact MyCloud Admin or drop an email to MyCloud-Product-Supp@hcl.com.

To make the changes, user needs to follow the below steps:

1. Open KRS portal.

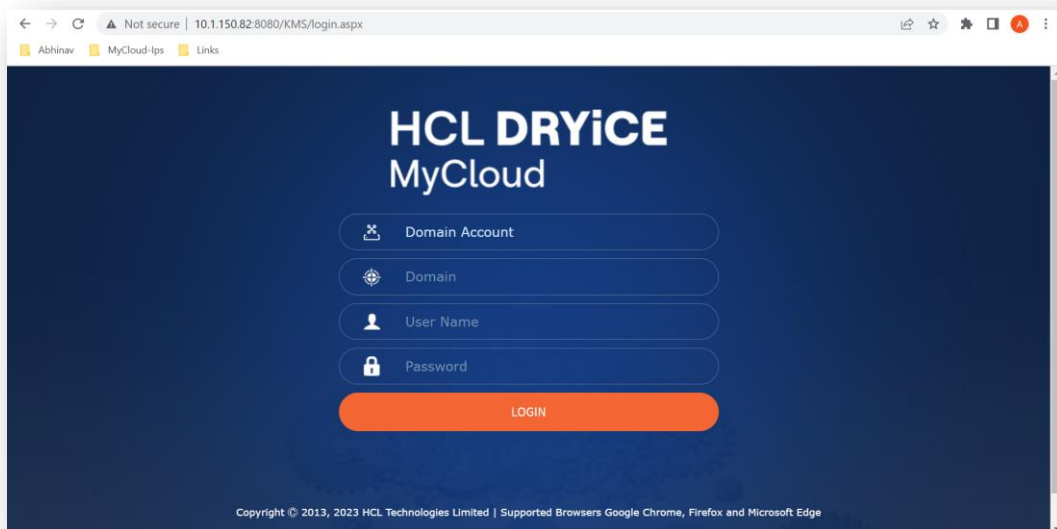


Figure 172 – KRS Login Screen

2. The login credentials of KRS portal are the same which were entered on the Server Configuration page of the Installer. For more details refer [Figure 50 – Server Configuration](#)
Or in simpler terms, the Service Account used as Application pool identity to run KRS Service.
3. On successfully login, navigate to **"Manage Admin User"** under Configurations menu.

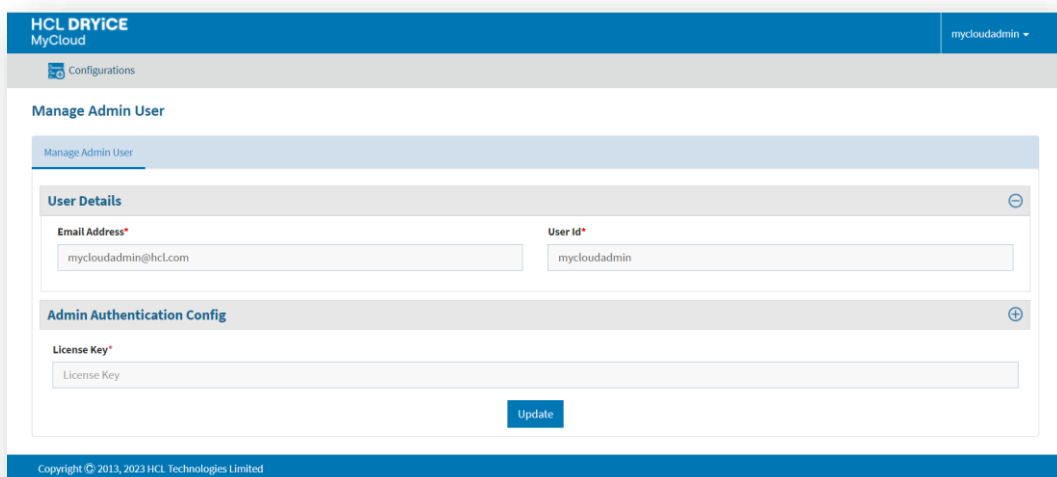


Figure 173 – Manage Admin User

4. Manage Admin user screen will appear.

5. The User Details sections will auto be populated with admin user information.
If a system contains more than one admin user, then any one admin user information will be auto filled. Using this admin user account, other admin users can be managed.
6. Following operations can be performed using this screen:
 - a. Update Admin Email address and User Id
 - b. Configure LDAP for Admin Users
 - c. Configure SAML for Admin Users
 - d. Change password for Admin User (In case of Form Based Authentication for admin users)

