Honeywell

Immersive Field Simulator
R110.2

Installation and Configuration Guide

IMSDOC-X712-en-110A
February 2022

Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Contents

CHAPTER

1 ABOUT THIS GUIDE

The purpose of this guide is to provide guidance for installing and configuring the Immersive Field Simulator (IFS) R110.2 on-premises.

Revision history

Revision	Date	Description
A	December 2021	Initial release of the guide.

Intended audience

This guide is intended for the Honeywell Engineers, System Engineers, and the Trainers who are responsible for installing the Immersive Field Simulator application.

Abbreviations and acronyms

Term	Description
CIS	Center for Internet Security
CLL	Common Licensing Layer
CPU	Central Processing Unit
CSR	Certificate Signing Request
CRT	Certificate Revocation Tree
FQDN	Fully Qualified Domain Name
GPO	Group Policy
IC	Immersive Competency
IFS	Immersive Field Simulator

Term	Description
IIS	Internet Information Services
OS	Operating System
OTS	Operator Training Simulator
SSL	Secure Sockets Layer
SQL	Structured Query Language
TLS	Transport Layer Security

CHAPTER

2 INTRODUCTION

IFS is an on-premises solution that provides a virtual platform to experience the virtual plant walkthrough and component interaction. With IFS, instructors and field operators can experience and interact with the plant in a virtual platform. IFS brings the virtual plant walkthrough experience to the training room wherein, the virtual training can be carried out in a hazard-free environment.

The virtual platform provides significant advantages of being available on-demand, giving freedom of accessibility, and delivering an immersive learning experience.

Salient features

IFS contains the following salient features.

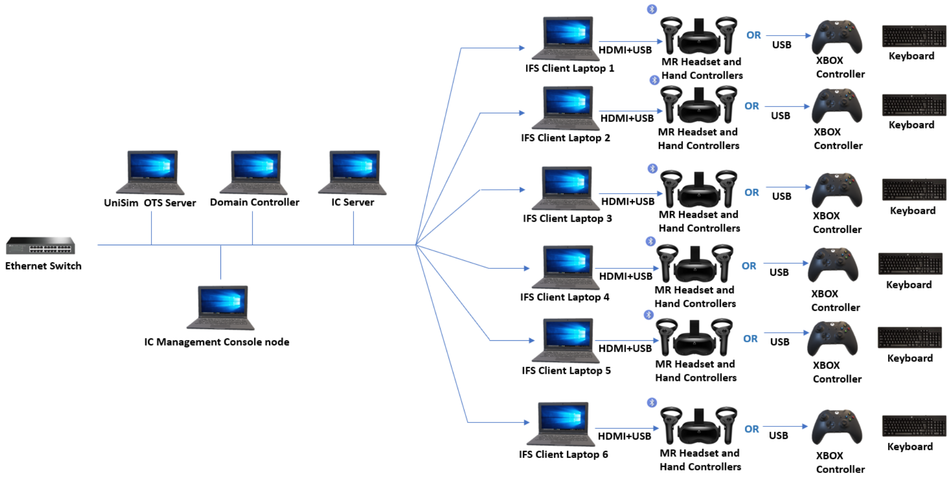
- **Plant Walkthrough**- Enables user to explore the plant.
- **Plant operations -** Enables user to explore and interact with the equipments as well.
- **Guided Lessons** - Enables user to select a starting point in the plant for navigation.
- **Lesson Assessment** - Enables the trainee to take the assessment for learnt lessons.
- **Search and Navigate** - Enables to Search for an equipment with the partial or full tag name.
- **Dynamic Animation** - Enables the Field Operator to visualize how the internal process functions based on the actions in the plant.

System components

This section provides information about components, terminology used, and a brief overview of user's tasks.

System set up

All the IFS components are connected on the same network. IFS supports up to 6 users in multi-mode scenario. The following diagrams show the IFS components and the communication.



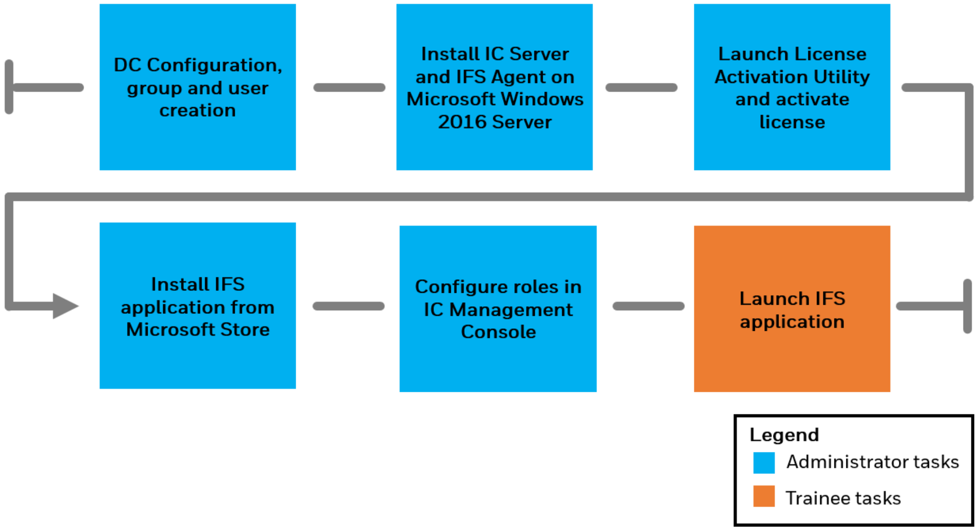
NOTE: For multi user, you must purchase Photon License. This supports up to 6 users. Photon license must be installed along with IFS licenses in IC server machine. For more information on Photon license installation, see Photon license installation.

Terms and Definitions

Component	Definition
IC Server	A centralized server to collect user information from Domain Controller. IC Server is hosted on an isolated network that runs on Windows 2016 system.
IC Management console	A web based IC Management Console enables you to assign roles, import/export assets and upload tags.The web-based IC Management console enables you to activate the license and create users, assign roles, and map users to specific project. As an Administrator, you can launch IC Management Console from IC Server **Start>IFS>IFS Dashboard**. Other users can type **https//:<ICServer FQDN>:44340** address in the browser.
IFS Agent for OTS Server	IFS Agent for OTS Server
IFS Client application	IFS is an application that provides a virtual platform to experience the virtual plant. It can be installed from Microsoft store on gaming laptop.

Task overview

The following image provides an overview of tasks each user must perform.


DC Configuration, group and user creation
Install IC Server and IFS Agent on Microsoft Windows 2016 Server
Launch License Activation Utility and activate license
Install IFS application from Microsoft Store
Configure roles in IC Management Console
Launch IFS application
Legend
Administrator tasks
Trainee tasks

Users and Roles

IFS is a role-based application. Following are three distinct users.

Users	Capabilities
Administrator	Install the IFS components, configure user roles, create projects, assign users to the project and import/export assets. import/export hardware setup and training modules.
Trainer	Conduct trainings. Trainer has the privilege to provide trainee access to OTS Serverimport/export/create hardware setup and training modules, and oversee the Trainee progress.
Trainee	Field operators who are responsible to learn to operate a plant using a virtual training platform.

Each of the above users must be created in the Domain Controller and assigned to the required global security groups.

CHAPTER

3 SECURITY CONSIDERATION

This section covers some important security considerations while installing and configuring the IFS. See "System components" on page 9 for the system deployment diagram. IFS nodes include IC Server, IFS Client laptop, and Management Console node. It is recommended to adhere to the following security measures in conjunction with the site-specific measures. It is the responsibility of the user to protect all the IFS nodes and the environment in which it operates.

System and Network protections

Physical access

It is recommended to protect all the IFS nodes from unauthorized access by applying appropriate site-specific physical access control measures.

Communication controlled zone

Ensure IFS communications occur in a controlled network where the source of denial of service is identifiable and the risk of this occurring is minimal.

Intranet communications

Ensure that the IFS nodes are not connected to internet or other business/production networks within the site.

Enable anti-virus software

Ensure that anti-virus software is installed on all the IFS nodes and anti-virus data files are kept up to date.

Make sure that only the recommended secure ciphers are enabled on the system.

CIS level benchmark

It is recommended to install and maintain IFS software in the IFS nodes that adhere to CIS level 1 benchmark recommendations. This includes measures such as password policies, anti-virus scan, account lockout policy, windows updates, and so on. To know more about CIS Benchmark, see https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-cis-benchmark?view=o365-worldwide.

End-point encryption

It is highly recommended that the IFS server is protected with end-point encryption mechanism, so that the IFS data residing on the server is secured.

Backup and Restore

It is recommended to follow site-specific policies for taking periodic backups of all the IFS nodes. It is recommended to include the following IFS components as part of the backups.

- SQL databases
- IFS data files stored in the path *C:\ProgramData\Honeywell\IFS*

Password policies

It is strongly recommended to use CIS Level 1 benchmark recommended password policies. This includes policies on password complexity, password age/expiry, password history, and so on.

File protections

Scan files before uploading

Make sure that all the files being uploaded to Management Console are scanned using an anti-virus software.

Files from trusted sources

Ensure that any file read/written is protected and is retrieved from a trusted source. The following are a few scenarios where this is especially important.

- Importing files to Assets Management.
- Importing Tags Mapping files to Tags Management.
- Uploading License files.

- Uploading files to Asset Catalog.
- Importing OTS checklist during lesson creation.
- Importing lessons.

Web communications protections

Avoid using self-signed certificates

It is highly recommended to avoid using self- signed certificates. Use digital certificates issued by a trusted third-party Certificate Authority.

Enable only TLS v1.2

Ensure that only TLS v1.2 is enabled on all the IFS nodes and IFS Client laptops. SSLv1, SSLv2, SSLv3, TLS v1.0 and TLS v1.1 should be disabled.

Make sure that only the secure cipher suites are enabled on the system.

Firewall configuration for the ports

Ensure that all application-specific ports are closed by default on the windows firewall and only the following ports are opened for incoming communications on the IFS Client application. These ports are opened and used while installing IC Server.

- TCP-44336
- TCP-44339
- TCP-44343
- TCP-44340
- TCP-843
- TCP-4530
- TCP-4531
- TCP-44338

Passwords

It is strongly recommended to use CIS Level 1 benchmark recommended password policies. This includes policies on password complexity, password age/expiry, password history, and so on.

Password complexity

Provide a password that meets the following complexity requirements.

1. A minimum of 8 characters.
2. A maximum of 31 characters (optional).
3. At least one uppercase letter.
4. At least one number.
5. At least one special character.
6. Password should not contain the user's account name.

Password Age and Expiry

Ensure to set password age to 60 or fewer days to avoid brute force attack. Setting up minimum password age increases the risk of brute force attack.

Password History

Ensure that the password history is set to 24 or more passwords. This prevents using same password for longer time.

Use of Dictionary words

The password should not contain the following characters:

- Percentage (%)
- Comma (,)
- Double-quotes (“)
- Backslash (\)

Account Lockout or Authentication throttling

To protect the system from brute-force authentication attack, the system should have a feature that disables an user account when a certain number of failed logons occur due to wrong passwords within a certain interval of time.

When the maximum number of unsuccessful attempts is exceeded, the throttling mechanism must automatically do one of the following.

- Lock the account or node for a predetermined period
- Lock the account or node until it is released by an administrator
- Delay the next login attempt

Also, ensure that Account Lockout mechanism is configured for system accounts based on the number of failed attempts.

It is recommended to provide an appropriate value to the Account Lockout threshold to prevent any attack on the account. To know more about Account Lockout option, see https://docs.microsoft.com/en-us/services-hub/health/remediation-steps-ad/set-the-account-lockout-threshold-to-the-recommended-value#suggested-actions.

CHAPTER

4

INSTALLATION

This section provides information on downloading, installing, activating license, and configuring all the IFS components.

IFS has three installable components:

- IC Server
- IFS Agent
- IFS Client application

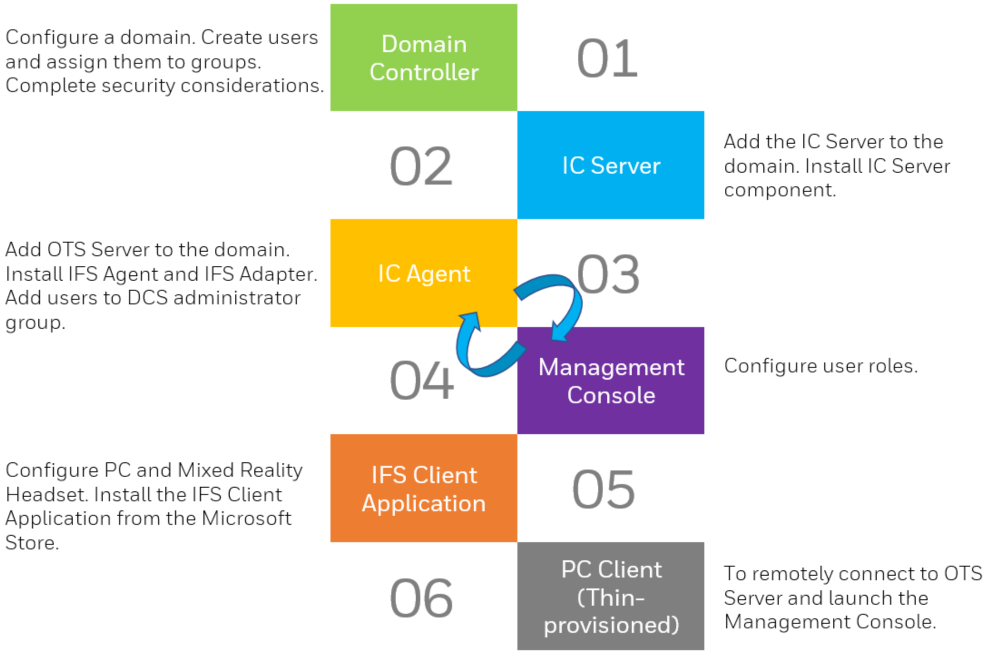
The components must be individually installed on separate systems. It is strongly recommended to harden the IFS nodes using CIS level 1 lockdown before installing the IFS application.

Accessing installer

The following table provides information on the installer location of different components of IFS.

Component	Installer Location
Installer Location	[Installation_Media]/Server_Media
IFS Agent	[Installation_Media]/Agent_Media
IFS Client application	Microsoft Store

The following image shows high-level installation tasks to start using the solution.



01 Domain Controller

Configure a domain. Create users and assign them to groups. Complete security considerations.

02 IC Server

Add the IC Server to the domain. Install IC Server component.

03 IC Agent

Add OTS Server to the domain. Install IFS Agent and IFS Adapter. Add users to DCS administrator group.

04 Management Console

Configure user roles.

05 IFS Client Application

Configure PC and Mixed Reality Headset. Install the IFS Client Application from the Microsoft Store.

06 PC Client (Thin-provisioned)

To remotely connect to OTS Server and launch the Management Console.

Make sure IC Server, IC Agent, IC Application, and thin-client are all connected to the same network.

Domain controller

You must first create domain groups and users and then assign user to the respective groups. For more information about setting up a domain controller, see the Windows Domain and Workgroup Implementation Guide specific to the server version. The following link provides information about configuring Domain for Windows 2016 - https://docs.microsoft.com/en-us/archive/blogs/canitpro/step-by-step-setting-up-active-directory-in-windows-server-2016.

