

- Web Server
 - Common HTTP Features (select all options)
 - FTP Server (select all options)
 - Health and Diagnostics
 - HTTP Logging
 - Logging Tools
 - Request Monitor
 - Tracing
 - IIS Hostable Web Core
 - Management Tools (select all options)
 - Security (select all options)
 - 8. Click **Next**.
- The **Select features** page appears, showing the Application Server Features menu.
- 9. Do the following:
 - a. Select .NET Framework 3.5 Features.
 - b. Select Quality Windows Audio Video Experience.
 - c. Select SMTP Server.
 - 10. Click **Next**.
- The Confirm installation selections page appears.
- 11. Click **Install**.
 - 12. After installation, follow the instructions in [Setting SMTP, FTP, and Quality Windows Audio Video Experience Properties](#) on page 183.

Microsoft Windows Server 2016 Configuration

Before you install MiVoice Connect server software, you must prepare Microsoft Windows Server 2016 to run MiVoice Connect services by installing the proper server roles and features. This section describes how to prepare a Microsoft Windows Server 2016 server to use MiVoice Connect software.



Note

- Windows Server 2016 must be activated through Microsoft before installing the MiVoice Connect server software.
 - During installing the server operating system, select the **Server with a GUI** option, instead of **Server Core Installation** option.
-

Server Roles and Features

This section describes how to configure the server roles and features required to run the MiVoice Connect server.



Note

Run the Windows updates and all the related patches before adding the server roles and features.

1. On the Windows desktop, click **Start > Programs > Administrative Tools > Server Manager** to launch the Server Manager Dashboard.
2. In the Server Manager Dashboard, under **Configure this local server**, click **Add roles and features**.

The **Add Roles and Features Wizard** appears, showing the **Before you begin** page.

3. After reading the **Before you begin** page, click **Next**.

The **Select installation type** page appears.

4. In the middle pane, select **Role-based or feature-based installation**, and then click **Next**.

The **Select server selection** page appears.

5. Check **Select a server from the server pool**, and then highlight a server in the pool and click **Next**.

The **Select server roles** page appears.

6. Select all of the following roles and sub-roles:
 - File and Storage Services
 - File and iSCSI Services
 - File Server
 - File Server Resource Manager
 - Storage Services
 - Web Server (IIS)
 - Web Server
 - FTP Server
 - Management Tools
 - IIS 6 Management Compatibility
 - IIS 6 WMI Compatibility
 - IIS 6 Scripting Tools
 - IIS Management Scripts and Tools
 - Management Service
 - Application Development
 - ASP
 - ASP.NET (all version)

7. Click **Next**. The **Select features** page appears.
8. Select all of the following features and sub-features:
 - .NET Framework 3.5 Features
 - .NET Framework 3.5
 - HTTP Activation
 - Non-HTTP Activation
 - .NET Framework 4.6 Features
 - .NET Framework 4.6
 - ASP.NET 4.6
 - WCF Services
 - IIS Hostable Web Core
 - Internet Printing Client
 - LPR Port Monitor
 - Media Foundation
 - Message Queuing
 - Message Queuing Services
 - Message Queuing Server
 - Directory Service Integration
 - HTTP Support
 - Message Queuing Triggers
 - Multicasting Support
 - Routing Service
 - Message Queuing DCOM Proxy
 - Quality Windows Audio Video Experience
 - Remote Assistance
 - Remote Server Administration Tools
 - Feature Administration Tools
 - SMTP Server Tools
 - Role Administration Tools
 - File Services Tools
 - File Server Resource Manager Tools
 - SMB 1.0/CIFS File Sharing Support
 - SMTP Server
 - Windows Defender Features
 - Windows PowerShell
 - Windows PowerShell 5.1
 - Windows PowerShell 2.0 Engine
 - Windows PowerShell ISE
 - Windows Process Activation Service
 - WoW64 Support

9. Click **Next**.

The **Confirm installation selections** page appears.

10. Click **Install**.
11. After installation, follow the instructions in [Setting SMTP, FTP, and Quality Windows Audio Video Experience Properties](#).

Setting SMTP, FTP, and Quality Windows Audio Video Experience Properties

After SMTP, FTP, and Quality Windows Audio Video Experience services are installed, by default the SMTP and Quality Windows Audio Video Experience startup types are **Manual**, and for FTP the startup type is **Automatic**.



