

FORTRA

GoAnywhere MFT Agent Admin Guide

Version 2.1.4

Copyright Terms and Conditions

Copyright © Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from Fortra is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Fortra with appropriate and specific direction to the original content.

202401091103

Table of Contents

Agents	5	Installation - Linux	29
About Agents	5	Requirements	29
Agent Features	5	Linux Installation Consideration	29
Complete Management and Security ...	5	Installing Agents on Linux	29
Pre-Installation Notes	7	Agent Silent Install - Linux	30
GoAnywhere MFT Software Library	7	Updating or Repairing a Silent Install (of the same version)	31
Agent Installer Settings	7	Installation - Unix	32
Installing an Agent	19	Requirements	32
Changing the Location of Configuration Files	23	Installing Agents	32
Port Configuration	24	Agent Silent Install - Unix	34
Java Versions	24	Updating or Repairing a Silent Install (of the same version)	34
Agent Memory	25	Silent Install Parameters	36
Installation - Windows	26	Installation - IBM i (iSeries)	40
Requirements	26	Requirements	40
Installing Agents on Windows	26	Installing Agents on IBM i	41
Agent Silent Install - Windows	27	Changing Java Versions	51
Updating or Repairing a Silent Install (of the same version)	28	Installation - Mac OS X	52

Requirements	52	Disaster Recovery	84
Installing Agents on Mac OS X	52	Configuring an Agent to Run On a Different JVM	85
Agent Installer Management	54	Uninstalling Agents	86
Initial Configuration	54	Windows uninstall instructions	86
Software Library	55	Linux and Unix uninstall instructions	87
Browse Online Catalog	55	IBM i uninstall instructions	87
Configuring the Agent Installer	56	Mac OS X uninstall instructions	88
Pre-Upgrade Notes	65	Using FTP and FTPS in Passive Mode	88
2.1.3	65		
Network Shares Monitors	65		
2.0.0	65		
Upgrading Agents	66		
Java 11 Considerations	67		
Agent Configuration	69		
Advanced Configuration	71		
Agent Permissions	73		
Agent Security Settings	77		
Product Administration	82		
Starting and Stopping Agents	82		
Agent Logs	84		

Agents

About Agents

Agents are lightweight applications that can be deployed to virtually any operating system including Windows, Linux, IBM i, and more. Agents can run on systems inside an organization's network to move files throughout the data center. Agents can also be deployed to remote sites like branch offices, cloud networks, and other remote locations. Once an Agent is installed, it is connected to GoAnywhere MFT which takes over management of the Agents.

Agent Features

- Secures file transfers to and from a central GoAnywhere MFT environment
- Monitors for new, modified, and deleted files on systems where the Agent is installed
- Compresses and decompresses files on the Agent using Zip, Tar, and Gzip technology
- Translates data from databases, CSV, Fixed Width, XML, and JSON
- Executes native commands on Agents
- Controls which folders are accessible on the Agent

Complete Management and Security

GoAnywhere MFT is the centralized solution that manages all Agents. Administrators in GoAnywhere MFT configure the work that should be performed on Agents and can also view events that occurred, such as file transfers or completed jobs.

The communication between each Agent and GoAnywhere MFT is encrypted using SSL/TLS. The authentication is a multi-step secure process establishing trust between

Agents and GoAnywhere MFT. Since the administration is performed in GoAnywhere MFT's sophisticated browser based interface, no additional security concerns are placed on Agents.

GoAnywhere MFT automatically rolls out software upgrades to Agents as needed. This is a seamless process in which GoAnywhere MFT will upgrade Agents while they are not performing work to minimize disruption.

For more information about Agent features, see the *GoAnywhere MFT User Guide*.

Pre-Installation Notes

GoAnywhere MFT Software Library

Agents can be pre-configured from the Software Library in GoAnywhere MFT 5.5 and later. The Software Library in GoAnywhere MFT is where you can download Agent installation packages from the GoAnywhere Customer Portal and store them on your system. Fortra recommends configuring Agents from the Software Library. For more information, see the **GoAnywhere MFT User Guide**.

When an install package is created through the GoAnywhere MFT Software Library, the installer ZIP file will include an `agent_installer_settings.xml` file that contains the Agent configuration settings. When the installer is launched, the configuration settings from the XML file will populate the settings in the Agent installation wizard.

Agent Installer Settings

When installing an Agent, you can use the `agent_installer_settings.xml` file that is included in the installer ZIP file created from the Software Library or you can create your own XML file. For the installer to use the configuration settings from the XML file you create, it must reside in the same location as the installation file.

The following table lists the elements that can be updated.

Element Name	Description	Values
agentName	The name of the Agent that will appear on the Agent Manager page when the Agent connects. If a name is not specified, a name will be created automatically using the Agent Registration rules on the Agent Configuration Registration page.	String
registrationCode	The Agent Registration Code the Agent will use to register with GoAnywhere MFT. If no registration codes are configured on the Agent Service, then this field can be left blank.	String
shutdownPort	The TCP/IP port number the Agent uses to shutdown.	Number: valid values are from 1023 to 65536
host	The host name or IP address of the GoAnywhere MFT Agent Service the Agent will connect to.	String

Element Name	Description	Values
port	The port number of the GoAnywhere MFT Agent Service the Agent will connect to. The default is 8009.	Number
maxJobRuntime	The maximum number of concurrent Jobs that can be run at any one time on the Agent. After the threshold is met, any additional jobs are placed in the queue and are processed in the order they were submitted.	Number
maxMonitorRuntime	The maximum number of concurrent Monitors that can be run at any one time on the Agent.	Number
contextProtocol	The desired SSL protocol to be used for the connection to GoAnywhere MFT. This setting should match the SSL protocol on the SSL tab in the Agent Configuration in GoAnywhere MFT. See the <i>GoAnywhere MFT User Guide</i> for more information.	String

Element Name	Description	Values
rootCert	The GoAnywhere MFT Server CA certificate from the SSL settings of the Agent Service in GoAnywhere MFT. The Server certificate must be copied from the PEM Format tab and then copied to the installation wizard. See the <i>GoAnywhere MFT User Guide</i> for more information.	PEM format
restrictTasks	Determines if certain Task types are restricted from being executed on the Agent.	Boolean: true or false
database	Allows the Agent to run Database tasks on the Agent system.	Boolean: true or false
email	Allows the Agent to run Email tasks on the server where the Agent is installed.	Boolean: true or false
excel	Allows the Agent to run Excel tasks on the server where the Agent is installed.	Boolean: true or false

Element Name	Description	Values
execNative	Allows the Agent to run Execute Native Command tasks on the Agent system.	Boolean: true or false
fileCatalyst	Allows the Agent to run FileCatalyst tasks on the Agent system.	Boolean: true or false
ftp	Allows the Agent to run FTP tasks on the server where the Agent is installed.	Boolean: true or false
ftps	Allows the Agent to run FTPS tasks on the server where the Agent is installed.	Boolean: true or false
gofast	Allows the Agent to run GoFast tasks on the server where the Agent is installed.	Boolean: true or false
pgp	Allows the Agent to run PGP tasks on the server where the Agent is installed.	Boolean: true or false
ssh	Allows the Agent to run SSH tasks on the server where the Agent is installed.	Boolean: true or false

Element Name	Description	Values
webService	Allows the Agent to run Web Service tasks on the server where the Agent is installed.	Boolean: true or false
zip	Allows the Agent to run File Compression tasks.	Boolean: true or false
amazonS3File	Allows the Agent to utilize the Amazon S3 Buckets Resource on the server where the Agent is installed.	Boolean: true or false
azureFile	Allows the Agent to utilize the Azure Blob Storage Resource on the server where the Agent is installed.	Boolean: true or false
networkShareFile	Allows the Agent to utilize the Network Shares Resource on the server where the Agent is installed.	Boolean: true or false
webdavFile	Allows the Agent to utilize the WebDAV Resource on the server where the Agent is installed.	Boolean: true or false

Element Name	Description	Values
folders	By default, the Agent cannot access any folders on the system where the Agent is installed. Modify or add folder locations that can be used by the Agent.	See Agent Permissions for a sample folder configuration.
fipsEnabled	When FIPS 140-2 Compliance Mode is enabled, GoAnywhere MFT will only use FIPS 140-2 validated algorithms (ciphers) for encrypting transmissions over SSH and SSL channels including SFTP, SCP, FTPS, and HTTPS protocols.	Boolean: true or false
disabledProtocols	The SSL/TLS protocol versions to disable globally. Some protocols may forcibly be disabled depending on your JVM and security provider.	A comma separated list of SSL/TLS protocol names.

Element Name	Description	Values
disabledCiphers	The SSL/TLS cipher suites to disable globally. Some cipher suites may forcibly be disabled depending on your JVM and security provider.	A comma separated list of cipher suite names.
certificateValidationCABasicConstraintServer	Verifies the Certificate Authority (CA) is marked as a CA with a valid path length in its basic constraints.	Boolean: true or false
certificateValidationCABasicConstraintEmail	Verifies the Certificate Authority (CA) is marked as a CA with a valid path length in its basic constraints.	Boolean: true or false
certificateValidationDateValidityServer	Applies date validity check to server certificates.	Boolean: true or false
certificateValidationDateValidityEmail	Applies date validity check to email certificates.	Boolean: true or false
certificateValidationExtendedKeyUsageServer	Applies extended key usage check to server certificates. The check will validate the intended purpose of the certificate - server authentication.	Boolean: true or false

Element Name	Description	Values
certificateValidationExtendedKeyUsageEmail	Applies extended key usage check to email certificates. The check will validate the intended purpose of the certificate - email protection.	Boolean: true or false
certificateRevocationListCheckServer	Applies Certificate Revocation List (CRL) check to server certificates.	Boolean: true or false
certificateRevocationListCheckEmail	Applies Certificate Revocation List (CRL) check to email certificates.	Boolean: true or false
certificateRevocationListRefreshInterval	How often to refresh all Certificate Revocation Lists (CRLs) if CRLs are enabled.	Number
certificateRevocationListURLs	The URLs to use for Certificate Revocation List (CRL) checking.	A pipe ' ' separated list of URLs.

