**Infosys Script Control Center – Installation Document**

**Sep-2022**

COPYRIGHT NOTICE

© 2022 Infosys Limited, Bangalore, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/or any named intellectual property rights holders under this document.

Infosys Limited

Electronic City,

Hosur Road,

Bangalore 560 100

India.

Telephone: 91 80 2852 0261

Fax: 91 80 2852 0362

Website: http://www.infosys.com

**Table of Contents**

[1. Prerequisites 4](#_Toc115168781)

[2. Installation package 4](#_Toc115168782)

[3. Database server: 6](#_Toc115168783)

[3.1 Prerequisites 6](#_Toc115168784)

[3.2 Add SQL Server Port to Windows firewall 6](#_Toc115168785)

[3.3 Database Creation 8](#_Toc115168786)

[4. Web Server 10](#_Toc115168787)

[4.1 Prerequisites 10](#_Toc115168788)

[4.2 Script Control Center API Setup 13](#_Toc115168789)

[5. Update Application Configuration 23](#_Toc115168790)

[6. Import Script Library 26](#_Toc115168791)

[7. User Access Management 26](#_Toc115168792)

[8. Utilities 26](#_Toc115168793)

[8.1 Export/Import Utility 26](#_Toc115168794)

[8.1.1 Export Functionality 26](#_Toc115168795)

[8.1.2 Import Functionality 29](#_Toc115168796)

[8.2 Administration Utility 32](#_Toc115168797)

[9. Enable Remote Execution 35](#_Toc115168798)

[10. Troubleshooting 36](#_Toc115168799)

[10.1 REST Services 36](#_Toc115168800)

[10.2 Cannot connect to SQL Server 36](#_Toc115168801)

[11. FAQ 37](#_Toc115168802)

# Prerequisites

1. Following software/components need to be installed on the target server:

SQL Server Standard Edition 2012,2014 or 2016

SQL Server Management studio v18

* Operating System: Windows Server 2012 R2 - 64-bit, 2016 R2 - 64-bit.
* .NET Framework 4.5
* MS Internet Information Services (IIS) v8.5, v10
* PowerShell 3.0 for running scripts remotely

1. Minimum Hardware/System Specification:

* Dual core CPU
* 4 GB RAM
* HDD 500 GB

1. Windows Service Account

# Installation package

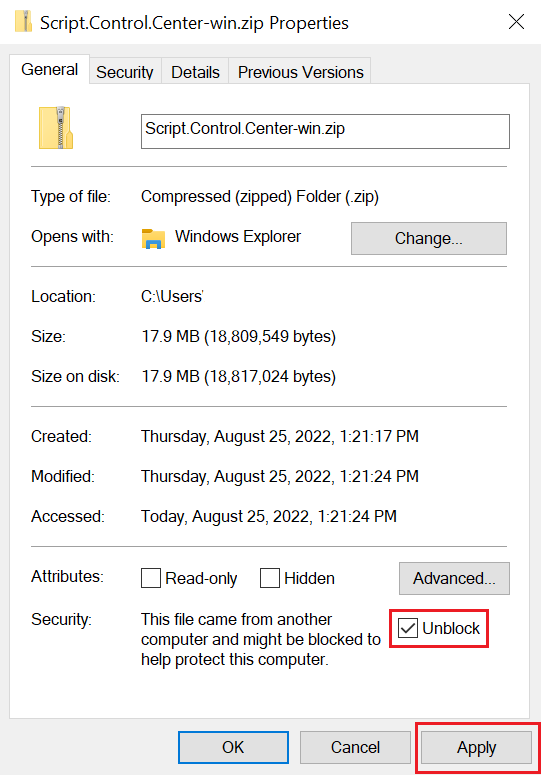
Installation package contains following:

* Database creation script
* Database master data creation script
* REST services creation related files
* Utilities related files

Installation Package is available at location –

**Release 1.0\Infosys\ScriptControlCenter**

Download the release package and unblock the zip file before extracting. To unblock, right click on the zip file > properties > Under General tab, select the Unblock checkbox > Apply > Ok



Extract all the zip files present under above location and save it at proper location on target server. It has following folders –

|  |  |
| --- | --- |
| **Server Folder** | **Target location** |
| db.zip | <Drive>:\Infosys\ScriptControlCenter\db (Ex: C: \Infosys\ScriptControlCenter\db) |
| services.zip | <Drive>:\Infosys\ScriptControlCenter\services |
| utilities.zip | <Drive>:\Infosys\ScriptControlCenter\utilities |
| references.zip | <Drive>:\Infosys\ScriptControlCenter\references  Copy “**Infosys.Lif.IisDoc.dll**” from target location to below locations  C:\Infosys.IntegrationLib\References\  And  C:\IAP\References\ |
| scripts.zip | <Drive>:\Infosys\ScriptControlCenter\scripts |

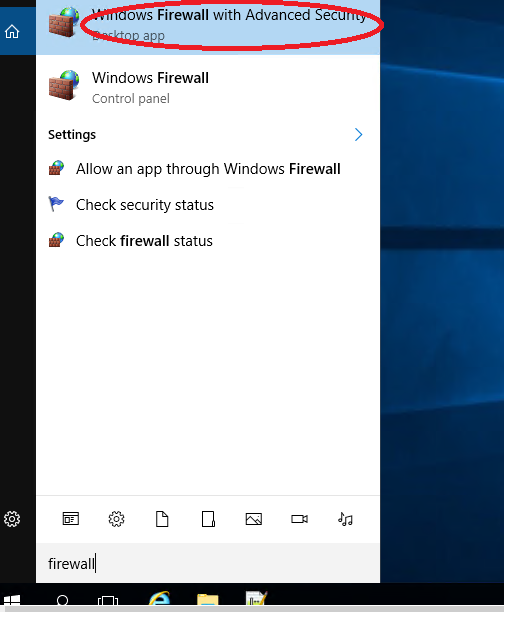
# Database server:

## Prerequisites

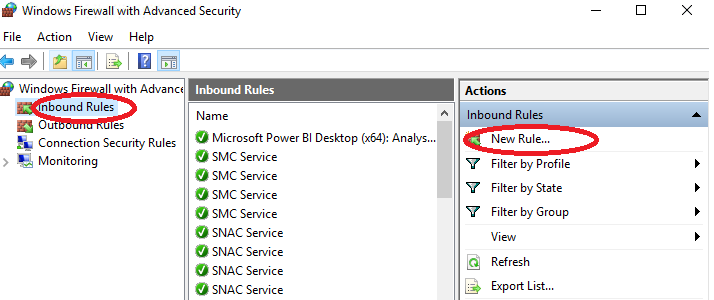
* + - * SQL server Standard Edition 2012,2014 or 2016 has been installed
      * SQL Server Management studio v18 has been installed
      * Windows Service account is required for windows integrated security.

## Add SQL Server Port to Windows firewall

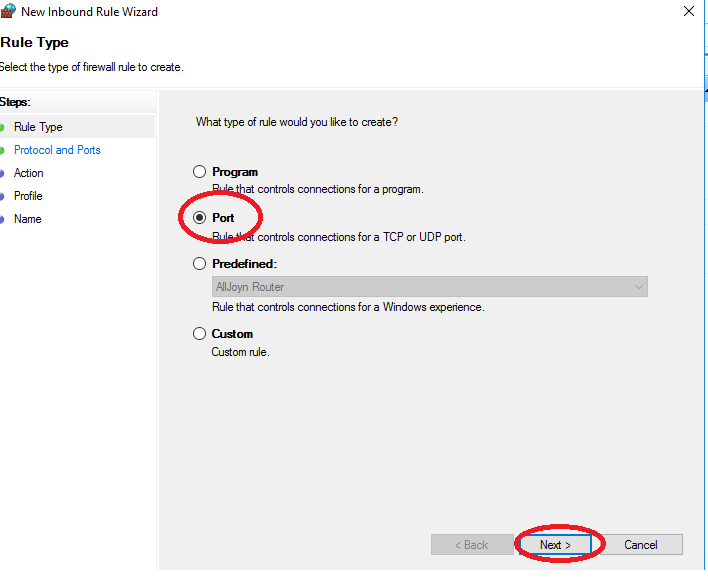
* + Click Start, type “Firewall” into the search box, and then click on “Windows Firewall with Advanced Security.”



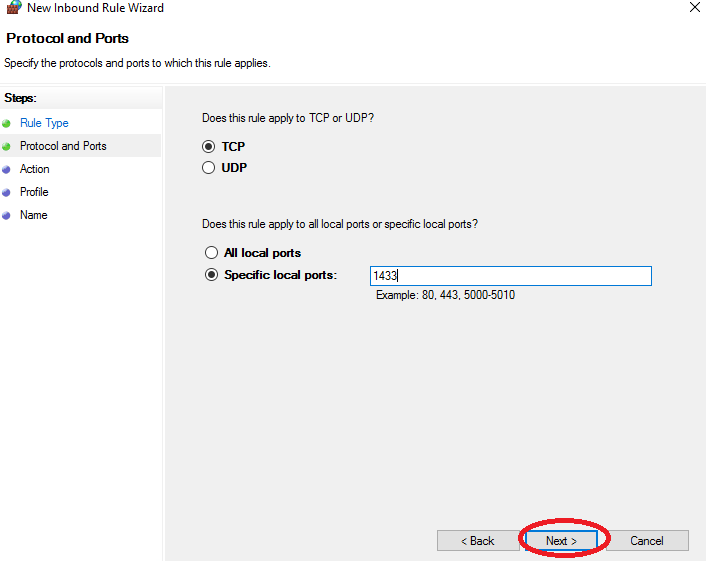
* + Click the “Inbound Rules” category on the left. In the far right pane, click the “New Rule” command.



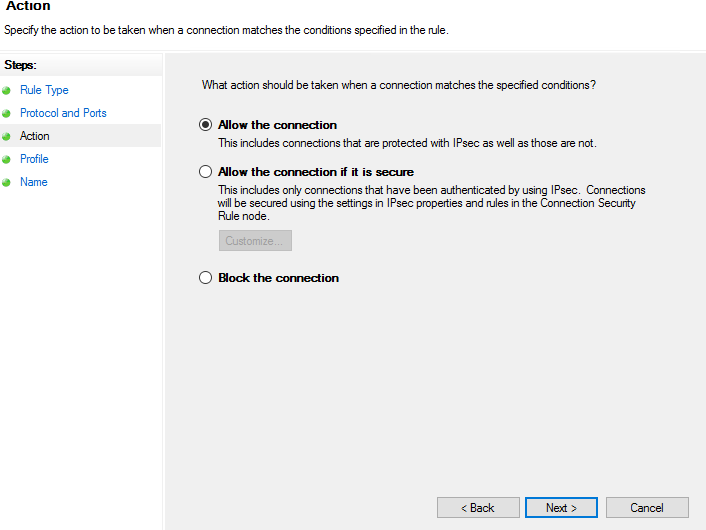
* + On the Rule Type page, select the “Port” option and then click “Next.”



