

GBC-IND LoRa Setup with Windows Server 2019

This document describes GBC-IND LoRa setup instructions on Windows Server 2019 due to security restriction or policy enforcement

Requirements	2
Prepare Setup	2
Copy Setup Folder	2
Rename the computer	2
Basic Environment Setup	2
Create Local Administrator Privilege Account (~2 min)	2
Disable Built-in Administrator Account (Optional) (~2 min)	4
Power Settings (~1 min)	5
Network Setting to MultiTech Gateway (~1 min)	6
Open a UDP Port for LoRaDataCollector (~2 min)	7
Enable Remote Desktop (Depending on the Requirement) (~1 min)	8
Third Party Software Setup	9
Database Setup	9
SQL Server 2019 Express (~12 min)	9
SQL Server Management Studio - SSMS 18.12.1 or later (~5 min)	13
IIS Setup	14
Enable IIS Features (~6 min)	14
PuTTY Setup (~2 min)	21
OPC Dependent DLL Setup (~1 min)	22
Matrikon OPC Explorer Setup (Optional) (~1 min)	22
Cypress Envirosystems Software and Environment Setup	23
Run Installation Batch (~2 min)	23
Environment Setup	23
Set the Device Importer To Run as Administrator (~1 min)	23
Set the Image Viewer To Run as Administrator (~1 min)	26
Set the Device Target (~1 min)	26
Set Browser Start Pages (~1 min)	27
OPC Setup for Local Access (~6 min)	28
OPC Setup for Allowing Remote Access (Depending on the Requirement) (~15 min)	32
Database Backup Location (Depending on the Environment) (~2 min)	33
Add MultiTech Gateway Links as Favorite (Optional) (~1 min)	34
Quick Access Pins (Optional) (~1 min)	34

Requirements

- Windows Server 2019 64 bit machine
- Local Administrator Privilege Account Access
- 8GB or Greater RAM
- SSD with 120 GB or Greater Free Space

Prepare Setup

Copy Setup Folder

- Download the file “Setup_2019Server.zip” file from [here](#)
- Copy downloaded “Setup_2019Server.zip” file to the target computer’s C drive and extract to the Setup folder.

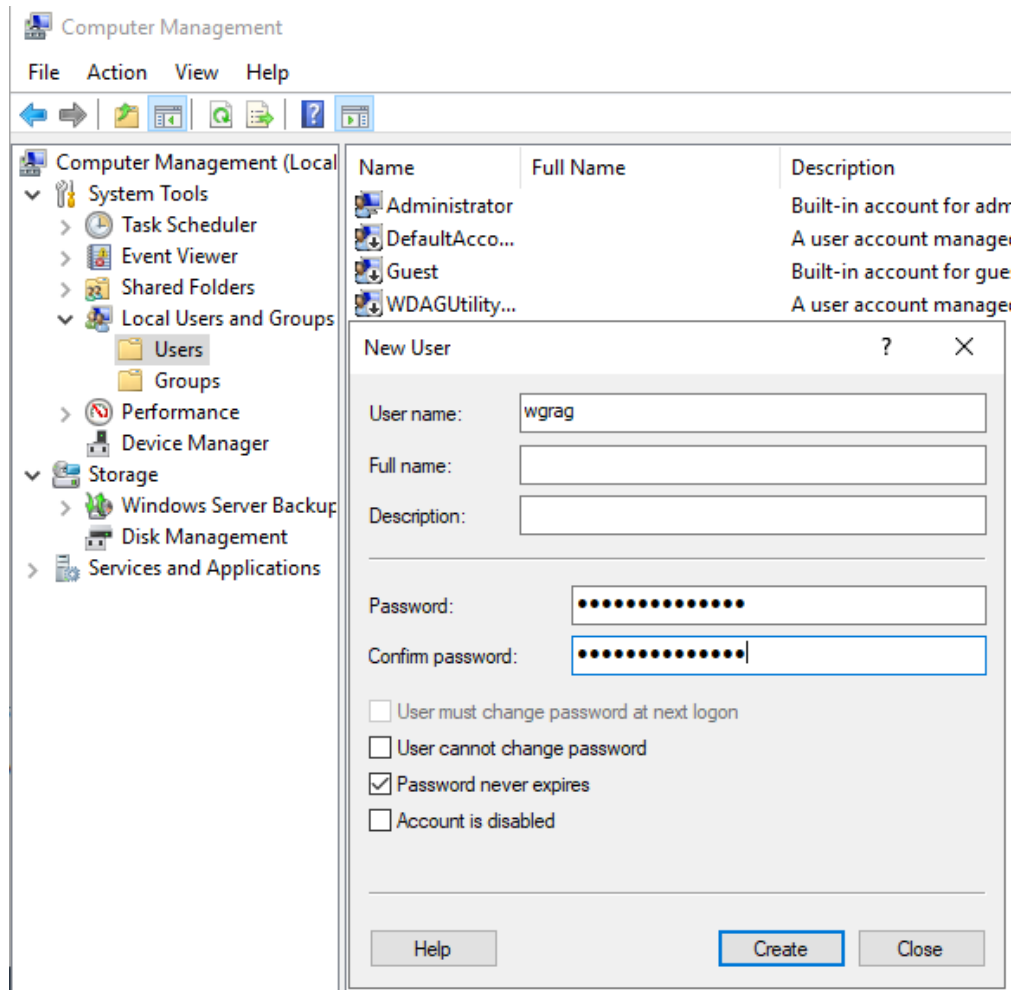
Rename the computer

- If required, change the computer name (Settings->System->About->Rename this PC) and restart it to take effect

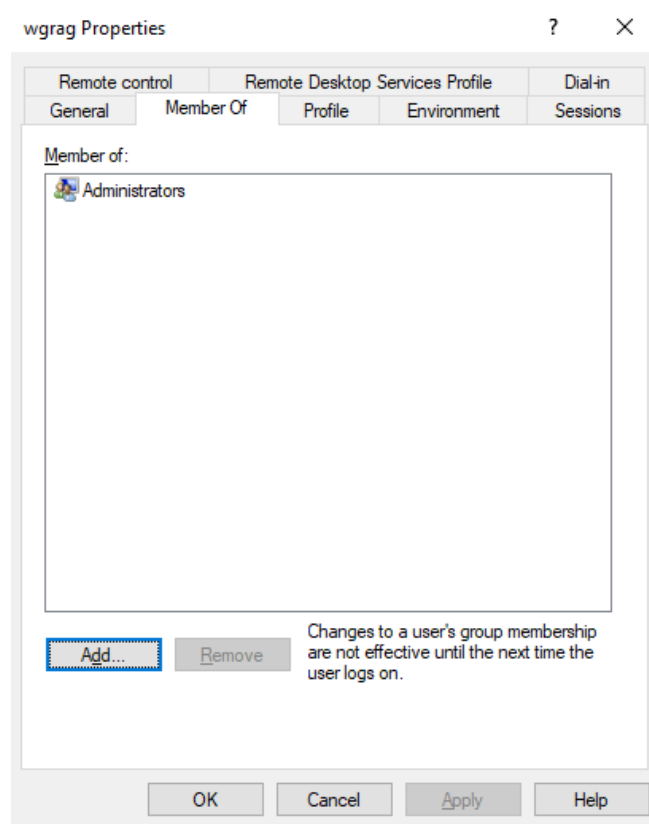
Basic Environment Setup

Create Local Administrator Privilege Account (~2 min)

- Create a local (offline) user account named **wgrag** with administrator privilege
- From Control Panel->System and Security->Administrative Tools, open Computer Management
 - From the left tree, under Local Users and Groups, select Users
 - Right click on the middle pane, select New User
 - Create an account info using:
 - User name: **wgrag**
 - Password: **Cypr3ssEnv1r0!**
 - Check only **Password never expires**



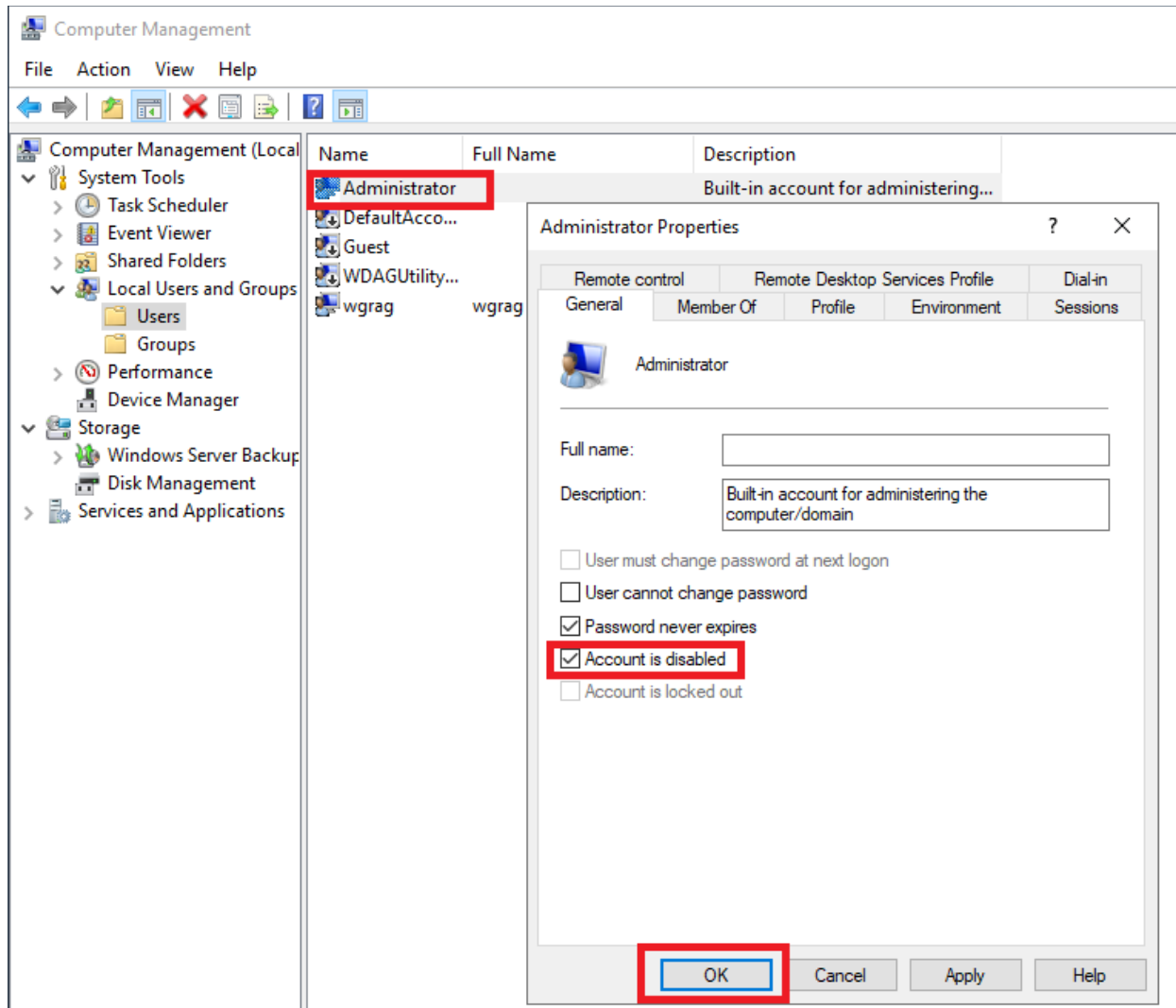
- Once created, right click on the account and select Properties
 - On the Member Of tab, press Add button to be on Administrators group (only Administrators group by removing from Users group as below)