As part of security considerations, enable authentication only through the Kerberos and disable NTLM. For more information about enabling and disabling authentication, see "Configuring Active Directory Authentication" on page 25.

Creating Domain Groups

Create the following global security groups shown in the table.

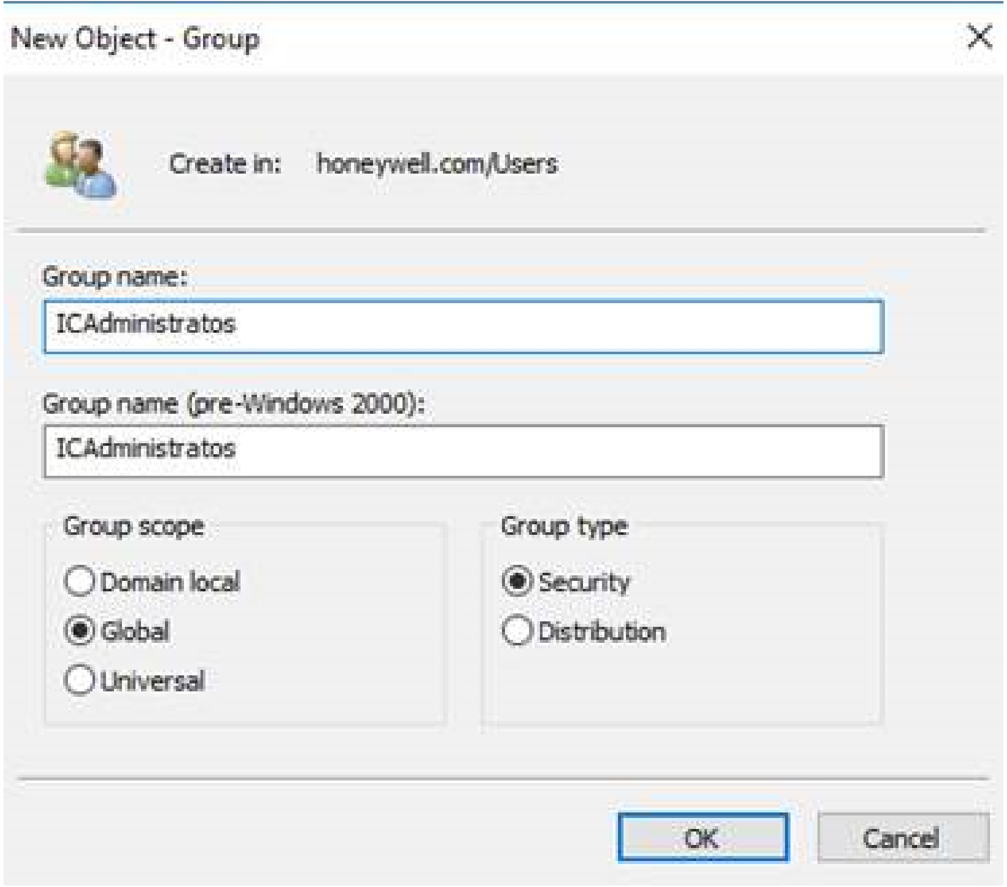
User group	Specification
ICAdministrators	Administrative access to the IFS Components, to configure roles, manage license, perform field operator actions and view 3D plant environment and process simulation data.
ICArtists	Access to upload asset bundles on Asset Catalog.
ICDBAdministrators	Access database with Administrative privilege.
ICDomainExperts	Define assets, review or comment on asset bundles
ICLeadArtists	Review, comment, approve or reject the asset bundles uploaded on Asset Catalog.
ICOTSUsers	Authorise IFS-OTS usage.
ICTrainees	Trainee access to the IFS Components to perform field operator actions, view 3D plant environment and process simulation data.
ICTrainers	Trainer access to the IFS Components to define lessons, perform field operator actions and view 3D plant environment and process simulation data.
ICUsers	Contains all IFS user accounts as members.

> **NOTE:** Groups definition on Domain controller are case-sensitive, hence make sure groups are created with same capitalization as mentioned above. In case of mismatch, ICAdministrators user will be unable to edit permission.
>
> Make sure to assign a unique user or access ID to every person accessing the system to prevent multiple users from sharing the same account or access ID.

Perform the following procedure to create Domain Groups.

1. Go to **Start > Control Panel > Administrative Tools** and then click **Active Directory Users and Computers**.
2. In the Active Directory Users and Computers window, click **Users in the current domain**.

3. Right-click on Users and go to **New > Group**.
4. Fill in the Group details and then click **OK**.



New Object - Group

Create in: honeywell.com/Users

Group name:
ICAdministratos

Group name (pre-Windows 2000):
ICAdministratos

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

By using the above procedure, you can create all the Domain Groups.

Users and Roles

IFS is a role-based access system. Following are six distinct users. The following table provides information on the users and their roles.

Users	Capabilities
ICAdministrator	Install the IFS components, create projects, import/export assets, upload tags and configure user rolesmap user to OTS Server and Client.
ICTrainer	Trainer has access to load USO model and Freeze\Unfreeze simulation on OTS Server.
ICTrainee	Field operators who are responsible to learn to operate a plant

Users	Capabilities
	using virtual training platform.
ICDomainExpert	Register, edit, approve, publish, and download the assets. Upload map view layout file.
ICArtist	Download, review, upload, and delete the assets (Self created).
ICLeadArtist	Download, upload, and delete the assets (Self created).
Service User Account	Communicate between services and access information

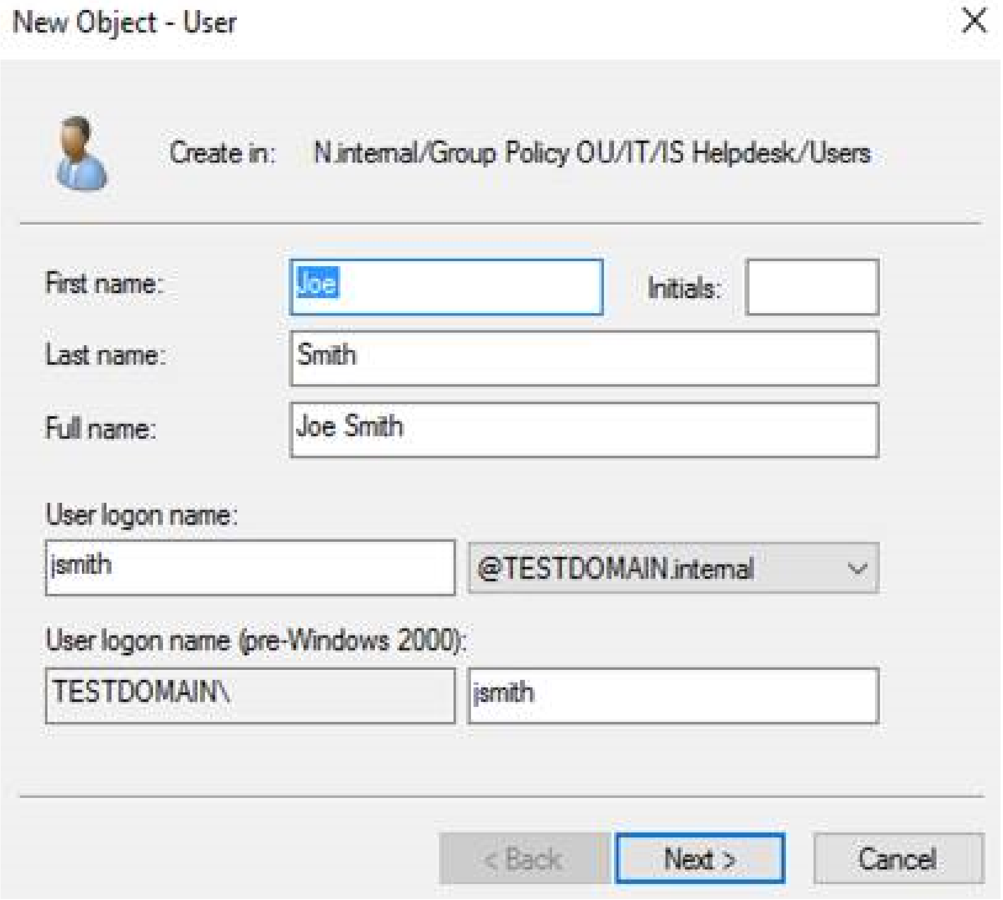
Each of the above users must be created in the Domain Controller and assigned to the required global security groups. For more information about the domain group, see Creating Domain Groups and Creating Domain Users.

> **NOTE:** Make sure that Service user account is denied logon permissions.

Creating Domain Users

1. Go to **Start > Control Panel > Administrative Tools** and then click **Active Directory Users and Computers**.
2. In the Active Directory Users and Computers window, click **Users in the current domain**.
3. Right-click on **Users** and go to **New > Users**.

4. Right-click on **Users** and go to **New > Users**.



New Object - User

Create in: N.internal/Group Policy OU/IT/IS Helpdesk/Users

First name: Joe

Initials:

Last name: Smith

Full name: Joe Smith

User logon name: jsmith @TESTDOMAIN.internal

User logon name (pre-Windows 2000): TESTDOMAIN\ jsmith

5. Enter the new password and confirm the same password again.

Select the "**User must change password at next logon**" check box. Click **Next** to finish creating Domain Users.

By using this procedure, you can create all the Domain Users.

Associating the created Domain Users with the Domain Groups

Domain User	Domain Group
Adminuser	ICAdministrators and ICDBAdministrators
Domainexpertuser	ICDomainExperts
Leadartistuser	ICLeadArtists
Artistuser	ICArtists
Traineruser	ICTrainers and ICOTSUsers
Traineeuser	ICTrainers and ICOTSUsers
ICServiceuser	ICUsers
ICAdministrators, ICDBAdministrators, ICDomainExperts, ICLeadArtists, ICArtists, ICTrainers, ICTrainees, and ICOTSUsers	ICUsers

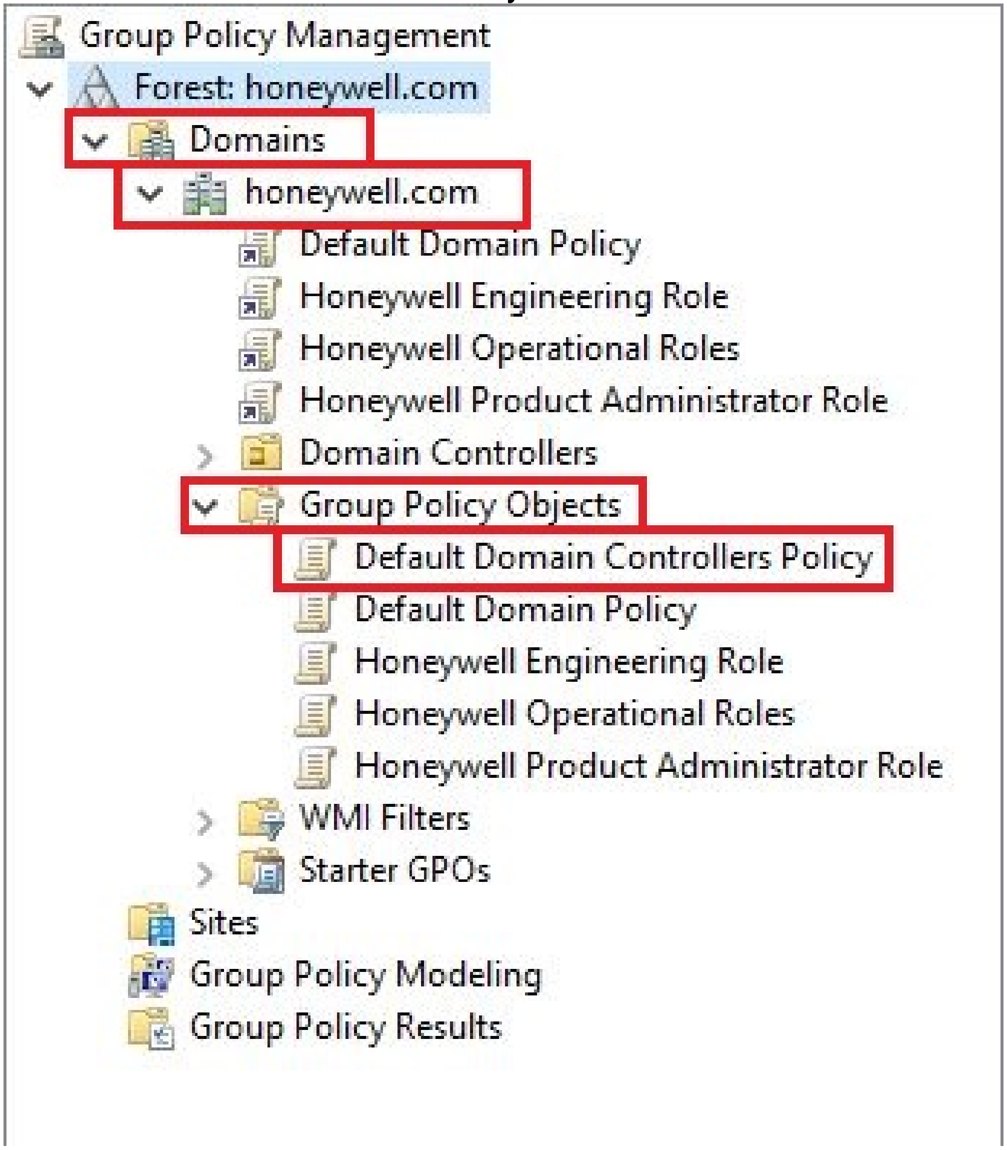
NOTE: Users names can be modified but Groups names are by default and can’t be modified.

Deny interactive logon for Service Account

This section provides information on the procedure to deny interactive logon for service user account. This procedure is applicable for Domain Controller. Use the following procedure to deny interactive logon for service user account.

1. Open command prompt and type **gpmc.msc.**
2. On the Group policy Management pane, expand **Forest** node.

3. Navigate to **Domains > honeywell.com > Group Policy Objects**, right-click **Default Domain Controllers Policy** and click **Edit.**



- Group Policy Management
  - Forest: honeywell.com
    - Domains
      - honeywell.com
        - Default Domain Policy
        - Honeywell Engineering Role
        - Honeywell Operational Roles
        - Honeywell Product Administrator Role
        - Domain Controllers
        - Group Policy Objects
          - Default Domain Controllers Policy
          - Default Domain Policy
          - Honeywell Engineering Role
          - Honeywell Operational Roles
          - Honeywell Product Administrator Role
        - WMI Filters
        - Starter GPOs
    - Sites
    - Group Policy Modeling
    - Group Policy Results

4. On the Computer Configuration pane, navigate to **Policies > Windows Settings > Security Settings > Local Policies.**
5. Click **User Rights Assignments > Deny log on locally.**
6. Enter the service account **Username** created and save the GPO.
7. Allow the workstations and servers to apply the new GPO, then attempt to do an interactive logon from a workstation or server using service account username created. The logon attempt should fail.