Element Name	Description	Values
allowImplicitTrust	Whether implicit trust is allowed for certain connections that support this configuration. If implicit trust is not allowed, implicit trust will be globally disabled and all connections will be required to validate certificates.	Boolean: true or false
localAddress	The local IP address of the Agent that will be used when connecting to GoAnywhere MFT.	String
localPortFrom	The inclusive starting range port number to use when restricting local ports for outgoing Agent connections to GoAnywhere MFT. The localPortTo attribute must also be specified to restrict port range.	Number: valid values are from 1023 to 65536
localPortTo	The inclusive ending range port number to use when restricting local ports for outgoing Agent connections to GoAnywhere MFT. The localPortFrom attribute must also be specified to restrict port range.	Number: valid values are from 1023 to 65536

Element Name	Description	Values
localAddressRequestTimeout	The time to wait in seconds for a local address to become available. This attribute only applies when the localPortTo and localPortFrom attributes are specified.	Number: valid values are from 1 to 240.
socketLinger	A socket option indicating how long after usage of a local socket should it stay in TIME_WAIT status. Typically, sockets are left in a TIME_WAIT status after connections are closed.	Number: valid value is any number greater than -1 (value of 0 indicates it will not wait).
reuseAddress	A socket option that tells the kernel to reuse the port even if the port is busy in the TIME_WAIT status.	Boolean: true or false

Sample Configuration

The following is a sample `agent_installer_settings.xml` file for an Agent.

```
<?xml.version="1.0" encoding="UTF-9" standalone="no"?>
<settings>
  <agentName>agent</agentName>
  <shutdownPort>1401</shutdownPort>
  <host>1.1.1.1</host>
  <port>9009</port>
  <maxJobRuntime>20</maxJobRuntime>
```

```
<maxMonitorRuntime>20</maxMonitorRuntime>
<contextProtocol>TLSv1.2</contextProtocol>
<rootCert>PEM formatted certificate</rootCert>
<restrictTasks>false</restrictTasks>
<database>true</database>
<email>true</email>
<excel>true</excel>
<execNative>true</execNative>
<fileCatalyst>true</fileCatalyst>
<ftp>true</ftp>
<ftps>true</ftps>
<gofast>true</gofast>
<pgp>true</pgp>
<ssh>true</ssh>
<webService>true</webService>
<zip>true</zip>
<amazonS3File>true</amazonS3File>
<azureFile>true</azureFile>
<networkShareFile>true</networkShareFile>
<webdavFile>true</webdavFile>
<folders>
    <folder alias="root" path="/" readOnly="true"/>
</folders>
<fipsEnabled>false</fipsEnabled>
<disabledProtocols/>
<disabledCiphers/>
<certificateValidationCABasicConstraintServer>true
</certificateValidationCABasicConstraintServer>
<certificateValidationCABasicConstraintEmail>true
</certificateValidationCABasicConstraintEmail>
<certificateValidationDateValidityServer>true
</certificateValidationDateValidityServer>
<certificateValidationDateValidityEmail>true
</certificateValidationDateValidityEmail>
<certificateValidationExtendedKeyUsageServer>true
```

```

</certificateValidationExtendedKeyUsageServer>
<certificateValidationExtendedKeyUsageEmail>true
</certificateValidationExtendedKeyUsageEmail>
<certificateRevocationListCheckServer>false
</certificateRevocationListCheckServer>
<certificateRevocationListCheckEmail>false
</certificateRevocationListCheckEmail>
<certificateRevocationListRefreshInterval>5
</certificateRevocationListRefreshInterval>
<certificateRevocationListURLS/>
<allowImplicitTrust>false</allowImplicitTrust>
<localAddress>1.2.3.4</localAddress>
<localPortFrom>23000</localPortFrom>
<localPortTo>24000</localPortTo>
<localAddressRequestTimeout>30</localAddressRequestTimeout>
<reuseAddress>true</reuseAddress>
<socketLinger>10</socketLinger>
</settings>

```

Installing an Agent

The Agent installation wizard will prompt for the fields listed in the following table.

Field	Definition
Agent Name	The name of the Agent that will appear on the Agent Manager page when the Agent connects. If a name is not specified, a name will be created automatically using the Agent Registration rules on the Agent Configuration Registration page.
Registration Code	The Agent Registration Code the Agent will use to register with GoAnywhere MFT. If no registration codes are configured on the Agent Service, then this field can be left blank.

Field	Definition
Shutdown Port	The TCP/IP port number the Agent uses to shutdown. The default is 8015.
GoAnywhere MFT Server Host	The host name or IP address of the GoAnywhere MFT Agent Service the Agent will connect to.
GoAnywhere MFT Server Port	The port number of the GoAnywhere MFT Agent Service the Agent will connect to. The default is 8009.
SSL Context Protocol	Specify the desired SSL protocol to be used for the connection to GoAnywhere MFT. This setting should match the SSL protocol on the SSL tab in the Agent Configuration in GoAnywhere MFT. See the <i>GoAnywhere MFT User Guide</i> for more information.
Agent Server CA Certificate	Provide the GoAnywhere MFT Server CA certificate from the SSL settings of the Agent Service in GoAnywhere MFT. The Server certificate must be copied from the PEM Format tab and then copied to the installation wizard. See the <i>GoAnywhere MFT User Guide</i> for more information.
Path to Agent CA Certificate	When configuring an Agent in command line mode, you will be prompted for the path to the Agent Server CA Certificate. The certificate must be accessible from the system the Agent is being installed on.
Security	
Enable FIPS 140-2 Compliance Mode	When FIPS 140-2 Compliance Mode is enabled, GoAnywhere MFT will only use FIPS 140-2 validated algorithms (ciphers) for encrypting transmissions over SSH and SSL channels including SFTP, SCP, FTPS, and HTTPS protocols.
Disabled Cipher Suites	Specify the SSL/TLS cipher suites to disable globally. Some cipher suites may forcibly be disabled depending on your JVM and security provider. Values must be comma separated.

Field	Definition
Disabled Protocols	Specify the SSL/TLS protocol versions to disable globally. Some protocols may forcibly be disabled depending on your JVM and security provider. Values must be comma separated.
CA Basic Constraints Validation	Select check box to verify the Certificate Authority (CA) is marked as a CA with a valid path length in its basic constraints.
Date Validation	Select check box to apply date validity check to server and email certificates.
Extended Key Usage Validation	Select check box to apply extended key usage check to server and email certificates. The check will validate the intended purpose of the certificate - server authentication and email protection.
Certificate Revocation Lists (CRL)	Select check box to apply CRL check to server and email certificates.
Certificate Revocation Lists (CRL) URLs	Specify the URLs to use for CRL checking. Must be a pipe ' ' separated list.
Refresh Interval	If CRLs are enabled, specify how often to refresh all CRLs. Default Value: 5 minutes.
Implicit Trust Allow All	Specify whether to allow implicit trust for certain connections that support this configuration. If unchecked, implicit trust will be globally disabled and all connections will be required to validate certificates.
Permissions	
Alias	By default, the Agent cannot access any folders on the system where the Agent is installed. To add a folder the Agent can access, specify the Alias and Path for the folder location that appears in the Agent file chooser.
Path	The path to the folder location on the Agent installation.

Field	Definition
Read Only	Indicates if the Agent will have Read Only access to the folder location.
Restrict Tasks	When selected, the types of Tasks the Agent can execute are restricted to the selected Task types.
Allow Amazon S3 File Syntax	Allows the Agent to utilize the Amazon S3 Buckets Resource on the server where the Agent is installed.
Allow Azure File Syntax	Allows the Agent to utilize the Azure Blob Storage Resource on the server where the Agent is installed.
Allow Network Share File Syntax	Allows the Agent to utilize the Network Shares Resource on the server where the Agent is installed.
Allow WebDAV File Syntax	Allows the Agent to utilize the WebDAV Resource on the server where the Agent is installed.
Allow Execute Native Command	Allows the Agent to run Execute Native Command tasks on the Agent system.
Allow FileCatalyst Tasks	Allows the Agent to run FileCatalyst tasks on the Agent system.
Allow Database Tasks	Allows the Agent to run Database tasks on the Agent system.
Allow Email Tasks	Allows the Agent to run Email tasks on the server where the Agent is installed. Valid values are true or false.
Allow Excel Tasks	Allows the Agent to run Excel tasks on the server where the Agent is installed. Valid values are true or false.
Allow FTP Tasks	Allows the Agent to run FTP tasks on the server where the Agent is installed. Valid values are true or false.
Allow FTPS Tasks	Allows the Agent to run FTPS tasks on the server where the Agent is installed. Valid values are true or false.
Allow GoFast Tasks	Allows the Agent to run GoFast tasks on the server where the Agent is installed. Valid values are true or false.

Field	Definition
Allow PGP Tasks	Allows the Agent to run PGP tasks on the server where the Agent is installed. Valid values are true or false.
Allow SSH Tasks	Allows the Agent to run SSH tasks on the server where the Agent is installed. Valid values are true or false.
Allow WebService Tasks	Allows the Agent to run Web Service tasks on the server where the Agent is installed. Valid values are true or false.
Allow Zip Tasks	Allows the Agent to run File Compression tasks on the Agent system.

Changing the Location of Configuration Files

By default, Agent config files are located in the [installdirectory]/config folder.

On install, you have an option to specify a custom location for Agent config files. If a custom location is specified, the path will be written to system.properties and the config files will be moved to the user defined directory.

If you want to change the location of the Agent config files after installing or upgrading an Agent, you will need to add the new path to the system.properties file and manually move the config files to the user defined directory.

To create a user defined directory and to manually move the Agent config files, complete the following steps:

1. Change the directory in the system.properties file. For example:

com.linoma.config.directory=C:\\ProgramData\\Fortra\\GoAnywhere

NOTE:

All backslash ('\\') characters need to be escaped in a given file path with an additional backslash as noted in the example above.

2. Create a new folder in the user defined directory named 'config'.
3. Move the following Agent config files from the install directory into the user defined config folder:
 - agent.xml
 - database.xml
 - log4j2.xml
 - permissions.xml
 - security.xml

Port Configuration

There are two port numbers to configure when installing Agents, the Agent shutdown port and the GoAnywhere MFT Agent Service port. The Agent shutdown port is locally bound and used as part of the Agent shutdown process. The GoAnywhere MFT Agent Service port is the port number of the Agent Service in GoAnywhere MFT that the Agent will connect to.

Port Number	Description
8015	Agent shutdown port
8009	GoAnywhere MFT connection port

These port numbers can be overridden either during the installation or at any time after the installation.

Java Versions

Java version 11 is bundled with the Windows and Linux installers. Refer to the [UNIX](#) and [IBM i](#) sections for their respective Java version requirements.

Agent Memory

You can adjust the maximum JVM memory usage for an Agent on a Windows or Linux system by following the instructions below.

1. Create a text file and name it **agentd.vmoptions**.
2. Paste the following text in the file:

```
# Enter one VM parameter per line
# For example, to adjust the maximum memory usage to 2 GB,
# uncomment the following line:
-Xmx2048m
# To include another file, uncomment the following line:
# -include-options [path to other .vmoption file]
```


3. Save the file and place it in the **<installdir>/bin** folder.

Installation – Windows

A Windows installation wizard is provided for GoAnywhere Agents which installs the product files into the directory of your choice. Agents will be implemented as a Windows Service which will automatically start (by default) when Windows starts.

The Windows Agent installer application can be pre-configured and generated through GoAnywhere MFT via the Software Library manager. For instruction on how to configure and generate a Windows Agent installer application .ZIP file, refer to the *GoAnywhere MFT User Guide*. Otherwise, you can download the Agent installer through the GoAnywhere Customer Portal.

Requirements

Operating Systems supported	Windows Server 2012 [®]	
	Windows Server 2012 R2 [®]	
	Windows Server 2016 [®]	
	Windows 8 [®]	
	Windows 10 [®]	
Disk space	160 MB	
Memory	512 MB minimum	

Installing Agents on Windows

Perform the following steps to install an Agent onto a Windows machine.

1. Login to the target Windows system as an administrator.
2. Navigate to the file location of the Agent installer or pre-configured Agent ZIP file.

NOTE:

If you have a 64-bit operating system, make sure you have the 64-bit version.

3. If you are using the Agent ZIP file, extract the contents of the file.
4. Launch the installer application.
5. The GoAnywhere Agent Setup Wizard will then guide you through the remainder of the installation process.
6. When prompted, specify the Agent [configuration](#) settings. If your Agent installer application was pre-configured, all required Agent Configuration settings will be populated using data provided when the installer was initially configured in GoAnywhere MFT.

NOTE:

Agents are configured in Windows as an automatic startup Service. This means that the Agent will automatically start whenever Windows starts.

Agent Silent Install - Windows

The installation of an Agent can be automated by using a silent install option. Silent install uses the Windows command line to execute the installation.

NOTE:

The `agent_installer_settings.xml` file must be in the same directory as the Agent installer file or the silent install will fail.