- Log off from the current account and log into **wgrag** account

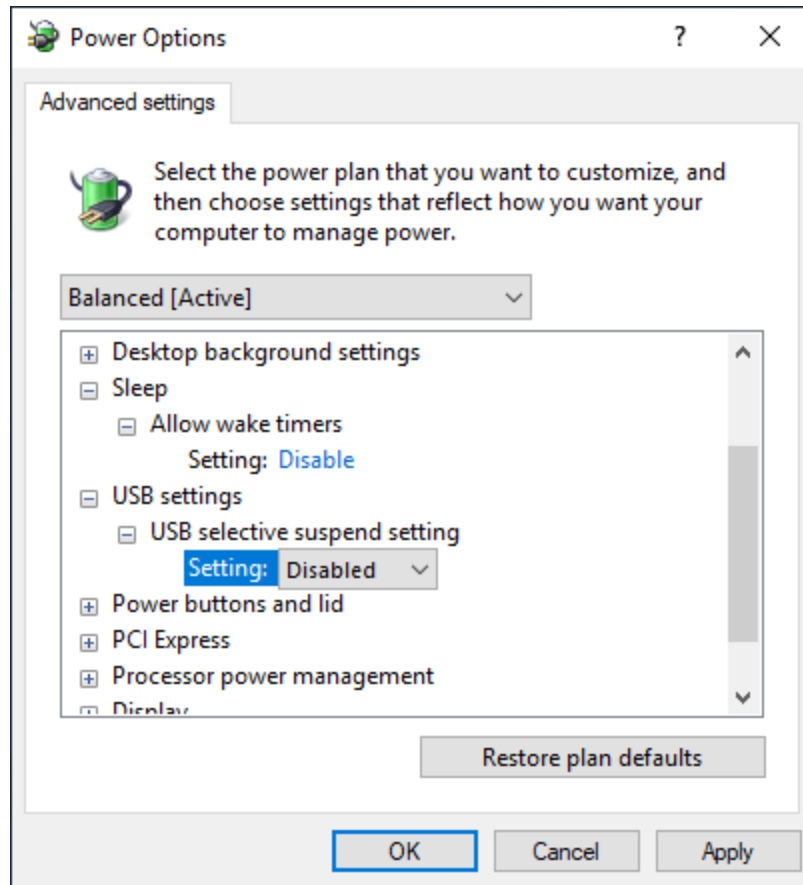
Disable Built-in Administrator Account **(Optional)** (~2 min)

- From Control Panel->System and Security->Administrative Tools, open Computer Management
 - From the left tree, under Local Users and Groups, select Users
 - Right click on the Administrator in the middle pane
 - Under the General tab, check Account is disabled and press OK



Power Settings (~1 min)

- From Control Panel->System and Security->Power Options, press Change plan settings on Balanced. Press Change advanced power settings. Change settings to:
 - Hard disk->Turn off hard disk after: 0
 - Sleep
 - Allow wake timers: Disable
 - USB settings->USB selective suspend setting: Disabled



Network Setting to MultiTech Gateway (~1 min)

- This assumes the machine has two Ethernet port and one port is directly connected to the Multitech Gateway
- From Control Panel->Network and Internet->Network and Sharing Center, press Change adapter settings and select the network which would connect to MultiTech Gateway (name could be Ethernet, Ethernet 2, Network Connection 1 or Network Connection 2 depending on computer's own setup). Right click to access Properties.
 - Select Internet Protocol Version 4 (TCP/IPv4). Press Properties and select Use the following IP address. Set the IP address to 192.168.2.2 and Subnet mask to 255.255.255.0. Press OK.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 2 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

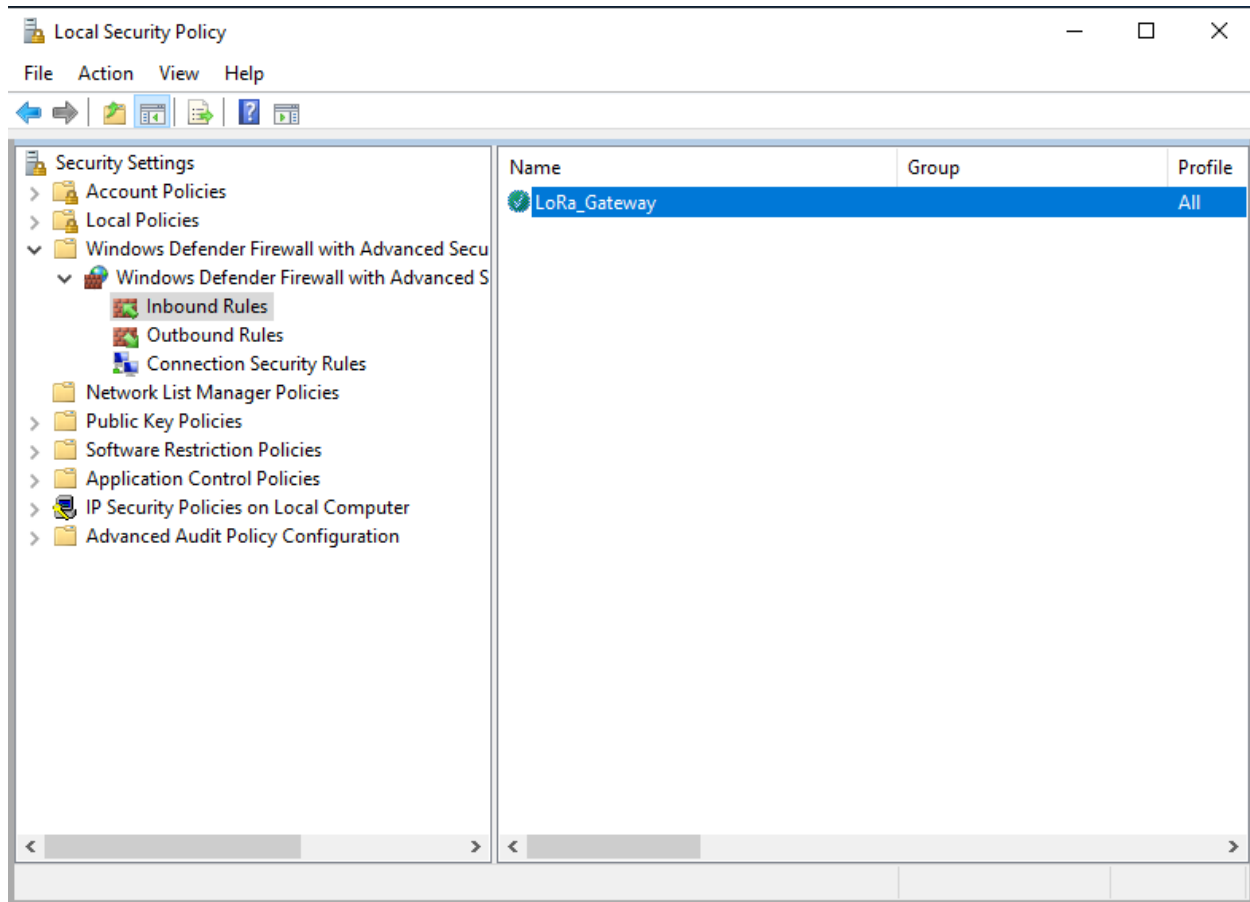
☐ Validate settings upon exit

Advanced...

OK Cancel

Open a UDP Port for LoRaDataCollector (~2 min)

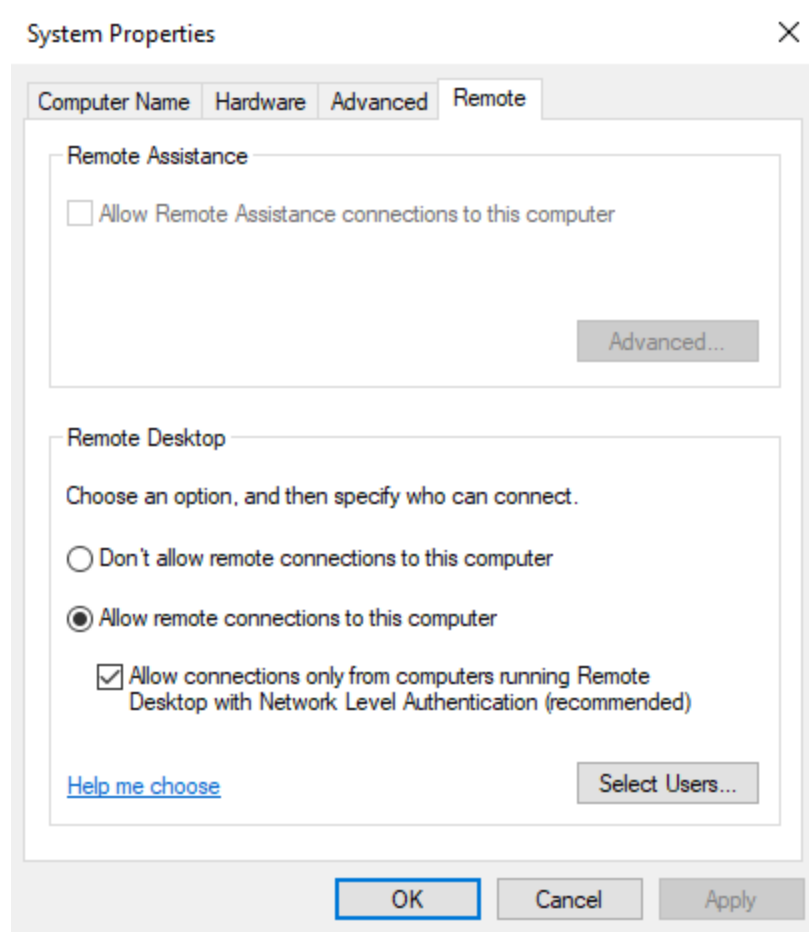
- Open Local Security Policy from Control Panel->System and Security->Administrative Tools, navigate to "Security Settings->Windows Defender Firewall with Advanced Security->Windows Defender Firewall with Advanced Security - Local Group Policy Object->Inbound Rules" and create an inbound rule for a UDP port 27500 to allow connection for all profiles and name it as "LoRa GW Inbound UDP 27500"



- Repeat to create an outbound rule for a UDP port 27500 and name it as “LoRa GW Outbound UDP 27500”

Enable Remote Desktop **(Depending on the Requirement)** (~1 min)

- From Control Panel->System and Security->System, select Remote settings from the left and check Allow remote connection to this computer



Third Party Software Setup

Database Setup

SQL Server 2019 Express (~12 min)

- Run setup.exe from "Setup_2019Server\Third Party\SQLEXPADV_x64_ENU"
- From SQL Server Installation Center, select New SQL Server stand-alone installation ...
- Accept the license terms and click Next
- Uncheck Use Microsoft Update to check for updates and click Next
- Install Rules may show a warning for Windows Firewall, ignore and click Next
- For Feature Selection page, **uncheck** the following features but accept other defaults on Shared Features and click Next
 - SQL Server Replication
 - Machine Learning Services
 - Full-Text and Semantic Extraction for Search

SQL Server 2019 Setup

Feature Selection

Select the Express features to install.