Configuring Active Directory Authentication

For secure communication, Honeywell recommends to enable Kerberos and disable NTLM authentication.

Perform the following configuration on Domain Controller to secure the communication.

1. Enable the Kerberos authentication.
   a. Click **Start > Control Panel > Administrative Tools > Active Directory Users and Computers**.
   b. Expand **<domain>.com** and select **Domain Controller**.
   c. Right-click on Domain Controller machine and select **Properties**.
   d. In the **Delegation** tab, select **Trust this computer for delegation to any service (Kerberos only)** option.
   e. Click **Apply** and then **OK**.
2. Disable the NTLM authentication.
   a. Open **Local Group Policy Editor** and perform the following steps.
      i. Click **Windows+R** button.
      ii. Enter ***gpedit.msc*** and click **OK**. The Local Group Policy Editor window appears.
   b. Expand the **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.
   c. Navigate to Security Option and click **Network Security: Restrict NTLM: NTLM authentication in this domain**.
   d. Right-click on **Network Security: Restrict NTLM: NTLM authentication in this domain** and select **Properties**.
   e. Select **Deny all** option from the drop-down list.
3. Add IC Server and OTS Server to the exception list. Add IC Server and all the OTS Server to the exception list after **Network Security: Restrict NTLM: NTLM authentication in this domain** policy is enabled. User is not able to add any server exception if the policy is not enabled.
   a. Open the **Local Group Policy Editor**, and perform the following steps.
      i. Click **Windows+R** button.
      ii. Enter ***gpedit.msc*** and click **OK**. The Local Group Policy Editor window appears.
   b. Expand the **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.
   c. Navigate to Security Options and click **Network Security: Restrict NTLM: Add server exception in this domain**.

d. Right-click on **Network Security: Restrict NTLM: Add server exception in this domain** and select **Properties**.

e. Enter the host name of IC Server and OTS Server. To enter multiple servers, click **Enter** after specifying each server.

> **NOTE:** Make sure to enter only the machine names in exception list. For example, if the server name is SIQIC, then only SIQIC must be entered here.

f. Click **Apply** and then click **OK**.

IC Server

This section provides information about installing and configuring IC Server component.

IC Server requirement

This section provides information about the specifications of physical machine or VMs for IC Server.

Hardware requirements

Requirement	Specification
RAM	Minimum of 16 GB (Make sure reserved space is 16 GB on the Virtual Machine during the run-time)
Disk space	Minimum 80 GB
CPU	Single Intel quad-core, 3.0 GHz Processor (or higher)
Network	Full duplex 100 Mbps Ethernet or higher

Software requirements

Requirement	Specification
Operating System	Microsoft Windows Server 2016 Standard Edition (64-bit)
OpenSSL	Light version (64-bit) – (Required for certificate binding). For more information about installing, see Generating Private key.
Anti-virus	VSE + ASE 8.8.0 Patch 10 and Engine 5900 or higher.
Microsoft Hotfixes	Windows10.0-kb4103723-x64_ 2adf2ea2d09b3052d241c40ba55e89741121e07e.msu
Browsers supported	Microsoft Edge, version 86.0 and later, Google Chrome, version 86.0 and later, Firefox, version 86.0 and later.

Pre-installation tasks

Before installing IC Server component, complete the following configurations.

1. Set DNS server IP Address and add the Server to the Windows Domain.

   For more information about configuring, see *Adding workstation/server to Windows domain* in the following guide: https://docs.microsoft.com/en-us/archive/blogs/canitpro/step-by-step-setting-up-active-directory-in-windows-server-2016.

   > **NOTE:** Do not change the IP Address. No specific host file update is required.

   > **NOTE:** If you change the IP address after the installation, it may result in a communication breakage between the machines. For support, contact the TAC team.

2. Log in with local administrator user account and then add installation account to the local administrators' group.

   > **NOTE:** Log in with a domain user, who has the privileges of domain **ICAdministrators**, domain **ICUsers**, domain **ICDBAdministrators**, and also login domain user must be part of **Local Administrators** group.

3. Procure a trusted certificate.

   For more information about certificate creation and binding, see "Creating the SSL certificate on the IC Server" on the facing page.

4. Ensure that Remote Registry service is running on all the machines. For more information about enabling service, see "Enabling Remote Registry Service" on page 36.
5. Disable Windows Updates. For more information, see "Disabling the Microsoft Windows Updates" on page 37.

> **NOTE:** Make note of the Fully Qualified Domain Name (FQDN) of the server. The FQDN of the server is required while installing the IFS Agent on the OTS Server and launching the IC Management Console from OTS Server.

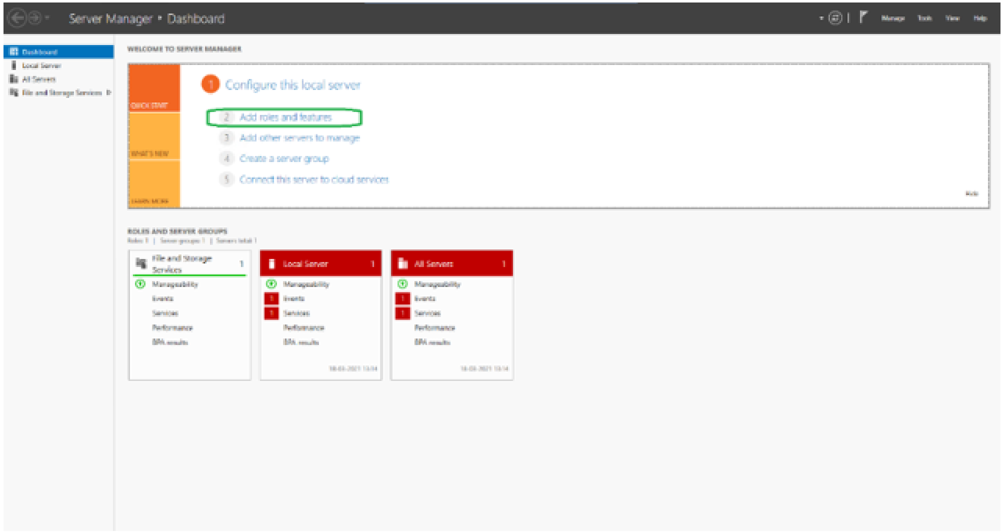
> **NOTE:** At some point during the installation process, the server reboots and attempts to complete the installation afterward. While rebooting, Windows automatically unmounts the **.iso** file, the installation comes to a halt at that point, but the installation package does not give any feedback about this issue. It just stops.
>
> Make sure you copy the contents into a separate folder under a local drive so that it will not be unmounted when the server reboots automatically.

Creating the SSL certificate on the IC Server

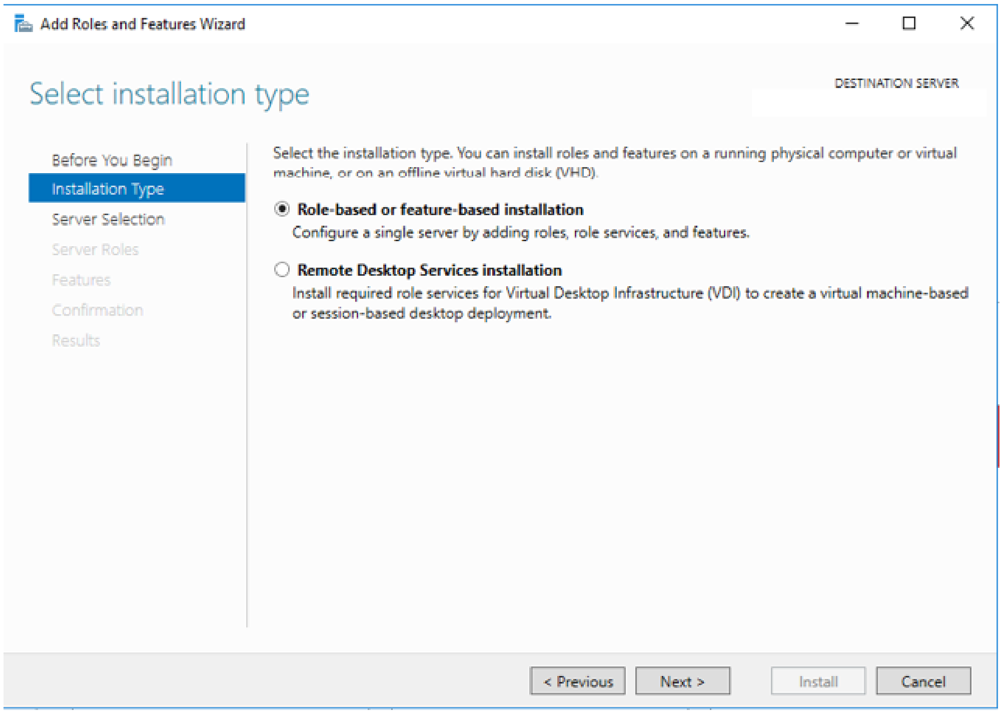
SSL certificate signed by Certificate Authority is required for securing the communication. Choose to request for new certificate either before or after installing the IC Server component. The SSL certification process can be performed in two-stages. In first stage, request for new certificate, generate private key and share the CSR with agency for approval. Once it is approved, user receives a CRT file. This CRT file must be installed. In stage 2, after installing IC Server, install the certificate, bind the IC Server specific sites displayed to certificate and add these sites to the trusted sites in the browser.

Prerequisite:

1. Enable the Internet Information Services (IIS) console.
   a. Click **Start Server Manager Add roles and features**. **Add Roles and Features Wizard** screen appears.



b. Follow the on-screen instructions and Click **Next**.



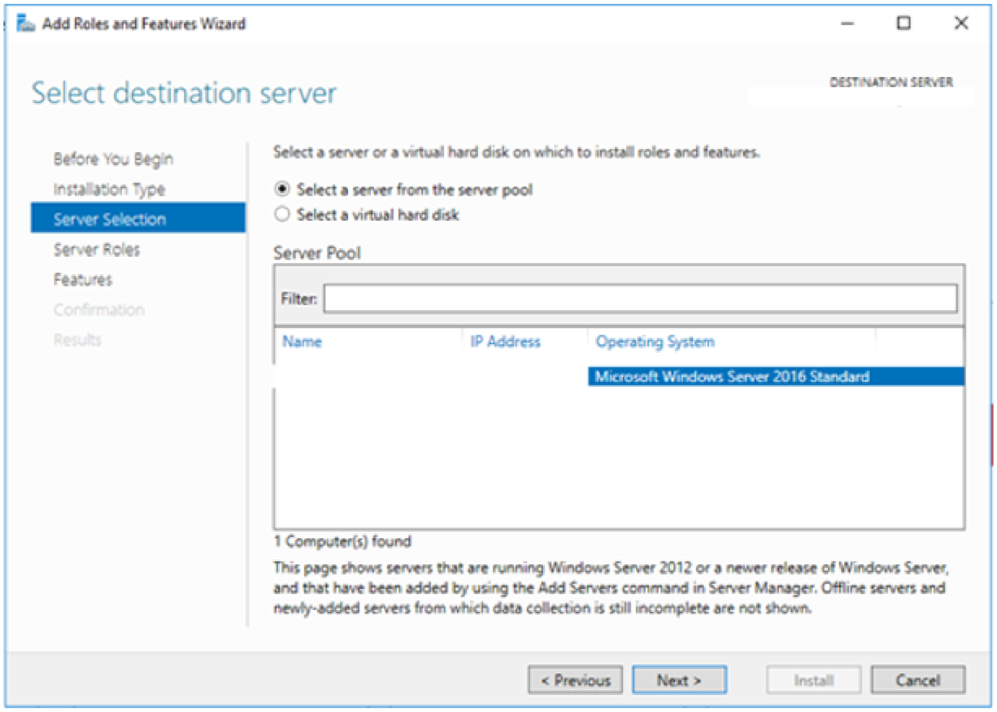
Select installation type

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

c. Click **Next**.



Select destination server

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

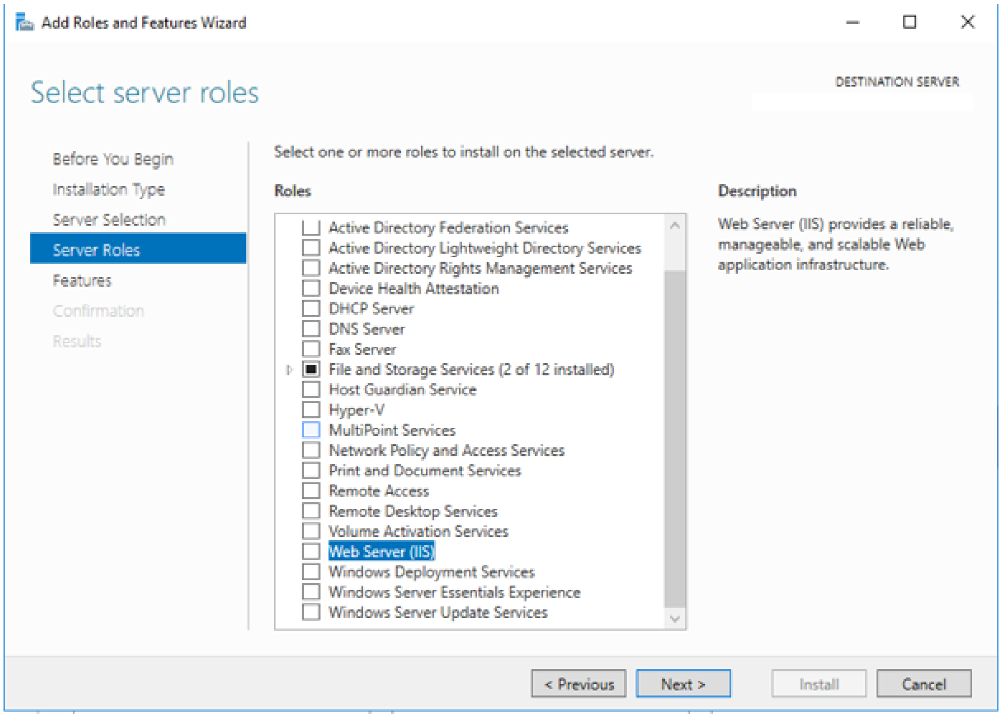
Filter:

Name	IP Address	Operating System
		Microsoft Windows Server 2016 Standard

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.

d. Select **Web Server (IIS)**.



Select server roles

DESTINATION SERVER

Select one or more roles to install on the selected server.