6.5.1 Update Admin Email and User Id

To update admin Email address or User id, follow the below steps:

1. Fill the details listed in the following table.

Figure 174 – Edit Manage Admin User Details

Refer the below table to understand the fields mentioned in the above figure:

Table 20 – Edit Manage Admin User Details

File Name	Description
Email Address	Admin Email Address
User Id	User Id of the Admin User. Mainly used in the case of Ldap and Saml configurations.
License Key	License Key of the Product.

2. Update the Email address or User Id
3. Enter License Key of the Product
4. Click on Update button.
5. A confirmation box will appear.

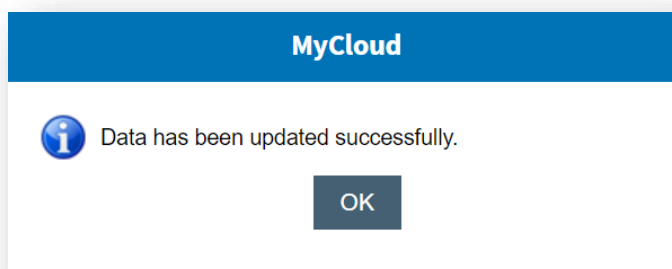


Figure 175 – Successful Update message – Manage Admin User

6.5.2 Configure LDAP Authentication

To configure LDAP authentication, follow the below steps:

1. Fill the details listed in the following table.

 The screenshot shows a web form titled "Manage Admin User". It has two main sections: "User Details" and "Admin Authentication Config".

 In the "User Details" section, there are two input fields: "Email Address*" with the value "mycloudadmin@hcl.com" and "User Id*" with the value "mycloudadmin".

 In the "Admin Authentication Config" section, there is a dropdown menu for "Authentication Type*" set to "LDAP". Below this are four input fields: "Domain Name*", "LDAP URL*" (with an information icon), "Domain Username*" (with an information icon), and "Domain Password*".

 At the bottom of the form is a "License Key*" section with a text input field containing "License Key". Below the input fields are two buttons: "Check Endpoint Connectivity" and "Update".

Figure 176 – Manage Admin User – LDAP Configuration

Refer the below table to understand the fields mentioned in the above figure:

Table 21 – Manage Admin User Details – LDAP Configuration

File Name	Description
Email Address	Admin Email Address
User Id	User Id of the Admin User. Mainly used in the case of Ldap and Saml configurations.
Authentication Type	Select LDAP from the drop down as LDAP authentication needs to be configured.
Domain Name	Name of the domain
LDAP URL	It is a string that is used to encapsulate the address and port of a directory server.
Domain Username	It is used to specify a user account in the selected domain.
Domain User Password	It is used to authenticate the username in the domain.
License Key	License Key of the Product.

2. Enter License Key of the Product

3. Click on Update button to update the configuration.
4. A confirmation box will appear.

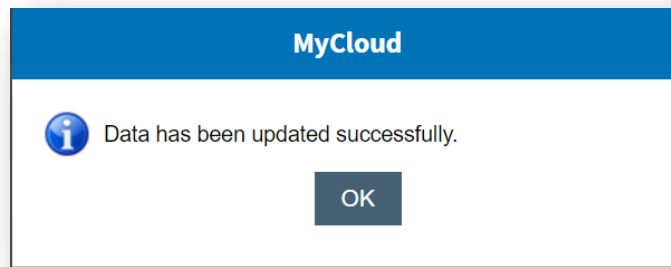


Figure 177 – Manage Admin User – LDAP Configuration – Saved Successfully

All the fields marked with an asterisk (*) are mandatory.