Install Rules

Feature Selection

Feature Rules

Instance Configuration

Server Configuration

Database Engine Configuration

Feature Configuration Rules

Installation Progress

Complete

Looking for Reporting Services? [Download it from the web](#)

Features:	Feature description:
<p>Instance Features</p> <p><input checked="" type="checkbox"/> Database Engine Services</p> <p><input type="checkbox"/> SQL Server Replication</p> <p><input type="checkbox"/> Machine Learning Services and Language Ext</p> <p><input type="checkbox"/> R</p> <p><input type="checkbox"/> Python</p> <p><input type="checkbox"/> Java</p> <p><input type="checkbox"/> Full-Text and Semantic Extractions for Search</p> <p><input type="checkbox"/> PolyBase Query Service for External Data</p> <p><input type="checkbox"/> Java connector for HDFS data sources</p> <p>Shared Features</p> <p><input checked="" type="checkbox"/> Client Tools Connectivity</p> <p><input checked="" type="checkbox"/> Client Tools Backwards Compatibility</p> <p><input checked="" type="checkbox"/> Client Tools SDK</p> <p><input checked="" type="checkbox"/> SQL Client Connectivity SDK</p> <p><input type="checkbox"/> LocalDB</p> <p>Redistributable Features</p>	<p>The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on the same computer.</p> <p>Prerequisites for selected features:</p> <p>Already installed:</p> <p>... Windows PowerShell 3.0 or higher</p> <p>To be installed from media:</p> <p>... Microsoft Visual C++ 2017 Redistributable</p> <p>Disk Space Requirements</p> <p>Drive C: 1315 MB required, 98965 MB available</p>

Select All Unselect All

Instance root directory: C:\Program Files\Microsoft SQL Server\ ...

Shared feature directory: C:\Program Files\Microsoft SQL Server\ ...

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\ ...

< Back Next > Cancel

- For the Instance Configuration page, select Named instance and enter MSSQLSERVER. Set to MSSQLSERVER for Instance ID too. Click Next

SQL Server 2019 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Installation Progress
Complete

☐ Default instance

☒ Named instance: MSSQLSERVER

Instance ID: MSSQLSERVER

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version
---------------	-------------	----------	---------	---------

< Back Next > Cancel

- Choose **Automatic** for SQL Server Database Engine and **Disabled** for SQL Server Browser (default). Click Next

Server Configuration

Specify the service accounts and collation configuration.

Install Rules

Feature Selection

Feature Rules

Instance Configuration

Server Configuration

Database Engine Configuration

Feature Configuration Rules

Installation Progress

Complete

Service Accounts Collation

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Database Engine	NT Service\MSSQLSERVER		Automatic ▾
SQL Server Browser	NT AUTHORITY\LOCAL ...		Disabled ▾

☐ Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service

This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.

[Click here for details](#)

< Back

Next >

Cancel

- For Database Engine Configuration page,
 - Choose **Mixed Mode** and type **Cypr3ss!MSSQL123** as **sa** password
 - Accept other defaults on other tabs and click Next

SQL Server 2019 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories, TempDB, Max degree of parallelism, Memory limits, and Filestream settings.

Install Rules

- Feature Selection
- Feature Rules
- Instance Configuration
- Server Configuration
- Database Engine Configuration**
- Feature Configuration Rules
- Installation Progress
- Complete

Server Configuration | Data Directories | TempDB | Memory | User Instances | FILESTREAM

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

☐ Windows authentication mode

☒ Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: [password field]

Confirm password: [password field]

Specify SQL Server administrators

WIN-05NA9HDSEFE\wgrag (wgrag)

SQL Server administrators have unrestricted access to the Database Engine.

Add Current User | Add... | Remove

< Back | Next > | Cancel

- Once Installation is complete, click Close

SQL Server Management Studio - SSMS 18.12.1 or later (~5 min)

*Note: You can choose to download and install the latest version available. Please find more information [here](#).

- Run SSMS-Setup-ENU.exe from "Setup_2019Server\Third Party"
- Accept default location and press Install



RELEASE 18.0

Microsoft SQL Server Management Studio

Welcome. Click "Install" to begin.

Location:

C:\Program Files (x86)\Microsoft SQL Server Management Studio 18

Change

By clicking the "Install" button, I acknowledge that I accept the [License Terms](#) and [Privacy Statement](#).

SQL Server Management Studio transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the [documentation](#).

Install

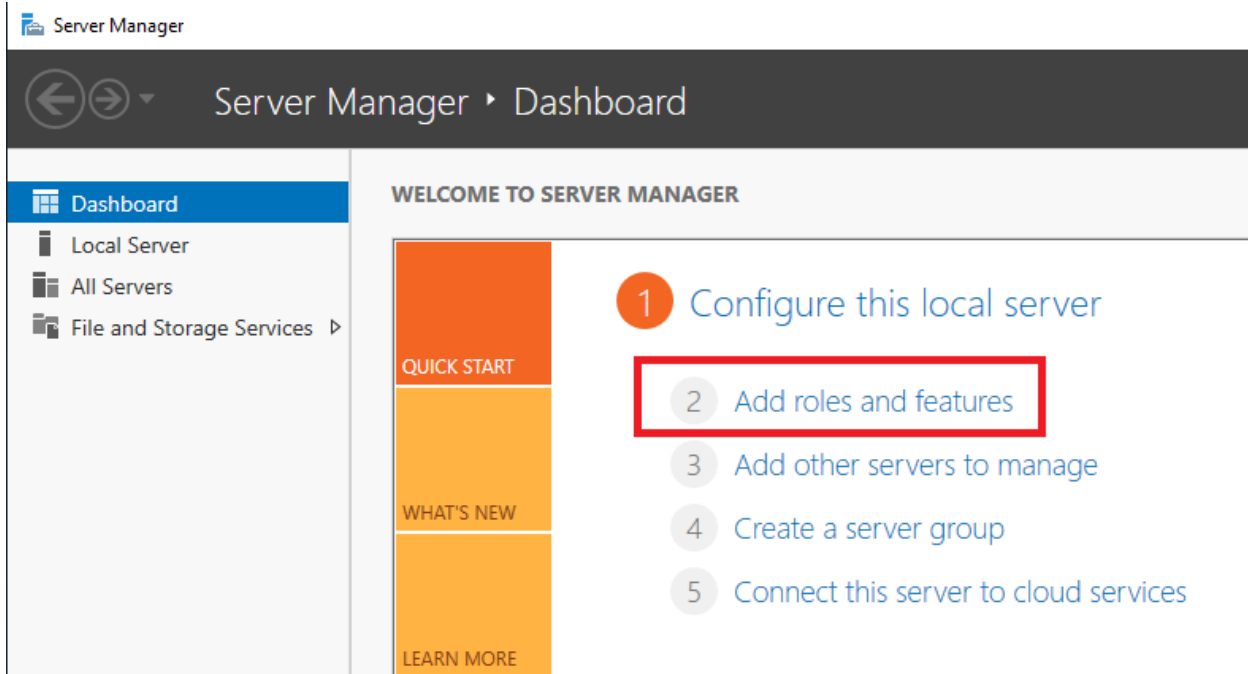
Close

- Once installation is finished, restart the computer

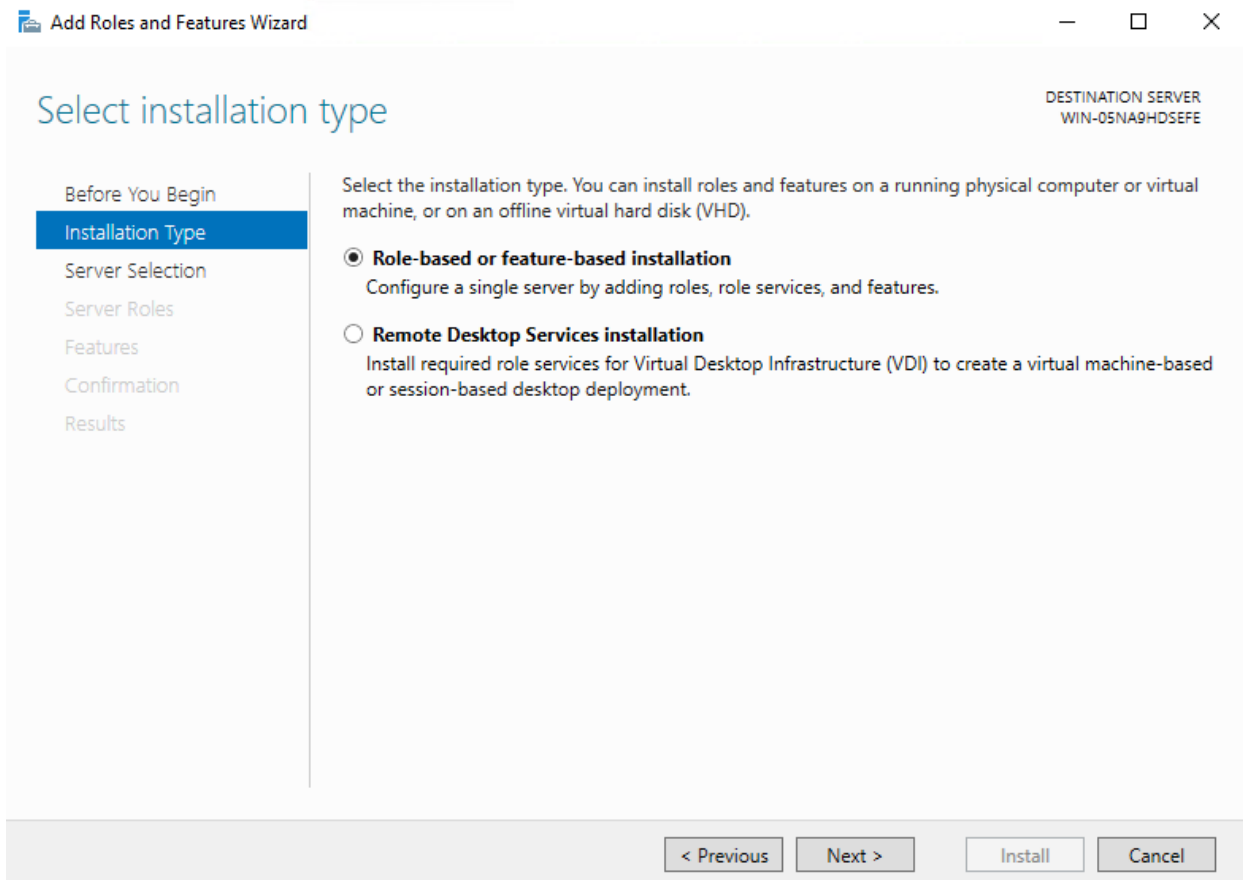
IIS Setup

Enable IIS Features (~6 min)

- From Server Manager, select Add roles and features



- Press Next on the Before you begin page
- Select Role-based or feature-based installation on the Select installation type page and press Next



- Accept the default destination server with Select a server from the server pool selected and press Next

Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
WIN-05NA9HDSEFE

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool
☐ Select a virtual hard disk

Server Pool

Filter:

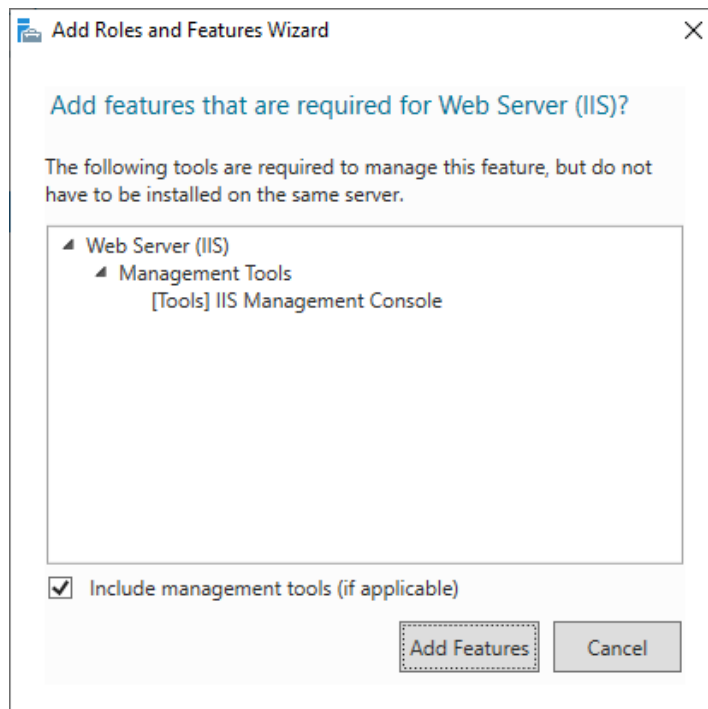
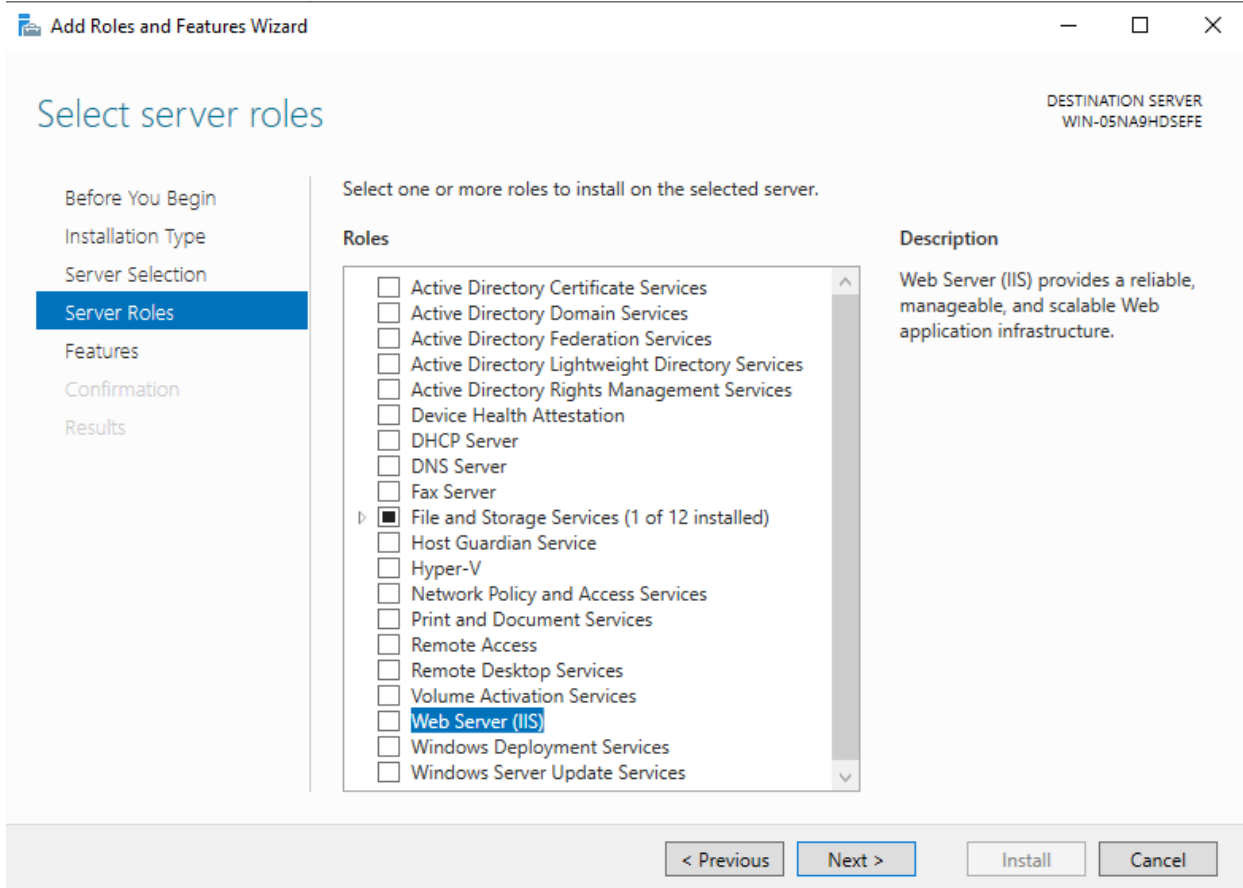
Name	IP Address	Operating System
WIN-05NA9HDSEFE	169.254.103.71...	Microsoft Windows Server 2019 Standard Evaluation

1 Computer(s) found

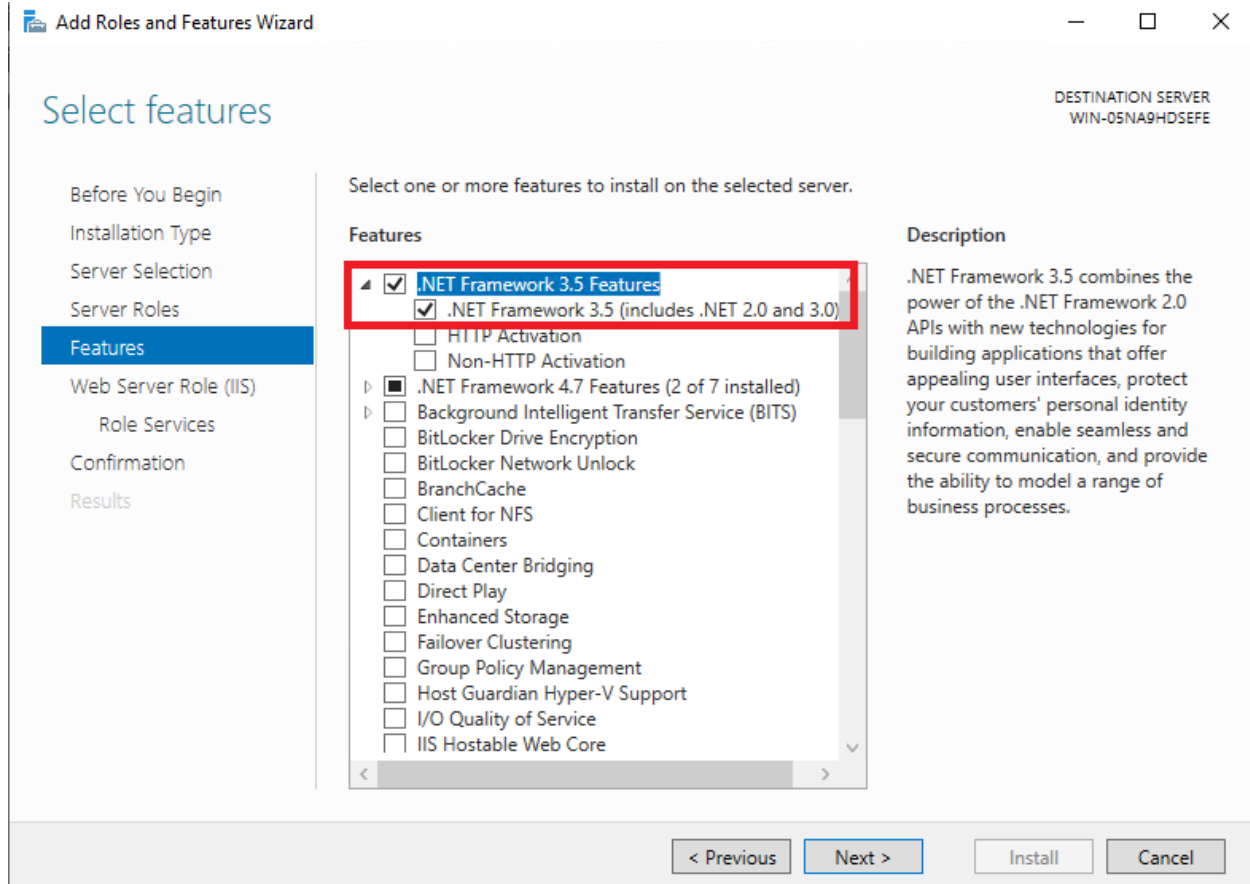
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous Next > Install Cancel

- Check Web Server, then press Add Features. Press Next.



- Check **.NET Framework 3.5** (includes .NET 2.0 and 3.0). Press Next.



- Press Next and make sure these are selected for the Role Services
 - Management Tools
 - IIS Management Console
 - Application Development
 - .NET Extensibility 3.5
 - .NET Extensibility 4.7 (or later)
 - ASP
 - ASP.NET 3.5
 - ASP.NET 4.7 (or later)
 - CGI
 - ISAPI Extensions
 - ISAPI Filters
 - Common HTTP Features
 - Static Content

Select role services

DESTINATION SERVER
WIN-05NA9HDSEFE

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Web Server Role (IIS)

Role Services

Confirmation

Results

Select the role services to install for Web Server (IIS)

Role services

- ☒ Web Server
 - ☒ Common HTTP Features
 - ☒ Default Document
 - ☒ Directory Browsing
 - ☒ HTTP Errors
 - ☒ Static Content
 - ☐ HTTP Redirection
 - ☐ WebDAV Publishing
 - ☒ Health and Diagnostics
 - ☒ Performance
 - ☒ Security
 - ☒ Application Development
 - ☒ .NET Extensibility 3.5
 - ☒ .NET Extensibility 4.7
 - ☐ Application Initialization
 - ☒ ASP
 - ☒ ASP.NET 3.5
 - ☒ ASP.NET 4.7
 - ☒ CGI
 - ☒ ISAPI Extensions
 - ☒ ISAPI Filters
 - ☐ Server Side Includes
 - ☐ WebSocket Protocol
- ☐ FTP Server
 - ☐ FTP Service
 - ☐ FTP Extensibility
- ☒ Management Tools
 - ☒ IIS Management Console
 - ☐ IIS 6 Management Compatibility
 - ☐ IIS Management Scripts and Tools
 - ☐ Management Service

Description

Security provides infrastructure for securing the Web server from users and requests. IIS supports multiple authentication methods. Pick an appropriate authentication scheme based upon the role of the server. Filter all incoming requests, rejecting without processing requests that match user defined values, or restrict requests based on originating address space.