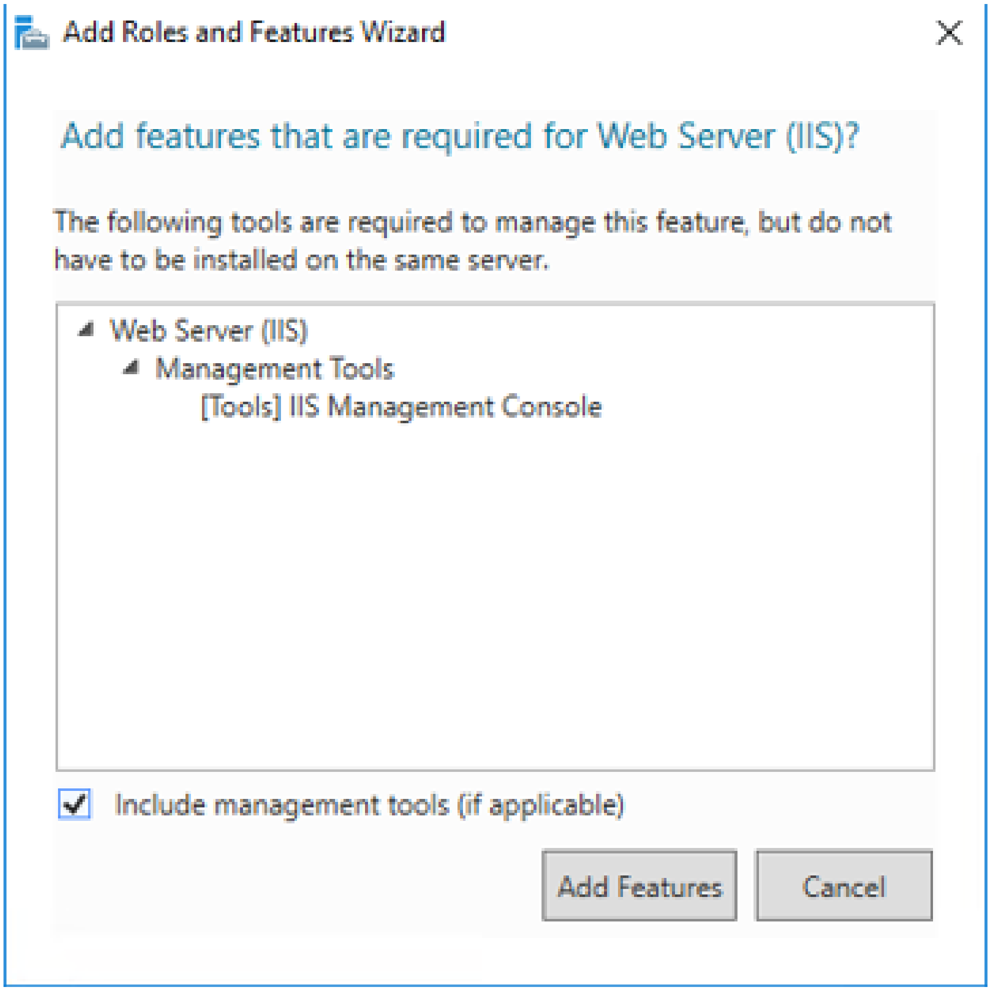
Roles

- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Essentials Experience
- □ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

e. Click **Add Features**.



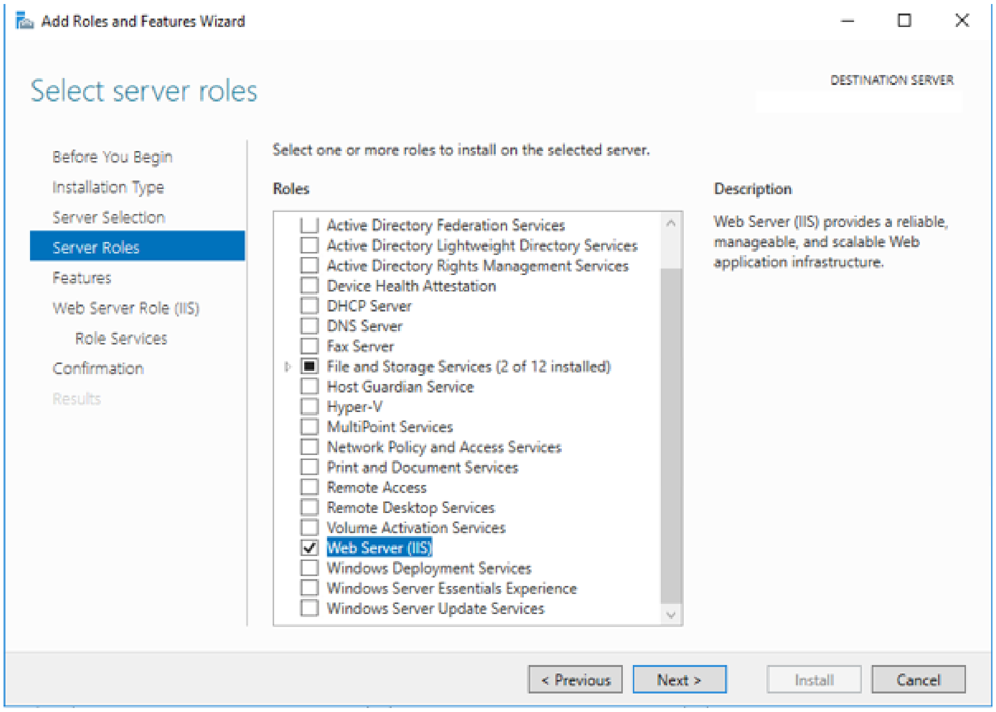
Add features that are required for Web Server (IIS)?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Web Server (IIS)
  - Management Tools
    - [Tools] IIS Management Console

☑ Include management tools (if applicable)

f. Click **Next**.



Select server roles

DESTINATION SERVER

Select one or more roles to install on the selected server.

Roles

- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Essentials Experience
- □ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

g. Follow the on-screen instructions and Click **Next**.

h. Click **Install**.

i. Once installation is successful, click **Close**.

Create the certificate

You can perform the following steps after installing the IC Server component. If you choose to start before installing, complete steps 4-5 after installing the IC Server.

1. Request new certificate.
2. Generate private key.
3. Submit CSR and required information to the Certificate Authority.
4. Install the received signed certificate.

> **NOTE:** Procedure for certificate request and creation is specific to **DigiCert** certificate. In case you are using different Certificate Authority (CA), see the relevant documentation.

Requesting new certificate

1. Click **Start > Administrative Tools > Internet Information Services (IIS) Manager** and Open IIS Manager.
2. In the **Connections** pane, select the server name.
3. In the **Home** pane, double-click Server Certificates **Server Certificate**.
4. In the **Actions** pane, click **Create Certificate Request**.
5. Enter the following details and click **Next**.

Fields	Description
Common name	The FQDN of the server.
Organization	Complete organization title.
Organization unit	Division of organization handling the certificate.
City/locality	Geographical location details.
State/province	
Country/region	

6. Retain the default value in **Microsoft RSA SChannel Cryptographic Provider** field. Enter **2048** as the **Bit length** and click **Next**.

> **NOTE:** Make sure to note the bit length used in certificate creation as the bit length is required to generate the key.

7. Browse to the location where you want to save the CSR file and click **Finish**.

> **NOTE:** Make sure to note the title of the file as it will be required for regenerating the certificate. For example, CERT_REQ.CSR

Generating private key

1. Download and install Win64 OpenSSL from, http://slproweb.com/products/WinOpenSSL.html.

   > **NOTE:** After downloading and installing installing Win64 OpenSSL, ensure that the IC Server is connected back to the training network without Internet access.

   > **NOTE:** While installing the OpenSSL, in the **Select Additional Tasks** page, select **The Windows system directory** option.

2. Open the command prompt to run as administrator, change directory to the <openSSl installation folder>\bin folder.
3. Run the following command to set the environment property OPENSSL-CONF.

   ```
   set OPENSSL_CONF=openssl.cfg
   ```

4. Run the following command to generate the key.

   ```
   openssl genpkey -out <privatekey.pem> -algorithm
   RSA -pkeyopt rsa_keygen_bits:2048 -pass
   pass:<PASSWORD>
   ```

   > **NOTE:** Make sure to change <privatekey.pem> and <PASSWORD> field with applicable information.

5. Run the following command to regenerate the CSR and tag.

   ```
   openssl req -in <CERT_REQ.CSR> -out SIGNED_
   CER.CSR -key <PRIVATEKEY.PEM>
   ```

6. Send the SIGNED_CER.CSR Certificate Request file for approval either to the internal certificate team or to third-party certificate authority (such as DigiCert, Symantec, GlobalSign, or other CA). Provide the details requested by the agency such as bit length (2048), server type (example, IIS 10), algorithm (RSA), and so on for approval. The certificate is validated and CER file is resent. For more information about approval process, refer to Agency documents.

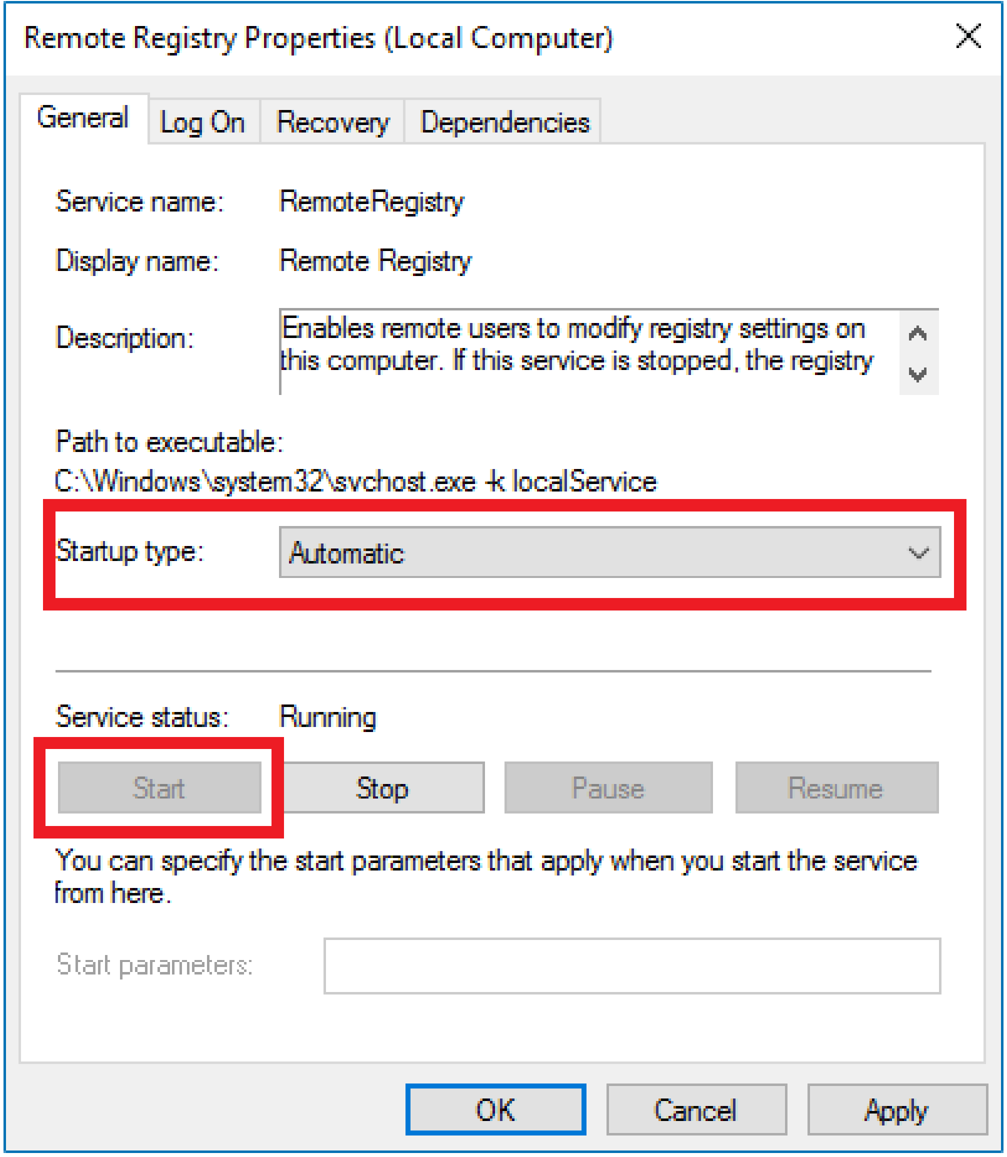
For more information about creating CSR, private key, and certificate generation, see https://forums.iis.net/t/1178233.aspx?II7+5+Complete+Certificate+Request+Dissapears.

After installing the IC Server, you must install the signed certificate and bind all the IFS sites.

Enabling Remote Registry Service

For Service Fabric to install on Standalone Cluster environment, you must enable the remote registry service. Follow the steps to enable:

1. Click **Start > Windows Administrator Tools > Services**.
2. In the **Services** dialog, locate the **Remote Registry** service.
3. Right-click the service and select **Properties**. The Remote Registry Properties (Local Computer) dialog appears.
4. In the **General** tab, select **Automatic** in the **Startup type** parameter drop-down list and click **Start** and click **OK**.



Remote Registry Properties (Local Computer)

Service name: RemoteRegistry

Display name: Remote Registry

Description: Enables remote users to modify registry settings on this computer. If this service is stopped, the registry

Path to executable:
C:\Windows\system32\svchost.exe -k localService

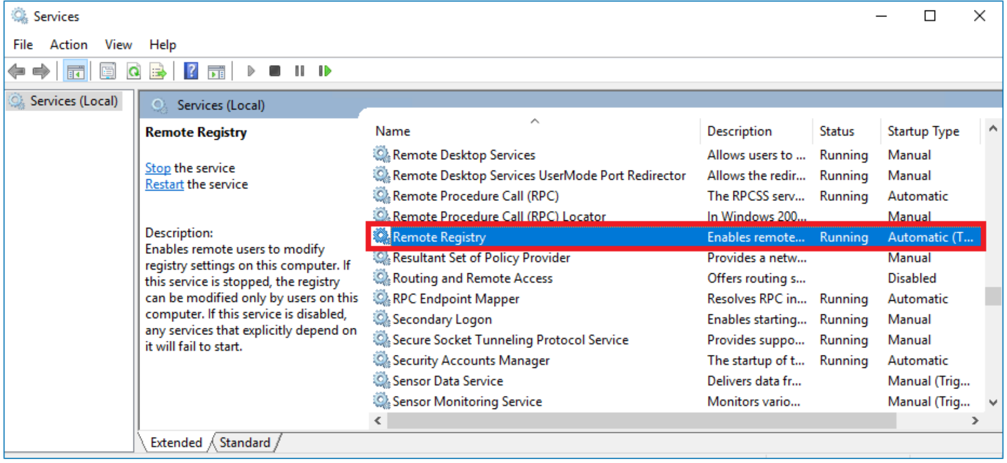
Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

5. In the **Services** window, verify if the **Remote Registry** service is running.



Remote Registry

Stop the service
Restart the service

Description:
Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type
Remote Desktop Services	Allows users to ...	Running	Manual
Remote Desktop Services UserMode Port Redirector	Allows the redir...	Running	Manual
Remote Procedure Call (RPC)	The RPCSS serv...	Running	Automatic
Remote Procedure Call (RPC) Locator	In Windows 200...		Manual
Remote Registry	Enables remote...	Running	Automatic (T...
Resultant Set of Policy Provider	Provides a netw...		Manual
Routing and Remote Access	Offers routing s...		Disabled
RPC Endpoint Mapper	Resolves RPC in...	Running	Automatic
Secondary Logon	Enables starting...	Running	Manual
Secure Socket Tunneling Protocol Service	Provides suppo...	Running	Manual
Security Accounts Manager	The startup of t...	Running	Automatic
Sensor Data Service	Delivers data fr...		Manual (Trig...
Sensor Monitoring Service	Monitors vario...		Manual (Trig...