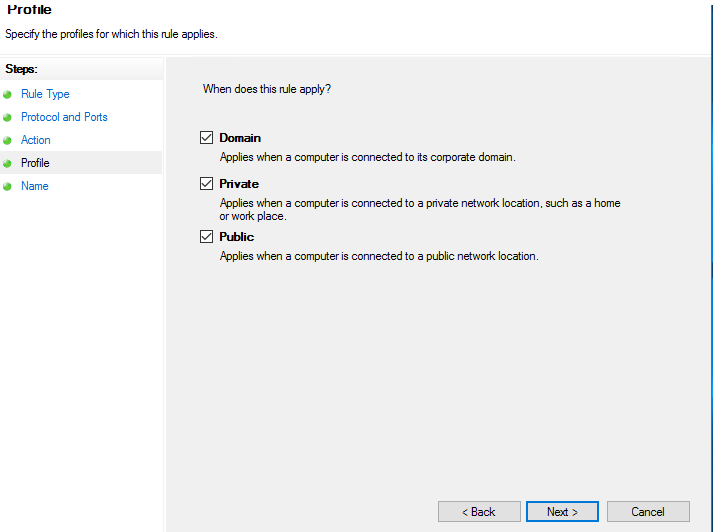
* + Enter the Port Number 1433 and click “Next”



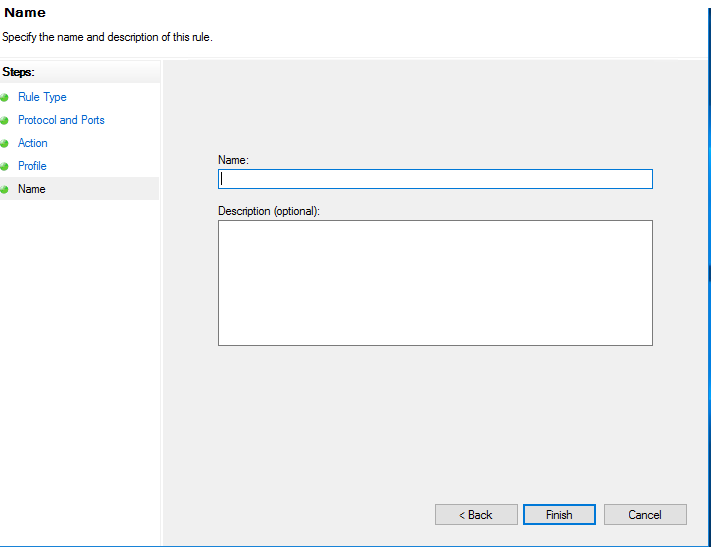
* + On the next page, click “Allow the Connection” and then click “Next.”



* + choose All the rules and click “Next.”

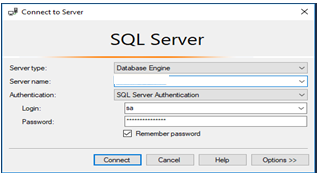


* + Give your new rule a name and an optional, more detailed description. Click “Finish” when you’re done



## Database Creation

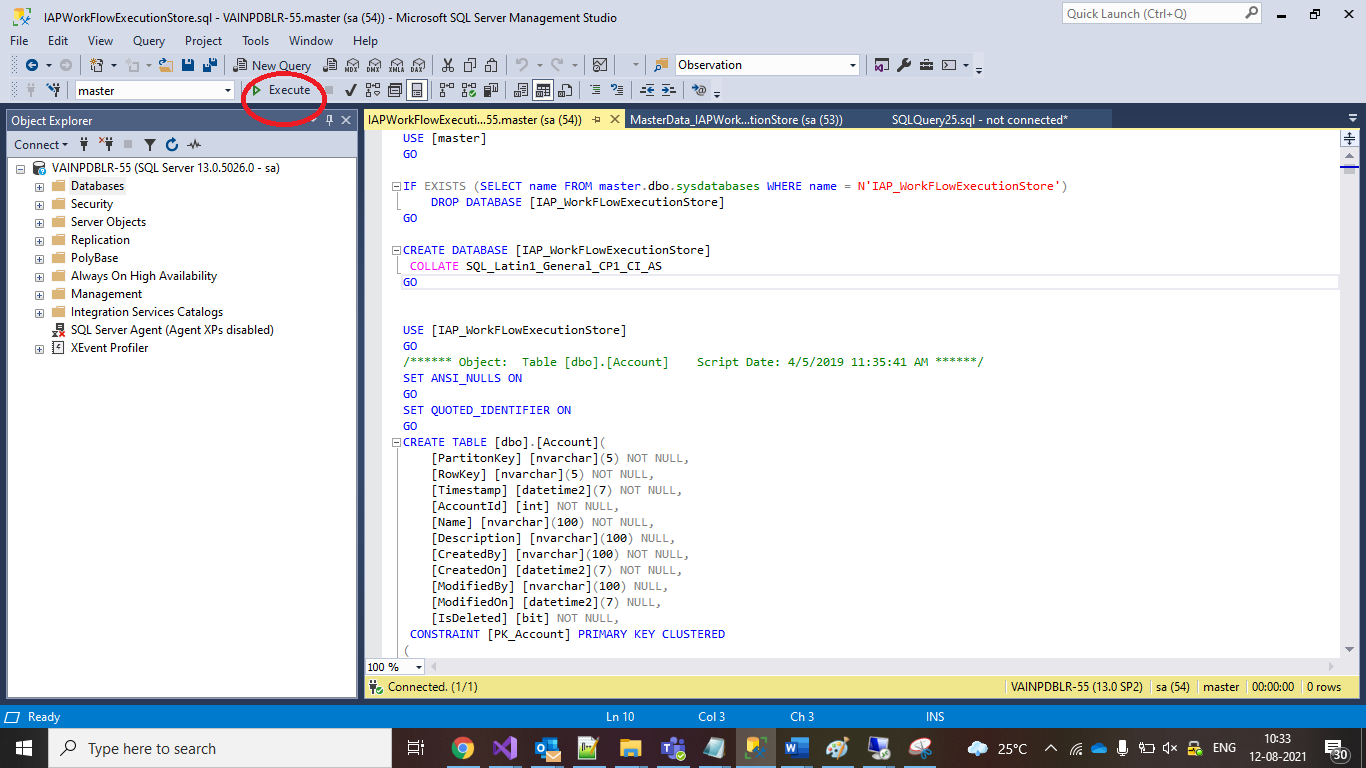
1. Login to Sql server on target machine

****

1. Ensure that Database folder ‘db’ copied to target location from deployment package on server and execute script in following sequence .

|  |  |
| --- | --- |
| **Script** | **Remarks** |
| IAPWorkflowExecutionStore.sql | Execute the script to create DB And tables |
| CreateObjects\_IAPWEM\_Logs.sql | Execute the script to create db and tables for logging |
| MasterData\_IAPWEM\_Logs.sql | Execute the script to insert master data to IAPWEM\_Logs db |
| Object\_IAPContentStore.sql | Execute the script to create db and tables for Content store |

* 1. Go to File > Open > File > Choose IAP\_WorkflowExecutionStore.sql file > Press Open > the file will be opened within SQL Server Management Studio, press Execute button.



* 1. Go to File > Open > File > Choose CreateObjects\_IAPWEM\_Logs.sql file > Press Open > the file will be opened within SQL Server Management Studio, press Execute button.
  2. Go to File > Open > File > Choose MasterData\_IAPWEM\_Logs.sql file > Press Open > the file will be opened within SQL Server Management Studio, press Execute button.
  3. Go to File > Open > File > Choose Object\_IAPContentStore.sql file > Press Open > the file will be opened within SQL Server Management Studio, press Execute button.

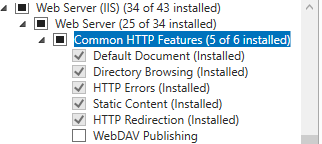
# Web Server

## Prerequisites

* + IIS v8.5 or v10 has been installed
  + Windows Service account is required for authentication and authorization.
  + Admin privilege required for IIS
  + Make sure following features are installed while installing IIS –

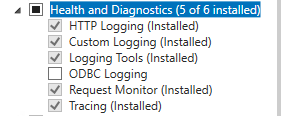
1. Go to Turn Windows Features On or Off
   1. Web Server (IIS)
      1. Common Http features

Check in the below features as shown in the figure below



* + 1. Health and Diagnostics

Check in the below features as shown in the figure below



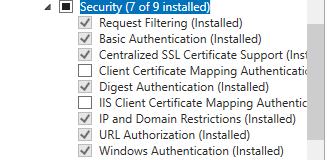
* + 1. Performance

Check in the below features as shown in the figure below



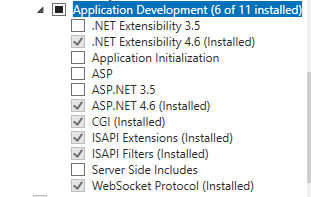
* + 1. Security

Check in the below features as shown in the figure below



* + 1. Application Development Features

Check in the below features and install as shown in the figure below



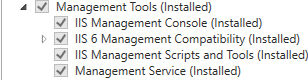
* 1. FTP Server

Check in the below features and install as shown in the figure below



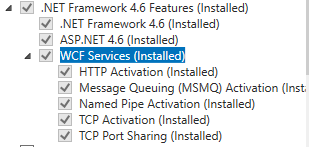
* 1. Management Features

Check in the below features and install as shown in the figure below



* 1. Click on Next
  2. .NET Framework 4.6 Features

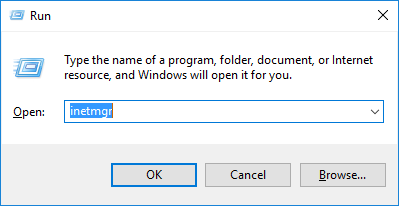
Check in the below features and install as shown in the figure below