To perform a silent install of an Agent on Windows:

1. Log in to the target Windows system as an administrator.
2. Open the command prompt and use the `cd` command to navigate to the directory containing the Agent installer.
3. Enter the command to execute the Agent installer in the desired location.

Parameters that begin with -V must be specified as a key=value pair. Separate each -V parameter with a space.

EXAMPLE:

```
[installer file name].exe -q -Vgaagent.port=8009 -Vgaagent.shutdownPort=8015
```

The following command is used to silently install an Agent.

```
[installer file name].exe -q -dir "[path]"
```

For parameters for silent install on Windows, see the [Parameters](#) table.

Updating or Repairing a Silent Install (of the same version)

Use the following instructions to update or repair an Agent:

1. Log in to the target Windows system as an administrator.
2. Open the command prompt and use the cd command to navigate to the directory containing the Agent installer.
3. Execute the following command where "[path]" is the location of the Agent installation you want to update or repair:

```
[installer file name].exe -q -dir "[path]"
```

EXAMPLE:


```
agent1_3_1_windows_x64.exe -q -dir "C:\Agents"
```

Installation - Linux

GoAnywhere Agents can be installed onto any Linux server including Red Hat, CentOS, SUSE, Ubuntu, and others.

A graphical installation wizard is provided for Agents which installs the product files into the directory of your choice.

Requirements

Disk space	160 MB	
Memory	512 MB minimum	

Linux Installation Consideration

GoAnywhere Agents are capable of executing native Linux commands and programs, as well as file actions such as read, write, and delete. It is recommended to designate a non-root user on the system that will be used to install and run the Agent application. This user will be the owner of all files created during installation as well as files written to the file system during use.

Installing Agents on Linux

Perform the following steps to install an Agent onto a Linux system.

1. Create or designate a non-root user on the system that will be used to install and run the Agent application. This user will be the owner of all files created during installation as well as files written to the file system during use.
2. Login to the target Linux system as the user designated in step 1.
3. Copy the Agent Linux installer file to the Linux server.
4. If you are using the Agent ZIP file, extract the contents of the file.

5. If needed, set the Executable bit on the file (e.g. **chmod 755 filename.sh**).
6. If you have a graphical desktop for Linux, execute the downloaded installer file and follow the prompts on the screens. Otherwise, execute the downloaded installer file with a -c option (e.g. **installer_filename.sh -c**) and follow the prompts.

NOTE:

When installing an Agent in command line mode, you will be prompted for the path to the Agent Server CA Certificate. If you would like to use a certificate other than one pre-configured, that certificate must be accessible from the system the Agent is being installed on.

1. Specify the Agent [configuration](#) settings. If your Agent installer application was pre-configured, all required Agent Configuration settings will be populated using data provided when the installer was initially configured in GoAnywhere MFT.
2. Start the Agent by following these instructions:
 - a. Open a Terminal window.
 - b. Change the working directory to the directory where the Agent was installed (for example, **cd /usr/local/Fortra/GoAnywhere_Agent/bin**)
 - c. Start the Agent by executing the following shell script:
./agentd start
3. The installation and startup of the Agent is complete.

NOTE:

You can setup an Agent so it starts automatically when the Linux system is booted. Please refer to your operating system manual for more details on setting up auto-start services.

Agent Silent Install - Linux

The installation of an Agent can be automated by using a silent install option.

NOTE:

The agent_installer_settings.xml file must be in the same directory as the Agent installer file or the silent install will fail.

To perform a silent install of an Agent on Linux:

1. Copy the Agent Linux installer file to the Linux server.
2. If you are using the Agent ZIP file, extract the contents of the file.
3. Execute the downloaded installer file using the following command:

```
[installer_filename].sh -q -dir "[path]"
```

Parameters that begin with -V must be specified as a key=value pair. Separate each -V parameter with a space.

EXAMPLE:

```
[installer file name].sh -q -Vgaagent.port=8009 -Vgaagent.shutdownPort=8015
```

For parameters for silent install on Windows, see the [Parameters](#) table.

Updating or Repairing a Silent Install (of the same version)

Use the following instructions to update or repair an Agent:

1. Copy the new Agent Linux installer file to the Linux server.
2. If you are using the Agent ZIP file, extract the contents of the file.
3. Execute the downloaded installer file using the following command where "[path]" is the location of the Agent installation you want to update or repair:

```
[installer_filename].sh -q -dir "[path]"
```

EXAMPLE:

```
agent0_9_0_linux_x64.sh -q -dir "/usr/local/Fortra/GoAnywhere_Agent"
```

Installation – Unix

This page includes Agent installation instructions for AIX, HP-UX, Solaris or non x86-based Linux systems (Unix).

An installation wizard is provided which installs the product files into the directory of your choice.

Requirements

Disk space	160 MB
Memory	512 MB minimum
JRE (Java Runtime Environment)	11

Installing Agents

Perform the following steps to install Agents onto a Unix server.

1. Create or designate a non-root user on the system that will be used to install and run the Agent application. This user will be the owner of all files created during installation as well as files written to the file system during use.
2. Login to the server as the user designated in step 1.
3. Copy the Agent Unix installer file to the server.
4. If you are using the Agent ZIP file, extract the contents of the file.
5. Open a Terminal window.
6. Change the directory to where the installer file was downloaded (e.g. `cd /root/Desktop`).
7. If needed, set the Executable bit on the file (e.g. `chmod 755 ga5_x_x_unix.sh`).
8. Run the installer (e.g. `./agent1_0_0_linux_x86.sh`).

9. The installer will attempt to find a compatible JRE (Java Runtime Environment) for the installation process. Follow the steps below if the installer cannot find a compatible JRE:
 - a. Define an environment variable named **INSTALL4J_JAVA_HOME** to point to the home directory of the JRE (e.g. **export INSTALL4J_JAVA_HOME=/usr/lib/jvm/java-11-openjdk/jre**).
 - b. Clear the Installer cache by removing the file named **.install4j** from your home directory (e.g. **rm /root/.install4j**).
 - c. Run the installer again (e.g. **./agent1_0_0_linux_x86.sh**).
10. Specify the Agent [configuration](#) settings. If your Agent installer application was pre-configured, all required Agent Configuration settings will be populated using data provided when the installer was initially configured in GoAnywhere MFT.

NOTE:

When installing an Agent in command line mode, you prompted for the path to the Agent Server CA Certificate. If you would like to use a certificate other than one pre-configured, that certificate must be accessible from the system the Agent is being installed on.

Start an Agent by following these instructions:

1. Open a Terminal window.
2. Change the working directory to the directory where Agents is installed. (eg, **cd /usr/local/Fortra/GoAnywhere_Agent/bin**)
3. Start the Agents by executing the following shell script:
./agentd.sh start.
4. If you receive an error indicating that no JRE could be found, set an environment variable named **JAVA_HOME** to point to the JRE's home directory (e.g. **export JAVA_HOME=/usr/lib/jvm/java-11-openjdk/jre**) and try starting Agents again.

NOTE:

You can setup Agents so it starts automatically when the system is booted. Please refer to your operating system manual for more details on setting up auto-start services. You can execute **goanywhere.sh** from your startup scripts.

Agent Silent Install - Unix

The installation of an Agent can be automated by using a silent install option.

NOTE:

The `agent_installer_settings.xml` file must be in the same directory as the Agent installer file or the silent install will fail.

To perform a silent install of an Agent on AIX, HP-UX, Solaris or non x86-based Linux systems (Unix):

1. Copy the Agent Unix installer file to the Unix server.
2. If you are using the Agent ZIP file, extract the contents of the file.
3. Execute the downloaded installer file using the following command:

```
[installer_filename].sh -q -dir "[path]"
```

Parameters that begin with -V must be specified as a key=value pair. Separate each -V parameter with a space.

EXAMPLE:

```
[installer file name].sh -q -Vgaagent.port=8009 -Vgaagent.shutdownPort=8015
```

For parameters for silent install on Unix, see the [Parameters](#) table.

Updating or Repairing a Silent Install (of the same version)

Use the following instructions to update or repair an Agent:

1. Copy the new Agent Unix installer file to the Unix server.
2. If you are using the Agent ZIP file, extract the contents of the file.
3. Execute the downloaded installer file using the following command where "[path]" is the location of the Agent installation you want to update or repair:

```
[installer_filename].sh -q -dir "[path]"
```

EXAMPLE:

```
agent0_9_0_unix_x64.sh -q -dir "/usr/local/Fortra/GoAnywhere_Agent"
```

Silent Install Parameters

The following table contains the required and optional parameters for a silent install on Windows, Linux, and AIX, HP-UX, Solaris or non x86-based Linux systems (Unix).

Parameter Name	Description	Required?
-q	Displays no user interface.	Yes
-dir	The directory path where the Agent is to be installed.	No
-console	Displays a console output.	No
-Vgaagent.serviceDisplayName	The display name of the GoAnywhere MFT Agent service. NOTE: This parameter is used only for silent install on Windows.	No

Parameter Name	Description	Required?
-Vgaagent.serviceName	<p>The name of the GoAnywhere MFT Agent service (this is typically the same as the serviceDisplayName).</p> <div> NOTE: This parameter is used only for silent install on Windows. </div>	No
-Vgaagent.port	The port number or IP address of the GoAnywhere MFT Agent service the Agent will connect to. The default is 8009.	No
-Vgaagent.shutdownPort	The TCP/IP port number the Agent uses to shutdown. The default is 8015.	No
-Vgaagent.maxJobRuntime	The maximum number of concurrent Jobs that can be run at any one time on the Agent.	No
-Vgaagent.maxMonitorRuntime	The maximum number of concurrent Monitors that can be run at any one time on the Agent.	No

Parameter Name	Description	Required?
-Vgaagent.localAddress	The local IP address of the GoAnywhere MFT instance this Agent will connect to.	No
-Vgaagent.localPortFrom	The inclusive starting range port number to use when restricting ports connecting to the GoAnywhere MFT instance. The localPortTo attribute must also be specified to restrict port range. Valid values are from 1023 to 65536.	No
-Vgaagent.localPortTo	The inclusive ending range port number to use when restricting ports connecting to the GoAnywhere MFT instance. The localPortFrom attribute must also be specified to restrict port range. Valid values are from 1024 to 65536.	No

Parameter Name	Description	Required?
-Vgaagent.localAddressRequestTimeout	The time to wait in seconds for a local address to become available. This attribute only applies when the localPortTo and localPortFrom attributes are specified. Valid values are from 1 to 240.	No
-Vgaagent.socketLinger	A socket option indicating how long after usage of a local socket should it stay in TIME_WAIT status. Typically, sockets are left in a TIME_WAIT status after connections are closed. Valid value is any number greater than -1 (value of 0 indicates it will not wait).	No
-Vgaagent.reuseAddress	A socket option that tells the kernel to reuse the port even if the port is busy in the TIME_WAIT status.	No

Installation - IBM i (iSeries)

GoAnywhere Agents can be installed on IBM i systems which meet the following requirements.

Requirements

Operating System	IBM i V7R3 or higher
Disk Space	160 MB for product (does not include user data)
Memory	512 MB minimum

Required licensed programs

The following IBM i licensed programs are prerequisites to the installation of Agents, which are dependent on IBM i release and your choice of supported Java version.

IBM i Release	Licensed Program	Product Option	Description
V7R3, V7R4, V7R5	5770JV1	19	Java SE 11 64 bit
	5770SS1	30	QShell
	5770SS1	33	Portable App Solutions Environment

To check if the licensed programs (listed above) are installed on your IBM i, execute the command **GO LICPGM** and select option 10 to display the installed licensed programs. Press F11 twice from that screen to display the **Product Options**.