Tip

When the startup type is **Manual**, you must click the Start button to start the service.



Note

Administrators must manually start the Quality Windows Audio Video Experience service. If this service is not manually started, the Compatibility Checker will determine that the service is not installed or running, and this will cause the installation to fail.

The following procedure changes the startup type for SMTP. Repeat these steps for the Quality Windows Audio Video Experience service.



Note

Verify that the FTProot folder in the Inetpubs directory has at least read access.

1. Access the Services page by selecting **Start > Administrative Tools > Services**.
2. Right click **Simple Mail Transfer Protocol** and select **Properties** on the menu.
The Simple Mail Transfer Protocol (SMTP) Properties page appears.
3. Select **Automatic** on the Startup Type drop down menu, and then click **OK**.
4. Return to the Services page.
5. Right click **Microsoft FTP Service** and select **Properties** on the menu.
The Microsoft FTP Service properties page appears.
6. In the **Startup type** field, confirm that the **Automatic** option is selected.
7. Click **OK**.

Additional Considerations

This section discusses additional recommendations and requirements for installing the MiVoice Connect server.

Maximum Transmission Unit (MTU) Size for Connections

The default Maximum Transmission Unit (MTU) setting for PPP (Point-to-Point Protocol) clients, VPN (Virtual Private Network) clients, PPP servers, or VPN servers running Routing and Remote Access on MiVoice Connect systems is 1400. To change the MTU value, you must edit the registry. For further information, contact Mitel Support.

Windows Firewall Settings

The basic Windows firewall must be disabled for the Headquarters server and Windows DVS.

IE Enhanced Security Configuration

The IE Enhanced Security Configuration parameter must be disabled for Administrators.

IPv6

IPv6 parameter must be disabled for the primary NIC.

Data Execution Prevention (DEP)

Data Execution Prevention is recommended for essential Windows Programs and Services only. The default is for all programs and services.

Adobe Acrobat Reader

Install Adobe Acrobat Reader on the server if you do not already have it, so that you can access the online documentation. You can install Adobe Acrobat Reader from the MiVoice Connect USB flash drive or download it from the Adobe web site.

Internet Information Server (IIS) Default Web Site

The web site for Connect Director is `http://<server_name>/shorewaredirector`. You should not change the default IIS web site of the server to redirect to Connect Director, since this will cause navigation problems within Connect Director.

Access to the Distributed Server Maintenance Page

If you are using Microsoft Internet Explorer and the distributed server is configured with an IP address rather than a server name, you must enable session cookies on your client computer to access the Distributed Server Maintenance Page. To enable session cookies:

1. Launch Internet Explorer.

2. Click **Tools > Internet Options**.

The Internet Options dialog box appears.

3. Click the **Privacy** tab then the **Advanced** button.

The Advanced Privacy Settings dialog box appears.

4. Check the **Override automatic cookies** check box.

5. Select **Always allow session cookies**.

6. Click **OK** to save the change.

Microsoft Updates on the Server

When releasing a new build, build notes listing the Microsoft patches that are certified against the build are published. Software changes required by the Microsoft patches are highlighted. No additional Microsoft updates should be applied to your MiVoice Connect server between MiVoice Connect builds. If you install Microsoft updates between MiVoice Connect builds, they may have an adverse effect on your telephone system.

Virus Protection on the Main and Distributed Servers

The use of industry-standard virus protection software on the main and distributed servers is supported.

Anti-Virus Folder Exclusions

The following folders and sub folders must be excluded from Virus checker software or disk backup/restore software:

- Mitel Connect client:

```
<Drive>:\Users\%User%\AppData\Local\ShoreTel  
<Drive>:\Program Files (x86)\ShoreTel  
<Drive>:\Program Files (x86)\ShoreTel Presenter
```

- MiVoice Connect Contact Center

```
<Drive>:\Users\%User%\AppData\Roaming\ShoreTel Contact Center  
<Drive>:\Users\%User%\AppData\Local\ShoreTel Contact Center
```

- HQ/ DVS Server:

```
<Drive>:\Program Files (x86)\Shoreline Communications  
<Drive>:\Shoreline Data\
```



WARNING!

If the folders listed above are not excluded before installation, your installation of the current version of MiVoice Connect will fail and your system will roll back to the previous version. This will also result in a corrupted database if you perform nightly backups.