* 1. Click on Install

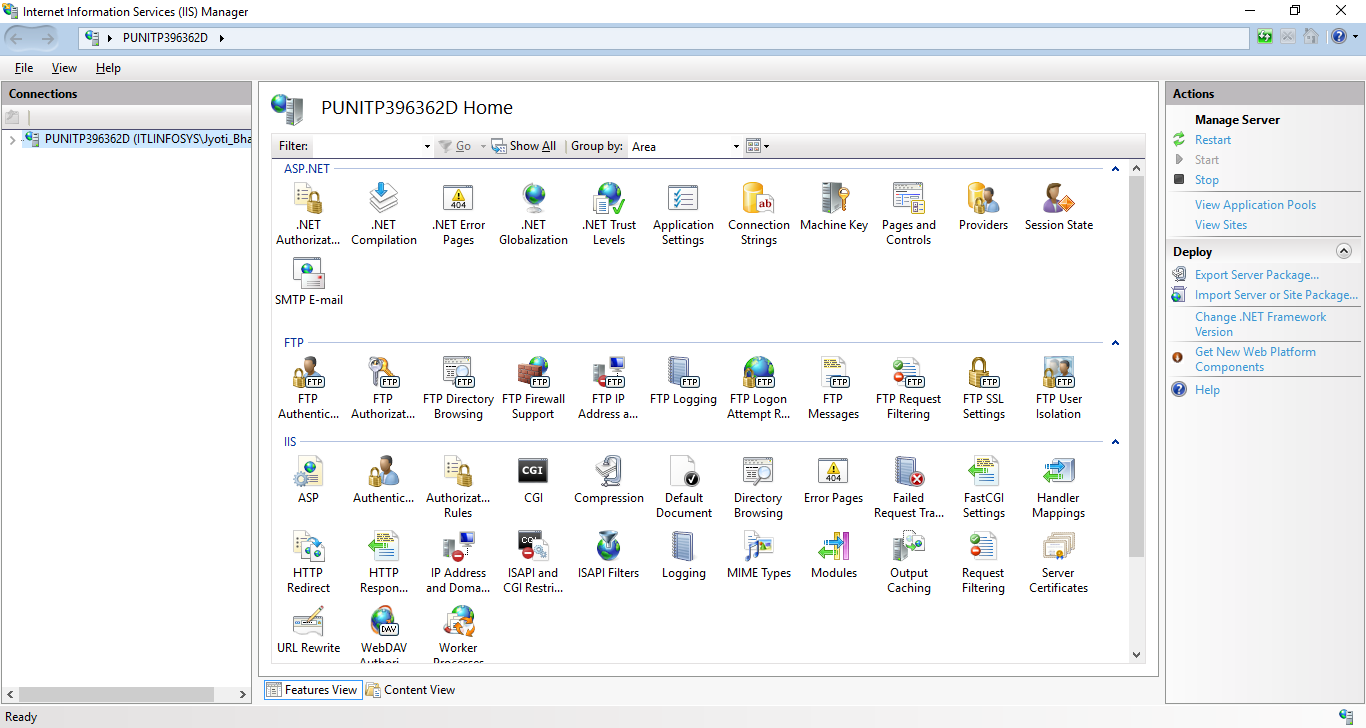
## Script Control Center API Setup

1. Open IIS. Go to run and type inetmgr.

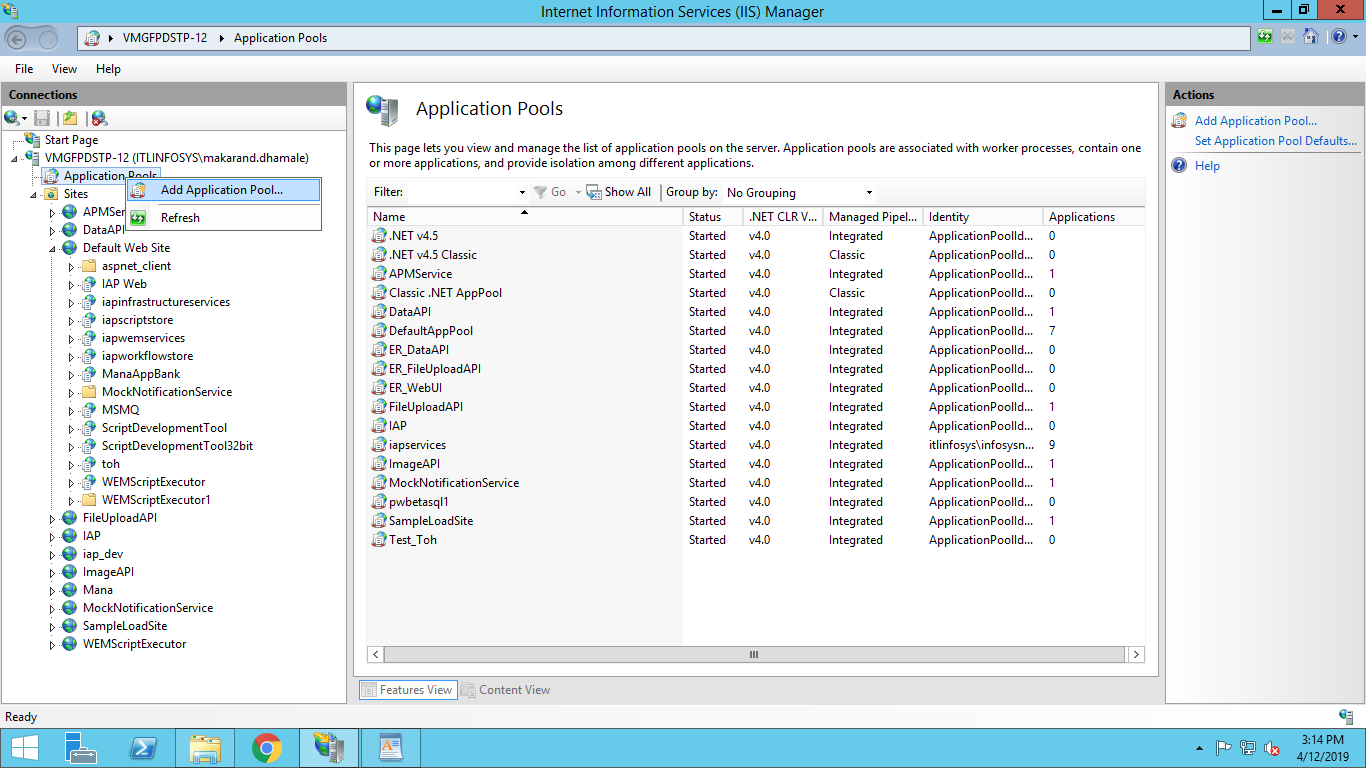
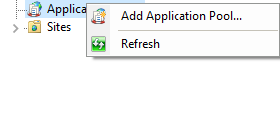


Click Yes

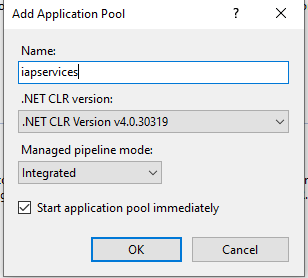




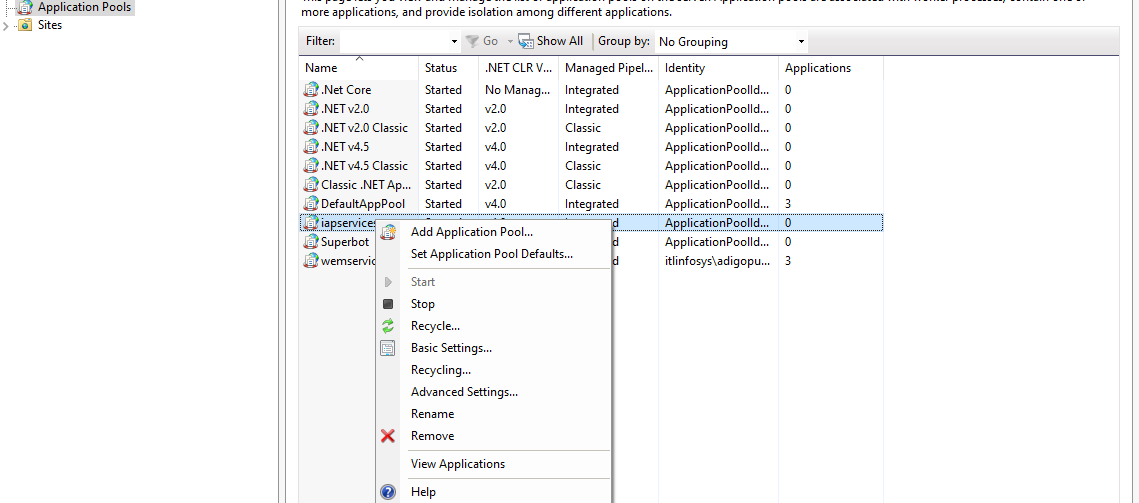
1. Once IIS is opened, expand the machine name listed on left hand side.
2. Right Click on Application Pool and select Add Application Pool to create an application pool required for the application.



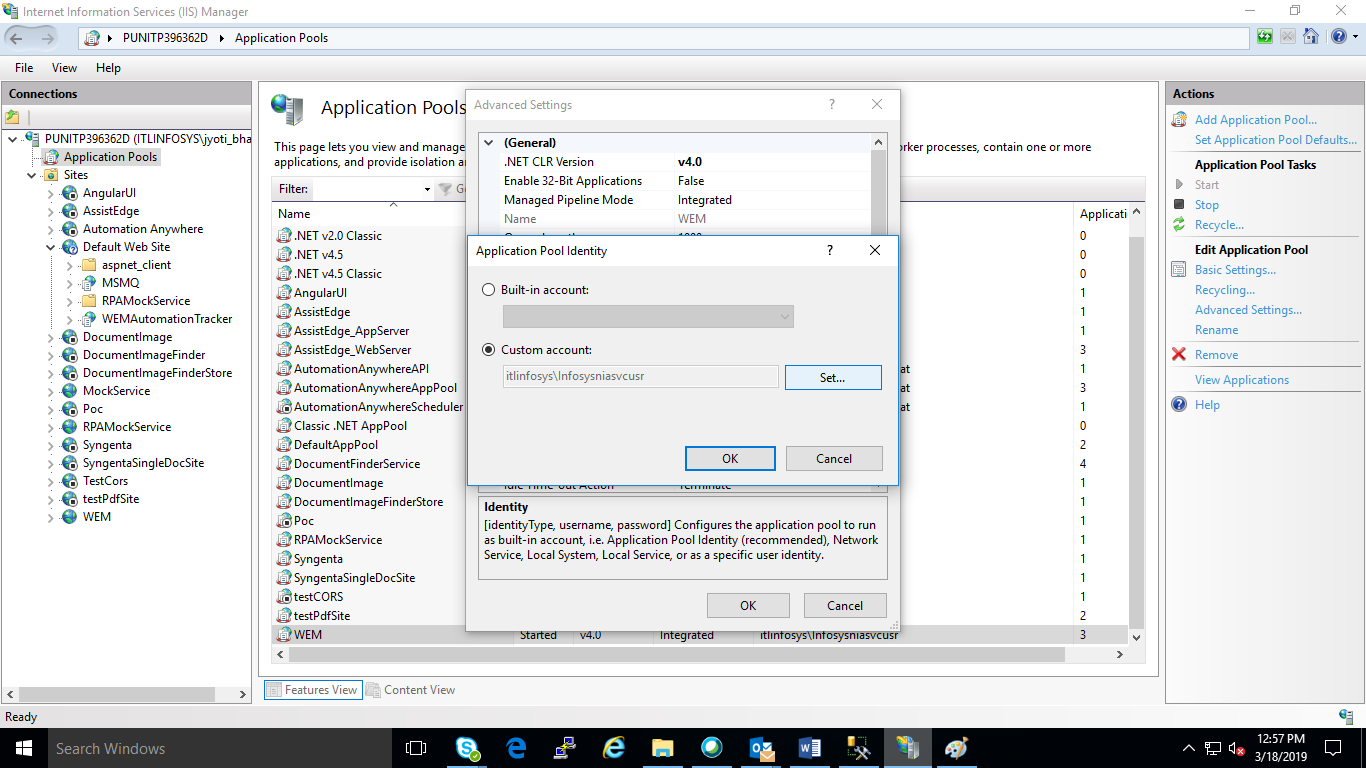
1. Provide application pool name as “**iapservices”**



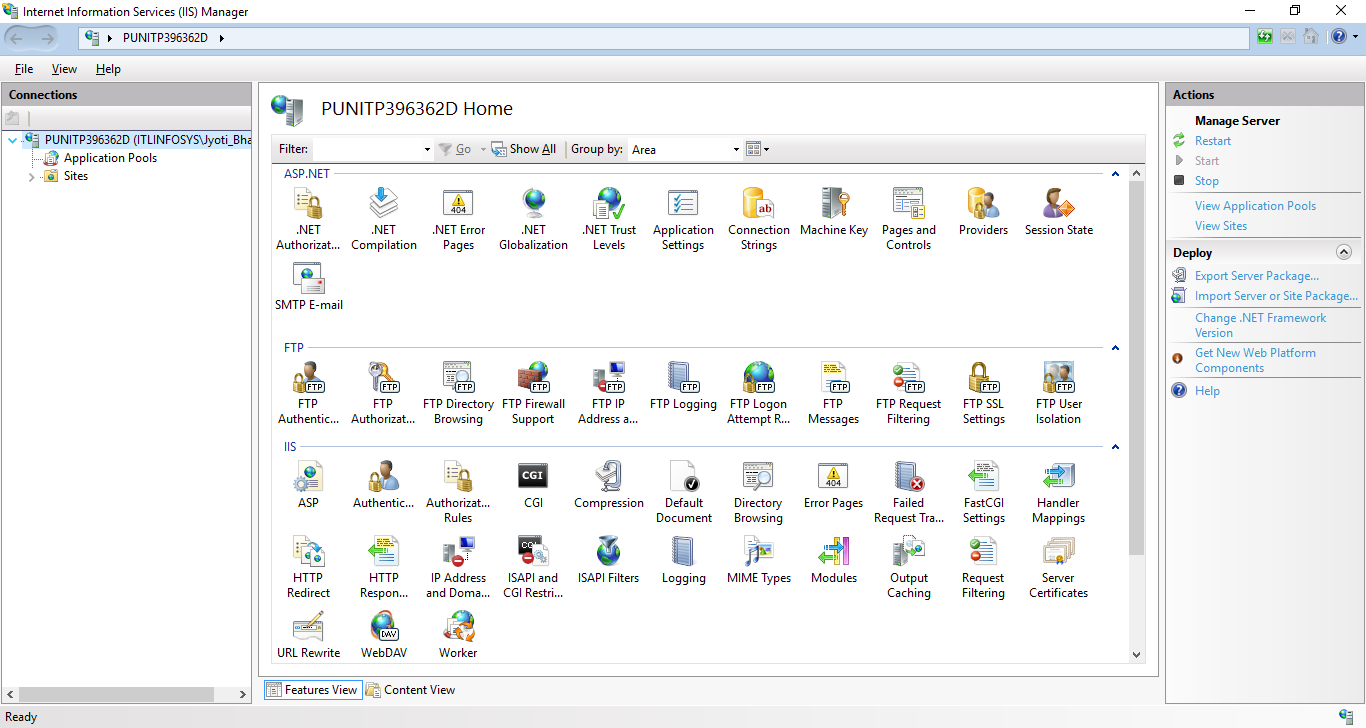
1. Change app pool account to service account
2. Select application pool and right click and select advanced settings



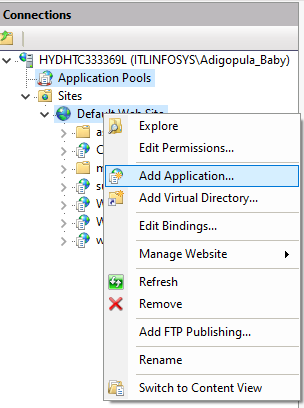
1. Select custom account and set the username and password for the service account.