If these licensed programs are not loaded on your IBM i, they may be available on the IBM software CDs that came with your IBM i. Otherwise, you will have to request those licensed programs from IBM, which are normally provided at no charge.

Required PTFs

The following IBM i Program Temporary Fixes (PTFs) and Group PTFs are prerequisites to installing Agents.

V7R3, V7R4, V7R5	Group PTF	Java group build 11
---------------------	--------------	---------------------

Use the command **DSPPTF** to verify that the required individual PTFs are applied. Use the command

WRKPTFGRP to verify that the required group PTFs are applied.

IBM i components installed

The following components will be installed onto the IBM i by the Agents installation process:

- A IBM i library will be created, which will contain the Agents commands and program objects. The default library name is **GAAGENT**, which can be changed during installation.
- An IFS folder will be created, which will contain the Agents software components. The default IFS folder name is **/fortra/gaagent**, which can be changed during installation.

Installing Agents on IBM i

Perform the following steps to install the Agents product onto the IBM i.

1. Sign on to the IBM i with the **QSECOFR** user profile OR with a profile which has *ALLOBJ authority.

2. Create a temporary Save file on your IBM i by executing the following IBM i command:
CRTSAVF FILE(QGPL/GAAGENT)
3. The Agents software needs to be uploaded to your IBM i using FTP. Before proceeding, ensure the FTP server is running on the IBM i. To start the native FTP server on the IBM i, you can issue the IBM i command of **STRTCPSVR SERVER (*FTP)**.
4. Download the Agents installer (for IBM i) from the Customer Portal at my.goanywhere.com or using the Software Library in GoAnywhere MFT.
5. Extract the files from the installer ZIP file into a new temporary folder on your workstation. The extracted files will be named **GAAGENT.SAVF** and **agent_installer_settings.xml**.
6. FTP the extracted **GAAGENT.SAVF** file from your PC to the Save file on the IBM i (that was created in step 2). Listed below are instructions for a Windows user:
 - a. Open a DOS window.
 - b. Enter the DOS command **FTP <hostname>**, where **<hostname>** is the host name or IP address of your IBM i.
 - c. Login with your IBM i user id and password, then enter the following highlighted FTP commands:

ftp> BINARY	Switches the FTP session to binary mode
ftp> LCD \<tempdir>	The <tempdir> is the PC directory containing the file named GAAGENT.SAVF
ftp> CD qqpl	Changes the remote directory to the QGPL library
ftp> PUT GAAGENT.SAVF GAAGENT	Sends the PC file GAAGENT.SAVF to the IBM i Save file named GAAGENT
ftp> QUIT	Ends your FTP session

7. FTP the extracted **agent_installer_settings.xml** file from your PC to a temporary location on the IFS. Listed below are instructions for a Windows user:
 - a. Open a DOS window.
 - b. Enter the DOS command **FTP <hostname>**, where **<hostname>** is the host name or IP address of your IBM i.
 - c. Login with your IBM i user id and password, then enter the following highlighted FTP commands:

ftp> BINARY	Switches the FTP session to binary mode
ftp> LCD \<tempdir>	The <tempdir> is the PC directory containing the file named agent_installer_settings.xml
ftp> CD /<ifsdir>	Changes the remote directory to a desired IFS folder, for example, /tmp
ftp> PUT agent_installer_ settings.xml agent_installer_ settings.xml	Sends the PC file agent_installer_settings.xml to the IFS folder location
ftp> QUIT	Ends your FTP session

8. Restore the installation objects into QTEMP by executing the following IBM i command:
RSTOBJ OBJ(*ALL) SAVLIB(QTEMP) DEV(*SAVF) SAVF(QGPL/GAAGENT)
9. Delete the temporary Save file by executing the following IBM i command (optional):
DLTF FILE(QGPL/GAAGENT)
10. If QTEMP library is not in your library list, then add it by executing the following IBM i command:
ADDLIB LIB(QTEMP) POSITION(*FIRST)

11. Prompt (F4) the command **QTEMP/INSTALLGAA** for installing Agents. The following screen appears.

```

                                Install GoAnywhere Agent (INSTALLGAA)

Type choices, press Enter.

Use settings from XML file . . . > *YES                *YES, *NO
Settings XML file . . . . .
-----

Install library . . . . . GAAGENT           Name
Install IFS directory . . . . "/Fortra/GAAgent"
-----
-----

F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys

```

12. If **NO** is selected for **Use settings from XML file**, the following screens appear.

```

                                Install GoAnywhere Agent (INSTALLGAA)

Type choices, press Enter.

Use settings from XML file . . . > *NO                *YES, *NO
Install library . . . . . GAAGENT                Name
Install IFS directory . . . . > '/Fortra/GAagent'

```

```

Agent name . . . . . GAAGENT
Registration code . . . . .
Shutdown port . . . . . 8015                1-65534
GoAnywhere MFT server host . . .
GoAnywhere MFT server port . . . 8009                1-65534
SSL context protocol . . . . .
Server CA Certificate . . . . .

```

```

                                More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys

```

Install GoAnywhere Agent (INSTALLGAA)		
Type choices, press Enter.		
Folder access:		
Alias name	_____	
Path	_____	
Read only	*NO	*YES, *NO
+ for more values	_____	
Restrict Usage	*NO	*YES, *NO
Allow Database Tasks	*NO	*YES, *NO
Allow Email Tasks	*NO	*YES, *NO
Allow Excel Tasks	*NO	*YES, *NO
Allow Execute Native Command . .	*NO	*YES, *NO
Allow FTP Tasks	*NO	*YES, *NO
Allow FTPS Tasks	*NO	*YES, *NO
Allow GoFast Tasks	*NO	*YES, *NO
Allow PGP Tasks	*NO	*YES, *NO
Allow SSH Tasks	*NO	*YES, *NO
More...		
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display		
F24=More keys		

Install GoAnywhere Agent (INSTALLGAA)		
Type choices, press Enter.		
Allow Webservice Tasks	<input checked="" type="checkbox"/> NO	*YES, *NO
Allow ZIP Tasks	*NO	*YES, *NO
Allow Amazon file permissions .	*NO	*YES, *NO
Allow Azure file permissions . .	*NO	*YES, *NO
Allow Network Share permission	*NO	*YES, *NO
Allow WebDAV file permissions .	*NO	*YES, *NO
Maximum job runtime	20	1-999
Maximum monitor runtime	20	1-999
Enable FIPS 140-2 Compliance . .	*NO	*YES, *NO
Disabled SSL/TLS Protocols . . .	_____	
Disabled SSL/TLS Cipher Suites		
Allow Implicit Trust	*NO	*YES, *NO
CA Validation Server Certs . . .	*NO	*YES, *NO
CA Validation Email Certs . . .	*NO	*YES, *NO
More...		
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display		
F24=More keys		

```

Install GoAnywhere Agent (INSTALLGAA)

Type choices, press Enter.

Date Validation Server Certs . . *NO          *YES, *NO
Date Validation Email Certs . . *NO          *YES, *NO
Ext Key Validation Serv Certs . *NO          *YES, *NO
Ext Key Validation Email Certs *NO          *YES, *NO
CRL Server Certs . . . . . > *yes         *YES, *NO
CRL Email Certs . . . . . *NO          *YES, *NO
CRL Refresh Interval . . . . . 5          1-2147483647
CRL URLs . . . . .

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

```

Parameter descriptions

Field name	Description
Use Settings from XML file	Indicate whether to use the settings XML file that was created on the GoAnywhere MFT server.
Settings XML file	Full IFS path of the settings XML file created by MFT to use to install the Agent, the path designated in step 7.
Install Library	The library to contain the Agents product objects. The specified library name must not already exist.
Install IFS directory	The directory to contain the Agents product files. The specified directory name must not already exist.
Agent name	The name of the Agent that will appear on the Agent Manager page in GoAnywhere MFT.
Registration code	Registration code to pass to the GoAnywhere MFT instance that the Agent will connect to. The registration code is set up in advance in the GoAnywhere MFT server.
Shutdown port	The port number which the Agents will listen to for shutdown requests. Default is 8015. *

Field name	Description
GoAnywhere MFT server host	The host domain or IP address of the GoAnywhere MFT server that the Agent will connect to.
GoAnywhere MFT server port	The port number of the GoAnywhere MFT server that the Agent will connect to. The default port is 8009.*
SSL context protocol	Specify the desired SSL protocol to be used for the Agent Control Channel. Some examples include TLSv1, TLSv1.1 and TLSv1.2
Server CA certificate	The full IFS path of the file that holds the GoAnywhere MFT server certificate.
Folder access	Enter up to five IFS paths that the Agent will have access to. Each path contains three parts: the alias name, alias path and a read only indicator. Sub folders will inherit permissions from the defined folder permissions.
Restrict usage	If set to "true", the types of Tasks the Agent can execute are restricted to the selected Task types that follow. Valid values are true or false.
Allow Database tasks	Allows the Agent to run Database tasks on the server where the Agent is installed. Valid values are true or false.
Allow Email tasks	Allows the Agent to run Email tasks on the server where the Agent is installed. Valid values are true or false.
Allow Excel tasks	Allows the Agent to run Excel tasks on the server where the Agent is installed. Valid values are true or false.
Allow execute native command	Allows the Agent to run Execute Native Command tasks on the server where the Agent is installed. Valid values are true or false.
Allow FileCatalyst tasks	Allows the Agent to run FileCatalyst tasks on the server where the Agent is installed. Valid values are true or false.
Allow FTP tasks	Allows the Agent to run FTP tasks on the server where the Agent is installed. Valid values are true or false.

Field name	Description
Allow FTPS tasks	Allows the Agent to run FTPS tasks on the server where the Agent is installed. Valid values are true or false.
Allow GoFast tasks	Allows the Agent to run GoFast tasks on the server where the Agent is installed. Valid values are true or false.
Allow PGP tasks	Allows the Agent to run PGP tasks on the server where the Agent is installed. Valid values are true or false.
Allow SSH tasks	Allows the Agent to run SSH tasks on the server where the Agent is installed. Valid values are true or false.
Allow Webservice tasks	Allows the Agent to run Webservice tasks on the server where the Agent is installed. Valid values are true or false.
Allow ZIP tasks	Allows the Agent to run File Compression tasks on the server where the Agent is installed. Valid values are true or false.
Allow Amazon file permissions	Allows the Agent to utilize the Amazon S3 Buckets Resource on the server where the Agent is installed.
Allow Azure file permissions	Allows the Agent to utilize the Azure Blob Storage Resource on the server where the Agent is installed.
Allow Network Share permission	Allows the Agent to utilize the Network Shares Resource on the server where the Agent is installed.
Allow WebDAV file permissions	Allows the Agent to utilize the WebDAV Resource on the server where the Agent is installed.
Enable FIPS 140-2 Compliance	When FIPS 140-2 Compliance Mode is enabled, Agents will only use FIPS 140-2 validated algorithms (ciphers) for encrypting transmissions over SSH and SSL channels including SFTP, SCP, FTPS and HTTPS protocols.
Disabled SSL/TLS Protocols	Specify the SSL/TLS protocol versions and cipher suites to disable globally. Some allowed protocols and cipher suites may forcibly be disabled depending on your JVM and security provider. Values must be comma-separated.

