Cloud On-Premise: Overview of what gets installed, procedures performed (Express installation type)

Scott Leonard - 2022-08-17 - in FAQs

The Cloud On-Premise system (AssetCloud or InventoryCloud) installs a number of components, and requires a certain order of pre- and post-installation tasks. A summary and explanations follow. Links to the mentioned articles are at the bottom of this article in the Related Pages section.

==========

Installation steps:

Log into system as local administrator (not a domain administrator)
Perform article: Cloud On-Premise installation: IIS Settings Prerequisites

Perform article: Cloud On-Premise installation: PowerShell permission configuration
Run the CloudOP's setup.exe as administrator. Choose the Allow or Run option if prompted. Reboot the system when prompted.
Perform article: Cloud On-Premise: IIS Settings to improve performance
Windows Firewall: Add Inbound rule to allow TCP port 8702 (AssetCloud) or 8703 (InventoryCloud)

We recommend keeping the extracted installation files intact on the server in case they're needed during the course of support later.

==========

The Welcome page displayed at the end of a successful installation shows the web server address users will browse, as well as the initial administrator user credentials, which are:
username: admin
password: `Wa5p(Cl0ud)Adm1n`
The password contains 16 characters and includes the numbers 5, 0, and 1. The username and password can be changed through the Cloud system's user interface (Manage, Users).

Adding new users: See article "Cloud On-Premise: Adding additional users"

Either:

1. Follow the article to add new users without SMTP, or

2. SMTP settings must be entered, validated, and saved. Upper right, gear icon, Settings, Email. If you do not have your own SMTP server, you can use a Gmail account (Google mail). The following article has steps and tips for getting that to work with the CloudOP system:
"Alternative email server to use if email alerts are not passing through your server"

When inviting additional users to the system, the user will receive an email with links that must be clicked from a system which is on the same network as your server in order to accept the invitation.

After installation, the Cloud product must be registered within 45 days. When logged in, click the link at upper right "Ready to Activate? Click here". Call the phone number specified and give the Machine Key from the screen to the Sales Agent, who will provide the Activation Key, which must be entered exactly into the activation screen. In the future, if a license for additional users or support contract is purchased, this can be entered by clicking the Help icon (question mark), then About.

Wasp Configuration Tool: Utility for advanced users and Tech Support to access configuration settings. We highly recommend you do not change anything here (except for

steps from knowledgebase articles, and advice from Tech Support). Always run the Config Tool as Administrator. Path to executable:
C:\Program Files\Wasp Barcode Technologies\Wasp On-Premises Software\License\configure\Wasp.Installer.Configure.exe

==========

There are a number of components that are installed for the Cloud system:

Services:

RabbitMQ: Open-source message-broker software. Receives messages from, and sends messages to, the various components of the Cloud system. Schedules notifications and reports. This service is robust and should always be running.
description: https://en.wikipedia.org/wiki/RabbitMQ
webpage: https://www.rabbitmq.com/
Erlang is a programming language and runtime system used by RabbitMQ.
webpage: http://erlang.org
Redis (Remote Dictionary Server): Open-source in-memory database, which does many things, e.g. store user sessions for load-balancing. This service is robust and should always be running.
description: https://en.wikipedia.org/wiki/Redis
webpage: https://www.redislabs.com/Redis
WASP Later Service: This Service schedules Reports and notifications for the future. This service is robust and should always be running.
Wasp Now Service: Wasp Report Rendering and Notification Worker Service. This service stops and restarts itself; this is expected behavior.
SQL Server Management Studio v18.2

SQL Server (WASPDATA): Microsoft SQL 2017 Express instance containing three databases:
WaspAuth: users/passwords
WaspConfig: licensing, other metadata
WaspTrack: main production database

We create and use several SQL user accounts for the Cloud system:

dbo_Writer: read/write account which edits the WaspTrack database.
password: `db0-Wr1ter_P455w0rd`

dbo_Reader: read-only account for accessing the WaspTrack database, for reporting and other purposes when there should be no need to alter data.
password: `db0_Re4der-P455w0rd`

sa: SQL Administrator account. Wasp is not disclosing the password, but the following article can be followed to change to a different password (this is optional):

Cloud On-Premise: How to change sa password (Express installation type)

We give the (SQL) Server Role of sysadmin to the logged-in Windows user and the local machine's Administrators group. This allows someone to do Run As Administrator on SQL Server Management Studio and Wasp Configuration Tool, then use Windows Authentication to get in.

==========

IIS Sites:

WaspMVC
WaspSTS
WaspAPI

IIS Application Pools:

WaspPMVC
WaspPSTS
WaspPAPI

If you need to stop/start multiple IIS sites as a troubleshooting step, first stop them all, then start them in this order: WaspSTS, WaspAPI, then WaspMVC. The application pools can be recycled in any order.

==========

TCP Port list:

6379: Redis
8080: STS Service
8081: API Service
8082: AssetCloud
8703: InventoryCloud
5672: RabbitMQ (secondary)
15672: RabbitMQ (primary)
25672: RabbitMQ (secondary)

Ports for these services must be available on the server before you install:
6379: Redis
5672: RabbitMQ (secondary)
15672: RabbitMQ (primary)
25672: RabbitMQ (secondary)

Ports for these services can be configured during or after the installation:
8700: STS Service

8701: API Service
8702: AssetCloud
8703: InventoryCloud

Important! Of all the above ports, the only ports that should be open to the public are these ports:
8702: AssetCloud
8703: InventoryCloud

All the other Ports are for internal communication only and need no cloud exposure thru the firewall or gateway.

The other ports need only be available on the server or in case of multiple servers, within the server farm.

==========

Antivirus/Protection software exclusions: Sometimes these can interfere with the Cloud system or pop up messages (e.g. AVG does this). These folders can be set as exclusions in the software:

C:\Program Files\erl10.2
C:\Program Files\Microsoft SQL Server
C:\Program Files\RabbitMQ
C:\Program Files\Redis-3.0.504-64bit
C:\Program Files\Wasp Barcode Technologies
C:\ProgramData\Wasp Barcode Technologies
C:\inetpub\wwwroot\WaspAPI
C:\inetpub\wwwroot\Wasp_AC
C:\inetpub\wwwroot\Wasp_IC
C:\inetpub\wwwroot\WaspSTS

Related Pages

- Cloud On-Premise: Adding additional users
- Cloud On-Premise: How to change sa password (Express installation type)
- Cloud On-Premise installation: IIS Settings Prerequisites
- Cloud On-Premise: IIS Settings to improve performance
- Cloud On-Premise installation: Summary & Prerequisites
- Alternative email server to use if email alerts are not passing through your server