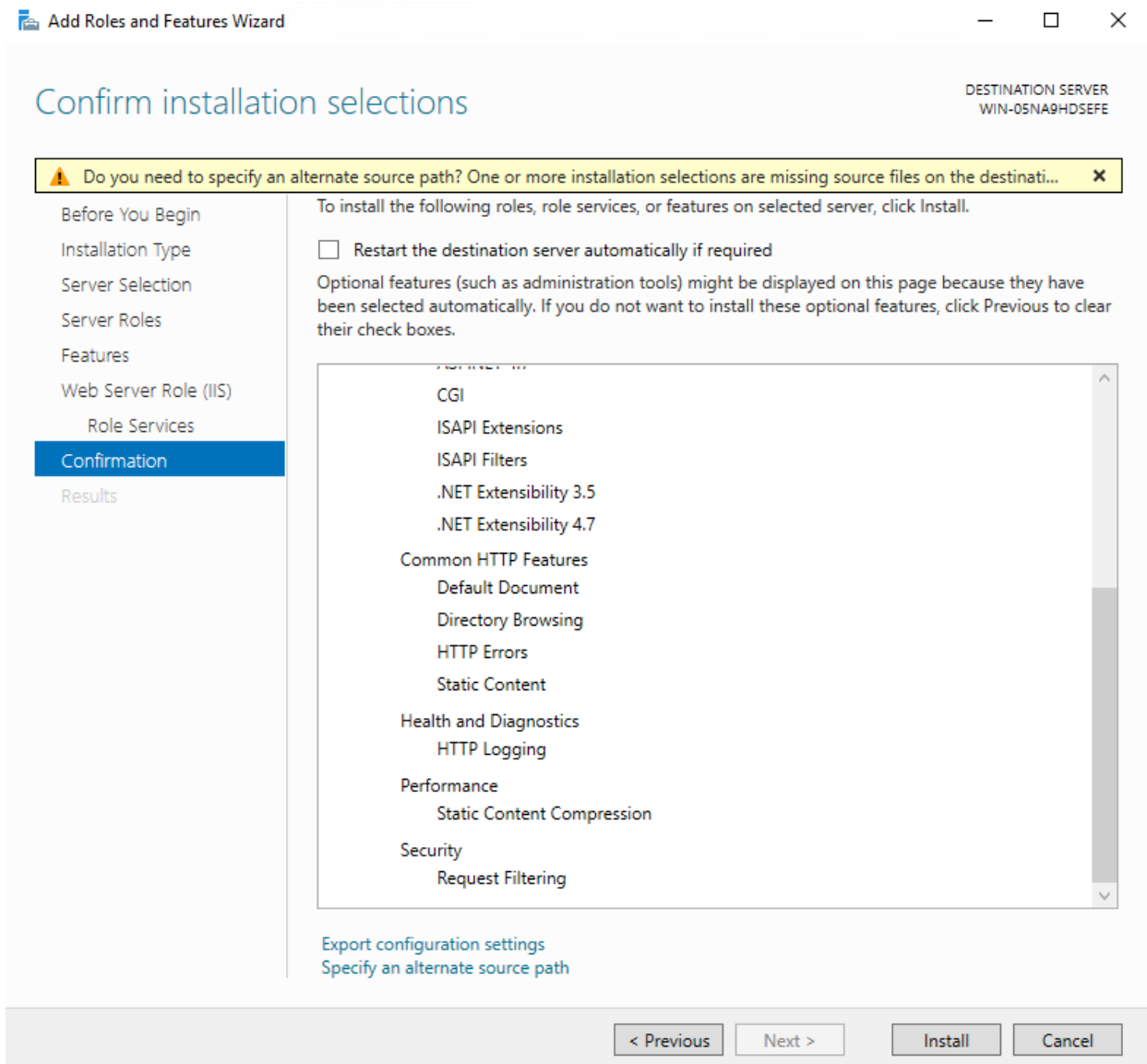
< Previous

Next >

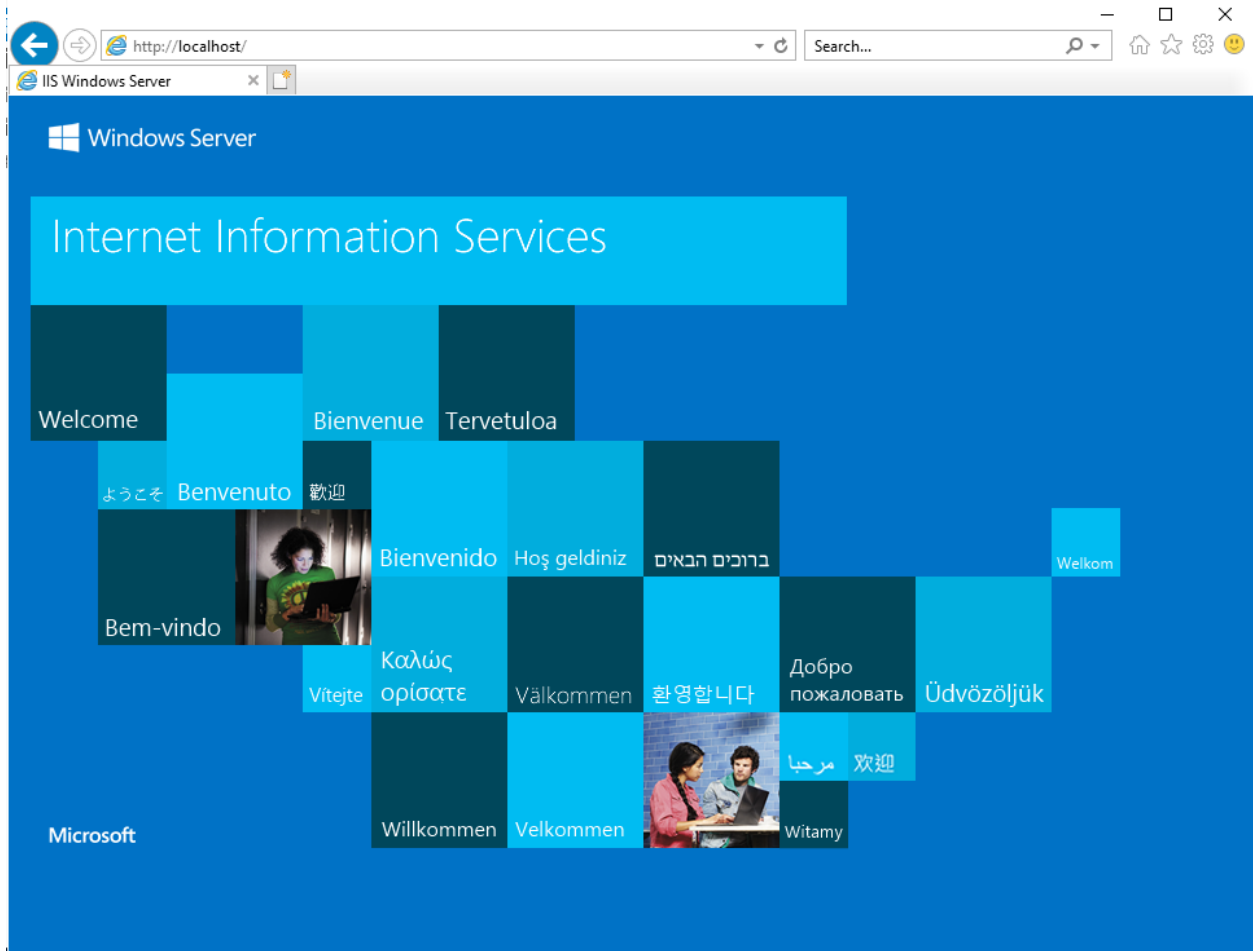
Install

Cancel

- Make sure the settings and press Install.

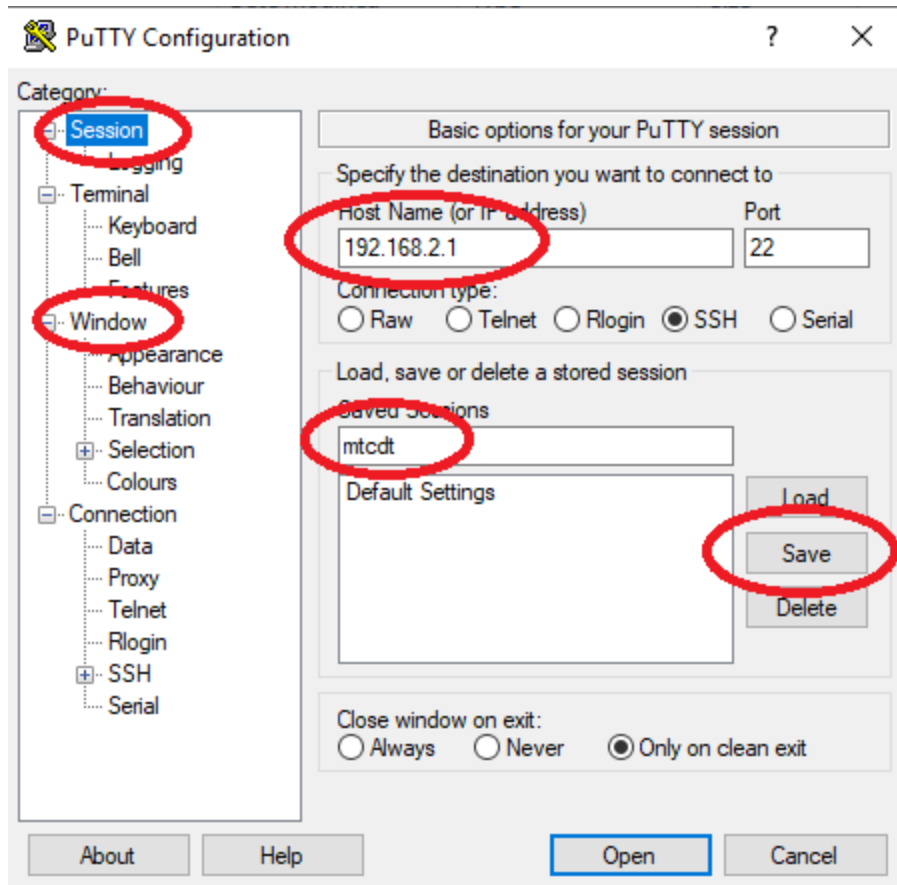


- It may ask to download required files, accept it
- Test by setting URL to <http://localhost> using IE Explorer



PuTTY Setup (~2 min)

- Run **putty-64bit-0.73-installer.exe** from "Setup_2019Server\Third Party"
 - Accept default settings
- Once installed, create a shortcut by right-click on putty.exe at "C:\Program Files\PuTTY" and select Send to Desktop
- Set the Windows columns to 170 and a session named "mtcdt" with IP address 192.168.2.1 to point to the Gateway and save it

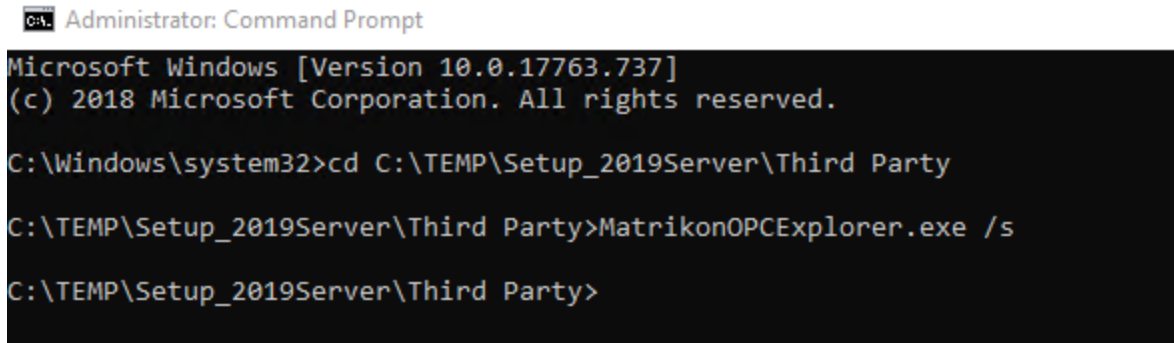


OPC Dependent DLL Setup (~1 min)

- Run **setup.exe** from "Setup_2019Server\Third Party\OPCEnvSetup"
 - Select Install to **Everyone**
 - Accept all other default settings

Matrikon OPC Explorer Setup (**Optional**) (~1 min)

- Run **MatrikonOPCExplorer.exe** from "Setup_2019Server\Third Party"
 - Open Command Prompt with Run as administrator
 - Go to the installation exe directory and run **MatrikonOPCExplorer.exe** with **/s** option
 - <https://honeywellprocess-community.force.com/opcsupport/s/article/How-do-I-run-Matrikon-OPC-Installers-which-use-Flash-on-Windows-where-flash-is-not-enabled>



