

Agent and Controller Compatibility

This page provides an overview of compatibility mapping between Agent and Controller versions.

About Agent and Controller Compatibility

Please refer to the [Language Agent Backward Compatibility](#) table below for AppDynamics Agents and AppDynamics Controller compatibility.

A monitored environment may have agents of different versions deployed in it at a given time, as long as all agents are compatible with the Controller version. However, the oldest agents should be on originating tiers of any business transactions. This ensures that agents on downstream nodes can process the correlation header created by the originating tier.

It's an important point to consider when rolling out agent upgrades—be sure to start upgrading the agents on the nodes of downstream tiers first and then upgrade the agents on the originating tier nodes last.

Language Agent Backward Compatibility

Starting in release 4.5, AppDynamics language agents are backward-compatible with any 4.4.1 or later Controller. This enables you to upgrade your language agents – and take advantage of the latest agent-side enhancements, features, and bug fixes – without upgrading your 4.4 Controller. The following table outlines the Controller and language agent releases that are compatible.

Starting in 20.2, the AppDynamics language agents are backward-compatible with any 4.5.0 or later Controller, including Controllers using [Calendar Versioning](#) from 20.3 and higher.

Controller Release	Language Agent Release	Notes
20.3 or higher	4.4 or higher, 20.2 or higher, 20.3 or higher	20.3 or higher Controllers can accept connections from 4.4 or higher agents as well as 20.2 or higher and 20.3 or higher agents that use Calendar Versioning. As of 20.3, Controllers cannot accept connections from 4.1 agents.
4.5.x	4.1 or higher, 20.2 or higher, 20.3 or higher	4.5.x Controller can accept connections from 4.1 or higher agents, including agents that use Calendar Versioning .
4.4.1 or higher	4.1 or higher	4.4.1 and newer Controllers can accept connections from newer agents.
4.3.x	4.1.x – 4.3.x	4.3.x Controllers cannot accept connections from newer agents.



The above table is only a reference for general software compatibility. For specific maintenance and support terms, please refer to your specific EULA.

Backward compatibility is supported on the following agents starting in Release 4.5:

- C/C++
- Cluster
- Go SDK
- Java
- Machine
- .NET
- Node.js
- PHP
- Python



While using the Enterprise Console to upgrade the Controller, several folders (including the `appagent` folder) are removed and reinstalled. If you deployed a Java agent with a newer version than the Controller in the `controller/appserver/glassfish/domains/domain1/appagent` folder, the upgrade will fail and internal monitoring will be lost. To prevent this, you must [update the `domain.xml` file](#) to point to the new Java agent or avoid using customized installation for Java agents.

For notes on SSL protocol compatibility between versions of the agent and Controller, see [SSL Compatibility Matrix for App Agent for Java - Controller](#).

Agent Versions Supported by Controller Version 20.x

Agent Version/ Agent Type	Languages Agents							Cluster Agent	Database Agent	AppDynamics for Databases	Machine Agent	Network Agent
	Java Agent	.NET Agent	Node.js Agent	PHP Agent	Python Agent	Web Server Agent	C / C++ Agent (SDK)					
20.x or higher	✓	✓	✓	✓	✓			✓	✓		✓	✓
4.5.x	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
4.4.x	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓

i The ability to customize Business Transaction detection, supported by .NET Agent for Linux version 4.5.9, requires Controller versions 4.5.2 and higher. The .NET Agent version 4.5.9 works with Controller version 4.4.1 and higher, but the customizable transaction detection and configuration capabilities require 4.5.2 and later versions of the Controller. See [.NET Agent for Linux Business Transaction Configuration](#).

SSL Compatibility between Java Agent and Controller

The default protocol used by the Controller is TLSv1.2. See [Secure the Platform](#) for information on changing the default security protocol used by the Controller or agent.

For the Java Agent, the default protocols are:

- For Java 8 SE applications: TLSv1.2.
- For Java 7 or higher applications: TLSv1.2.

i SSLv3 has been disabled for SaaS Controllers because of the [CVE-2014-3566 vulnerability](#). SSLv3 connections are no longer supported.

Introduction of New Agent Features

Even when new and old agents are supported by the same up-to-date Controller, new functionality introduced by later agents is not available on the older agents.

Information about when an agent feature was introduced is documented in the *New and Enhanced Features* section for a new major release (such as 4.5) and *<minor_release_number> Updates* sections for minor releases in the [Release Notes](#).