Disabling the Microsoft Windows Updates

1. From the **Start** menu, launch the **Run**, enter the ***services.msc*** and click **OK**.
2. In the services, locate **Windows Update**. Right-click the **Windows Update** and click **Properties**.
3. In the **General** tab, in the Startup type, select the **Disabled**.
4. Click **Apply** and **OK**.
5. Restart the system.

Or

1. Run the following command from the command prompt: sc config Windows Update start= disabled.
2. Restart the system.

After meeting the requirements and completing the pre-installallation tasks, begin the installation.

Installing the Certificate

After sending request for certificate approval, Certification Authority will review and approve or deny it. Once it is approved, you will receive a response with a .crt file which can be installed. After receiving the certificate from Certification Authority you must install the certificate.

Installing certificate using IIS

Use the following procedure to install the certificate by launching IIS.

1. Launch IIS and navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, select the server name.
3. In the **Home** pane, double-click Server Certificates **Server Certificate**.
4. In the **Actions** pane, click **Complete Certificate Request**.
5. Enter the following details and click **OK**.

Field	Description
File name containing the certificate authority's response	Navigate to the location where the CER file validated by the certificate Agency is stored.
Friendly name	Enter the fully qualified domain name FQDN.
Select a certificate store for the new certificate	Select **Web Hosting** option to store the certificate.

Installing certificate using .crt file

There is an alternative way to install the certificate. Use the following procedure to install the certificate by opening the .crt file.

1. Right-click the **Certificate** and click **Install PFX**.
2. Select **Local Machine** radio button on Welcome to the Certificate Wizard window and click **Next**.
3. Click **Browse** and select the certificate that you want to import and click **Next**.
4. Select **Automatically select the certificate store based on the type of certificate** radio button and click **Next**.
5. Click **Finish** to complete the Certificate Installation process.

Downloading and Installing IC SERVER

Installer is provided as a media, which contains installation package. You can download the media folder from the website.

Installing IC Server

Download the IC Server installer from the media provided to proceed with IC Server installation.

To install IC Server:

1. Log in to the server with your credentials.
2. Navigate to ***<IFS Media path>\Server_Media*** and copy the installer on to the local folder on the IC server, right-click on the exe and click **Mount**. Double-click the **IFS_Server_installer.exe** file.
   a. A pre-check tool is launched to verify if all the prerequisites are met. If prerequisites are met, then IFS_Server_Installer.exe is automatically launched. If pending reboots are detected, then you are prompted to restart the system. Click **Yes** and then click **OK**.
   b. Log in to the Server with your credentials.

   > **NOTE:** Make sure that you enter user name in <domain>/<username> format and also mention the product admin user name.

   c. The IFS page appears. Click **Next**.

   In case prerequisites are incomplete, error or warning appears.

   You can proceed with installation only after fixing the errors.
3. Accept the end user license agreement and click **Next**. The Software Information window appears.
4. Select a valid certificate from the list.
5. Click **Next**.
6. Enter **Username** and **Password** of service account.
   a. In the User Name field, enter the user details in the <domain>\<user> format. The service account is different from Logon user account. Make sure the user is part of the ICUSERS group of the domain.
   b. In the **Password** field, enter the **Password**.

   > **NOTE:** Make sure Username does not contain an ampersand (&) or a single quote (‘).
   >
   > The password should not contain the following characters:

> - Percentage (%)
> - Comma (,)
> - Double-quotes (“)
> - Backslash (\)
> - Should not exceed 31 characters
> - Do not end the password with a backslash (\) or blank space.

c. In the **IP Address detected** field, retain the system IP Address that is detected and click **Install**.

> **NOTE:** If you change the IP address after installation, it may result in a communication breakage between the machines. For support, contact the TAC team.

7. A system reboot is initiated after installation of Microsoft SQL Server is complete. Click **Yes** to proceed with reboot.

> **NOTE:** After system reboot is complete, log in with the same user account to resume installation process.

8. After the installation is complete, click **Finish**.
9. A system reboot dialog appears. Click **Yes** to proceed with reboot.

Post-installation tasks

This section provides information about enabling Microsoft updates, certificate binding, and license procurement.

1. Enable the Windows Updates.
2. Install the certificate.
3. Procure License, create registry entries and Define policy for validating certificate path.

Post-installation tasks

Enabling Microsoft Windows updates

To enable Microsoft Windows updates:

1. From the **Start** menu, launch the **Run** command, enter the ***services.msc*** and click **OK**.
2. In the services, locate **Windows Update**. Right-click the **Windows Update** and click **Properties**.
3. In the **General** tab, in the Startup type, select the **Automatic** option.
4. Click **Apply** and **OK**.
5. Restart the system.

Adding IC Server to Trusted Sites

Add the server name to a trusted site in browser, follow the steps.

On the Google Chrome:

1. Open Google Chrome in administrator login or run as administrator.
2. Launch **Google Chrome** and click ⋮ on the top-right of the page and select **Settings**.
3. Scroll down and click **Advanced**.
4. Under the **System**, click Open proxy settings link. The Internet Properties dialog box appears.
5. In the **Security** tab, click ✓ Trusted sites and click **Sites**.
6. In the **Add this website to the zone** field, enter the IC Server name (For example, https://<FQDN>) and click **Add**.
7. Click **Close**.

Create Registry Entries

If necessary registry entries are not created, then you might encounter the following error while applying license.

```
System.IO.FileNotFoundException: The system cannot find
the file specified.
```

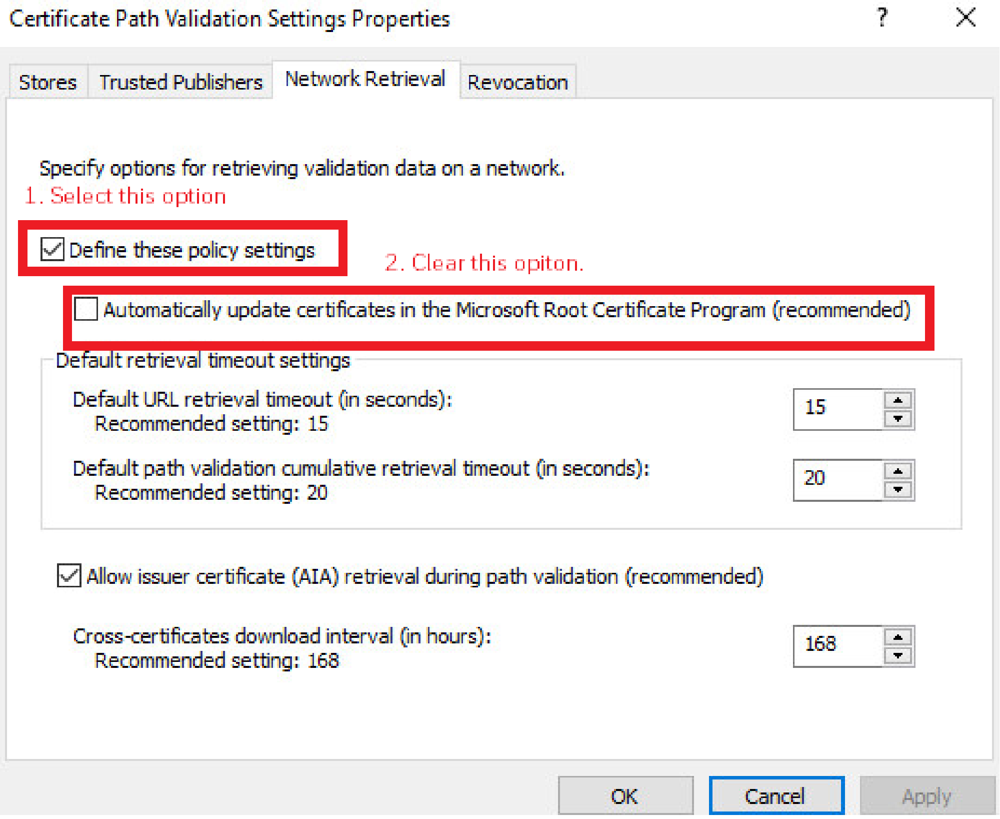
Use the following procedure to create registry entries.

1. Press **Windows+R** button, type ***regedit*** and press Enter.
2. In the **Registry Entry** pane, navigate to ***HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion***.
3. Right-click **CurrentVersion** and select **New > String Value**. A new entry is created in the right pane.
4. Right-click the new registry entry and select **Rename**. Rename the registry as **RegisteredOrganization**.
5. Right-click the renamed registry and select **Modify**.
6. In the **Value data** field, enter your Organization name and click **OK**.
7. Repeat step 3- 6 and create **RegisteredOwner** entry.
8. Restart the services.

Define policy for Certificate Path Validation

1. From the **Start** menu, launch the **Run** command, enter the **gpedit.msc** and click **OK**. The Local Group Policy Editor appears.
2. In the **Local Computer Policy** pane, expand **Computer Configuration > Windows Settings > Security Settings > Public Key Policies**.
3. In the **Object Type** pane, right-click the **Certificate Path Validation Settings** and select **Properties**.

4. In the **Network Retrieval** tab, select the **Define these policy settings** check box. Clear Automatically update certificates in the **Microsoft Root Certificate Program (recommended)** check box.



Certificate Path Validation Settings Properties

Specify options for retrieving validation data on a network.

1. Select this option

☑ Define these policy settings

2. Clear this opiton.

☐ Automatically update certificates in the Microsoft Root Certificate Program (recommended)

Default retrieval timeout settings

Default URL retrieval timeout (in seconds): 15
Recommended setting: 15

Default path validation cumulative retrieval timeout (in seconds): 20
Recommended setting: 20

☑ Allow issuer certificate (AIA) retrieval during path validation (recommended)

Cross-certificates download interval (in hours): 168
Recommended setting: 168

5. Click **OK**.

Antivirus Exclusion Rules

The following are recommended Antivirus (AV) exclusion rules for the IC Server:

- C:\SfDevCluster\Data_App_Node_0*.exe
- C:\inetpub\wwwroot\IC\ICWebAPI\mtsWebApi.exe
- C:\inetpub\wwwroot\IC\ICAdminWebApi\mtsAdminWebApi.exe
- C:\inetpub\wwwroot\IC\ICAdminApp\mtsAdminApp.exe
- C:\inetpub\wwwroot\IC\ICLicenseWebapi\mtsLicenseWebApi.exe
- C:\inetpub\wwwroot\IC\ICStorageWebApi\mtsStorageWebApi.exe
- C:\SfDevCluster\Data_App_Node_0\mtsDeviceServiceType_App0\ContainerActorPkg.Code.1.0.0\ContainerActor.exe
- C:\SfDevCluster\Data_App_Node_0\mtsDeviceServiceType_App0\CableActorPkg.Code.1.0.0\CableActor.exe
- C:\SfDevCluster\Data_App_Node_0\mtsDeviceServiceType_App0\DeviceActorPkg.Code.1.0.0\DeviceActor.exe
- C:\SfDevCluster\Data_App_Node_0\mtsDeviceServiceType_App0\Catalog.CableResolverPkg.Code.1.0.0\Catalog.CableResolver.exe
- C:\SfDevCluster\Data_App_Node_0\mtsDeviceServiceType_App0\Catalog.ResourceFactoryPkg.Code.1.0.0\Catalog.ResourceFactory.exe
- C:\SfDevCluster\Data_App_Node_0\mtsDeviceServiceType_App0\Catalog.AgentGatewayPkg.Code.1.0.0\Catalog.AgentGateway.exe
- C:\SfDevCluster\Data_App_Node_0\mtsDeviceServiceType_App0\Catalog.ContainerResolverPkg.Code.1.0.0\Catalog.ContainerResolver.exe
- C:\SfDevCluster\Data_App_Node_0\mtsDeviceServiceType_App0\Catalog.DeviceResolverPkg.Code.1.0.0\Catalog.DeviceResolver.exe
- C:\SfDevCluster\Data_App_Node_0\mtsDeviceServiceType_App0\Catalog.TenantResolverPkg.Code.1.0.0\Catalog.TenantResolver.exe

IFS Agent

IFS Agent should be installed on OTS Server. This section provides information about installing and configuring IFS Agent component.

Each user must be assigned with independent OTS Server to view the resulting state changes of user's action in the hardware (IFS client application). Make sure requirements are met in each of the OTS Server and the IC-OTS Agent is installed.

Requirement

Software requirement

Software	Version
Process Simulator	Honeywell Forge Workforce Competency R520.1
Operating System	IFS Agent is supported only for Operating System Windows Server 2016 with versions from or above 1607.

Pre-installation Tasks

Before starting the installation, verify if the following procedures are completed.

1. Set DNS server IP Address and add the Server to the same Windows Domain as IC Server.

   > **NOTE:** Do not change the IP Address. Make sure both the IC Server and OTS Server are part of the same domain and network.

2. Add all the OTS Servers to the exception list in the domain controller. For more information, see Add OTS Server to Exception List.
3. The host file must be configured as per OTS Server guidelines.

Downloading and Installing IFS Agent

Installer is provided as a media which contains the installation package. You can download the media folder from the website.

Installing IFS Agent

Use the following procedure to install IFS Agent.

1. Log in to OTS Server with administrator privilege.
2. Navigate to ***<IFS Media path>\IFS_Agent_Media*** and copy the installer on to the local folder on the IC server, right-click on the exe and Mount. Double-click the **IFS_Agent_installer.exe** file.
   a. A pre-check tool is launched to verify if all the prerequisites are met. If prerequisites are met, then the *IFS_Agent_Installer.exe* is automatically launched. The IFS Welcome page appears.

   > **NOTE:** Any pending OTS Server reboots are checked as this might hinder IFS Agent installation. In case pending reboots are detected, a message suggesting to restart is displayed. Restart the system and repeat Step 1 and Step 2 to start the IFS Agent installation.

   In case prerequisites are incomplete, error or warning is displayed, you are able to proceed with installation only after fixing the errors.

3. Click **Next**.
4. Accept the end user license agreement and click **Next**.
5. Enter your **Username** and **Password.**and click **Install**.
   a. In the **IC Server Name** field, provide the Fully Qualified Domain Name (FQDN) of the IC server detected while installing IC Server component.
   b. In the **User Name** field, enter the user details in the ***<domain>\<user>*** format. The service account is different from Logon user account. Make sure the user is part of the ICUsers group and ensure that this user does not have interactive logon permissions.

   > **NOTE:** Ignore the note mentioned in IFS Server and Service Account window.

   c. In the **Password** field, enter the password.

   > **NOTE:** Make sure Username does not contain an ampersand (&) or a single quote (‘).
   >
   > The password should not contain the following characters:

> - Percentage (%)
> - Comma (,)
> - Double-quotes (“)
> - Backslash (\)
> - Should not exceed 31 characters
> - Do not end the password with a backslash (\) or blank space

6. Click **Install**.
7. After the installation is complete, click **Finish**.
8. Restart the IC-OTS Agent service:
   a. From the **Start** menu, launch the **Run**, enter the ***services.msc*** and click **OK**.
   b. In the services, locate the IC-OTS Agent service. Right-click the **Restart**.