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\TEMP\Setup_2019Server\Third Party

C:\TEMP\Setup_2019Server\Third Party>MatrikonOPCExplorer.exe /s

C:\TEMP\Setup_2019Server\Third Party>
```

Cypress Envirosystems Software and Environment Setup

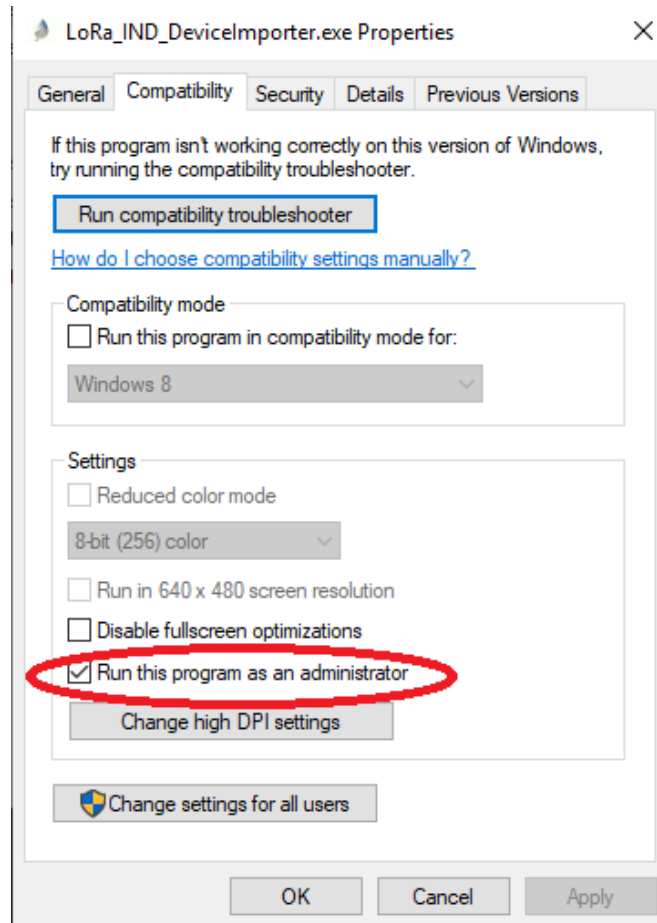
Run Installation Batch (~2 min)

- Run **Install_WinServer19.bat** as **administrator** from “Setup_2019Server\Software”
 - Create folders and copy files
 - Set up registries
 - Create shortcuts
 - Set up database
 - Install CYE Software Tools
 - Install LoRa DataCollector Service
 - Install WGR SMS Service
 - Install WGR OPC Service
 - Install Web App and Set up Web App Env
 - Install Web API and Set up Web API Env
 - Set up certificates
 - Set up scheduled tasks

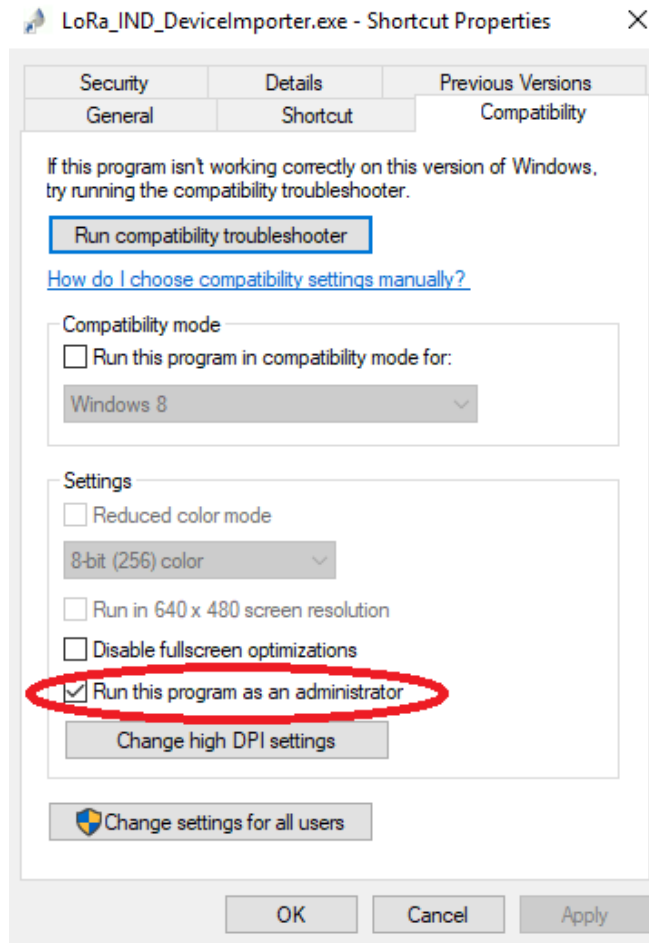
Environment Setup

Set the Device Importer To Run as Administrator (~1 min)

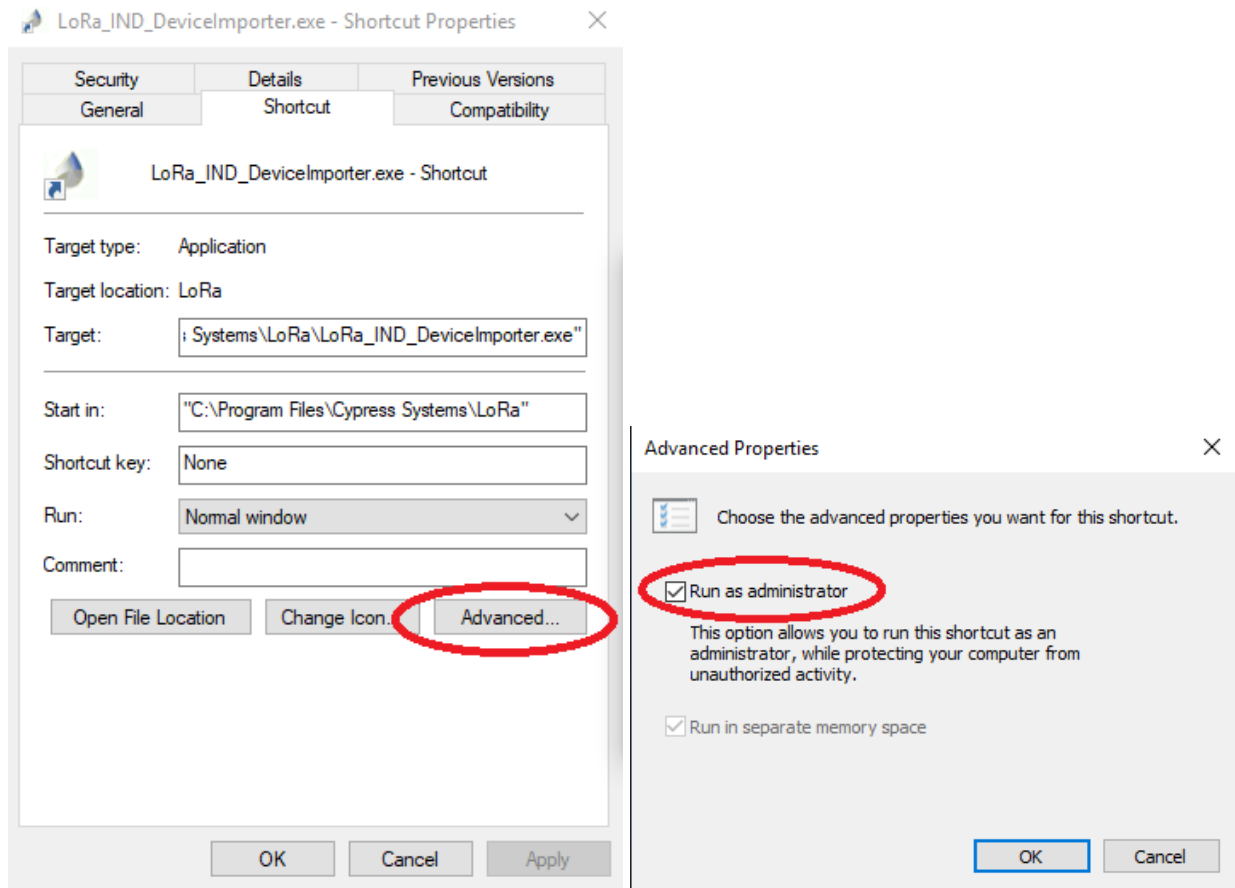
- Right click on the “LoRa_IND_DeviceImporter.exe” in the folder “C:\Program Files\Cypress Systems\LoRa”
 - Select Properties and check “Run this program as an administrator” on the Compatibility tab



- Right click click on the shortcut "LoRa_IND_DeviceImporter.exe - Shortcut" on the desktop
 - Select Properties and check "Run this program as an administrator" on the Compatibility tab



- Select the Shortcut tab and press “Advanced...”, then check “Run as administrator” on



Set the Image Viewer To Run as Administrator (~1 min)

- Right click on the “CYE_WDR_ImageViewer.exe” in the folder “C:\Program Files\Cypress Systems\LoRa”
 - Select Properties and check “Run this program as an administrator” on the Compatibility tab
- Right click on the shortcut “CYE_WDR_ImageViewer.exe - Shortcut” on the desktop
 - Select Properties and check “Run this program as an administrator” on the Compatibility tab
 - Select the Shortcut tab and press “Advanced...”, then check “Run as administrator” on

Set the Device Target (~1 min)

- Go the admin page and set the target device as “WGR/WTR”
 - Change the URL address to “https://localhost/wgrwebapp/admin.aspx” to access the admin page (with the credentials: master/wgrmaster)
 - Check the “WGR/WTR” only and press the “Update Site Devices” button

Configure Devices

Diagnostic Data-WGR/WTR

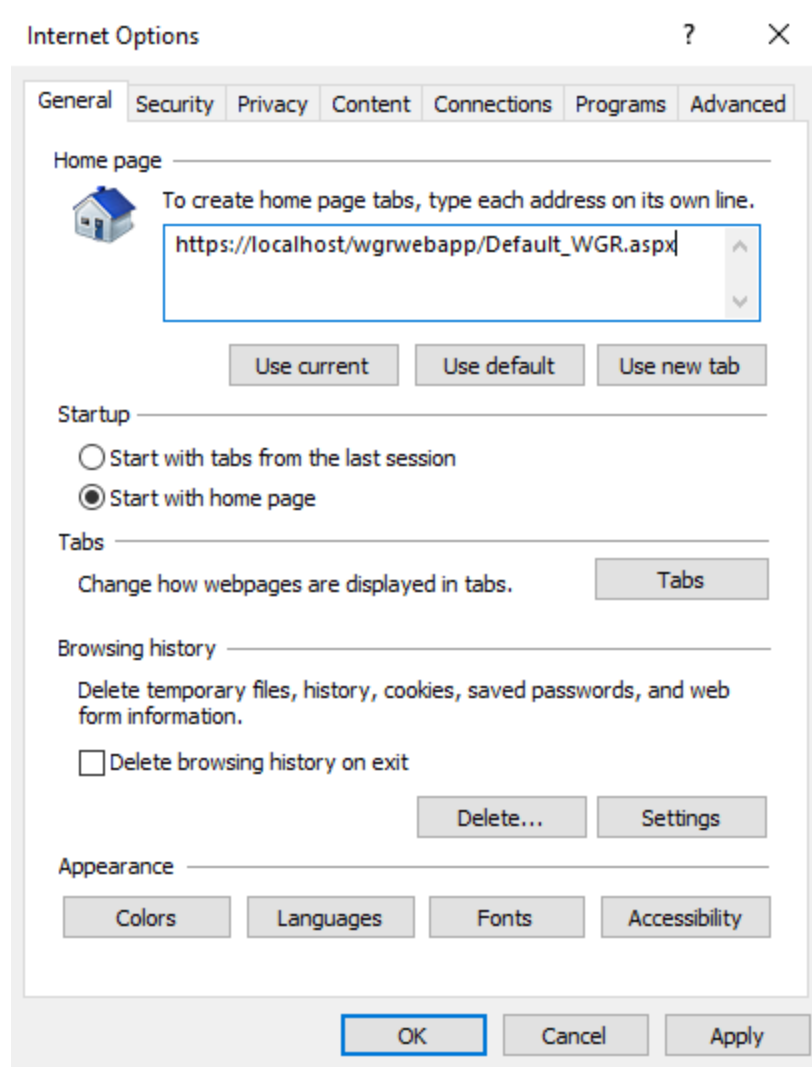
Configure Device

☒WGR/WTR
☐WFM
☐WSTM
☐WBM
☐WBCM

Update Site Devices

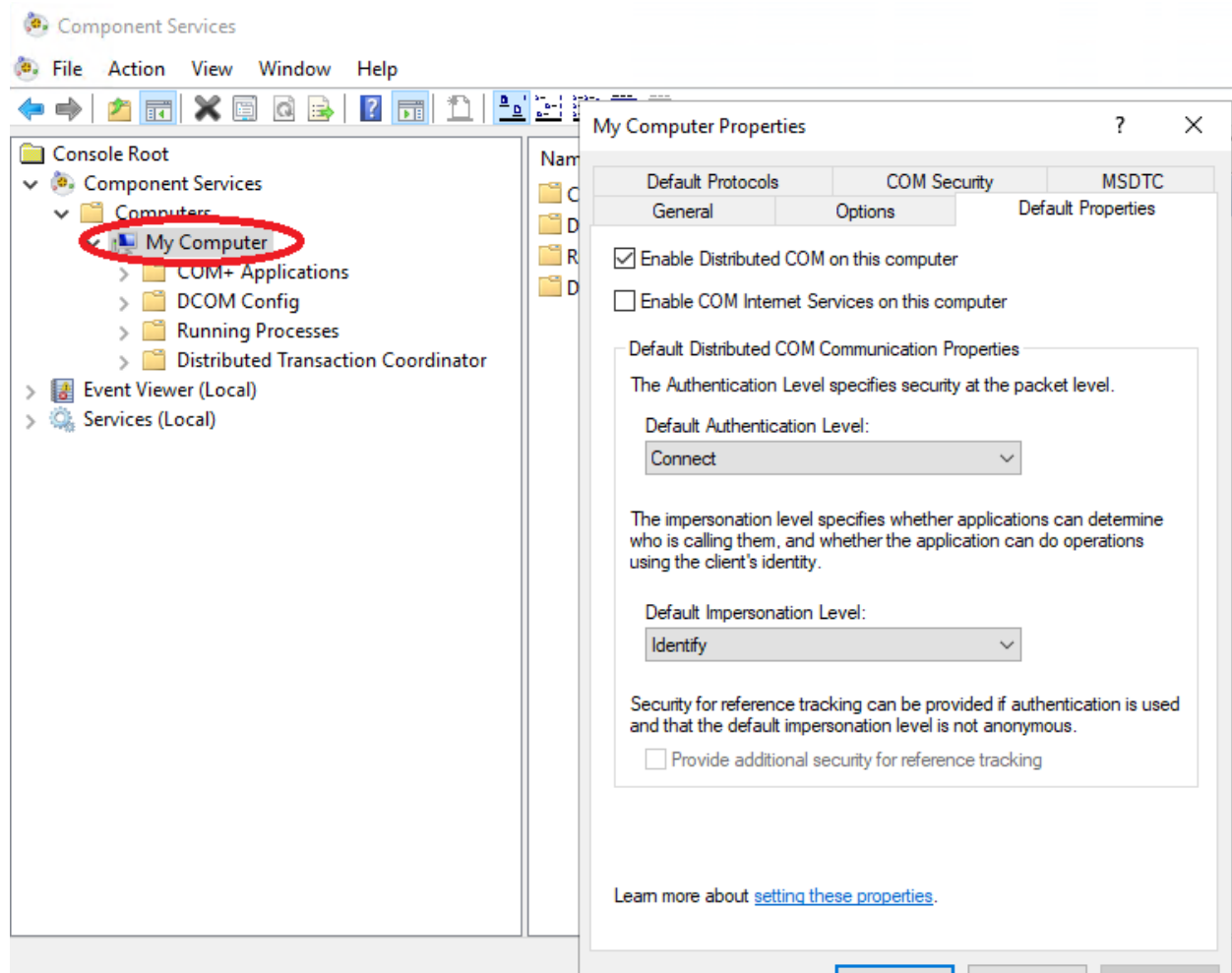
Set Browser Start Pages (~1 min)

- Set the home page for IE Explorer with following local link
 - https://localhost/wgrwebapp/Default_WGR.aspx

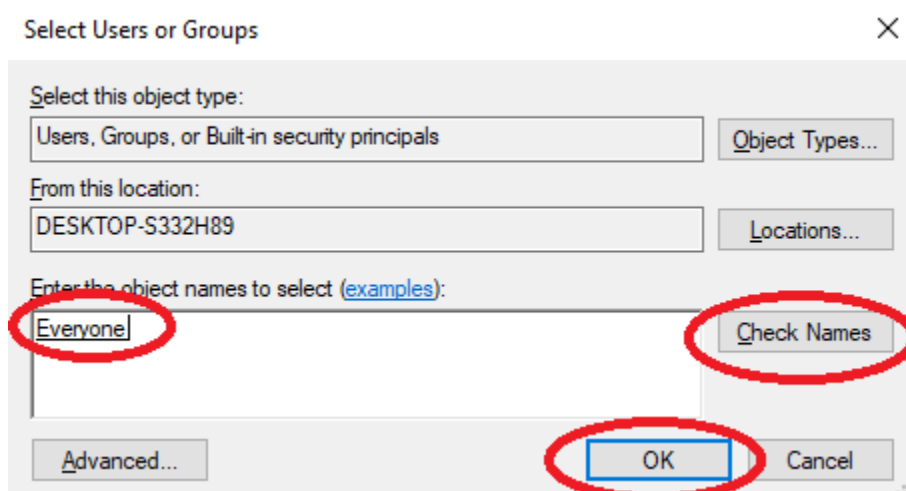
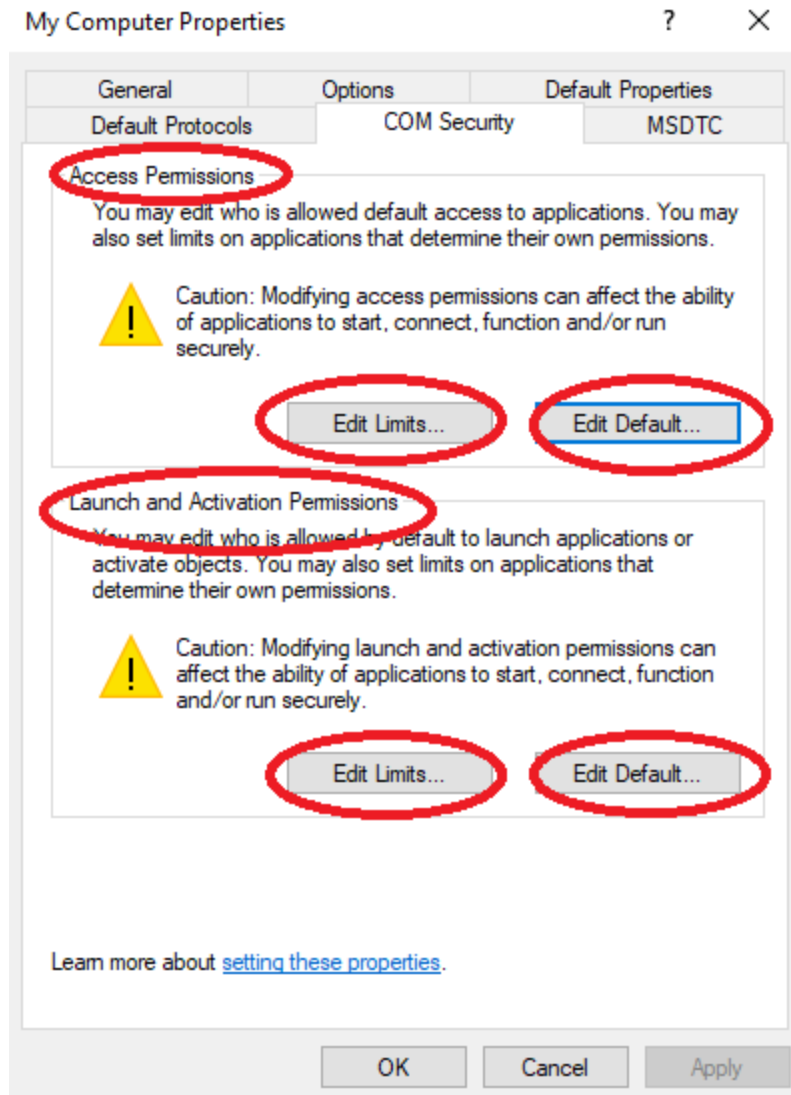


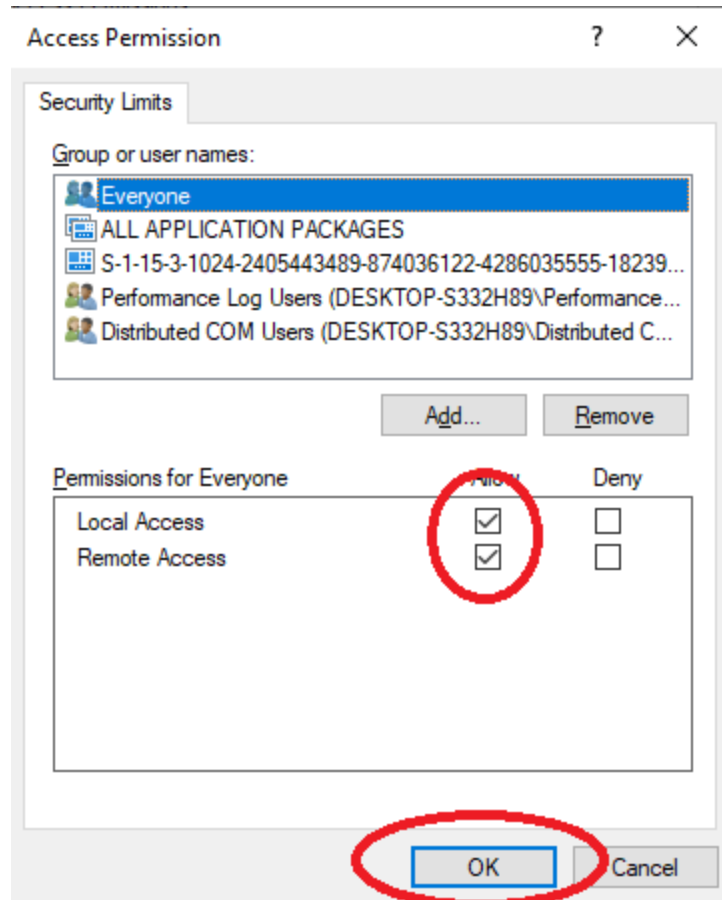
OPC Setup for Local Access (~6 min)

- Note that this makes it possible to access OPC data locally, suitable for the scenario that OPC client like Pi Interface is installed on the computer itself
- DCOM setup
 - From Component Services, navigate to **Console Root->Component Services->Computers->My Computer** and right click to **Properties**
 - On the **Default Properties** tab, make sure **Default Authentication Level** to **Connect**

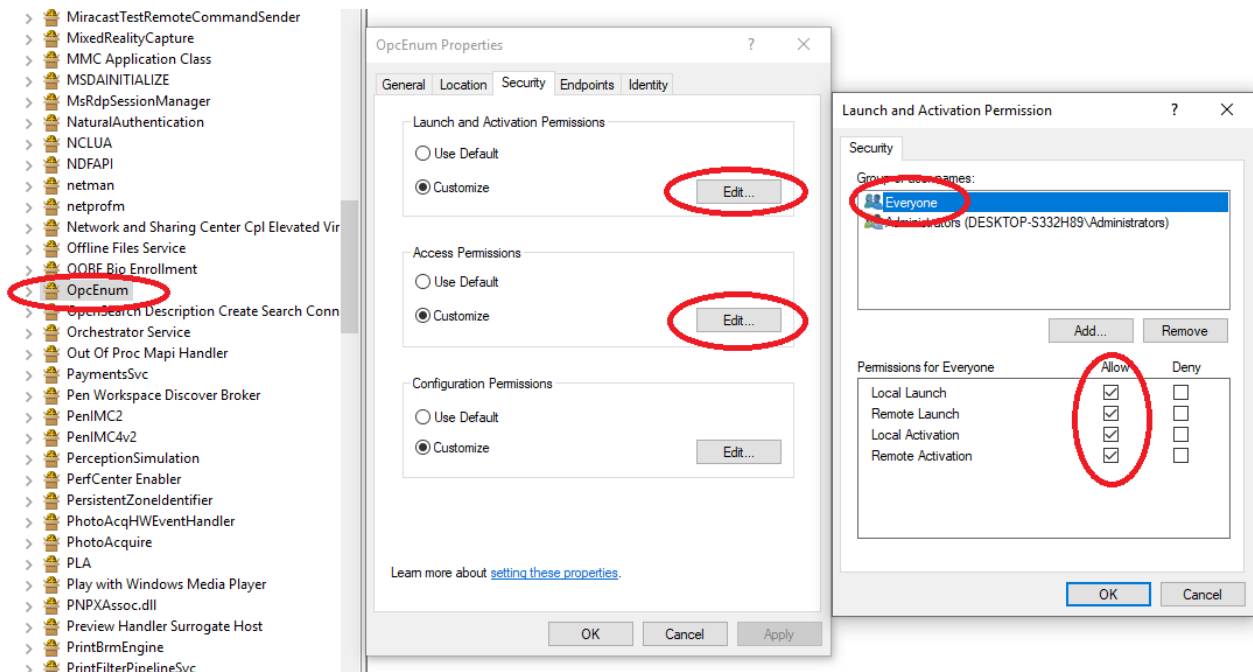