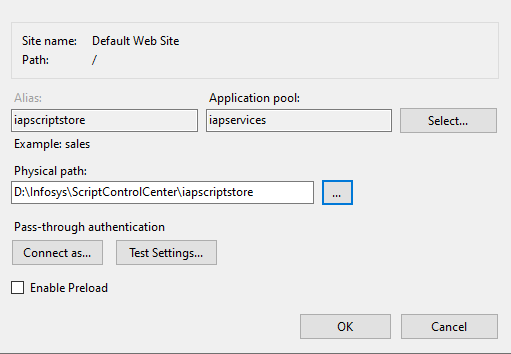
1. After that expand sites.



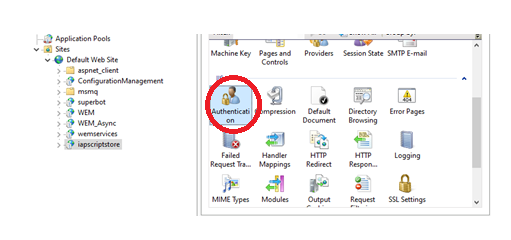
1. Create a REST service with name “iapscriptstore” in IIS and map it to physical location where respective web.config of “iapscriptstore” service have been copied
2. Expand Sites and Right click on “Default Web Site” and click on “Add application”



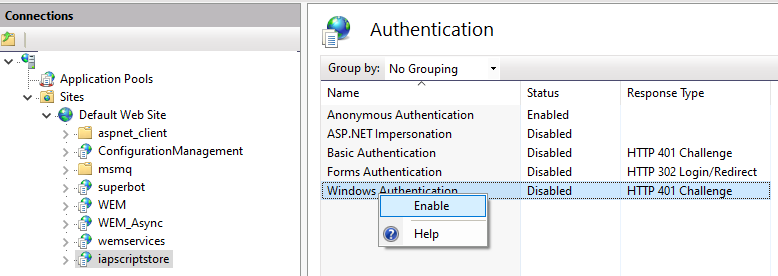
1. Enter the Alias as REST Service name i.e., “iapscriptstore” and select Application pool as “iapsesrvices” and Enter/Select the physical path of the service on targeted machine



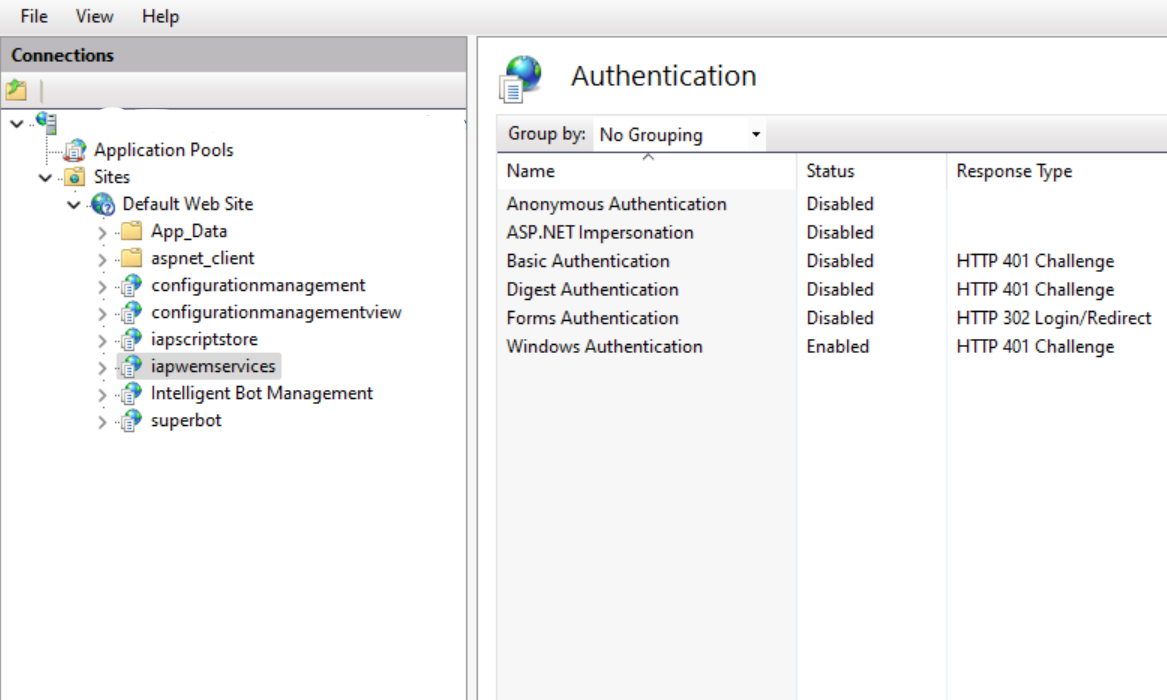
1. Click “OK” button, it will add web service with name “iapscriptstore” on IIS.
2. Set authentication to windows.
   * 1. Click on the Authentication



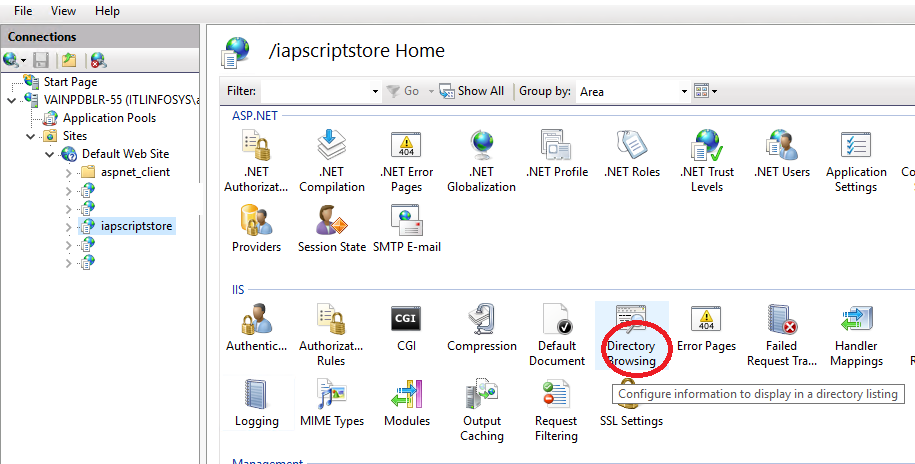
* + 1. It will open the “Authentication” window as shown in below screen shot where it needs to select “Window Authentication” row in list.



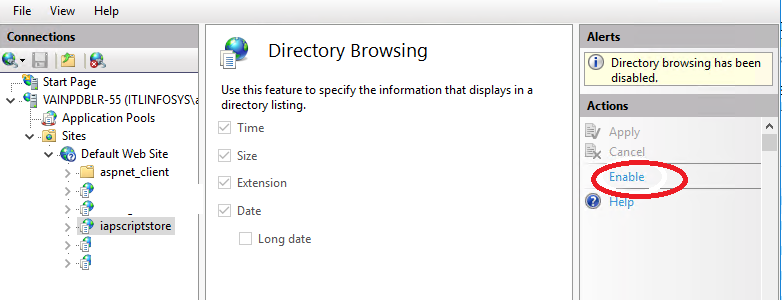
* + 1. Right click on selected row and click on “Enable” option as shown in above screen shot. It will enable the Windows authentication.
    2. If Anonymous Authentication is Enabled, then right click on Anonymous Authentication and click on Disable option.



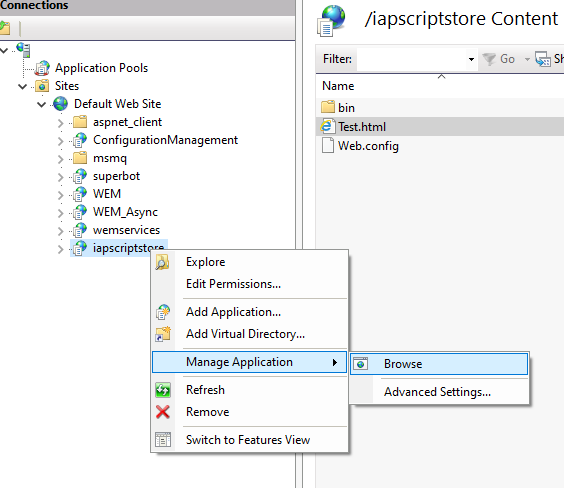
1. Enable Directory Browsing
   * 1. Click on the Directory Browsing



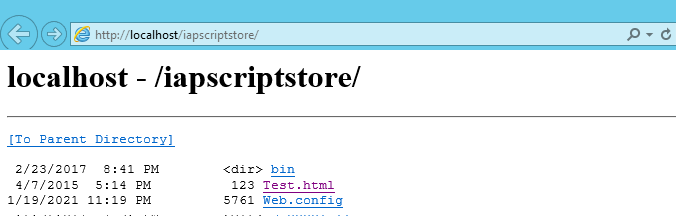
* + 1. Click “Enable” as shown below



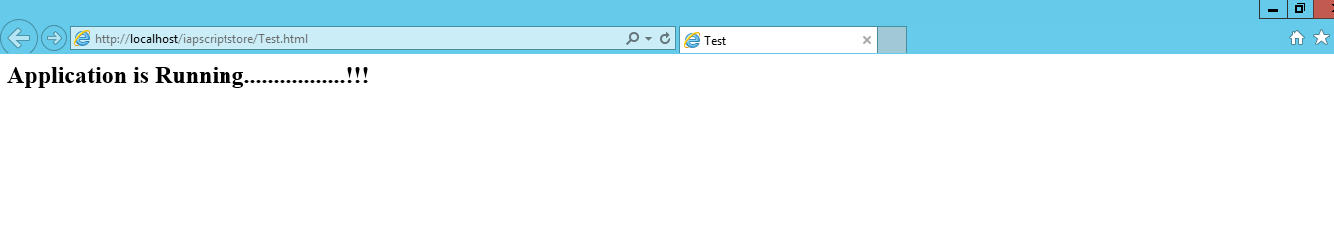
1. Select and right click on the application and click on browse