6.5.3 Configure SAML Authentication

To configure SAML authentication, follow the below steps:

1. Fill the details listed in the following table.

Figure 178 – Manage Admin User – SAML Configuration

Refer the below table to understand the fields mentioned in the above figure:

Table 22 – Manage Admin User Details – SAML Configuration

File Name	Description
Email Address	Admin Email Address
User Id	User Id of the Admin User. Mainly used in the case of Ldap and Saml configurations.
Authentication Type	Select SAML from the drop down as SAML authentication needs to be configured.
SSO Id	Identity Provider might need this to establish the identity of the service provider requesting the login. Basically, it is used for handshaking of the application.
SSO URL	Identity Provider Single Sign-on URL, where our website redirect for

	Authentication.
Name Id	NAMEID is the complete path of xmlnode where NameID value (USERNAME/EMAIL) exist. It based on identity provider.
SSO Tool	Tool used to configure Single Sign On.
Logout URL	Identity Provider Single Sign-on URL, used to logout the URL from SSO login.
License Key	License Key of the Product.

2. Enter License Key of the Product
3. Click on Update button to update the configuration.
4. A confirmation box will appear.

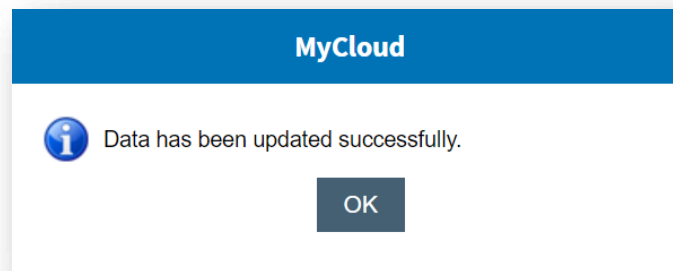


Figure 179 – Manage Admin User – SAML Configuration – Saved Successfully

All the fields marked with an asterisk (*) are mandatory.

6.5.4 Change Admin User Password (Form based Authentication Type)

To change the password of admin user when authentication type authorization is configured, follow the below steps:

1. Fill the details listed in the following table.

 A screenshot of the 'Manage Admin User' web interface. The form is divided into two main sections: 'User Details' and 'Admin Authentication Config'.

 The 'User Details' section contains two input fields: 'Email Address*' with the value 'mycloudadmin@hcl.com' and 'User Id*' with the value 'mycloudadmin'.

 The 'Admin Authentication Config' section contains a dropdown menu for 'Authentication Type*' set to 'Form Based'. Below this is a checkbox labeled 'Change admin user password' which is checked. To its right is a 'Password*' input field and a 'Generate Password' button. At the bottom of this section is a 'License Key*' input field with the placeholder text 'License Key'.

 An 'Update' button is located at the bottom right of the form.

Figure 180 – Manage Admin User – Form Based – Change Password

Refer the below table to understand the fields mentioned in the above figure:

Table 23 –Manage Admin User Details –Change Password

File Name	Description
Email Address	Admin Email Address
User Id	User Id of the Admin User. Mainly used in the case of Ldap and Saml configurations.
Authentication Type	Select SAML from the drop down as SAML authentication needs to be configured.
Change admin user password	Identity Provider might need this to establish the identity of the service provider requesting the login. Basically, it is used for handshaking of the application.
License Key	License Key of the Product.

2. Check the checkbox for change admin user password.
3. Click on Generate Password.
4. Copy the password by clicking on Copy Password button.
5. Enter License Key of the Product
6. Click on Update button to update the configuration.
7. A confirmation box will appear.

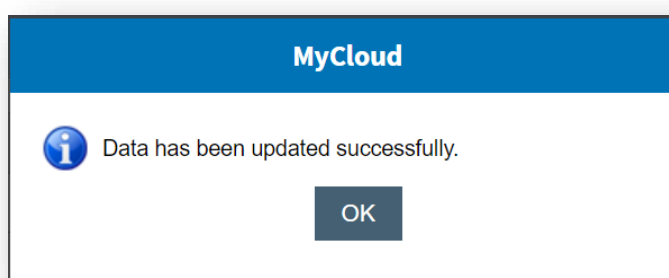


Figure 181 – Manage Admin User – Form Based – Change Password – Save Successfully

All the fields marked with an asterisk (*) are mandatory.

