Networking and Security

Default Ports

Below are the default ports that are created when you install Continua. These values can be changed by modifying the specified configuration files. Note that it is highly recommended that you backup the configuration file before any changes are made.

The server and agent configuration files can be located in the following locations:

- **Server Configuration file**: <install_dir>/VSoft Technologies/ContinuaCI/Server/Continua.Server.Service.exe.config
- **Agent Configuration file**: <install_dir>/VSoft Technologies/ContinuaCI Agent/Continua.Agent.Service.exe.config

	Incoming	Outgoing	Used for	Set in	Value to Change
Server	9000	9002	Communication with agents	<server_install_dir>\Server\Continua.Server.Service.exe.config	<endpoints **port="9000"** serverHostName="localhost" **serverPort="9000"** serverSSHPort="9010"/>
Server	80		Web UI	IIS configuration	
Server*	9010		SSH/SFTP communication with agents	<server_install_dir>\Server\Continua.Server.Service.exe.config	<endpoints port="9000" serverHostName="localhost" serverPort="9000" **serverSSHPort="9010"**/>
Agent	9002	9000	Communication with server	<agent_install_dir>\Server\Continua.Agent.Service.exe.config	<endpoints **port="9002"** serverHostName="localhost" **serverPort="9000"**/>
Agent*		9010	SSH/SFTP with server	<agent_install_dir>\Server\Continua.Agent.Service.exe.config	<endpoints port="9002" serverHostName="localhost" serverPort="9000" **serverSSHPort="9010"**/>

*SSH access is optional, however agents must be able to access files on the server via either SSH or a UNC share. See below for more info.

Note that if you change the server port or the server ssh port then the server ports on all of the agents must then point to the new port.

Services

The Server and Agent both run under the Windows user that was specified during the installers. Continua does not use the Local System user an many external tools (Version Control Systems, build tools, etc.) must be run in a user context.

Shares and SSH

Files can be transported between the agent and server via a UNC share or via SSH.

A UNC share is preferred if the server and all the agents are on the same domain as this will perform significantly faster than SSH. The server must have a data share which is responsible for storing all repository and build information that is required to run and access builds successfully. Check out our Server Data Share page for more information.

Each agent must be run under a Windows user that has access to both the agent workspace and the server data share. Each agent only accesses its own workspace and the server data share. The agent does not need its own share nor should any agents access other agent workspaces.

Continua CI also ships with an embedded SSH server for communication between the Server and Agent, which means that access to the share can be locked down. This is useful if you are working in a more secure network or if your agents are not on the same domain as your sever.

HTTPS

It is possible to enable HTTPS in IIS for use with Continua CI. Please see this IIS Config guide for more details: http://learn.iis.net/page.aspx/144/how-to-set-up-ssl-on-iis/#IISManager