IFS Client application installation

IFS Client Application is available for Microsoft Windows Mixed Reality on Microsoft store. This section provides information about preparing and installing the IFS Client application on Microsoft Windows Mixed Reality and .exe based PC Client.

Mixed Reality Portal based installation

Downloading and Installing IFS Client application

You can download the IFS Honeywell Immersive Competency SM Client application from the Microsoft Store. Use the Following procedure to download the IFS Client application on Windows Mixed Reality Portal.

> **NOTE:** In case you have previous version of IFS application installed, then complete the uninstallation first. For more information about uninstall, see "Uninstall IFS Client Application" on page 65.

IFS Client components are loaded into the IFS Client (Microsoft Mixed Reality device).

Desktop requirement

Software Requirement

Minimum Windows 10 Version 1703 OS Build 15063.

Microsoft Windows Mixed Reality requirement

IFS Client application is supported on Microsoft Windows Mixed Reality headsets available till date. For more information about supported headsets, see https://www.microsoft.com/en-us/store/collections/vrandmixedrealityheadsets.

Following are the Honeywell-Supported Microsoft Windows Mixed Reality devices.

- Asus HC102
- Samsung HMD Odyssey
- HP VR1000-127il
- Dell Visor
- Acer AH101-D8EY
- Lenovo Explorer

System requirements

The Following table provides information about system requirements to use IFS Client application in a Mixed Reality environment.

System requirement	Specification for Windows Mixed Reality Ultra PCs
Operating System	Windows 10 Fall Creators Update (RS3) - Home, Pro, Business, Education. **NOTE:** Microsoft Windows Mixed Reality is not supported on N versions or Windows 10 Pro in S Mode.
Processor	Intel Core i5 4590 (4th generation), quad-core (or better) AMD Ryzen 5 1400 3.4Ghz (desktop), quad-core (or better)
RAM	16GB DDR3 (or better)
Free disk space	At least 20GB
Graphics Card	NVIDIA GTX 1060 (or greater) DX12-capable discrete GPU

System requirement	Specification for Windows Mixed Reality Ultra PCs
	AMD RX 470/570 (or greater) DX12-capable discrete GPU **NOTE:** GPU must be hosted in a PCIe 3.0 x4+ Link slot. Hybrid graphics configurations are compatible. Remember discrete card of hybrid system must be similar specification as listed in this table.
Graphics Driver	Windows Display Driver Model (WDDM) 2.2
Graphics display port	HDMI 2.0 or DisplayPort 1.2
Display	Connected external or integrated VGA (800x600) display (or better). For better performance, use laptop with screen of minimum 15 inches.
USB connectivity	USB 3.0 Type-A or Type-C
Bluetooth connectivity (for motion controllers)	Bluetooth 4.0
Expected headset framerate	90 Hz

For more information about the hardware requirements, see https://docs.microsoft.com/en-us/windows/mixed-reality/enthusiast-guide/windows-mixed-reality-minimum-pc-hardware-compatibility-guidelines.

Enable Windows Mixed Reality Applications in the Enterprise

You can add Windows features packages known as Features on Demand (FOD) at any time. You can request the feature package from Microsoft Windows Update, when a Microsoft Windows 10 Computer needs a new feature. In case your organization uses Microsoft Windows Server Update Services (MWSUS), you must enable the Microsoft Windows Mixed Reality.

1. Microsoft Windows 10 must be of latest version to enable Mixed Reality feature. You must check and update to the latest version of Microsoft

Windows 10.

2. Microsoft Windows Mixed Reality Feature on Demand (FOD) is downloaded from Microsoft Windows Update. If access to Microsoft Windows Update is blocked, then you must manually install the Microsoft Windows Mixed Reality FOD.
   a. Select the FOD.cab file that matches your operating system version and download the file from Windows 10, version 1903 or Windows 10, version 1909.
   b. Use Add-Package to add Windows Mixed Reality FOD to the image.

      Add-Package

      Dism /Online /add-package /packagepath:(path)

   c. In **Settings > Update & Security > Windows Update**, click **Check for updates**.

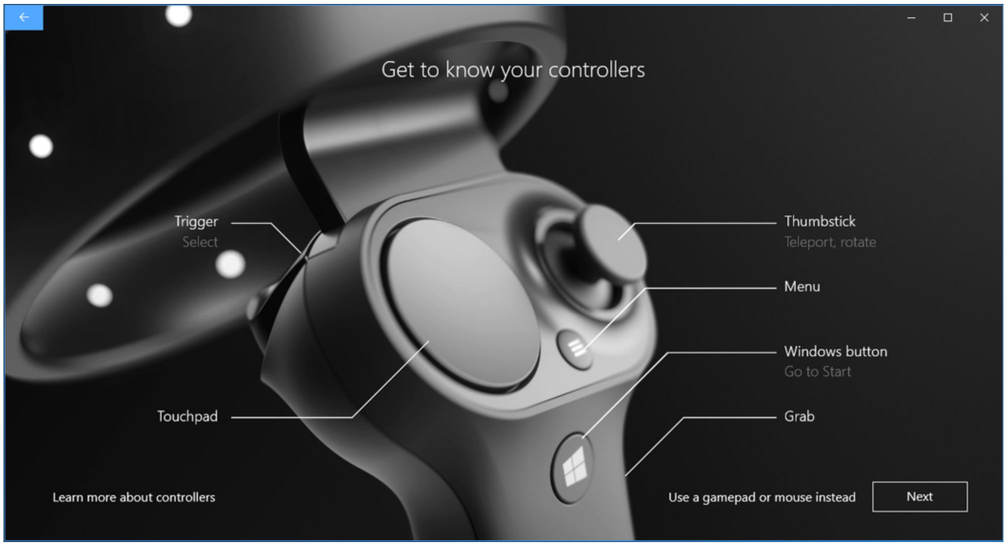
For more information about enabling, see https://docs.microsoft.com/en-us/windows/application-management/manage-windows-mixed-reality.

Set up Microsoft Windows Mixed Reality

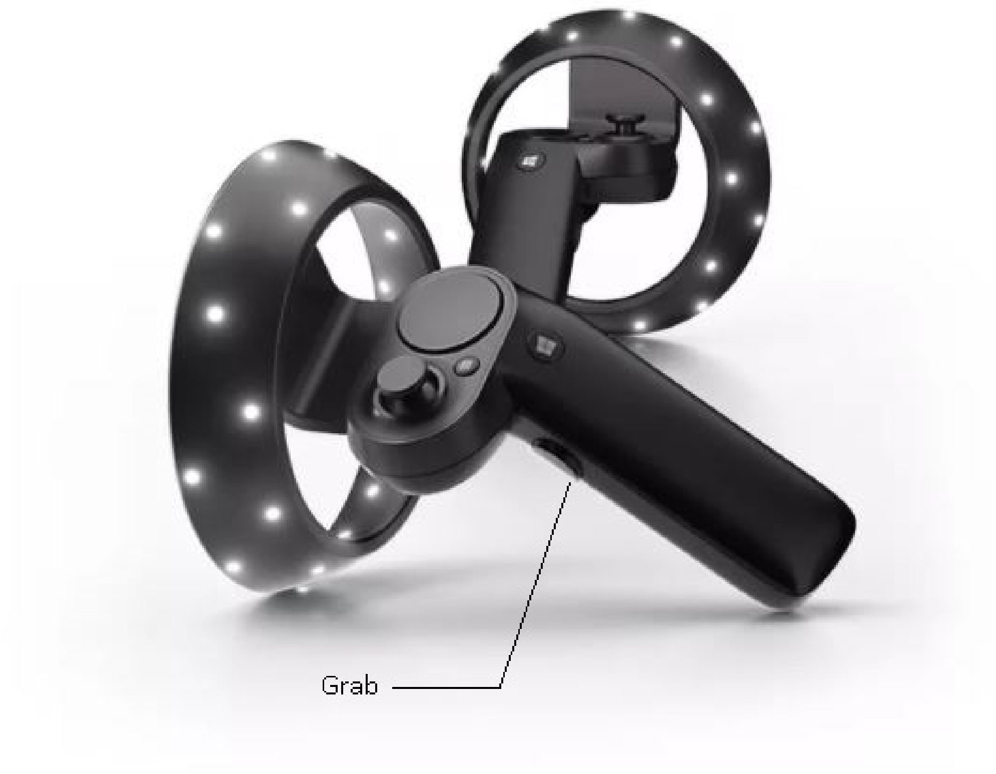
Use the following procedure to set up the Microsoft Windows Mixed Reality.

1. Pair the motion controllers.

> **NOTE:** Make sure to plug-in a USB Bluetooth 4.0 adapter to enable motion controllers. In case you plan to use an Xbox Gamepad or Mouse, you can skip this step.



Get to know your controllers



a. Press the Windows button for 2 seconds until the lights glow indicating controller is powered on.
b. Remove the battery cover of the motion controller and find a small pairing button at the edge of the controller. Follow the instructions on the Microsoft Windows Mixed Reality to pair the controller with your PC.

On update completion, controller will automatically restart, connection to the host is established, and LED will glow bright constantly.

2. Choose either room-scale or desk-scale experience as follows.
   a. Desk-scale: You will be confined to your desk and still be able to indulge in immersive reality experience. You must select **Set up for seated and standing** option. No further configuration is required.
   b. Room-scale: You will be able to walk around the room and experience immersive reality motion. For this you must select **Set**

me up for all experiences option. Make sure to clear up space to be able to move around. Center your headset and start tracing the boundary. To complete the boundary keep the headset pointed towards your PC. You will now be able to experience mixed reality in the defined boundary.

For more information, see https://docs.microsoft.com/en-us/windows/mixed-reality/enthusiast-guide/set-up-windows-mixed-reality.

Motion Controllers

The following section provides the information about Controllers on Motion Controller and their usage.

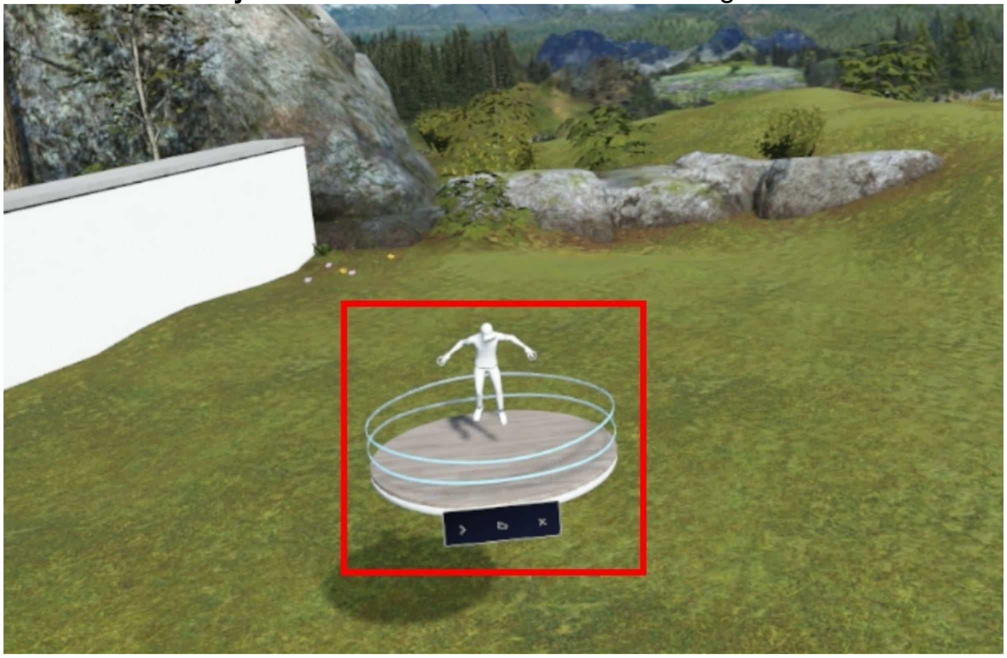
- **Trigger**: Enables user to select any option on the dashboard.
- **Thumbstick**: Enables user to navigate from one point to another by teleporting.
- **Grab**: Activates the pointer to point towards any equipment.
- **Menu**: Enables user to launch the Dashboard.
- **Home**: Enables user to power on the motion controllers.

Floor height calibration

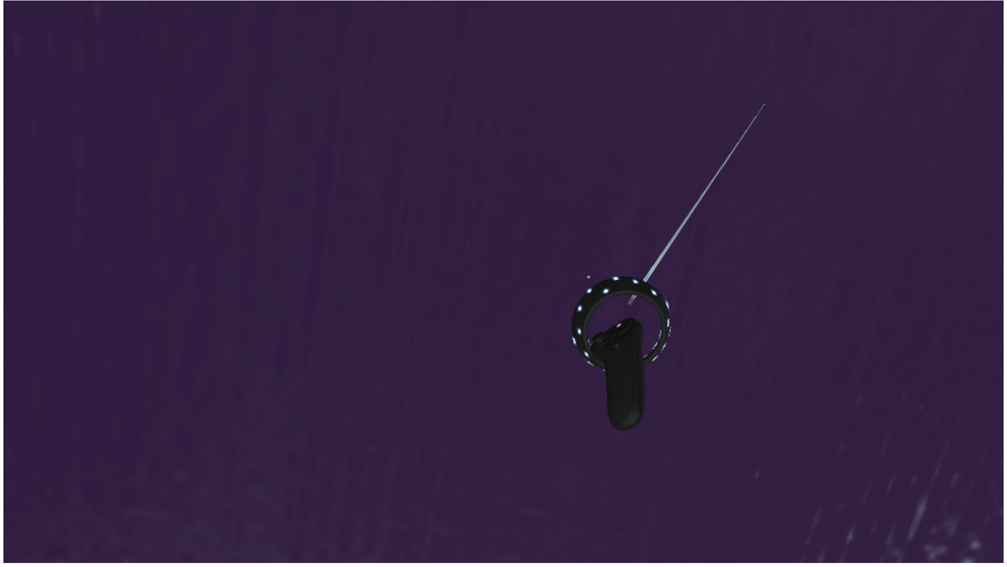
Use the following procedure to calibrate the height of floor in Microsoft Windows Mixed Reality headset.

1. From the **Start menu**, launch **Microsoft Windows Mixed Reality portal** .
2. Hit **Windows** button on the Motion Controller and select **All apps**.
3. Scroll through your apps to select **Floor Adjustment**.