6.6 Manage White Resource Lists

A new section in KRS application,

Root Admin/Service Account User can add URLs and Python Import modules into the White Source listed Module. From this screen - User can perform Test Urls only with white sources URLs.

Manage Custom Script - User is not able to create new PowerShell scripts. Existing PowerShell script is working without any concerns. Managing Custom Script is working with API and with Actions.

Using Manage Custom Scripts with API, then it is validating URLs and Import modules with Whitelisted resources.

To do that, the user must have the Service Account used as Application pool identity to run KRS Service. If user doesn't have the credentials, please contact MyCloud Admin or drop an email to MyCloud-Product-Supp@hcl.com.

To make the changes, user needs to follow the below steps:

1. Open **KRS** portal.

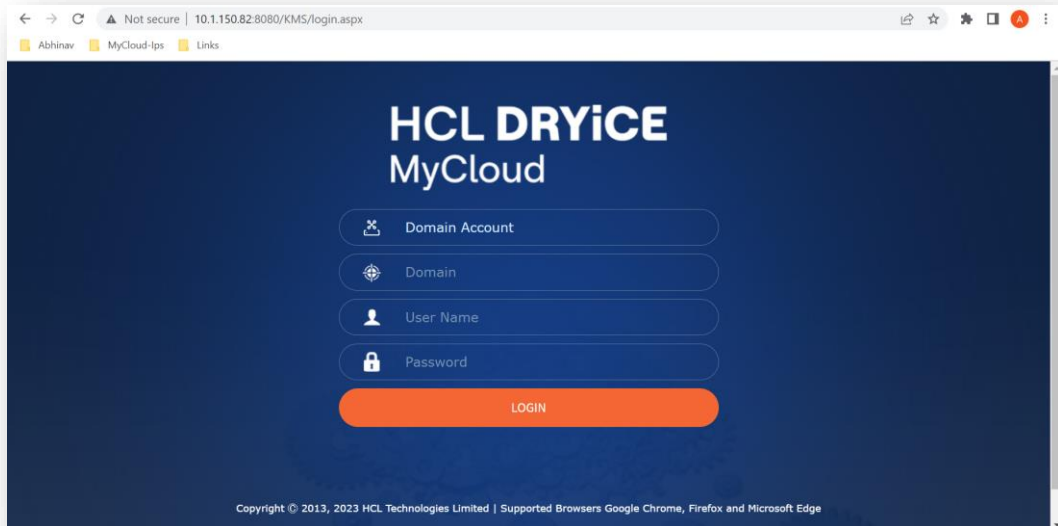


Figure 182 – KRS Login Screen

2. Login credentials of KRS portal are the same which were entered on the Server Configuration page of the Installer. For more details refer [Figure 50 – Server Configuration](#) Or in simpler terms, the Service Account used as Application pool identity to run KRS Service.
3. On successfully login, navigate to “**Manage white resources**” under Configurations menu.