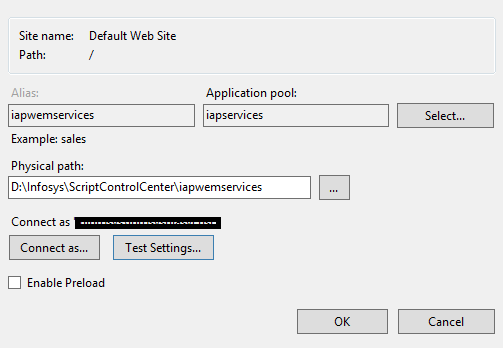
1. Displays list of files in application



1. Click on test.html

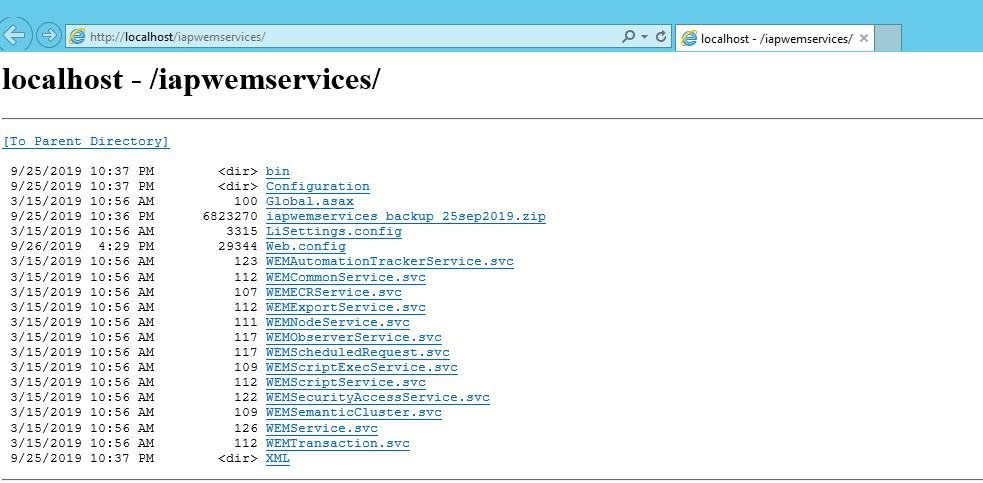


1. Proceed to next step if you are able to test the file as mentioned in previous step
2. Similarly create another REST service with named “iapwemservices” in IIS and map it to physical location where bin and web.config of “iapwemservices” service have been copied as shown in below screen shot. Follow all steps as mentioned in points 9-16



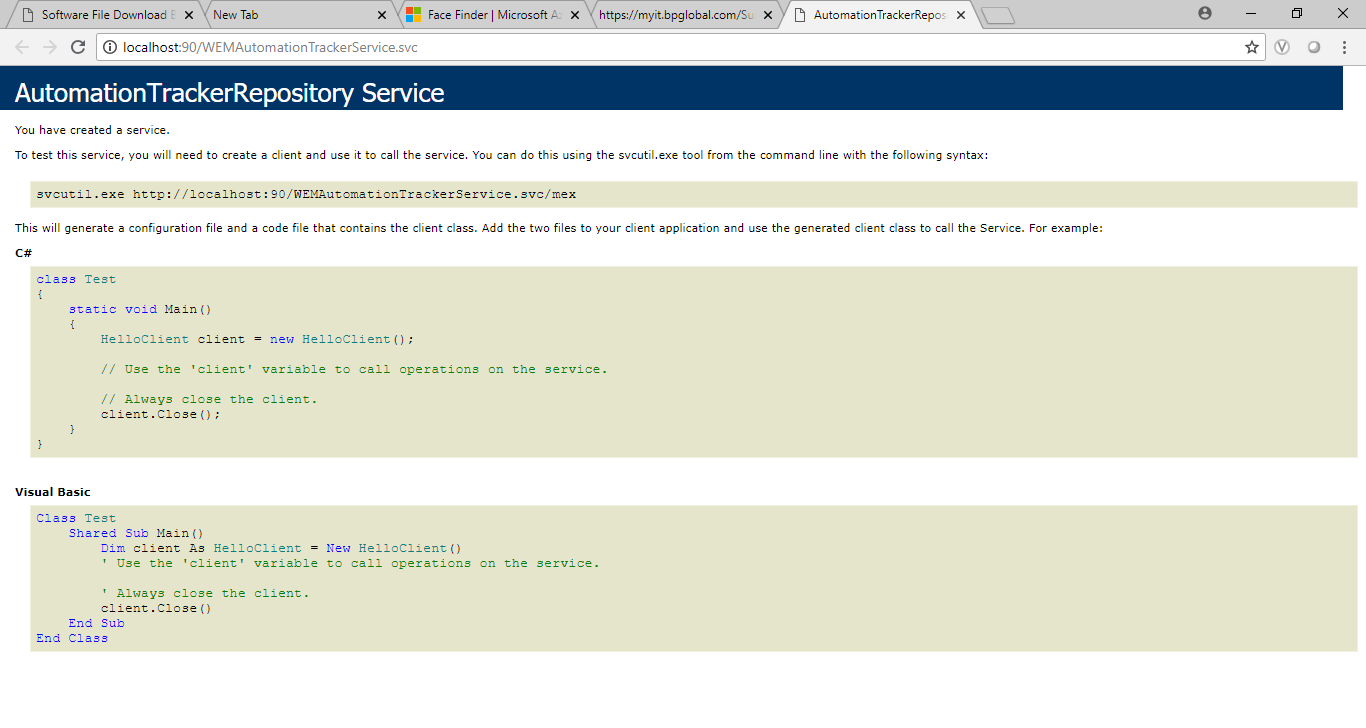
1. To check services are working fine.

* Open the IIS Manager window
* Select “iapwemservices” webservice and click on Browse website.
* List of .svc files will be displays on browser.



Browse each service and check if it is working

Following page should be displayed

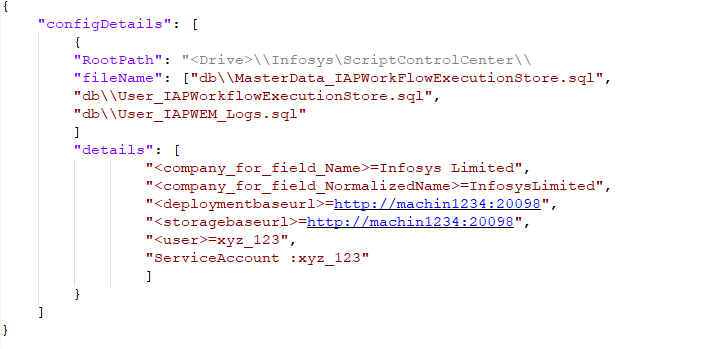


# Update Application Configuration

* Update below fields in “<Drive>:\Infosys\ScriptControlCenter\scripts\configuration.json”

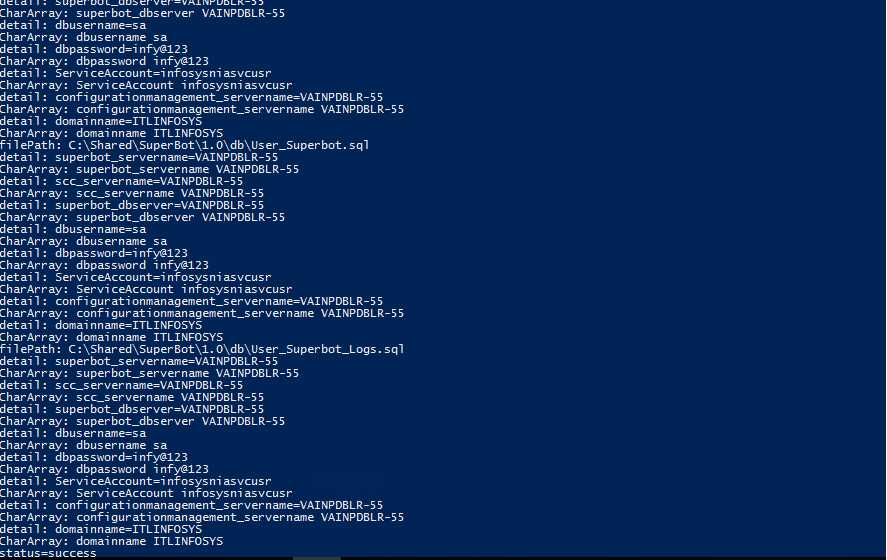
|  |  |  |
| --- | --- | --- |
| **Property** | **Value** | **Description** |
| RootPath | <Drive>:\\Infosys\ScriptControlCenter\\ | Update <Drive> name in root path |
| <company\_for\_field\_Name> | Infosys Limited | Provide the name of the Comany e.g. Infosys Limited |
| <company\_for\_field\_NormalizedName> | InfosysLimited | Provide the name of the Comany (i.e., name without spaces) e.g. InfosysLimited. |
| <deploymentbaseurl> | [http://machin1234](http://machin1234:20098) | Provide the hostname or ipaddress on which “iapwemservices” REST services has been configured |
| <storagebaseurl> | <http://machin1234:20098> | Provide the hostname or ipaddress on which “iapscriptstore” REST services has been configured |
| <user> | xyz\_123 | Provide name of user to grant SuperAdmin access |
| ServiceAccount | xyz\_123 | Provide windows service account id e.g., xyz\_123, etc. |
| DomainName | ad.xyz.com | Specify the LDAP domain name in which the module is getting deployed |

Below is the sample json format



* Execute Below Command on windows PowerShell to update the properties

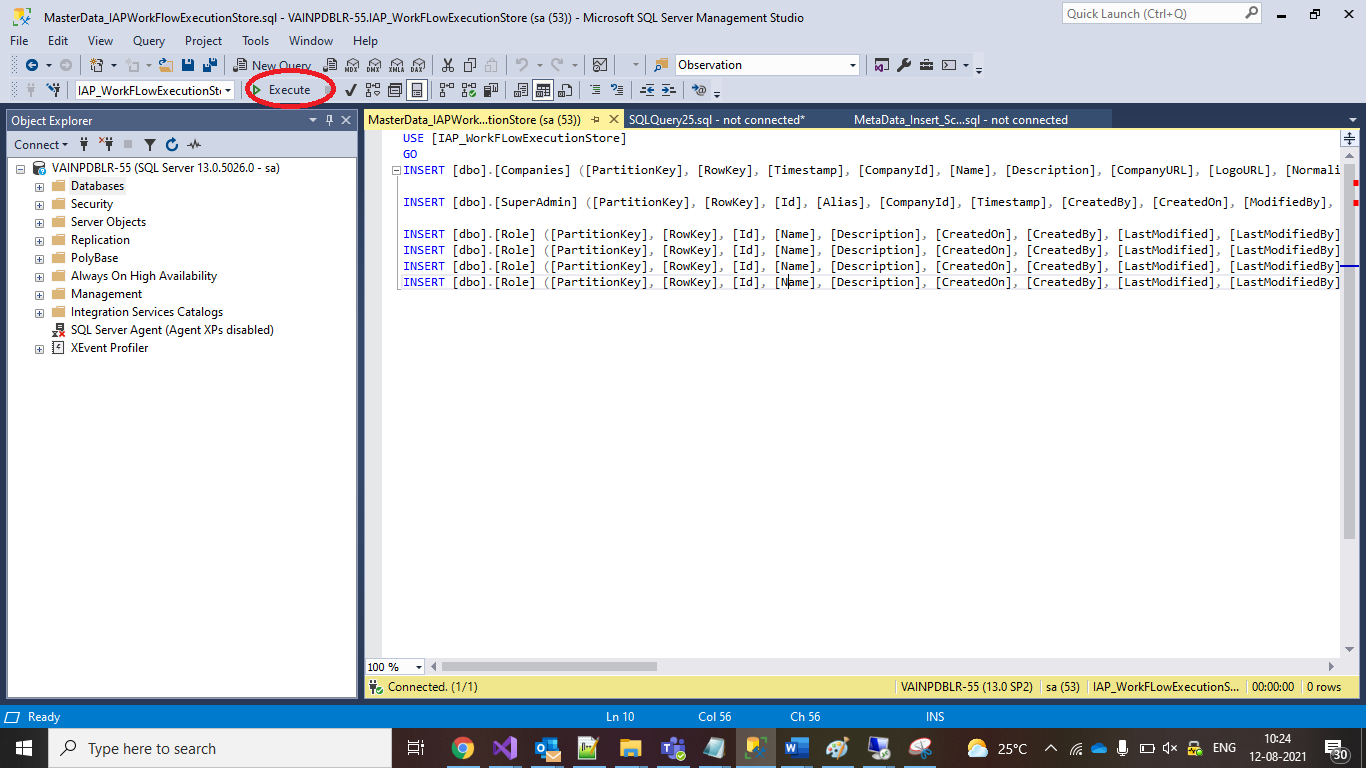
**[**



* Ensure that Database folder ‘db’ copied to target location from deployment package on server and execute script in following sequence.

|  |  |
| --- | --- |
| **Script** | **Remarks** |
| MasterData\_IAPWorkFlowExecutionStore.sql | Execute the script to insert master data to workflowExecutionStore db |
| User\_IAPWorkflowExecutionStore.sql | Execute the script to add service account user for integrated security |
| User\_IAPWEM\_Logs.sql | Execute the script to add service account user for integrated security |
| User\_IAPContentStore.sql | Execute the script to add service account user for integrated security |

1. Go to File > Open > File > Choose MetaData\_IAPWorkFlowExecutionStore.sql file > Press Open > the file will be opened within SQL Server Management Studio, press Execute button.