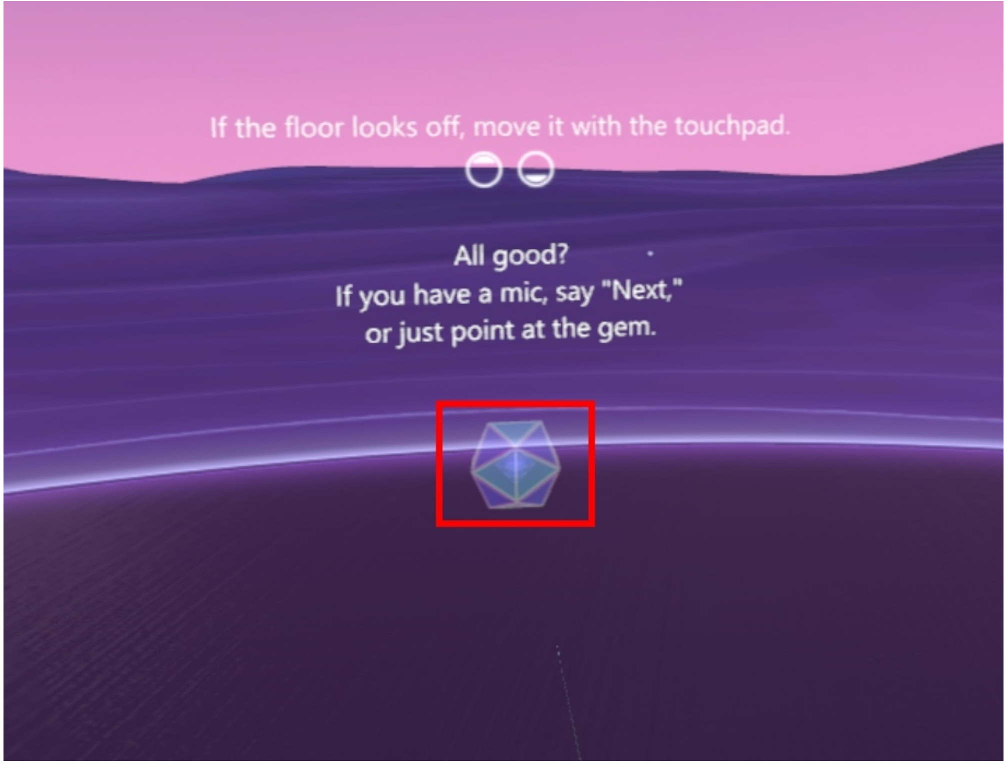
4. Click the **Floor Adjustment** icon to calibrate the floor height.



5. **Place** the Motion Controller on the physical floor and adjust the height by using Touchpad on the Motion controller.



6. Once the motion controller is aligned with the floor click the **Gem** to complete the calibration.



If the floor looks off, move it with the touchpad.

All good?
If you have a mic, say "Next,"
or just point at the gem.

.exe based PC Client Installation

1. Right-click on **Honeywell immersive Field Simulator R110.2.exe** and select **Run as Administrator**.
2. Click **Next** on the Welcome screen.
3. Select **i accept the terms in the license agreement** and click **Next**.
4. Click **Install** to begin the installation. The installation progress status appears.
5. Once the installation is completed, Click **Finish**.

CHAPTER

5

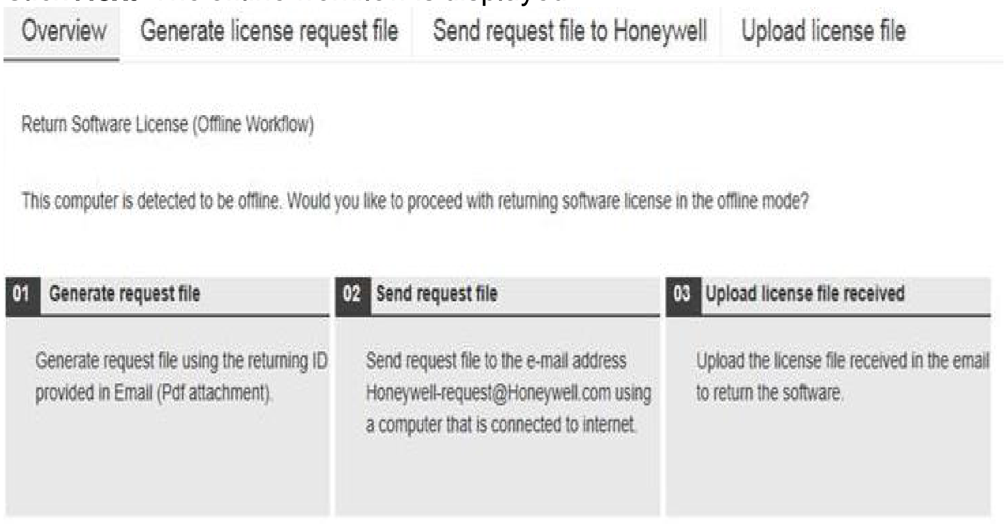
LICENSE MANAGEMENT

Flexera License

Returning License

To return the license offline, perform the following steps:

1. Launch the License Activation Utility application.
2. On the left pane, click **Return Software License**. The application automatically selects Offline or Online workflow based on the internet connectivity of the system.
3. Click **Next**. The offline workflow is displayed.



Return Software License (Offline Workflow)

This computer is detected to be offline. Would you like to proceed with returning software license in the offline mode?

01 Generate request file

Generate request file using the returning ID provided in Email (Pdf attachment).

02 Send request file

Send request file to the e-mail address Honeywell-request@Honeywell.com using a computer that is connected to internet.

03 Upload license file received

Upload the license file received in the email to return the software.

4. In the **Generate license request file** tab, select **01 Generate request file**. The Return Software License screen is displayed.
5. In the **License Key** field, enter the unique license identification number that must be returned.
6. Click **Generate Request File** to download the capability request file. A request file is downloaded which has to be processed to complete the license return process.
7. On successful download of Capability request file, the **Send request file to Honeywell** tab is displayed.
8. Follow the instructions and send an e-mail attaching the capability request file and Order ID to ***Honeywell-request@Honeywell.com*** requesting the response file to return the license.

9. Click **Next**.
10. In the **Upload license file** tab, upload the file received in Step 8 to complete the license return process.
    a. Click **Browse** and navigate to locate where the response file is saved.
    b. Select the response file and click **Return Software**.

The Immersive Field Simulator solution is returned to Honeywell.

Procure License

After installing the IC Server and binding the certificate, you must activate the license from the IC Management Console. Use the following procedure to activate the license.

To procure the license, perform the following steps:

1. Launch **Start > Honeywell > License Activation Utility**.

> **NOTE:** Performance deteriorates while using License Activation Utility.
>
> In machines where internet access is forbidden, there are chances that the License Activation utility consumes more time to respond. This is due to Certificate Revocation check done for Flexera dlls.
> Solution: Turn off certificate revocation check in the machines where no internet access is available.
>
> Follow the steps:
>
> a. Click **Start > Control Panel > Internet Options > Advanced**.
> b. Scroll down to the **Security** section.
> c. Clear the following check boxes:
>   - Check for publisher's certificate revocation
>   - Check for server certificate revocation
>   - Check for signatures on downloaded programs
> d. Click **OK**.
> e. Restart the system.

2. Sign In with user credential in ***<domain>/<username>*** format (For example, Honeywell/icadmin).
3. Click the **License Management**.

   You are navigated to Honeywell License Utility.

4. In the **Activate Software License (Offline Workflow)** page, select **This computer is detected to be offline. Would you like to proceed with activating software license in the offline mode?** radio button.
5. Click **Next**. Workflow to offline license activation is displayed.
6. Click **01 Generate request file** option.
7. In the Generate license request file tab, enter following details:
   a. In the **Activation ID** field, enter the unique license identification number which is available in the Software License certificate provided by the Honeywell order management.
   b. Select **No** from the drop-down if you want to install multiple license on the same server.
   c. Click **Generate Request File** button on the bottom of the screen to download the capability request file.

      A request file is downloaded which has to be processed to complete the License activation process.

8. In the **Send request file to Honeywell** tab, send an e-mail attaching the downloaded capability request file and Order ID to **Honeywell-request@Honeywell.com** requesting a response file to activate the license.

   A file is shared to the email ID provided.

9. Click **Next**.
10. In the **Upload license file** tab, upload the file.
    a. Select the license file and click **Activate Software**.
    b. Click **Browse** and navigate to locate where the response file is saved.
11. To confirm license activation, perform the following steps.
    a. Navigate to **Start > Honeywell > License Activation Utility** and open **License Management Portal.>Feature Information.**You can see the license details.
    b. Navigate to **Start>IFS>IFS Dashboard** and click **License management**. Information on expiry date of the license and the license type indicates successful activation of license.

> **NOTE:** It is recommended to restart ICLicenseWebApi site in IIS, post License activation.

Renew License Plan

You can renew your license if you want to continue using Immersive Competency solution. Administrator receives an email notifying the remaining duration of the license and further actions for renewal.

To renew the license term, you must contact Honeywell License Team - ACT. On completing the renewal process with Honeywell License Team, launch the IC Management Console and perform the following.

1. Open the IC Management Console.
2. Click **License Management** option.
3. Click **Renew**.
4. Select the check box to confirm reception of renewal from the License Team and click **Renew**.

On completion, a successful message is displayed.

Activating the Photon License

Photon Server is installed as a part of IC Server installation. After completing the installation you must activate Photon license. Photon license activation process consist of 2 steps.

- Sending Hardware ID to ACT team
- Copying license file

In order to activate the Photon license, user needs to send the Hardware ID to ACT team (ACTHPSLicense@Honeywell.com). Use the following procedure to send Hardware ID to ACT team.

1. Log on to IC Server.
2. Navigate to notification tray and click **Photon Server** Icon.
3. Click **License Info > Hardware ID > Copy to clipboard.**
4. Send the copied Hardware ID to ACT Team.

After receiving the Hardware ID, ACT team works with Photon to generate license activation file. It takes on an average 2-3 working days or maximum 5 working days to get license activation file from Photon. ACT receives license activation file from Photon and sends the license activation key to user. After receiving the license key from ACT, user must copy the license key. Use the following procedure to copy the license file.

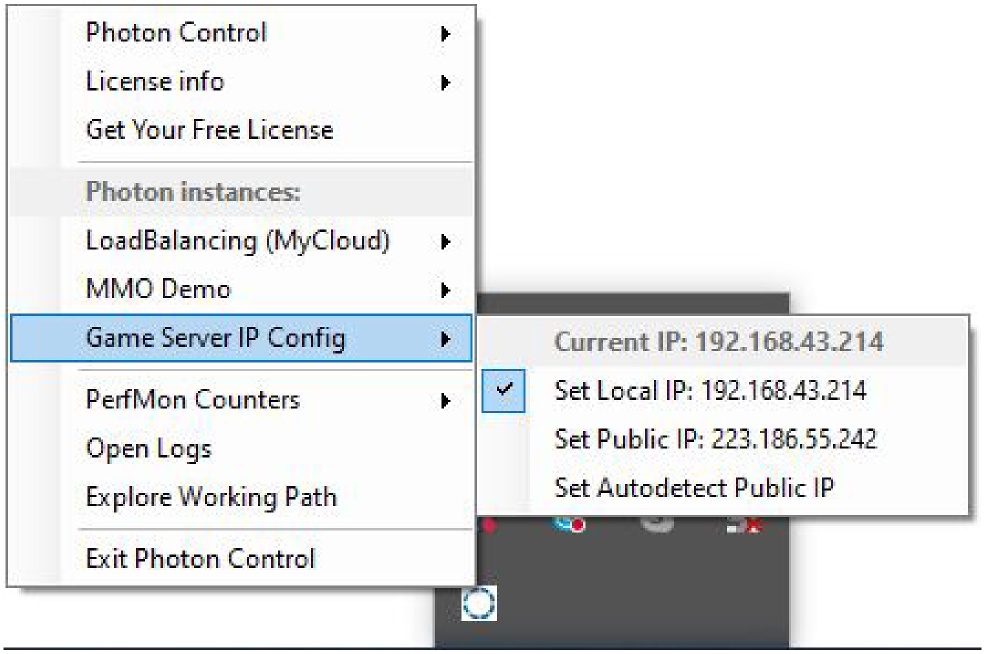
1. After receiving the license file from ACT, click **Photon Server > Explore Working Path**. A file explorer window appears.
2. Copy the license file in the opened window.
3. Click **Photon Server > Exit Photon Control**.

4. Open **Photon Control** from the file explorer window that opened in step 2.
5. To confirm license activation, click **Photon Control > License Info**.

Photon IP Configuration

To select the game server IP, use the following steps.

1. On the **Toolbar**, click **Show hidden icons**.
2. Right-click on **Photon Icon** ○, go to **Game Server IP Config>Set Local IP Address**.



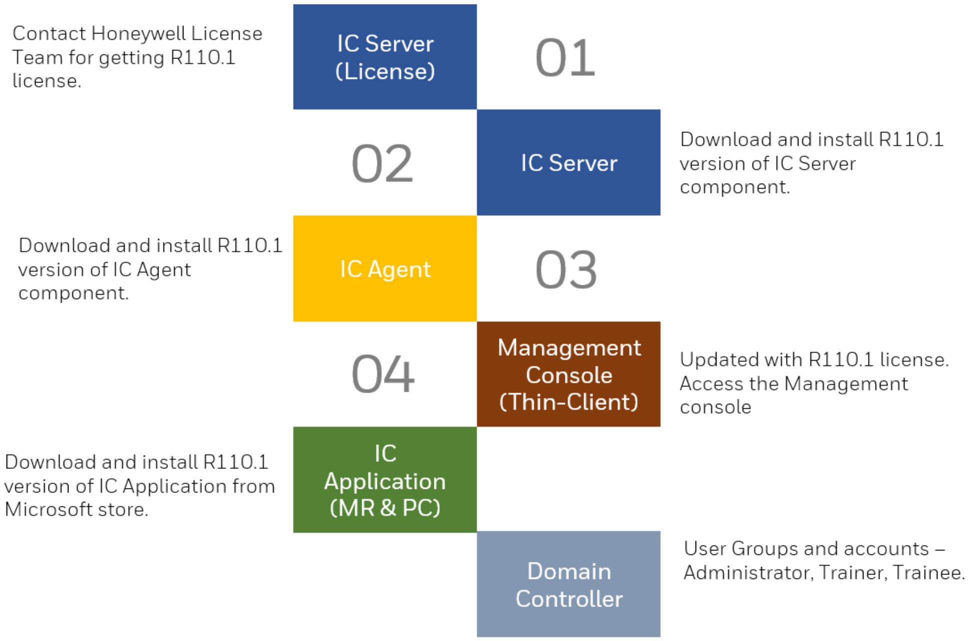
> **NOTE:** In case of any network changes if the IP address is changed, perform the Photon IP Selection actions once more and contact the TAC team.

CHAPTER

6

UPGRADE TO IMMERSIVE FIELD SIMULATOR R110

Following is an overview of update work flow to upgrade Immersive Competency to 110 version.


Contact Honeywell License Team for getting R110.1 license.
IC Server (License)
01
02
IC Server
Download and install R110.1 version of IC Server component.
Download and install R110.1 version of IC Agent component.
IC Agent
03
04
Management Console (Thin-Client)
Updated with R110.1 license. Access the Management console
Download and install R110.1 version of IC Application from Microsoft store.
IC Application (MR & PC)
Domain Controller
User Groups and accounts – Administrator, Trainer, Trainee.

Make sure that IC Server, IC Agent, IC Application, and Thin-Provisioned client is connected to the same network.

Downloading and Upgrading

Installer is provided as media which contains the installation package. You can download the media folder from the website.