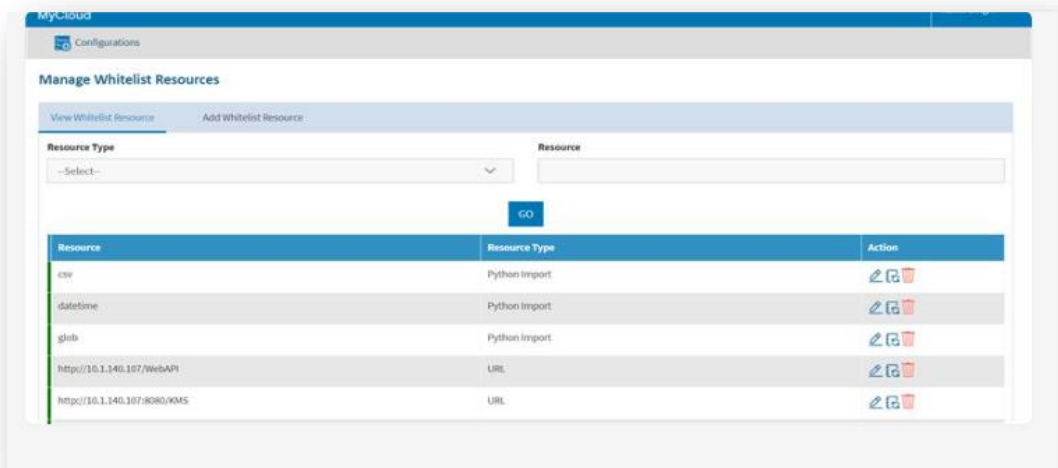


Figure 183 – Manage White Resource Lists

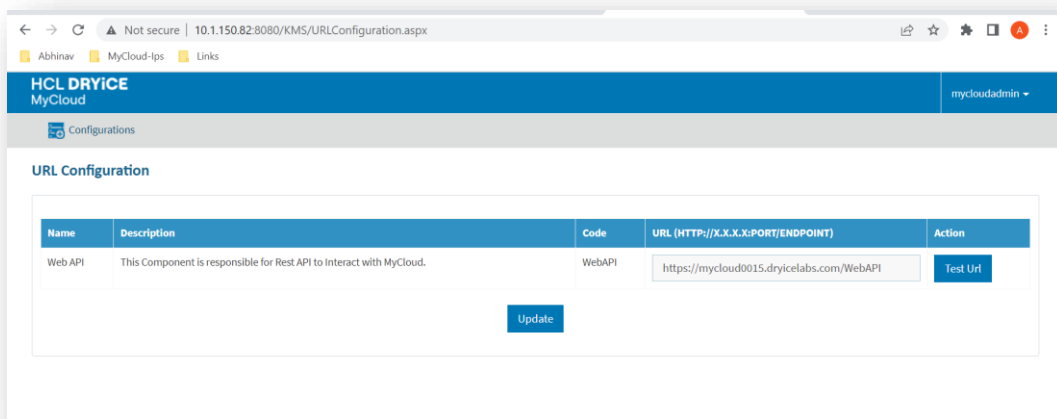
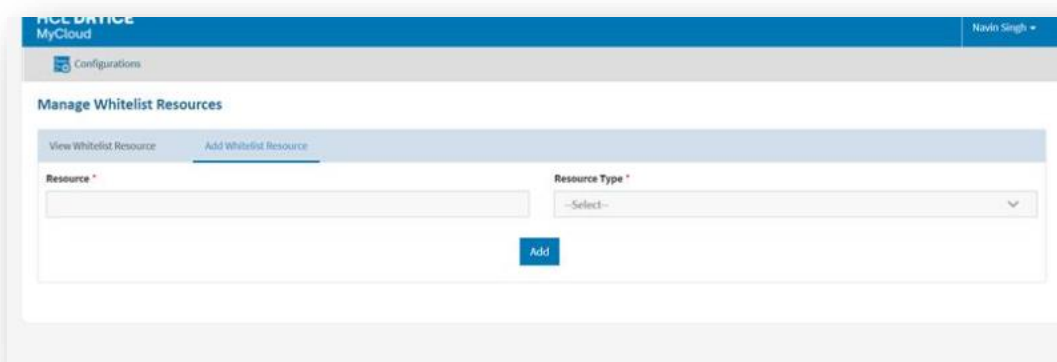


Figure 184 – Manage White Resource Lists (Cont.)

4. Fill the details listed in the following table.



Refer below table to understand the fields mentioned in the above figure:

Table 24 – Add White Resource

File Name	Description
Resource	Url or module name to include in white resource lists
Resource Type	Resource Type (Possible values are: Python and URL) to mention the type of resource include in white resource lists

5. After fill all information Click on Add button to information
6. A success message dialogue box will appear.

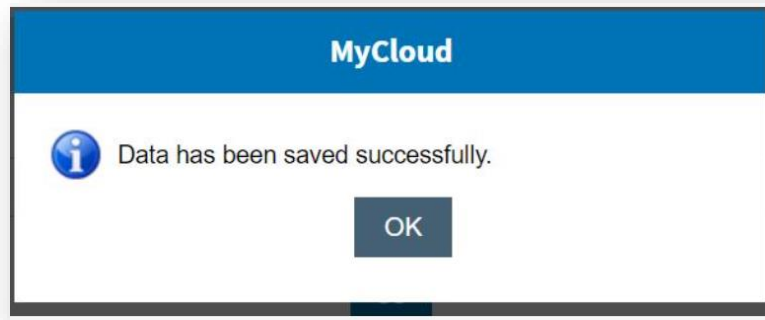


Figure 185 – Success Message

6.7 Rotate Encryption Key

Using this Encryption Key all secret information is encrypted and saved into the database.