- On the **COM Security** tab, press **Edit Limits...** under **Access Permissions** to **allow all the permissions** for **Everyone**. (If **Everyone** is missing, use the **Add...** button and type **Everyone** under Enter the object names to select and press Check Names. Press OK.) Repeat the same procedure for **Edit Default...**
- Repeat the above for each **Edit Limits...** and **Edit Default...** under **Launch and Activation Permissions** to **allow all the permissions** for **Everyone**.





- Under the **DCOM Config** branch, right click on **OpcEnum** to select **Properties**
 - On the **General** tab, set **Authentication Level** to **Connect**
 - On the **Security** tab, press each **Edit...** button for under **Launch and Activation Permissions** and **Access Permissions** with **Customize** selected to allow all the permissions for **Everyone** (If **Everyone** is missing, use **Add...** button and type **Everyone** under Enter the object names to select and press Check Names. Press OK.)



- Under the **DCOM Config** branch, right click on **WGROPCServer** to select **Properties**
 - On the **General** tab, set Authentication Level to **Connect**
 - On the **Security** tab, press each **Edit...** button for under **Launch and Activation Permissions** and **Access Permissions** with **Customize** selected to allow all the permissions for **Everyone** (If **Everyone** is missing, use **Add...** button and type **Everyone** under Enter the object names to select and press Check Names. Press OK.)

OPC Setup for Allowing Remote Access (**Depending on the Requirement**) (~15 min)

- Note that this might be necessary only if the computer is accessed remotely over the network for OPC data
- Repeat the steps in OPC Local Setup for more users
 - For setting My Computer properties, repeat the set up steps of **Everyone** for other users such as **SYSTEM, NETWORK, INTERACTIVE, ANONYMOUS LOGON**
 - For setting **OpcEnum** and **WGROPCServer** properties. repeat the set up steps of **Everyone** for other users such as **SYSTEM, NETWORK, INTERACTIVE**
- Add Firewall exceptions
 - From the Control Panel, navigate to System Security->Windows Defender Firewall, select Allow an app or feature through Windows Defender Firewall. Press Change settings
 - Press another app and browse to select following apps and press Add
 - OpcEnum.exe under "C:\Windows\SysWOW64"

- WGRPCServer.exe under "C:\Program Files\Cypress Systems\WGRPCServer"
- OPCExplorer.exe under "C:\Program Files (x86)\Matrikon\OPC\Explorer"
- Restart the computer

Database Backup Location (**Depending on the Environment**) (~2 min)

- Default database backup location is created at "D:\DB_Backup". However, if the target computer does not have D drive or must have E drive instead, an alternative location should be designated. This example assumes "C:\DB_Backup" as an alternative.
 - Create a folder "C:\DB_Backup"
 - Using notepad, open "DB_Backup.cmd" from "C:\Program Files\Cypress Systems" and replace all "D:\DB_Backup" strings with "C:\DB_Backup". Then save it as "DB_Backup.cmd" at "C:\share". Copy (overwrite) this file to the original location "C:\Program Files\Cypress Systems".

DB_Backup.cmd - Notepad

File Edit Format View Help

@echo off