Upgrading IC Server from R101.1 to R110.1

Perform these steps to upgrade IFS IC Server from R101.1 to R110.1:

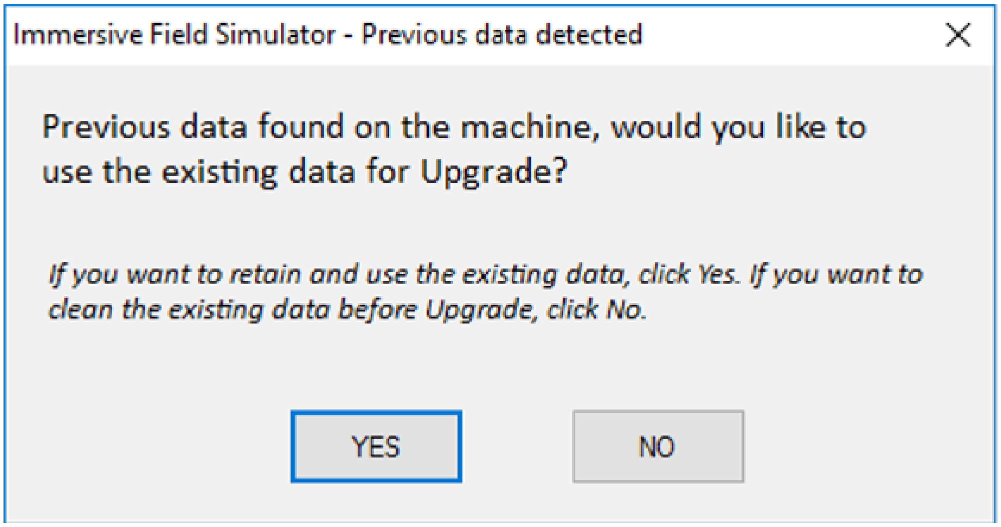
1. Download the IC Server installer from the media provided to proceed with IC Server installation.
2. Log in to the server with your credentials.

> **NOTE:** Make sure that you are entering user name in **<domain / username>** format and also mention the product admin user name.

3. Navigate to ***<IFS Media path>\Server_Media*** and copy the installer on to the local folder on the IC server, right click on the exe and Mount. Double-click the **IFS_Server_installer.exe** file. Select **Yes**.
4. A pre-check tool is launched to verify if all the prerequisites are met. If prerequisites are met, then IFS_Server_Installer.exe is automatically launched.

> **NOTE:** In case prerequisites are incomplete, an error or warning message is displayed. You are able to proceed with installation only after fixing the errors.

5. Accept the end user license agreement and click **Next**, **Software Information** window appears.
6. Select valid certificate from the list.
7. Click **Next** on **Software Information** window.
8. **Service Account Credentials** window opens with pre-populated user name which is used to install IFS R101.1. Enter the password and click **Upgrade**.
9. Select **YES** if you want to use the existing R101.1 data else select **NO**.



Immersive Field Simulator - Previous data detected

Previous data found on the machine, would you like to use the existing data for Upgrade?

If you want to retain and use the existing data, click Yes. If you want to clean the existing data before Upgrade, click No.

10. Once users selects **YES** or **NO** for data retention, upgrade starts and command prompt window opens and it will automatically close as part of the installation. After few minutes installation is finished, and **Install Completed** window appears. Select **Finish**.

11. A system reboot dialog box appears. Click **Yes** to proceed with reboot.

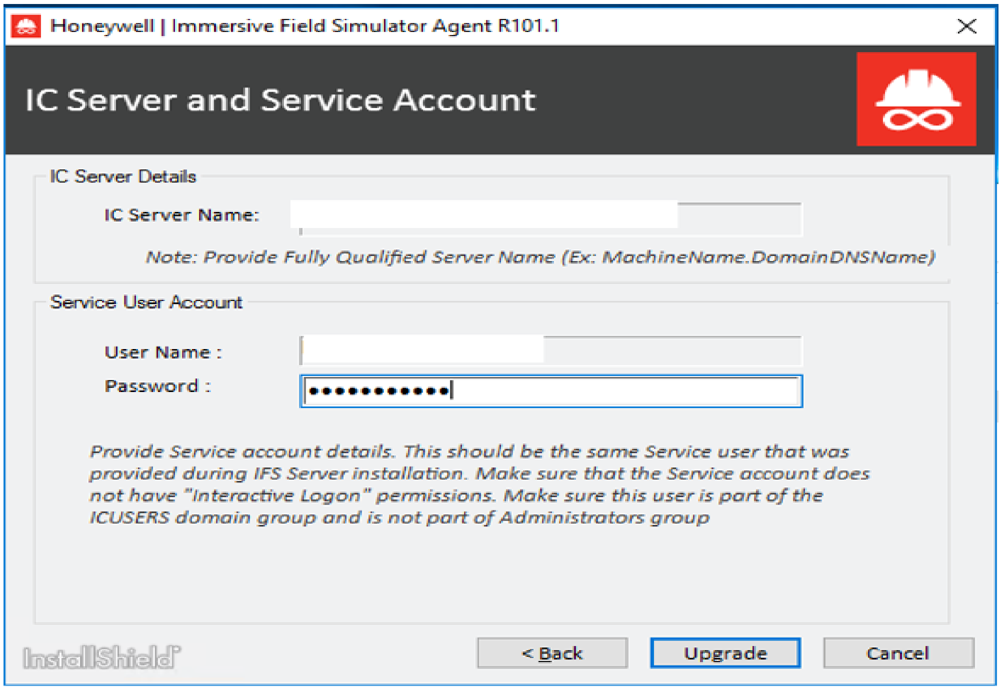
Upgrading IFS Agent from R101.1 to R110.1

Perform these steps to upgrade IFS Agent from R101.1 to R110.1:

1. Log in to OTS Server with administrator privilege.
2. Download the media folder and navigate to the download location <IFS Media path>/IFS_Agent_Media and double-click the IFS_ Agent_ installer.exe file.
3. Double-click on the installer, a pre-check tool is launched to verify if all the prerequisites are met. If prerequisites are met, then the IFS_Agent_ Installer.exe is automatically launched. The **IFS Welcome** page appears.

   > **NOTE:** In case prerequisites are incomplete, an error or warning message is displayed, you are able to proceed with installation only after fixing the errors.

4. Accept the end user license agreement and click **Next**, **Software Information** window appears.
5. Click **Next** on **Software Information** window.
6. **IC Service and Service Account** window opens with pre-populated user name which is used to install IFS R101.1. Enter the password and click **Upgrade**.



Honeywell | Immersive Field Simulator Agent R101.1

IC Server and Service Account

IC Server Details

IC Server Name:

Note: Provide Fully Qualified Server Name (Ex: MachineName.DomainDNSName)

Service User Account

User Name :

Password : ••••••••••••

Provide Service account details. This should be the same Service user that was provided during IFS Server installation. Make sure that the Service account does not have "Interactive Logon" permissions. Make sure this user is part of the ICUSERS domain group and is not part of Administrators group

7. Click **Finish** when installation completes.

CHAPTER

7

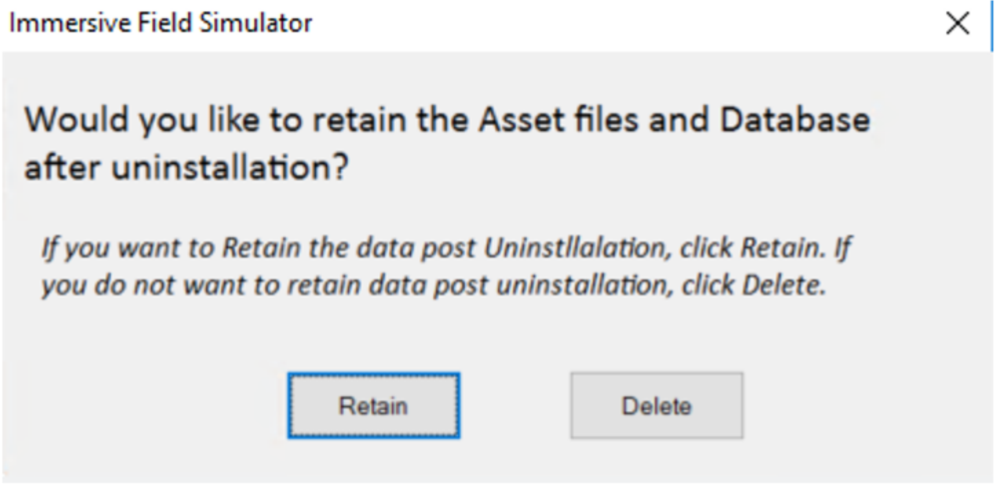
UNINSTALLATION

This section provides information on uninstalling each of the IFS components. Uninstall each of the following components individually:

Uninstall IC Server

Use the following procedure to uninstall IC Server.

1. Go to control panel, select **Uninstall a program**.
2. Click **Immersive Field Simulator > Uninstall**.
3. Select **Remove**.
4. Select **Retain** if user wants to use the existing data, else click **Delete**.



Immersive Field Simulator

Would you like to retain the Asset files and Database after uninstallation?

If you want to Retain the data post Uninstllalation, click Retain. If you do not want to retain data post uninstallation, click Delete.

5. Uninstallation will start and select **Finish**.
6. A system reboot dialog box appears. Click **Yes** to proceed with reboot.

Uninstall IFS Agent

Use the following procedure to uninstall IFS Agent:

1. Go to control panel, select **Uninstall a program**.
2. Click **Immersive Field Simulator Agent > Uninstall**.
3. Select **Remove**.
4. Uninstallation starts and select **Finish**.
5. A system reboot dialog box appears. Click **Yes** to proceed with reboot.

Uninstall IFS Client Application

If you have already installed the IFS application, then you must first uninstall the existing version from your PC or Mixed reality Headset.

Use the following Procedure to uninstall the IFS client application.

1. Click **Start** on your desktop and search open **Honeywell Immersive Field Simulator.**
2. Right click **Honeywell Immersive Field Simulator** and select **Uninstall**.

CHAPTER

8 COMPATIBILITY MATRIX

The following tables describe the compatibility matrix for IFS R110.1 release.

Honeywell Process Training Simulator	Supported	Validated
UCS RXXX	X	X
Honeywell Forge Workforce Competency R520.1	✓	✓

Operating System for IFS Agent Installation on Honeywell Process Training Simulator Server (OTS Machine)	Supported	Validated
Microsoft® Windows 10 (64-bit, Professional/Enterprise)	✓	X
Microsoft® Windows Server 2016 (64-bit, Standard)	✓	✓

CHAPTER

9 TROUBLESHOOTING

Error "Activation ID invalid"

Issue: Error "Activation ID invalid" reported while activating the license.

Solution:

1. Check if the activation ID is correct.
2. If the activation ID is correct, send the environment of the license to Honeywellrequest@ Honeywell.com

Error "Unauthorized to view this Application"

Issue: After opening License Activation Utility, an error pops up stating "Unauthorized to view this Application".

Solution: The above Error can happen due to multiple reasons. Few of the reasons are stated below:

1. If the CLL service account is domain-based account make sure that while accessing the CLL application it is under domain network. For example if the Honeywell LDAP account is used as CLL service account make sure that Honeywell VPN is connected.
2. It can happen if the CLL service account is not having read and write permissions to the path folder in the path C:\ProgramData\Honeywell\CommonLicense.

Feature is not available in the Feature Information tab

Issue: Feature is not available in the Feature Information tab after successful License activation.

Solution: Check/execute the following items:

1. Open **Honeywell License Utility**.
2. Navigate to **Activate Software License > Offline software activation**.
3. Click **Generate Request File**.
4. In the Activation ID box, give the Activation ID as 123456.
5. Click **Generate Request File**.

6. A Request file will be generated.
7. Send this Request file to Honeywell-request@honeywell.com.
8. You will receive a Response file.
9. Save this Response file and upload the same file in the Honeywell License Utility and click **Activate Software**.
10. You will receive an error message.
11. Click **Feature Information** tab, the features will be available.

Request file is corrupted

Issue: The Request file is corrupted.

Solution: Check/execute the following items:

1. Stop the following services:
   - Honeywell CLL UI
   - Honeywell CLL WebApi services.
2. Navigate to the path "C:\ProgramData\Honeywell\CommonLicense\Store".
3. Delete all files present in the path.
4. Restart the following services:
   - Honeywell CLL UI
   - Honeywell CLL WebApi services.
5. Create a new Request file and send it to Honeywell-request@Honeywell.com.

Change the service account password

Issue: Services are not started as the password update is required.

Solution: If the User changes the Password of the Service Account, user has to manually change the Password for the following Honeywell Services:

- Honeywell CLL UI
- Honeywell CLL WebApi services.

Check/execute the following items:

1. Go to run and type **services.msc**.
2. In the Services window search for Honeywell CLL UI and Honeywell CLL WebApi services.
3. Right click **Services** and click **Properties**.
4. Navigate to the **LogOn tab** and update the Password.

5. Click **Apply** and restart the service for the updating the Password for the services.

Blocked URL

Issue: Error URL is blocked pops up while opening the Honeywell License Utility.

Solution: Modify the proxy settings of your system.

Check/execute the following items:

To set the proxy settings in Internet Explorer:

1. Open **Internet Explorer**.
2. Select **Tools** icon on top right corner of the window.
3. Select **Internet Options**.
4. Navigate to **Connections>LAN Settings**.
5. Check **Automatically detect settings** option check box and click **OK**.

To set the proxy settings in Google chrome browser:

1. Open **Google Chrome** browser.
2. In the right pane, click **Settings**.
3. Under Network group, click **Change Proxy Settings**. The Connections dialog is displayed.
4. In the Connections dialog, click **LAN Settings** option.
5. In LAN Settings dialog, select **Automatically detect settings option** and click **OK**.

Capability request download fails

Issue: Capability request download fails in Internet Explorer.

Solution: Disable the Internet Explorer enhanced security option and restart the machine.

Unable to provide username to install R110

Issue: Unable to provide username to install R110 after uninstalling R101 with data retention.

Solution: Reinstall the R101 with data retention and then migrate from R101 to R110 by selecting data retention as YES.

CHAPTER

10 LOG FILES

A log file contains information about the events that have occurred within a software. Log files help in troubleshooting the errors occurred in a software.

In IFS, log files are created in the following components.

- IFS Client application
- IC Server
- IFS Agent

IFS Client application

IFS Client application log files are stored in *C:\Users\(user name)\AppData\LocalLow\Honeywell International Inc_\Honeywell Immersive Field Simulator*.

IC Server

The following log files are created in IC Server and are stored in *C:\ProgramData\Honeywell\IFS\ICLogs*.

- ICAssetCatalog log file
- ICAdminWebApi log file
- ICLicenseWebApi log file
- ICStorageWebApi log file
- ICWebApi log file

IFS Agent log files

IC Agent log files are stored in *C:\ProgramData\Honeywell\IFS\Logs\Agent.*

Notices

Trademarks

Immersive Field Simulator™ is a trademark of Honeywell International, Sàrl.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Third-party licenses

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_licenses on the media containing the product.

Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at:

- http://www.honeywellprocess.com/support

If you have comments about Honeywell Process Solutions documentation, send your feedback to:

- hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC).

How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

https://honeywell.com/pages/vulnerabilityreporting.aspx

Submit the requested information to Honeywell using one of the following methods:

- Send an email to security@honeywell.com.

  or

- Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support” section of this document.

Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx.

Training classes

Honeywell holds technical training classes about Immersive Field Simulator. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see http://www.automationcollege.com.