Through this module, the user can rotate the Encryption Key for the application. Rotation of the Encryption Key is to be performed by taking the down time of the application. It has the following modules:

- [Key Rotation](#)
- [Key Rotation History](#)

To do that, the user must have the root credentials and login into KRS portal. If user doesn't have the credentials, please contact MyCloud Admin or drop an email to MyCloud-Product-Supp@hcl.com.

6.7.1 Key Rotation

It is advised to plan a scheduled downtime for Web Application during the rotation of Encryption Key.

Once the status of the request is completed, then restart the IIS on all Application Servers. Listener and Generic Service should be in running status.

To rotate the Encryption Key, user need to follow the below steps:

1. Click on Encryption Key Rotation under Configurations Menu and then click on Key Rotation.

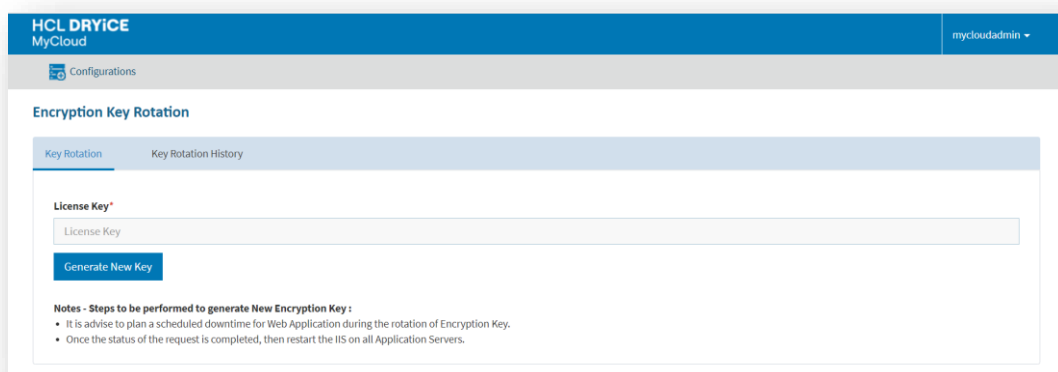


Figure 186 – Encryption Key Rotation

2. Enter the Product License Key
3. Click on Generate New Key
4. A pop message appears for confirmation as shown below.

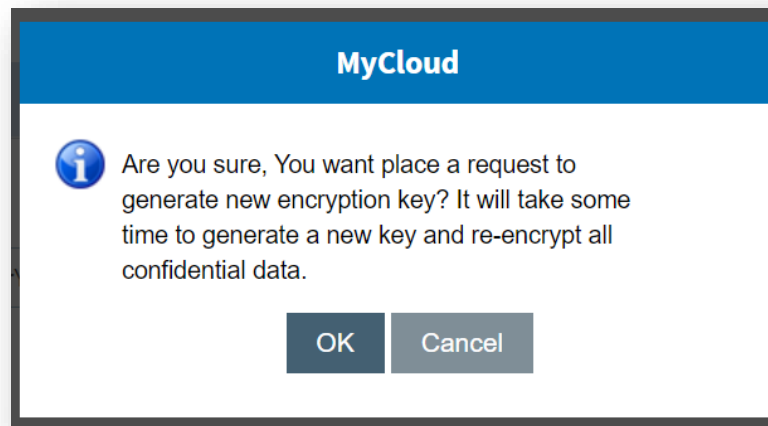


Figure 187 – Encryption Key Rotation – Confirmation Message

5. Click **OK** to generate the new Encryption Key.
6. Click **Cancel** to discard the changes.
7. On Clicking Ok, Request Id for rotating Encryption Key is generated, Background job will be triggered, this job will generate new Encryption Key and all data will be encrypted with new Encryption Key.