Field name	Description
Disabled SSL/TLS Cipher Suites	Specify the SSL/TLS protocol versions and cipher suites to disable globally. Some allowed protocols and cipher suites may forcibly be disabled depending on your JVM and security provider. Values must be comma-separated.
Allow Implicit Trust	Specify whether to allow implicit trust for certain connections that support this configuration. If unchecked, implicit trust will be globally disabled and all connections will be required to validate certificates.
CA Validation Server Certs	CA Basic Server Constraints Validation
CA Validation Email Certs	CA Basic Email Constraints Validation
Date Validation Server Certs	Date Validation of Server Certificates
Date Validation Email Certificates	Date Validation of Email Certificates
Ext Key Validation Serv Certs	Extended Key Usage Validation Server Certificates
Ext Key Validation Email Certs	Extended Key Usage Validation Email Certificates
CRL Server Certs	Server Certificate Revocation Lists (CRL)
CRL Email Certs	Email Certificate Revocation Lists (CRL)
CRL Refresh Interval	Specify in minutes how often the CRLs should be refreshed.
CRL URLs	Specify the URLs to use for CRL checking. Must be a pipe ' ' separated list.

To check if the port number is already in use, run the IBM i command of **NETSTAT and select option 3. Then press F14 to see the numeric port numbers.*

11. After reviewing and/or modifying the parameters on the **INSTALLGAA** command, press enter to start the installation process.
12. Prompt (F4) the command **GAAGENT/STRGAAGENT** for starting the Agents subsystem. The following screen will be displayed.

```
Start GoAnywhere Agent (STRGAAGENT)

Type choices, press Enter.

Server user profile . . . . . *CURRENT      Name, *CURRENT
```

For the **Server User Profile** parameter, keep the default of ***CURRENT** if you want to run the Agents application under your user profile. Otherwise, specify a different user profile to run the Agents application server under.

NOTE:

The user profile specified on the **STRGAAGENT** command must be enabled on the IBM i. This profile must have ***USE** authority to the **STRSBS** command and ***RWX** authority to the IFS folders where Agents is installed.

For security purposes, you may want to create a new user profile and consistently use that profile on the **STRGAAGENT** command. Then you would only have to grant authority for the Agents installation IFS folders to that user profile. There are certain user profiles that you cannot use to start the GAAGENT subsystem. These are: 'QSECOFR', 'QSPL', 'QDOC', 'QDBSHR', 'QRJE', 'QSYS', 'QLPAUTO', 'QLPINSTALL', 'QTSTRQS' Or 'QDFTOWN'

13. Press enter on the **STRGAAGENT** command to start the Agents subsystem.
14. Execute the **WRKACTJOB** (Work with Active Jobs) command to confirm that the Agents subsystem is running. You should find a subsystem which has the same name as the library name that was specified on the **INSTALLGAA** command in step 10 (named GAAGENT by default). This subsystem should contain Agent application jobs.

15. The installation and startup of Agents is complete.

NOTE:

The Agents can automatically start when the System i is powered up (IPL). To perform this automatic startup, place the **STRGAAGENT** command in the System i startup CL program (after the start of TCPIP).

CL example:

0001.00	QSYS/STRTCP	/* Start TCP	*/
0002.00	DLYJOB DLY(120)	/* Wait for TCP to fully start	*/
0003.00	GAAGENT/STRGAAGENT	/* Start GoAnywhere Agent server	*/

Changing Java Versions

Follow the instructions below to change the Java version for an Agent:

1. Log in to the IBM i using a terminal session.
2. End the Agent subsystem by running the **GAAGENT/ENDGAAGENT** command.
3. Run the **GAAGENT/CFGGAAGENT** command.
4. Under the Java Home section, edit the value as needed by choosing option 2.

Installation - Mac OS X

GoAnywhere Agents can be installed onto Apple's Mac OS X desktops, laptops, or servers.

Requirements

Operating Systems supported	Mac OS X
Disk space	160 MB for product (does not include user data)
Memory	512 MB minimum

Installing Agents on Mac OS X

Perform the following steps to install an Agent onto an Apple machine.

1. Login to the target Mac OS X system as an administrator.
2. Download the Agent .DMG installer from the GoAnywhere Customer Portal if you have not already pre-configured and downloaded one through GoAnywhere MFT.
If you are using the Agent ZIP file, extract the contents of the file.
3. Open the downloaded .DMG file, double click the Agent installer, and follow the prompts on the screen.

NOTE:

If you have not already done so, you may be prompted to install the legacy Java SE 7 runtime. Click the **More Info** button and follow the instructions from Apple to install Java. Repeat step 3 when Java is installed.

4. When prompted, specify the Agent [configuration](#) settings. If your Agent installer application was pre-configured, all required Agent Configuration settings will be

populated using data provided when the installer was initially configured in GoAnywhere MFT.

5. Start an Agent by following these instructions:
 - a. Open a Terminal window.
 - b. Change the working directory to the directory where the Agent was installed.
(for example, `cd /Applications/Fortra/GoAnywhere_Agent/bin`)
 - c. Start an Agent by executing the following shell script:
`./agentd.sh start`
6. The installation and startup of the Agent is complete.

Agent Installer Management

The GoAnywhere MFT Software Library provides Admin Users an online catalog of Agent installer and upgrader packages that can be downloaded to the Agents installation and used to pre-configure, install, and upgrade Agents.

To manage the available Agent installers, log in to GoAnywhere MFT as an Admin User with the **Product Administrator** role. (missing or bad snippet)

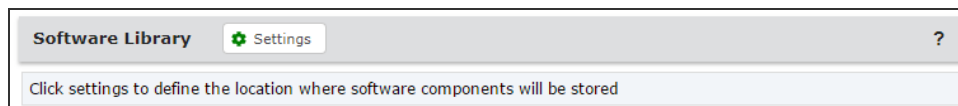
From the main menu bar, select **Help** and then click the **Software Library** link.

Initial Configuration

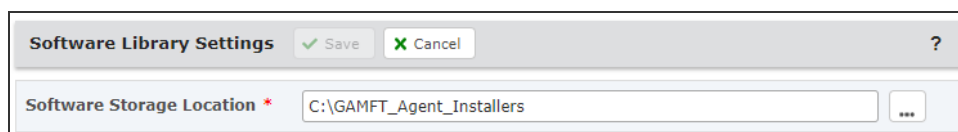
You must define a location on the Agents installation where Agent installers will be saved before you can browse the online catalog. When GoAnywhere MFT is in a clustered environment, this location needs to be a shared location available to all nodes in the cluster.

NOTE:

When Agents is running in a cloud hosted environment, the software storage location is disabled and users are unable to make changes.



Click the **Settings** button, and then specify a location where Agent installers will be stored.



Click **Save**. The Software Library's online catalog option will now be displayed.

Software Library

The Software Library lists Agent Installers that were downloaded from the Online Catalog or imported from a local directory.

Software Library 📁 Browse Online Catalog 📁 Import ⚙️ Settings ?						
	Product	Package	Version	Release Date	Operating System	File Name
⚙️	GoAnywhere Agents	Installer	1.3.1	2/7/19	Mac OS X	agent1_3_1_macos.dmg
⚙️	GoAnywhere Agents	Installer	1.3.1	2/7/19	UNIX, AIX, HP-UX, Solaris, etc.	agent1_3_1_unix.sh
⚙️	GoAnywhere Agents	Installer	1.3.1	2/7/19	Microsoft Windows 64-bit version	agent1_3_1_windows_x64.exe
						File Size
						142.46 MB
						141.68 MB
						181.88 MB

Page Toolbar

The following actions are available from the page toolbar:

- View and download available Agent installers and upgraders from the GoAnywhere Customer Portal by clicking the **Browse Online Catalog** button.
- Import an Agent Installer package by clicking the **Import** button. This option should be used when Agents cannot connect directly to the GoAnywhere Customer Portal.
- Change the Software Library storage location by clicking the **Settings** button.

Software Actions

The following actions are available by selecting the **Actions** icon:

- Configure an Agent installer by clicking the **Configure Installer** icon.
- Upgrade an Agent to the latest version by clicking the **Upgrade** icon.
- Delete an installer or upgrader by clicking the **Delete** icon.

Browse Online Catalog

The Online Catalog provides a list of Agent installers and upgraders that can be downloaded from the GoAnywhere Customer Portal. Use the following instructions to download an Agent package from the online catalog:

1. To download Agent installers and upgraders, log in as an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Help** and then click the **Software Library** link.
3. From the Software Library, click the **Browse Online Catalog** button. The list of Agent Installers and upgraders for specific operating systems appears.
4. Click **Download** to download an installer or upgrader. The package is downloaded to the Software Library's storage location.
5. Click the **Done** button to return to the Software Library.

Online Catalog Refresh Done ?						
	Product	Package	Version	Release Date	Operating System	File Name
✓	GoAnywhere Agent	Installer	1.3.1	2/7/19	Mac OS X	agent1_3_1_macos.dmg
ⓘ	GoAnywhere Agent	Installer	1.3.1	2/7/19	UNIX, AIX, HP-UX, Solaris, etc.	agent1_3_1_unix.sh
ⓘ	GoAnywhere Agent	Installer	1.3.1	2/7/19	IBM i (AS/400, iSeries)	GAAGENT.SAVF
ⓘ	GoAnywhere Agent	Installer	1.3.1	2/7/19	Linux 32-bit version	agent1_3_1_linux_x86.sh
ⓘ	GoAnywhere Agent	Installer	1.3.1	2/7/19	Linux 64-bit version	agent1_3_1_linux_x64.sh
ⓘ	GoAnywhere Agent	Installer	1.3.1	2/7/19	Microsoft Windows 32-bit version	agent1_3_1_windows_x86.exe
✓	GoAnywhere Agent	Installer	1.3.1	2/7/19	Microsoft Windows 64-bit version	agent1_3_1_windows_x64.exe
ⓘ	GoAnywhere Agent	Upgrader	1.3.1	2/7/19	All	agent_upgrade_1_3_1.jar

Configuring the Agent Installer

The Configure Agent Installer page allows Admin Users to configure a custom Agent Installer to work with their Agents installation. Once configured, the Agent installation software can be exported and deployed on the system that will run the Agent. On export, the Agent installer will include the connection properties used to connect and authenticate to Agents. The installer will also include folder and Project permissions that can be accessed or executed on the Agent system.

1. To configure an Agent installer, log in as an Admin User with the **Product Administrator** role. (missing or bad snippet)
2. From the main menu bar, select **Help** and then click the **Software Library** link.

3. Identify an install package for the Agent's operating system, click the **Actions** icon, and then select the **Configure Installer** icon.
4. Configure the Agent settings and then click the **Generate** button.
5. The custom Agent installer is downloaded to your browser's default location.
6. For instructions to install the Agent, view the *GoAnywhere MFT Agent Install Guide*.

General Tab

Configure Agent Installer [Generate] [Done] ?

Version: 1.3.0
Installer Type: Microsoft Windows 64-bit version

General | Permissions | FIPS 140-2 Compliance | Algorithms | Certificate Validation

Agent Configuration

Name: AG_Datacenter
Registration Code: DataCenter
Shutdown Port: 8015
Maximum Concurrent Jobs: 20
Maximum Concurrent Monitors: 20

GoAnywhere MFT Connection Information

Host: 10.1.2.94
Port: 8009

Allowed Folders

Add Folder...

Alias	Path	Read Only
root	C:\workspace	<input checked="" type="checkbox"/>

* Sub folders will inherit permissions from the defined folder location.

Agent Configuration

Name

The name of the Agent that will appear on the Agent Manager page when the Agent connects. If a name is not specified, a name will be created automatically using the Agent Registration rules on the Agent Configuration Registration page.

Registration Code

Specify an Agent Registration Code this Agent will use to register with GoAnywhere. Registration codes are configured on the Agent Configuration Registration page. If no registration codes are configured on the Agent Service, then this field can be left blank.