```
rem check for the existence of the backup folder, if it doesn't exist, then exit
if not exist D:\DB_Backup\ goto end) else (
```

```
rem del two week old backups if they exist:
```

```
if exist D:\DB_Backup\WGRData_Last.bak del D:\DB_Backup\WGRData_Last.bak
```

```
if exist D:\DB_Backup\WGRData_Arch_Last.bak del D:\DB_Backup\WGRData_Arch_Last.bak
```

```
rem rename week old backups if they exist:
```

```
if exist D:\DB_Backup\WGRData.BAK ren D:\DB_Backup\WGRData.BAK WGRData_Last.bak
```

```
if exist D:\DB_Backup\WGRData_Arch.bak ren D:\DB_Backup\WGRData_Arch.bak WGRData_Arch_Last.bak
```

```
rem Create new backup
```

```
@echo =====
```

```
@echo Backing up SQL Databases
```

```
sqlcmd -S . -i "c:\program files\cypress systems\DB_Backup.sql" -o "c:\WGRLog\DB_BackupLog.txt"
```

```
@echo =====
```

```
@echo wait for 10 sec...|
```

```
@ping 192.0.2.2 -n 1 -w 10000>nul
```

```
Exit )
```

```
:end
```

```
Exit
```

- Using notepad, open another file "DB_Backup.sql" from "C:\Program Files\Cypress Systems" and replace "D:\DB_Backup" with "C:\DB_Backup". Then save it as "DB_Backup.sql" at "C:\share". Copy (overwrite) this file to the original location "C:\Program Files\Cypress Systems".

```

DB_Backup.sql - Notepad
File Edit Format View Help
-- Backup SQL databases
DECLARE @name NVARCHAR(50) -- database name
DECLARE @path NVARCHAR(100) -- path for backup files

DECLARE @fileName NVARCHAR(200) -- path + filename for backup
DECLARE @fileDate NVARCHAR(40) -- used for file name

SET @path = 'D:\DB_Backup\'
SELECT @fileDate = CONVERT(NVARCHAR(40),GETDATE(),112)

SET @name = N'WGRData'
SET @fileName = @path + @name + '.BAK'
select @fileName
-- Backup the database with options to add the target set without any overhead or redundancy
BACKUP DATABASE @name TO DISK = @fileName WITH NOFORMAT, NOINIT, NAME = N'WGRData-Full Database Backup', SKIP

SET @name = N'WGRData_Arch'
SET @fileName = @path + @name + '.BAK'
select @fileName
-- Backup the database with options to add the target set without any overhead or redundancy
BACKUP DATABASE @name TO DISK = @fileName WITH NOFORMAT, NOINIT, NAME = N'WGRData_Arch-Full Database Backup', SKIP

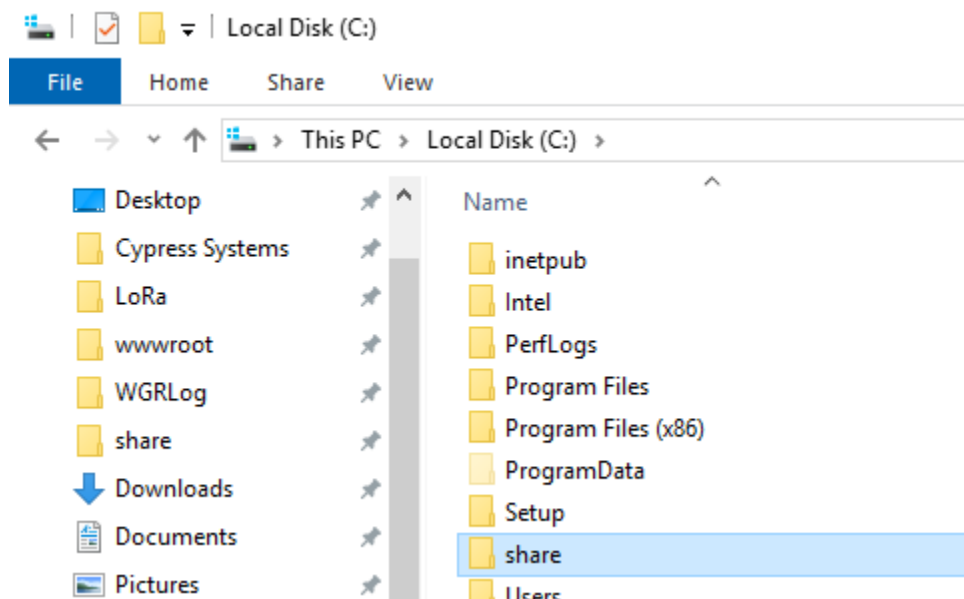
```

Add MultiTech Gateway Links as Favorite (Optional) (~1 min)

- For convenience, add the following link as an IE favorite (make sure network cable is connected to the MultiTech Gateway)
 - 192.168.2.1

Quick Access Pins (Optional) (~1 min)

- For convenience, create quick access links in Windows Explorer for frequent folders
 - Cypress Systems (C:\Program Files\Cypress Systems), LoRa (C:\Program Files\Cypress Systems\LoRa), wwwroot (C:\inetpub\wwwroot), WGRLog (C:\WGRLog) and share (C:\share)



- For convenience, add the Command Prompt and MS SQL Server Management Studio pins to the TaskBar