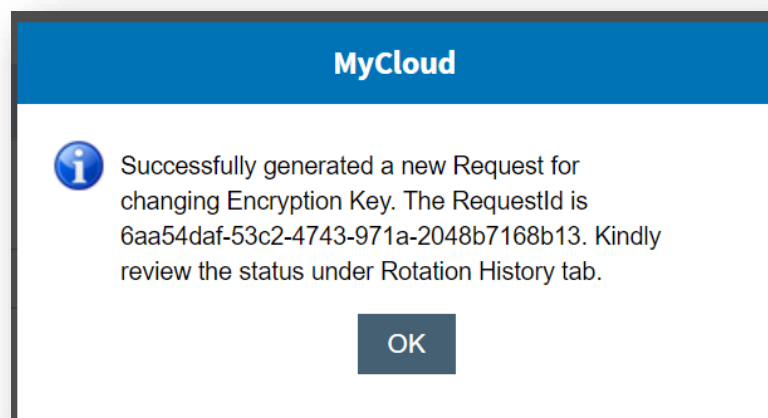


Figure 188 – Encryption Key Rotation – Request Successful Message

8. Now click on Key Rotation History tab and review the Status of the respective Request Id.

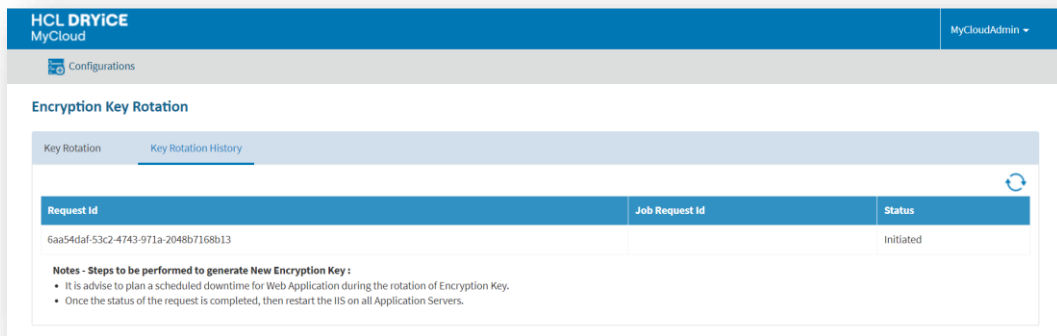


Figure 189 – Encryption Key Rotation History

6.7.2 Key Rotation History

To review the Rotate Encryption Key History and status of all Rotation Key requests, user need to follow the below steps:

1. Click on Rotate Encryption Key under Configurations Menu and then click on Key Rotation History.
2. The screen lists the last five Key Rotation execution.

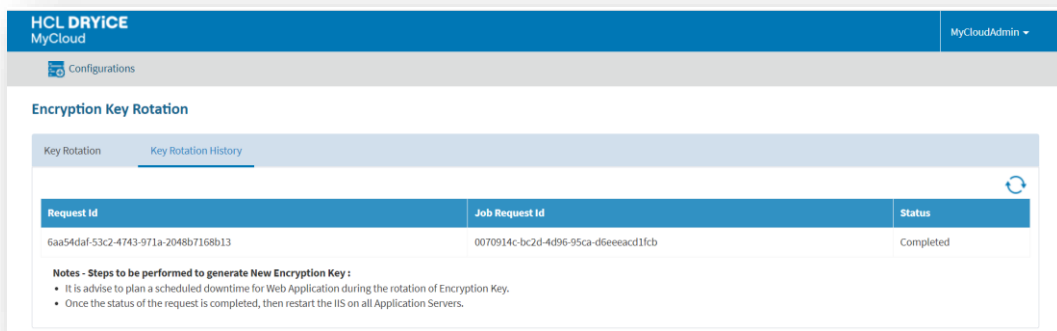


Figure 190 – Encryption Key Rotation History 2

7 Support

To get support for this product, please drop an email to MyCloud-ProdSupport-Team@hcl-software.com.

HCLSoftware

hcltechsw.com