Shutdown Port

The TCP/IP port number on which the Agent waits for shutdown commands.

Maximum Concurrent Jobs

Specify the maximum number of concurrent Jobs that can be run at any one time on the Agent. After the threshold is met, any additional jobs are placed in the queue and are processed in the order they were submitted.

Maximum Concurrent Monitors

Specify the maximum number of concurrent Monitors that can be run at any one time on the Agent.

GoAnywhere MFT Connection Information

Host

The host name or IP address of the Agents instance this Agent will connect to.

Port

The port number Agents connect to on the Agents instance.

Allowed Folders

By default, the Agent is provided a default read only folder on the server it is installed on. Click the **Add Folder** button to add additional folder locations that can be used by the Agent. Sub folders will inherit permissions from the defined folder permission.

NOTE:

Folder locations can be added to an Agent after installation by adding them to the permissions.xml file in the Agent's [Installation]\config directory. For more information, see the *GoAnywhere MFT Agent Install Guide*.

Alias

The Alias for the folder location that appears in the Agent file chooser.

Path

The path to the folder location on the Agent system.

Read Only

Indicates if the Agent will have Read Only access to the folder location.

Permissions Tab

Restrict Usage	<input type="checkbox"/>
Allow Amazon S3	<input checked="" type="checkbox"/>
Allow Azure	<input checked="" type="checkbox"/>
Allow Database	<input checked="" type="checkbox"/>
Allow Email	<input checked="" type="checkbox"/>
Allow Excel	<input checked="" type="checkbox"/>
Allow Execute Native Command	<input checked="" type="checkbox"/>
Allow FileCatalyst	<input checked="" type="checkbox"/>
Allow FTP	<input checked="" type="checkbox"/>
Allow FTPS	<input checked="" type="checkbox"/>
Allow GoFast	<input checked="" type="checkbox"/>
Allow Network Share	<input checked="" type="checkbox"/>
Allow PGP	<input checked="" type="checkbox"/>
Allow SSH	<input checked="" type="checkbox"/>
Allow WebDAV	<input checked="" type="checkbox"/>
Allow Web Service	<input checked="" type="checkbox"/>
Allow Zip	<input checked="" type="checkbox"/>

Agents can run Projects on the server where they are installed. All Agent Project permissions will be grouped across the Agent. For example, if FTP is allowed on the Agent, it will be allowed for all aspects of the Agent. However, you can restrict the type of tasks and file system resources that the Agent can utilize.

Restrict Usage

When selected, the types of tasks and file system resources the Agent can utilize are restricted to those selected.

Allow Amazon S3

Allows the Agent to utilize the Amazon S3 Buckets Resource on the server where the Agent is installed.

Allow Azure

Allows the Agent to utilize the Azure Blob Storage Resource on the server where the Agent is installed.

Allow Database

Allows the Agent to run Database tasks on the server where the Agent is installed.

Allow Email

Allows the Agent to run Send and Retrieve Email tasks on the server where the Agent is installed.

Allow Excel

Allows the Agent to run Read and Write Excel tasks on the server where the Agent is installed.

Allow Execute Native Command

Allows the Agent to run Execute Native Command tasks on the server where the Agent is installed.

Allow FileCatalyst

Allows the Agent to run FileCatalyst tasks on the server where the Agent is installed.

Allow FTP

Allows the Agent to run FTP tasks on the server where the Agent is installed.

Allow FTPS

Allows the Agent to run FTPS tasks on the server where the Agent is installed.

Allow GoFast

Allows the Agent to run GoFast tasks on the server where the Agent is installed.

Allow Network Share

Allows the Agent to utilize the Network Shares Resource on the server where the Agent is installed.

Allow PGP

Allows the Agent to run PGP tasks on the server where the Agent is installed.

Allow SSH

Allows the Agent to run SSH tasks on the server where the Agent is installed.

Allow WebDAV

Allows the Agent to utilize the WebDAV Resource on the server where the Agent is installed.

Allow Web Service

Allows the Agent to run Web Service tasks on the server where the Agent is installed.

Allow Zip

Allows the Agent to run File Compression tasks on the server where the Agent is installed.

NOTE:

All other standard tasks are always allowed to run on the Agent.

FIPS 140-2 Compliance Tab

General	Permissions	FIPS 140-2 Compliance	Algorithms	Certificate Validation
<p>When FIPS 140-2 Compliance Mode is enabled, Agents will only use FIPS 140-2 validated algorithms (ciphers) for encrypting transmissions over SSH and SSL channels including SFTP, SCP, FTPS and HTTPS protocols.</p> <p>Enable FIPS 140-2 Compliance Mode <input checked="" type="radio"/> Yes <input type="radio"/> No</p>				

When FIPS 140-2 Compliance Mode is enabled, Agents will only use FIPS 140-2 validated algorithms (ciphers) for encrypting transmissions over SSH and SSL channels including SFTP, SCP, FTPS, and HTTPS protocols.

NOTE:

This FIPS 140-2 Compliance Mode setting applies only to Agents version 1.4.0 and later.

Enable FIPS 140-2 Compliance Mode

FIPS 140-2 Compliance Mode can be enabled or disabled. By default, the FIPS 140-2 Compliance Mode is disabled.

Algorithms Tab

General | Permissions | FIPS 140-2 Compliance | **Algorithms** | Certificate Validation

Specify the SSL/TLS protocol versions and cipher suites to allow globally. Some allowed protocols and cipher suites may forcibly be disabled depending on your JVM and security provider.

Protocols	Disabled	Allowed
		TLSv1.1 TLSv1.2 TLSv1.3

Cipher Suites	Disabled	Allowed
		TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA TLS_DHE_DSS_WITH_AES_128_CBC_SHA TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 TLS_DHE_DSS_WITH_AES_256_CBC_SHA TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

Specify the SSL/TLS protocol versions and cipher suites to allow globally. Some allowed protocols and cipher suites may forcibly be disabled depending on your JVM and security provider. A JVM can disable protocols or cipher suites based on specific algorithms or rules (for example, key lengths). Additionally, your FIPS provider may further disable protocols and cipher suites in FIPS mode.

NOTE:

These algorithm settings apply only to Agents version 1.4.0 and later.

Protocols

Specify the SSL/TLS protocol versions to use. The column on the left displays the disabled protocols. The column on the right displays the allowed protocols. Click to select an option and then use the direction buttons between the columns to move the selection to the appropriate side.

Cipher Suites

Specify the cipher suites to use. The column on the left displays the disabled cipher suites. The column on the right displays the allowed cipher suites. Click to select an option and then use the direction buttons between the columns to move the selection to the appropriate side.

Certificate Validation Tab

The screenshot shows the 'Certificate Validation' tab in a configuration window. It includes tabs for 'General', 'Permissions', 'FIPS 140-2 Compliance', 'Algorithms', and 'Certificate Validation'. The main content area is titled 'Specify checks to enforce when validating server and email certificates.' and contains several sections:

- CA Basic Constraints Validation:** Checkboxes for 'Server Certificates' and 'Email Certificates' are both checked.
- Date Validation:** Checkboxes for 'Server Certificates' and 'Email Certificates' are both checked.
- Extended Key Usage Validation:** Checkboxes for 'Server Certificates' and 'Email Certificates' are both checked.
- Certificate Revocation Lists (CRL):** Checkboxes for 'Server Certificates' and 'Email Certificates' are both checked.
- Refresh Interval:** A spinner box set to '5' with the label 'Minutes'.
- URLs:** A section with an 'Add URL' link and a table with one row containing a red 'x' icon and an empty text input field.
- Implicit Trust:** A text box explaining the setting, followed by radio buttons for 'Allow Implicit Trust' with 'Yes' selected and 'No' unselected.

Specify checks to enforce when validating server and email certificates. When not enforced, a validation check is delegated to the JVM Security Providers. Deselecting a validation check does not necessarily mean the check will never be used.

When the **Server Certificates** check box is selected, validation checks are performed on presented server certificates when Agents connects as a client to another server.

When the **Email Certificates** check box is selected, validation checks are performed on tasks to validate signing and encryption certificates related to processing emails.

NOTE:

These certificate validation settings apply only to Agents version 1.4.0 and later.

CA Basic Constraints Validation

Select check box to verify that the issuer Certificate Authority (CA) certificate is marked as a CA in its basic constraints extension.

Date Validation

Select check box to apply date validity check to server certificates and email signing and encryption certificates.

Extended Key Usage Validation

Select check box to apply extended key usage check to server certificates and email signing and encryption certificates. The check will validate the intended key purpose of the

certificate - server authentication or email protection.

Certificate Revocation Lists (CRL)

Select check box to apply CRL check to server certificates and email signing and encryption certificates.

NOTE:

If a Certificate Revocation List (CRL) is expired and cannot be refreshed, the CRL validation check will reject all certificates until the CRL is removed or an updated CRL can be fetched.

Refresh Interval

If CRLs are enabled, specify how often to refresh all CRLs. **Default Value:** 5 minutes.

URLs

If CRLs are enabled, specify at least one URL in which to retrieve CRLs. To add more than one URL to the table, select the **Add URL** link. Select the **Delete** button to delete a URL, but there must be at least one URL entry if CRLs are enabled.

Implicit Trust

Specify whether or not to allow implicit trust for certain connections that support this configuration. If set to "No", implicit trust will be globally disabled and all connections will be required to validate certificates.

Allow Implicit Trust

Specify whether or not to allow any connections to be configured to use implicit trust (trust all).

Pre-Upgrade Notes

This section describes important upgrade considerations.

2.1.3

Network Shares Monitors

Upgrading to Agents 2.1.3 may fail if you have active monitors that use a Network Share resource **AND** whose event type is **File Created or Modified** or **File Modified**. If the upgrader fails you will be notified that in order to upgrade you need to disable these monitors and re-enable them once you have upgraded. This affects monitors on both Agents and Agent Groups.

2.0.0

The upgrade to version 2.0.0 requires Java 11. You'll need to upgrade to Agents 1.7.0 or later in order to switch to Java 11. To upgrade to Java 11, complete the upgrade instructions in the following sections in this order:

- [Java 11 Considerations](#)
- [Configuring Agents to Run on a Different JVM](#)

Once the Agent is running on Java 11, proceed with upgrading to version 2.0.0.

Upgrading Agents

Agents are upgraded from the Agent Manager in GoAnywhere MFT. The Agent Manager provides tools to automatically apply upgrades to Agents and Agent Groups.

The GoAnywhere MFT Upgrade Agents page provides Admin Users the ability to upgrade Agents to the latest software version. When an upgrade is applied, Agents ensures the Agent is not currently processing any Jobs before the Agent is upgraded. Once the Agent upgrade is finished, the Agent will reconnect to Agents automatically.

1. To apply an Agent Upgrade, log in to GoAnywhere MFT as an Admin User with the **Product Administrator** role. (missing or bad snippet)
2. From the main menu bar, select **Help** and then click the **Software Library** link.
3. Click the **Browse Online Catalog** button to find the latest Agent upgrade package, or import one if you have downloaded an Agent upgrader from the Agents Customer Portal.
4. From the **Software Library** page, identify the upgrade package, click the **Actions** icon, and then select the **Upgrade Agents** icon.
5. The Upgrade Agents page appears. Any outdated Agents will be selected for upgrade. Deselect any Agents that you do not wish to upgrade at this time.
6. Click the **Upgrade** button. The selected Agents will be upgraded once any work on the Agent is completed.