1. Go to File > Open > File > Choose User\_IAPWorkflowExecutionStore.sql file > Press Open > the file will be opened within SQL Server Management Studio, press Execute button.
2. Go to File > Open > File > Choose User\_IAPWEM\_Logs.sql file > Press Open > the file will be opened within SQL Server Management Studio, press Execute button.
3. Go to File > Open > File > Choose User\_IAPContentStore.sql file > Press Open > the file will be opened within SQL Server Management Studio, press Execute button.

# Import Script Library

This helps to upload scripts into scripts repository.

1. Get the scripts from **“<Drive>:\Infosys\ScriptControlCenter\scripts\import.zip”** for import
2. Follow the steps 1 to 5 mentioned in [section](#_Import_Functionality) by providing localpath as **“<Drive>:\Infosys\ScriptControlCenter\scripts\import.zip”** in step 4

# User Access Management

User Access Management (UAM), also known as identity and access management (IAM), is the administration of giving individual users

Refer the

# Utilities

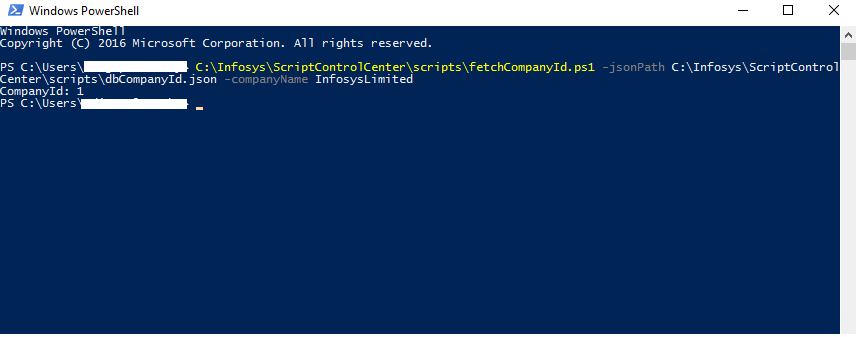
## Export/Import Utility

This utility allows us to export the scripts from server and import the scripts into server

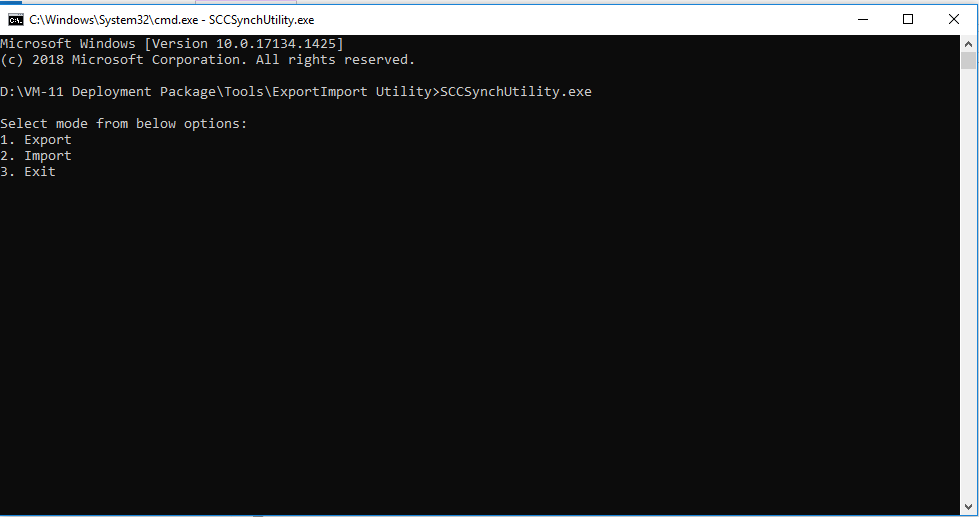
## Export Functionality

1. Execute Below Command on windows PowerShell to fetch company details required for import

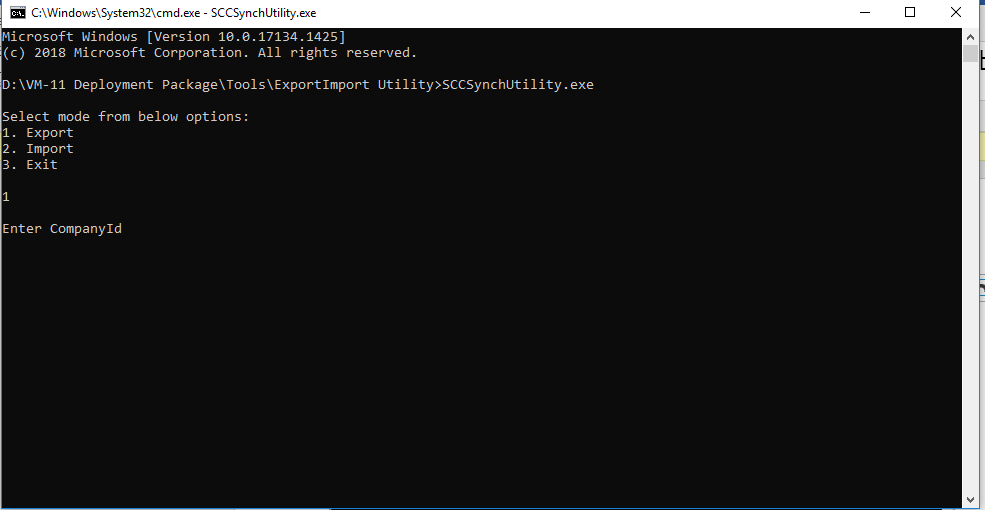
**<Drive>:\Infosys\ScriptControlCenter\scripts\fetchCompanyId.ps1** – jsonPath **<Drive>:\Infosys\ScriptControlCenter\scripts\** **dbCompanyId.json -companyName InfosysLimited**



1. Open ExportImport utility folder and run the SCCSynchUtility.exe in command Prompt



1. Select option 1 to export the script from sever to local.



1. Provide required input data to export the scripts.

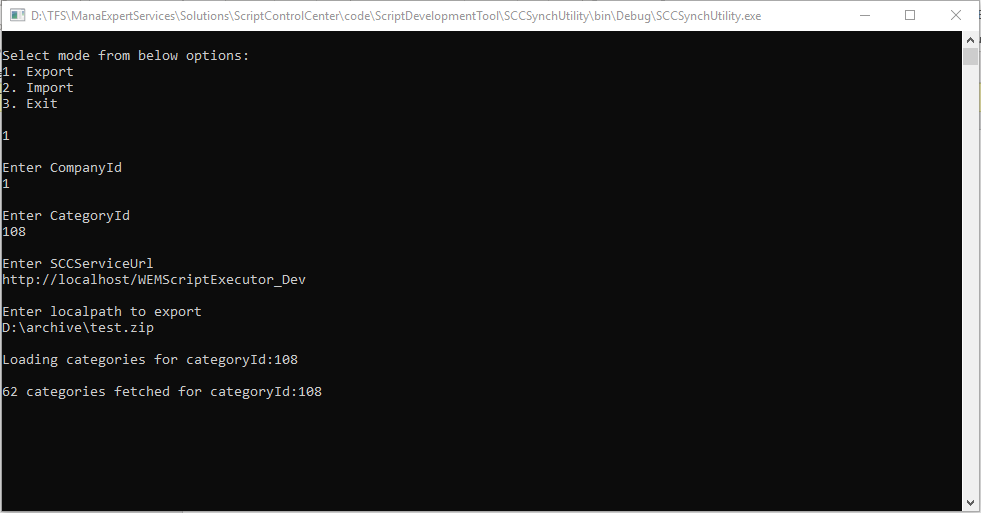
Company Id - Enter value for CompanyID

CategoryId - Enter the ID of category in which scripts need to be download

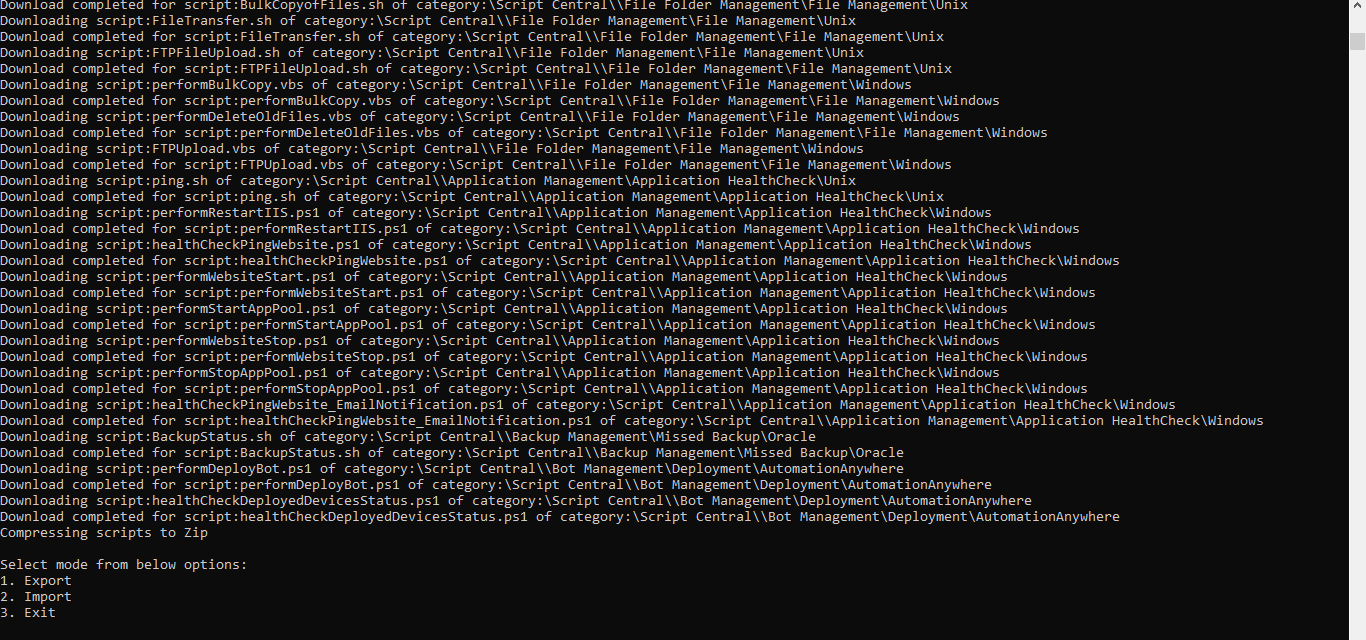
SCCServiceUrl – Enter serviceURL from which need to fetch scripts