Upgrade Agents		
<input type="button" value="Upgrade"/> <input type="button" value="Cancel"/> ?		
Version	1.3.1	
Release Date	2/7/19	
Release Summary	Added the ability to specify the encoding when writing to a file using the Print Task on Agents.	
Outdated Agents		
<input checked="" type="checkbox"/>	Agent	Current Version
<input checked="" type="checkbox"/>	PROD01	1.1.0

Java 11 Considerations

Java 11 is required to use Agents. However, migrating to Java 11 requires some additional considerations.

Updating Agent startup scripts for Java 11 on Linux and Unix systems

If your Agents are running on a Linux or Unix system, the Agent startup scripts must be updated. Follow the steps below to update the Agent startup scripts.

1. Shut down the Agent.
2. Navigate to the Agent install directory.
3. Modify the 'agent' startup script file. Remove all occurrences of the following text: -
XX:-UseVMInterruptibleIO
4. Save the changes to 'agent'.
5. Navigate to [install directory]/bin.
6. Modify the 'agentd' startup script file. Remove all occurrences of the following text: -
XX:-UseVMInterruptibleIO
7. Save the changes to 'agentd'
8. Start the Agent.

Updating Agent Startup Scripts for Java 11 on IBM i systems

If your Agents are running on an IBM i system, the Agent startup script must be updated. Follow the steps below to update the Agent startup script.

1. Shut down the Agent.
2. Navigate to [install directory]/os400-bin/.
3. Modify the 'start_agent.sh' file.
4. Remove all occurrences of the following text: -XX:-UseVMInterruptibleIO.

5. Save the changes to the 'start_agent.sh' file.
6. Start the Agent.

Updating the Uninstall Script for Linux and Unix

If your Agents are running on a Linux or Unix system running Java 11, the Agent uninstall script must be updated before you can uninstall an Agent. Follow the steps below to update the Agent uninstall script.

1. Shut down the Agent.
2. Navigate to the Agent install directory.
3. Modify the 'uninstall' script file.
4. Remove all occurrences of the following text: `-Djava.ext.dirs="$app_java_home/lib/ext:$app_java_home/jre/lib/ext`.
5. Save the changes to the 'uninstall' file.
6. You may now uninstall Agents running on Java 11.

Agent Configuration

Agents are typically pre-configured through the **Configure Agent Installer** screen in GoAnywhere MFT. After an Agent is installed, the configuration can be updated on the Agent system by modifying the Agent's XML configuration file.

To configure an Agent, open the `agent.xml` file from the `[installdirectory]/config` directory using a text or XML editor.

The following table lists the attributes that can be updated.

Attribute Name	Description
name	The name of the Agent that will appear on the Agent Manager page when the Agent connects. If a name is not specified, a name will be created automatically using the Agent Registration rules on the Agent Configuration Registration page.
host	The host name or IP address of the GoAnywhere MFT instance this Agent will connect to.
port	The port number to use when connecting to the GoAnywhere MFT instance.
shutdownPort	The TCP/IP port number on which the Agent waits for a shutdown commands. The default is 8015.
register	Indicates whether the Agent needs to be registered when it connects to GoAnywhere MFT. Valid values are true or false.
registrationCode	The Agent Registration Code this Agent will use to register with GoAnywhere MFT. If no registration codes are configured on the Agent Service, then this field can be left blank.
maxThreads	The maximum number of threads that the Agent is allowed to use. The default value is 500.

SSL Attributes

The following attributes can be added to the `agent.xml` file in the SSL element to enable and configure SSL to protect the channel between the Agent and GoAnywhere MFT.

Attribute Name	Description
<code>sslContextProtocol</code>	Specify the desired SSL protocol to be used for the connection to GoAnywhere MFT. This setting should match the SSL protocol on the SSL tab in the Agent Configuration. The default value is TLS.
<code>trustStore</code>	The local path to a Key Store that contains the Agent's Private Key. This is created automatically during installation.
<code>trustStorePassword</code>	The password to access certificates stored in the Key Store.
<code>trustStoreProvider</code>	The Service Provider to use for opening this Key Store. When no trust store provider is specified, the default JCE one is used.
<code>trustStoreType</code>	The type of this Key Store. The default is set to JKS.

NOTE:

The Agent must be restarted for any changes to take effect.

Sample agent.xml Configuration

Listed below are the contents of a sample configuration file for an Agent.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<agent host="localhost" maxThreads="100" name="Denver_001"
port="8009" register="false" registrationCode="2017"
shutdownPort="8015">
    <ssl sslContextProtocol="TLS" trustStore="C:\Program
Files\Fortra\GoAnywhere Agent\agentdata\
keys\x509\trustedCertificates.jks"
trustStorePassword="goanywhere" trustStoreProvider=""
trustStoreType="JKS"/>
</agent>
```

Advanced Configuration

To configure an Agent's local address and local port ranges, open the `agent.xml` file located in the `[installdirectory]/config` directory using a text or XML editor.

The following table lists the attributes that can be updated.

Attribute Name	Description
localAddress	The local address to use for outgoing Agent connections to GoAnywhere MFT.
localPortFrom	The inclusive starting range port number to use when restricting local ports for outgoing Agent connections to GoAnywhere MFT. The localPortTo attribute must also be specified to restrict port range. Valid values are from 1023 to 65536.

Attribute Name	Description
localPortTo	The inclusive ending range port number to use when restricting local ports for outgoing Agent connections to GoAnywhere MFT. The localPortFrom attribute must also be specified to restrict port range. Valid values are from 1023 to 65536.
localAddressRequestTimeout	The time to wait in seconds for a local address to become available. This attribute only applies when the localPortTo and localPortFrom attributes are specified. Valid values are from 1 to 240.
socketLinger	A socket option indicating how long after usage of a local socket should it stay in TIME_WAIT status. Typically, sockets are left in a TIME_WAIT status after connections are closed. Valid value is any number greater than -1 (value of 0 indicates it will not wait).
reuseAddress	A socket option that tells the kernel to reuse the port even if the port is busy in the TIME_WAIT status.
gofastMemoryLimit	The amount of memory allocated to GoFast. If not specified, GoFast will use up to 33% of the memory allocated to the Agent.
gofastMemoryLimitUnit	The unit of measurement for the memory allocated to GoFast. Valid values are GB, MB, or KB.

Sample Configuration

The following is a sample advanced configuration `agent.xml` file for an Agent.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<agent localAddress="10.10.1.4" reuseAddress="true"
socketLinger="0" localPortFrom="34000" localPortTo="35410"
shutdownPort="18015" registrationCode="" register="false"
port="10009" name="" maxThreads="500" host="10.10.20.250">
  <ssl trustStoreType="JKS" trustStoreProvider=""
```



```
trustStorePassword="password"
trustStore="C:\Program Files\Fortra\
GoAnywhere Agent\agentdata\
keys\x509\trustedCertificates.jks"
sslContextProtocol="TLSv1.2"/>
</agent>
```

Agent Permissions

To configure an Agent's runtime configuration, folder permissions, and Project Workflow permissions, open the `permissions.xml` file located in the `[installdirectory]/config` directory using a text or XML editor.

The following sections list the attributes that can be updated.

Runtime Configuration

To prevent system resources from being overloaded, you can limit the number of Jobs and Monitors that can be run on an Agent at any given time.

Attribute Name	Description
<code>maxJobRuntime</code>	Specify the maximum number of concurrent Jobs that can be run at any one time on the Agent. After the threshold is met, any additional jobs are placed in the queue and are processed in the order they were submitted.
<code>maxMonitorRuntime</code>	Specify the maximum number of concurrent Monitors that can be run at any one time on the Agent.

Folders

By default, the Agent cannot access any folders on the system where the Agent is installed. Modify or add folder locations that can be used by the Agent.

Attribute Name	Description
alias	The name of the folder that will appear in GoAnywhere MFT's Project File Chooser.
path	The local path to the folder.
readOnly	Set whether the Agent can write to the designated folder or read only. Valid values are true or false.

Sample Folder Attributes

Listed below are the contents of a sample folder configuration.

```
<folders>  
    <folder alias="temp" path="c:\temp" readOnly="false" />  
</folders>
```

Task Permissions

Agents can run Projects on the server where they are installed. You can restrict the type of Tasks that the Agent can execute.

Attribute Name	Description
restrictTasks	If set to "true", the types of Tasks the Agent can execute are restricted to the selected Task types that follow. Valid values are true or false.
allowDatabaseTasks	Allows the Agent to run Database tasks on the server where the Agent is installed. Valid values are true or false.
allowEmailTasks	Allows the Agent to run Email tasks on the server where the Agent is installed. Valid values are true or false.
allowExcelTasks	Allows the Agent to run Excel tasks on the server where the Agent is installed. Valid values are true or false.

Attribute Name	Description
allowExecNativeTasks	Allows the Agent to run Execute Native Command tasks on the server where the Agent is installed. Valid values are true or false.
allowFileCatalystTasks	Allows the Agent to run FileCatalyst tasks on the server where the Agent is installed. Valid values are true or false.
allowFTPTasks	Allows the Agent to run FTP tasks on the server where the Agent is installed. Valid values are true or false.
allowFTPSTasks	Allows the Agent to run FTPS tasks on the server where the Agent is installed. Valid values are true or false.
allowGoFastTasks	Allows the Agent to run GoFast tasks on the server where the Agent is installed. Valid values are true or false.
allowPGPTasks	Allows the Agent to run PGP tasks on the server where the Agent is installed. Valid values are true or false.
allowSSTasks	Allows the Agent to run SSH tasks on the server where the Agent is installed. Valid values are true or false.
allowWebServiceTasks	Allows the Agent to run Web Service tasks on the server where the Agent is installed. Valid values are true or false.
allowZipTasks	Allows the Agent to run File Compression tasks on the server where the Agent is installed. Valid values are true or false.

File System Resource Permissions

File System Resource Permission allow Agents to access file system resources using file syntax notation. You can restrict the File System Resources that the Agent has access to.

EXAMPLE:

The syntax for referencing an Amazon S3 share is: `resource:s3://[ResourceName]/[FilePath]`, where [ResourceName] is the name of the Amazon S3 share Resource.

Attribute Name	Description
allowAmazonS3FileSyntax	Allows the Agent to utilize the Amazon S3 Buckets Resource on the server where the Agent is installed.
allowAzureFileSyntax	Allows the Agent to utilize the Azure Blob Storage Resource on the server where the Agent is installed.
allowNetworkShareFileSyntax	Allows the Agent to utilize the Network Shares Resource on the server where the Agent is installed.
allowWebDAVFileSyntax	Allows the Agent to utilize the WebDAV Resource on the server where the Agent is installed.