“<http://[sytemname]/iapwemservices>” (replace systemname with Name of the system or IP address of where the iapwemservices are hosted

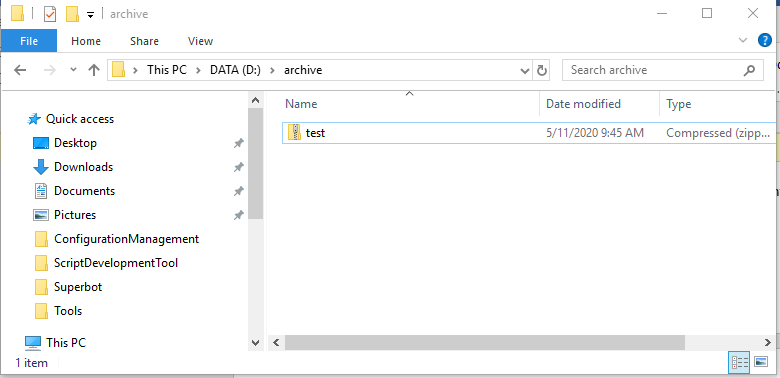
LocalPath to export - Enter local path to export scripts



1. Tool will fetch the scripts from given category and export into provided local path



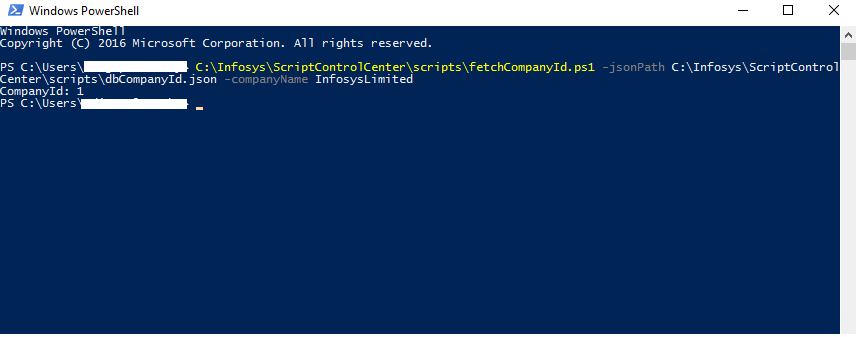
1. Check the folder path if scripts downloaded or not



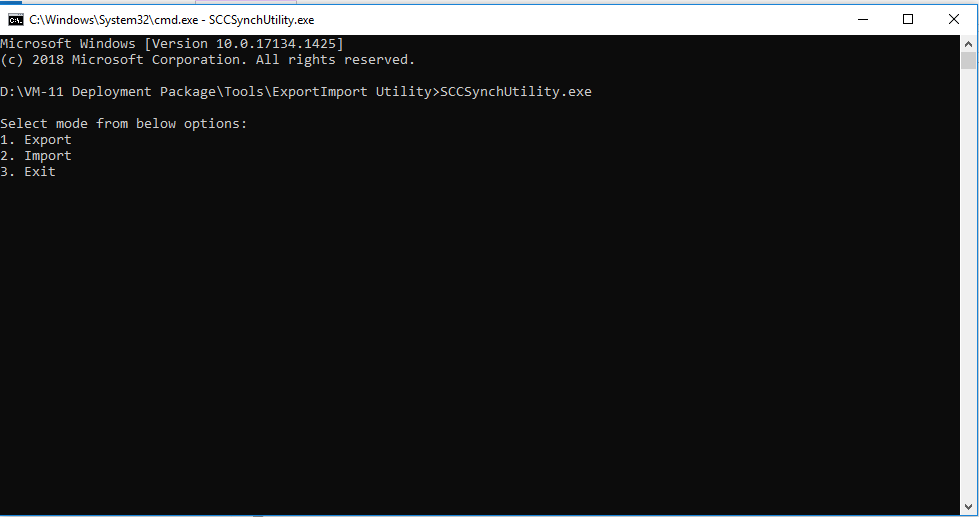
## Import Functionality

1. Execute Below Command on windows PowerShell to fetch company details required for import

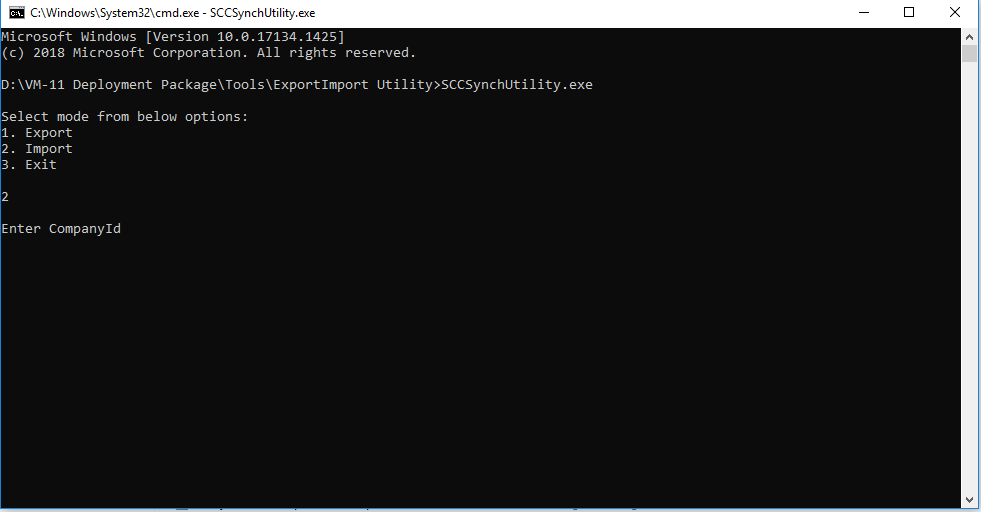
**<Drive>:\Infosys\ScriptControlCenter\scripts\fetchCompanyId.ps1** -jsonPath **<Drive>:\Infosys\ScriptControlCenter\scripts\** **dbCompanyId.json -companyName InfosysLimited**



1. Open ExportImport utility folder and run the SCCSynchUtility.exe in command Prompt



1. Select option 2 to import the script from local to server.

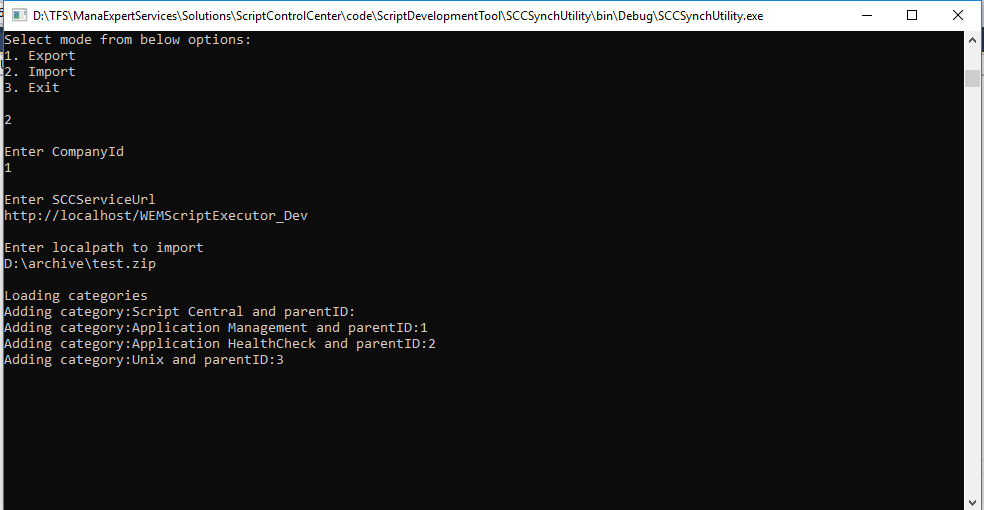


1. Provide required input data to import the scripts. (These details will get by executing the script as mentioned in step 1)

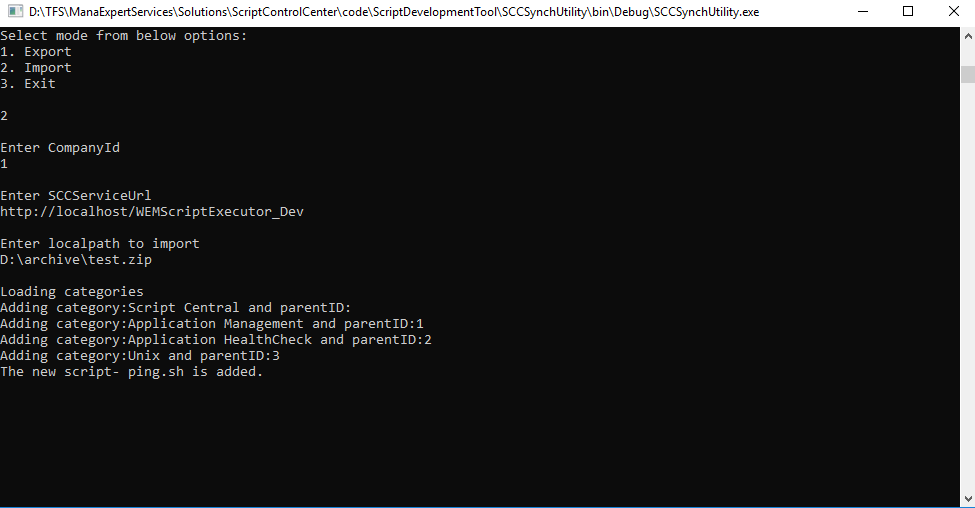
Company Id - Enter value for CompanyID (Enter the value fetched in step 1)

SCCServiceUrl - “<http://[sytemname]/iapwemservices>” (replace systemname with Name of the system or IP address of where the iapwemservices are hosted

LocalPath to import - Enter local path to import scripts



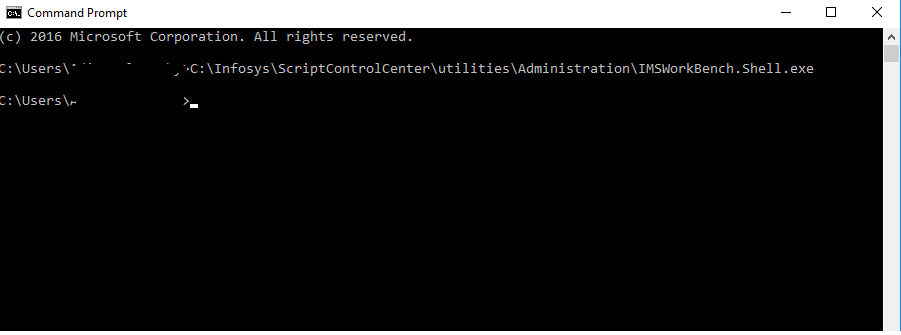
1. Tool will fetch the scripts from given path and upload into server

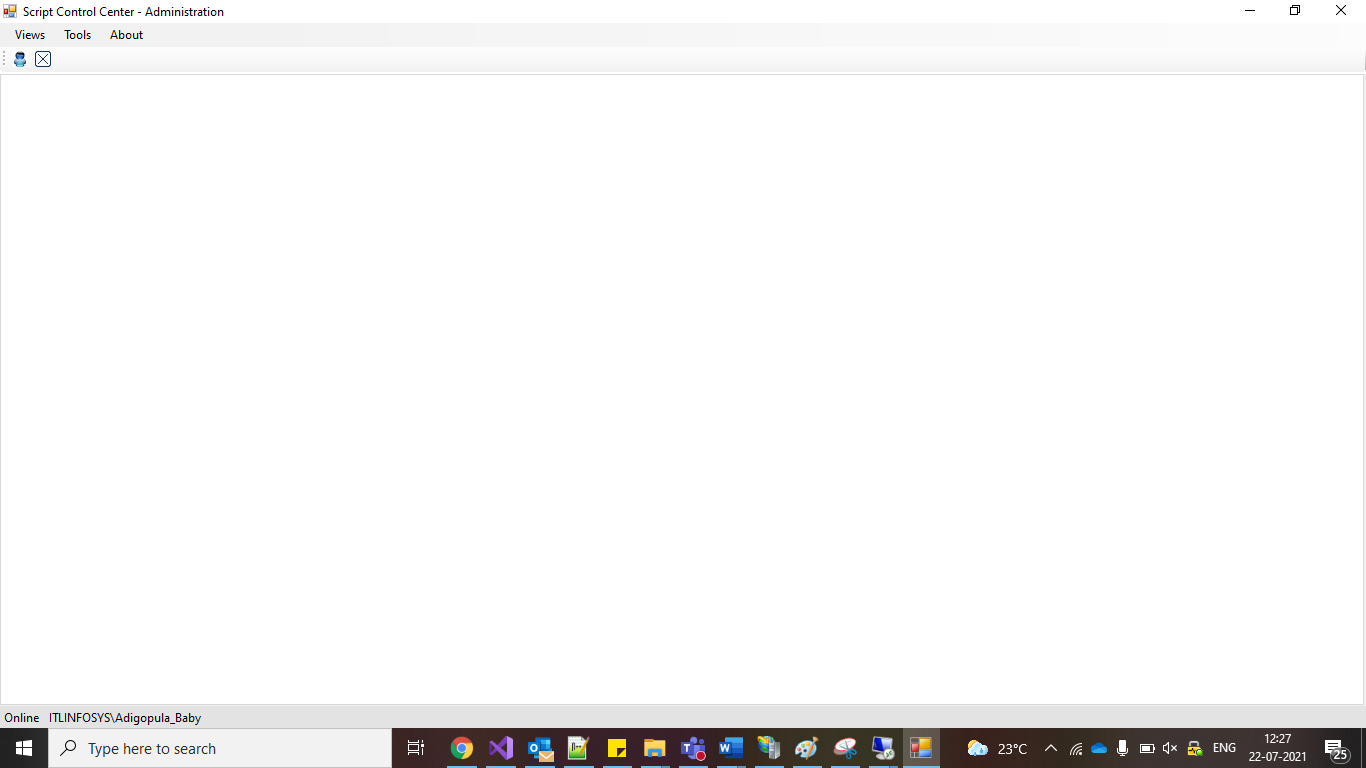


## Administration Utility

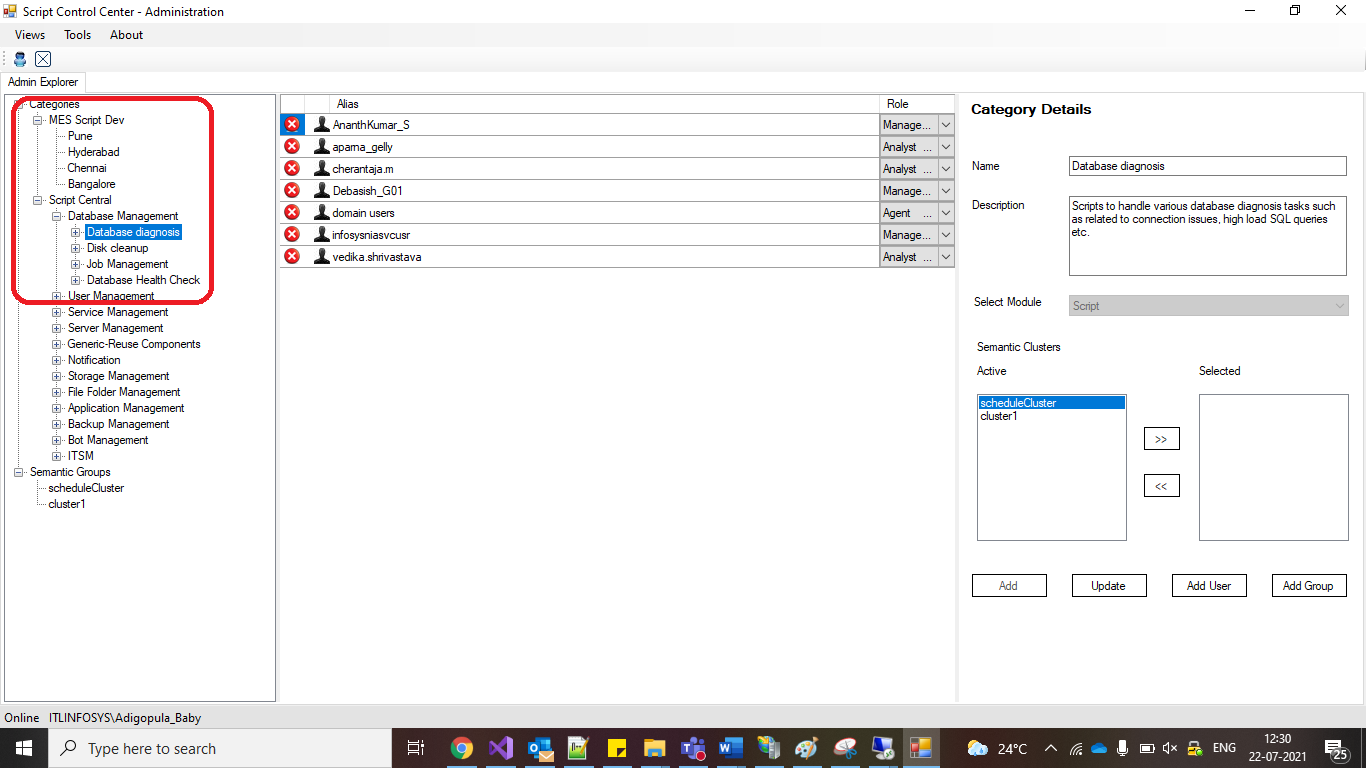
1. Open the Command Prompt and execute the below command

**<Drive>:\Infosys\ScriptControlCenter\utilities\Administration\IMSWorkbench.Shell.exe**

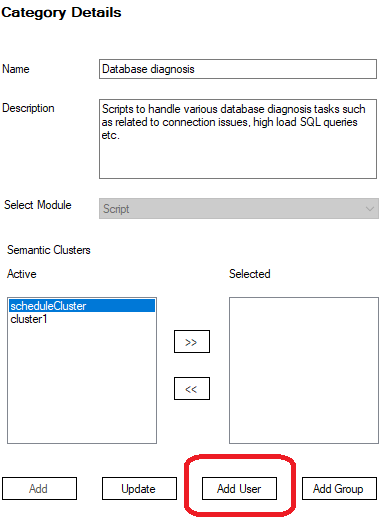




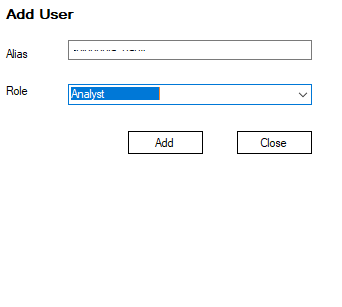
1. Click on “Admin View” icon  and select the category on which admin needs to add privileges



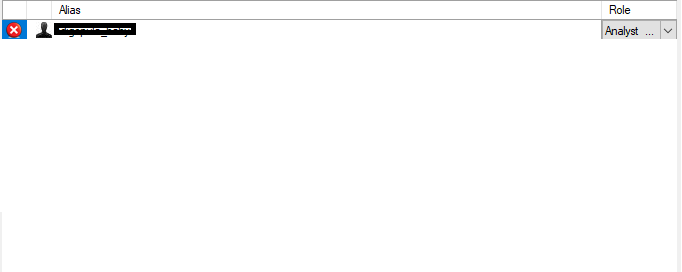
1. Click on “Add user” on Right hand side to provide access for selected category in above step.



1. Provide “alias” (user needs to mention the AD user id without domain name) value and select “role” and click on “Add”



1. User added for the selected category.



# Enable Remote Execution

**Steps to Enable Remote Execution on Local Machine using PowerShell**

1. Open PowerShell in Admin mode and run following command on the local machine on which Script Control center Shell EXE will be run.

Enable-PSRemoting

Specify Y for each prompt.

First prompt is confirmation to run this command for enabling this machine for remote management. Default value is Yes e.g. Y

The second, third and fourth (if any) prompt is for enabling proxy for Enable-PSSessionConfiguration. This changes the properties of the registered session configurations on the machine and allows users to run commands remotely. Default value for each prompt is Yes e.g. Y.

Note: In case you don’t want any prompts, run the following command. This will suppress all the prompts.

Enable-PSRemoting –Force

1. Setup client computer for delegation. Run the following command in powershell

Enable-WSManCredSSP –Role Client –DelegateComputer x

Replace x with name of computer where user credentials may be delegated. The application handles this implicitly for you, when running a script over powershell remoting option. However, if users wants to run remote scripts over the console utilities would require to run this command manually from a powershell console

**Steps to Enable Remote Execution on Remote Server using PowerShell**

1. The user running the scripts on remote machine should be added to administrators group of each remote machine. The recommended approach is to create a Windows Distribution List which is added as admin of the remote system(s). Users can be managed through DL.
2. Open PowerShell in Admin mode and run following command on the remote machine(s) where remote script execution needs to be done.

Enable-PSRemoting

Specify Y for each prompt.

First prompt is confirmation to run this command for enabling this machine for remote management. Default value is Yes e.g. Y

The second, third and fourth (if any) prompt is for enabling proxy for Enable-PSSessionConfiguration. This changes the properties of the registered session configurations on the machine and allows users to run commands remotely. Default value for each prompt is Yes e.g. Y.

Note: In case you don’t want any prompts, run the following command. This will suppress all the prompts.

Enable-PSRemoting -Force

1. Run following PowerShell command on the remote machine(s) where remote script execution needs to be done.

Set-ExecutionPolicy RemoteSigned

1. Run following command on each of the remote machine.

Enable-WSManCredSSP -Role Server –Force

Note: Points 2 & 3 are optional and should be executed only if f PowerShell Remoting has not been enabled on remote machine.

# Troubleshooting

## REST Services

* + 1. Logs related to REST services are available in logs database.
    2. Below is the query to get the latest logs

*SELECT TOP 1000 [LogID]*

*, [EventID]*

*, [Priority]*

*, [Severity]*

*, [Title]*

*, [Timestamp]*

*, [MachineName]*

*, [AppDomainName]*

*, [ProcessID]*

*, [ProcessName]*

*, [ThreadName]*

*, [Win32ThreadId]*

*, [Message]*

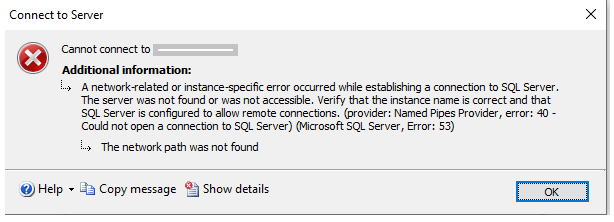
*, [FormattedMessage]*

*FROM [IAPWEM\_Logs]. [dbo]. [Log] order by LogID desc*

* + 1. Message and FormattedMessage give error details

## Cannot connect to SQL Server

“Cannot connect to the server” error occurred due firewall.



Add the sql server port “1433” to windows firewall as mentioned in [Section](#_Add_SQL_Server)

# FAQ

1. Which features of IIS to be selected?
2. Refer to the [section](#_Prerequisites)
3. How to Enable remote execution mode?

A. Refer to the [section](#_Enable_Remote_Execution)