Sample permissions.xml Configuration

Listed below are the contents of a sample permissions file for an Agent.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<permissions>
  <folders>
    <folder alias="temp" path="c:\temp" readOnly="false"/>
  </folders>
  <maxJobRuntime>20</maxJobRuntime>
  <maxMonitorRuntime>20</maxMonitorRuntime>
  <restrictTasks>true</restrictTasks>
  <allowDatabaseTasks>true</allowDatabaseTasks>
  <allowEmailTasks>true</allowEmailTasks>
  <allowExecNativeTasks>true</allowExecNativeTasks>
  <allowFileCatalystTasks>true</allowFileCatalystTasks>
  <allowExcelTasks>false</allowExcelTasks>
  <allowFTPTasks>false</allowFTPTasks>
  <allowFTPSTasks>false</allowFTPSTasks>
  <allowGoFastTasks>false</allowGoFastTasks>
  <allowPGPTasks>false</allowPGPTasks>
  <allowSSHTasks>false</allowSSHTasks>
  <allowWebServiceTasks>false</allowWebServiceTasks>
```

```
<allowZipTasks>false</allowZipTasks>
<allowAmazonS3FileSyntax>false</allowAmazonS3FileSyntax>
<allowAzureFileSyntax>false</allowAzureFileSyntax>
<allowNetworkShareFileSyntax>true</allowNetworkShareFileSyntax>
<allowWebDAVFileSyntax>true</allowWebDAVFileSyntax>
</permissions>
```

Agent Security Settings

To configure an Agent's security settings, open the `security.xml` located in the `[installdirectory]/config` directory using a text or XML editor.

The following table lists the key attributes that can be updated.

Key Attribute	Description	Value
fips.enabled	When FIPS 140-2 Compliance Mode is enabled, GoAnywhere MFT will only use FIPS 140-2 validated algorithms (ciphers) for encrypting transmissions over SSH and SSL channels including SFTP, SCP, FTPS, and HTTPS protocols.	Boolean: true or false

Key Attribute	Description	Value
tls.disabledCipherSuites	The SSL/TLS cipher suites to disable globally. Some cipher suites may forcibly be disabled depending on your JVM and security provider.	A comma separated list of cipher suite names.
tls.disabledProtocols	The SSL/TLS protocol versions to disable globally. Some protocols may forcibly be disabled depending on your JVM and security provider.	A comma separated list of SSL/TLS protocol names.
x509.implicitTrust.allowAll	Whether implicit trust is allowed for certain connections that support this configuration. If implicit trust is not allowed, implicit trust will be globally disabled and all connections will be required to validate certificates.	Boolean: true or false

Key Attribute	Description	Value
x509.server.basicConstraintChecking.enabled	Verifies the Certificate Authority (CA) is marked as a CA with a valid path length in its basic constraints.	Boolean: true or false
x509.email.basicConstraintChecking.enabled	Verifies the Certificate Authority (CA) is marked as a CA with a valid path length in its basic constraints.	Boolean: true or false
x509.server.dateValidityChecking.enabled	Applies date validity check to server certificates.	Boolean: true or false
x509.email.dateValidityChecking.enabled	Applies date validity check to email certificates.	Boolean: true or false
x509.server.extendedKeyUsageChecking.enabled	Applies extended key usage check to server certificates. The check will validate the intended purpose of the certificate - server authentication.	Boolean: true or false

Key Attribute	Description	Value
x509.email.extendedKeyUsageChecking.enabled	Applies extended key usage check to email certificates. The check will validate the intended purpose of the certificate - email protection.	Boolean: true or false
x509.server.crlChecking.enabled	Applies CRL check to server certificates.	Boolean: true or false
x509.email.crlChecking.enabled	Applies CRL check to email certificates.	Boolean: true or false
x509.crlChecking.refreshInterval	How often to refresh all CRLs if CRLs are enabled.	Number
x509.crlChecking.urls	The URLs to use for CRL checking.	A pipe ' ' separated list of URLs.

Sample Configuration

The following is a sample advanced configuration `security.xml` file for an Agent.

```
<?xml.version="1.0" encoding="UTF-9" standalone="no"?>
<!DOCTYPE properties SYSTEM
"http://java.sun.com/dtd/properties.dtd">
<properties>
  <entry key="fips.enabled">false</entry>
  <entry key="tls.disabledCipherSuites"/>
  <entry key="tls.disabledProtocols"/>
</properties>
```



```
<entry key="x509.implicitTrust.allowAll">true
</entry>
<entry key="x509.server.basicConstraintChecking.enabled">false
</entry>
<entry key="x509.email.basicConstraintChecking.enabled">false
</entry>
<entry key="x509.server.dateValidityChecking.enabled">false
</entry>
<entry key="x509.email.dateValidityChecking.enabled">false
</entry>
<entry
key="x509.server.extendedKeyUsageChecking.enabled">false
</entry>
<entry key="x509.email.extendedKeyUsageChecking.enabled">false
</entry>
<entry key="x509.server.crlChecking.enabled">false</entry>
<entry key="x509.email.crlChecking.enabled">false</entry>
<entry key="x509.crlChecking.refreshInterval">5</entry>
<entry key="x509.crlChecking.urls"/>
</properties>
```

Product Administration

Starting and Stopping Agents

Windows Instructions

Start the Agent by following these instructions:

1. Go to the Windows machine and logon with an administrator account.
2. Go to **Control Panel > Administrative tools > Services**.
3. In the **Services** window, right-click on GoAnywhereAgent and select **Start**. Within seconds after starting GoAnywhereAgent, its status should be updated to "Started".

Stop the Agent by following these instructions:

1. Go to the Windows machine and logon with an administrator account.
2. Go to **Control Panel > Administrative tools > Services**.
3. In the **Services** window, right-click on the GoAnywhereAgent and select **Stop**.

Linux and Unix Instructions

Start the Agent by following these instructions:

1. Open a Terminal window.
2. Change the working directory to the directory where the Agent is installed (for example, `cd /usr/local/Fortra/GoAnywhere_Agent/bin`)
3. Start the Agent by executing the following shell script:
`./agentd start`

Stop the Agent by following these instructions:

1. Open a Terminal window.
2. Change the working directory to the directory where GoAnywhere is installed
(for example, `cd /usr/local/Fortra/GoAnywhere_Agent/bin`)
3. Stop the Agent by executing the following shell script:
`./agentd stop`

IBM i (iSeries) Instructions

Start the Agent by following these instructions:

1. Open a Terminal window.
2. Start the Agent by executing the IBM i command of **GAAGENT/STRGAAGENT**.

Stop the Agent by following these instructions:

1. Open a Terminal window.
2. Stop the Agent by executing the IBM i command of **GAAGENT/ENDGAAGENT**.

Mac OS X Instructions

Start the Agent by following these instructions:

1. Open a Terminal window.
2. Change the working directory to the directory where the Agent is installed
(for example, `cd /Applications/Fortra/GoAnywhere Agent/bin`)
3. Start the Agent by executing the following shell script:
`./agent.sh start`

Stop the Agent by following these instructions:

1. Open a Terminal window.
2. Change the working directory to the directory where the Agent is installed
(for example, `cd /Applications/Fortra/GoAnywhere Agent/bin`)

3. Stop the Agent by executing the following shell script:

```
./agentd stop
```

Agent Logs

Agents maintain logs that record the Agent's activity. The log files record a timestamp and description of each action performed. A new log file is created each time the current log file reaches the maximum size defined in the log configuration. The log is stored in the Agent's `[Install Directory]\agentdata\logs` directory.

Change Log Level

If you encounter a problem with an Agent, a Fortra Support Specialist may ask you to provide them a Debug Log to troubleshoot the issue.

1. Navigate to the `[Install Directory]\config` folder (where `[InstallFolder]` is the installation location for Agents).
2. Open the `log4j.xml` file using an XML editor or Notepad.
3. Toward the bottom of the file, change the value for `<level value="INFO">` to `<level value="DEBUG">`.
4. Save the changes to the log configuration and close the editor.
5. Restart the Agent for the new changes to take effect.

Disaster Recovery

If an Agent loses connection to GoAnywhere MFT, it will continually attempt to reestablish a connection until GoAnywhere MFT becomes available on the IP address and port the Agent is attempting to connect to. If GoAnywhere Gateway is being used as a load balancer for a GoAnywhere MFT cluster, Gateway will direct the Agent connection to the next available system in the cluster. For more information on GoAnywhere Gateway, disaster recovery, automatic failover, and clustering, see the *GoAnywhere MFT Installation Guide*.

Configuring an Agent to Run On a Different JVM

Upgrading the External JRE

Follow your Java vendor's instructions to upgrade your external JRE. Once the JRE is upgraded to Java 11, ensure the Java execution environment is correct.

The latest supported version of Java is bundled in the installer for Windows and Linux. If you need to manually configure an Agent to run on a newer version of Java, follow the steps below.

1. Shutdown the Agent.
2. Navigate to [install directory]/.install4j/.
3. Edit the file 'pref_jre.cfg'.
4. Modify the path within 'pref_jre.cfg' to point to the desired Java version.

Upgrading the Embedded JRE (Windows)

Use the following instructions to upgrade the embeded Java version to 11 on Windows installations:

1. Download the appropriate [Java 11 version](#).
2. Shut down Agents.
3. Navigate to the installation directory. By default, this is C:\Program Files\Fortra\GoAnywhere Agent.
4. Rename the old 'jre' folder to 'jre.old'.
5. Create a new 'jre' folder in the installation directory and copy the downloaded JRE bundle into that directory.
6. Extract the contents of the JRE bundle into the current directory.

Upgrading the Embedded JRE (Linux)

Use the following instructions to upgrade the embeded Java version to 11 on Linux installations:

1. Download the appropriate [Java 11 version](#).
2. Log in as the user account that owns the Agents installation directory and its contents.
3. This is typically the same user account used to start and stop Agents.
4. Shut down Agents.
5. Navigate to the installation directory. For example, /usr/local/Fortra/GoAnywhere_Agent.
6. Rename the old 'jre' folder to 'jre.old'
7. Create a new 'jre' folder in the installation directory and copy the downloaded JRE bundle into that directory.
8. Extract the contents of the JRE bundle into the current directory.

- `$ gunzip linux-x86-11.tar.gz`
- `$ tar -xvf linux-x86-11.tar`

Uninstalling Agents

This section describes how to uninstall the Agents product.

Windows uninstall instructions

Perform the following steps to uninstall the Agents product from Windows:

Step	Description
1	Browse to the installation directory of Agents. The default install directory is C:\Program Files\Fortra\GoAnywhere Agent .

Step	Description
2	Run the file named uninstall.exe to uninstall the product.

Linux and Unix uninstall instructions

Perform the following steps to uninstall the Agents product from Linux:

Step	Description
1	Login to the Linux system as root and open a Terminal window.
2	Change the working directory to the directory where the Agent was installed (for example, cd /usr/local/Fortra/GoAnywhere_Agent).
3	Stop the Agents by executing the following shell script: ./agentd.sh stop
4	Uninstall the Agents product by executing the following shell script: ./uninstall.sh

IBM i uninstall instructions

Perform the following steps to uninstall the Agents product from the IBM i:

Step	Description	Example Commands
1	End the Agent service.	- GAAGENT/ENDGAAGENT
2	Verify that there are no locks on the Agent library. Default library name is GAAGENT.	- WRKOBJLCK OBJ(GAAGENT) OBJTYPE(*LIB)
3	Delete the Agent library. Default library name is GAAGENT.	- DLTLIB LIB(GAAGENT)

Step	Description	Example Commands
4	Delete the Agent folder from the IFS. The default main folder name is /fortra/gaagent.	- RMVLNK OBJLNK ('/fortra/gaagent/*.*') - RMVDIR DIR('/fortra/gaagent')

Mac OS X uninstall instructions

Perform the following steps to uninstall the Agents product from Mac OSX:

Step	Description
1	Login to the Mac OS X system as an administrator and open a Terminal window.
2	Change the working directory to the directory where the Agent was installed (for example, <code>cd /Applications/Fortra/GoAnywhere_Agent</code>).
3	Stop the Agents by executing the following shell script: <code>./agentd.sh stop</code>
4	Uninstall the Agent product by double clicking the Agent Uninstaller found in the /Applications/Fortra/GoAnywhere_Agent directory and follow the prompts on the screen.

Using FTP and FTPS in Passive Mode

As of Agents 2.1.3, using FTP or FTPS in passive mode will cause a connection failure.

As a security best practice, the address provided in the passive reply will no longer be trusted by default. To trust the addresses in a passive reply, set

org.apache.commons.net.ftp.addressFromPasvResponse=true in the Agent system properties file `[installdirectory]/config/system.properties`. This requires a restart of the Agent.