

activAeon Limited

# activAeon XA Technical Whitepaper



activAeon Limited  
Greenesfield Business Centre, Mulgrave Terrace,  
Gateshead, NE8 1PQ  
Tel: +44 (0)845 459 9207 Fax: +44 (0)845 459 9204  
Co. No. 05119485

[www.activaeon.com](http://www.activaeon.com)

# Contents

Introduction .....	3
Architectural Overview .....	3
System Components .....	3
activAeon XA Management Server (AMS) .....	3
activAeon XA Database .....	3
activAeon XA Managed Server Agent (MSA) .....	3
activAeon XA Remote Services Proxy (RSP) .....	3
activAeon XA Control Service (ACS) .....	3
activAeon XA Product Database (PDB) .....	3
activAeon XA Rules Engine.....	3
activAeon XA Management Console.....	4
activAeon XA Component Overview .....	4
Data Collection.....	4
Remote Services Proxy.....	4
Device information .....	5
User information.....	5
Other Information.....	5
Data Storage.....	5
Managed Server Agent .....	5
Device Information .....	5
User Information.....	5
Data Storage.....	5
Data Communication .....	6
CMS Initiated Communication .....	6
MSA Initiated Communication.....	6
activAeon Secure Communications Protocol.....	6
Firewall Issues .....	6

## Introduction

This white paper describes the collection, communication and storage of data within activAeon XA. It describes what data is collected, where it is cached, and how it is transmitted to and stored in the central database in a secure and reliable manner. It describes issues that may affect the transmission of the data, and what can be done to resolve those issues.

## Architectural Overview

### System Components

#### **activAeon XA Management Server (AMS)**

The AMS enables administrators to deploy and control activAeon XA agents across their enterprise using the activAeon XA management console. The AMS contains the Central Management Service (CMS); a Windows service that acts as a receiver for licensing data from the activAeon XA agents and as a link to the activAeon XA database.

#### **activAeon XA Database**

The activAeon XA database is a Microsoft SQL Server database that stores the system configuration data and all license information received from the activAeon agents.

#### **activAeon XA Managed Server Agent (MSA)**

The MSA is a Windows service that is deployed to devices across an enterprise to monitor license utilisation. This license information is passed to the AMS along with device-specific information, such as function, operating system and processor count.

#### **activAeon XA Remote Services Proxy (RSP)**

The RSP is a Windows service that is deployed to a device within a domain to interface with Active Directory.

#### **activAeon XA Control Service (ACS)**

The ACS is a Windows service that is deployed to devices alongside the RSP and MSA to control communication with the AMS.

#### **activAeon XA Product Database (PDB)**

The PDB is a binary encrypted file that is deployed to devices alongside the MSA to carry out a software product inventory check.

#### **activAeon XA Rules Engine**

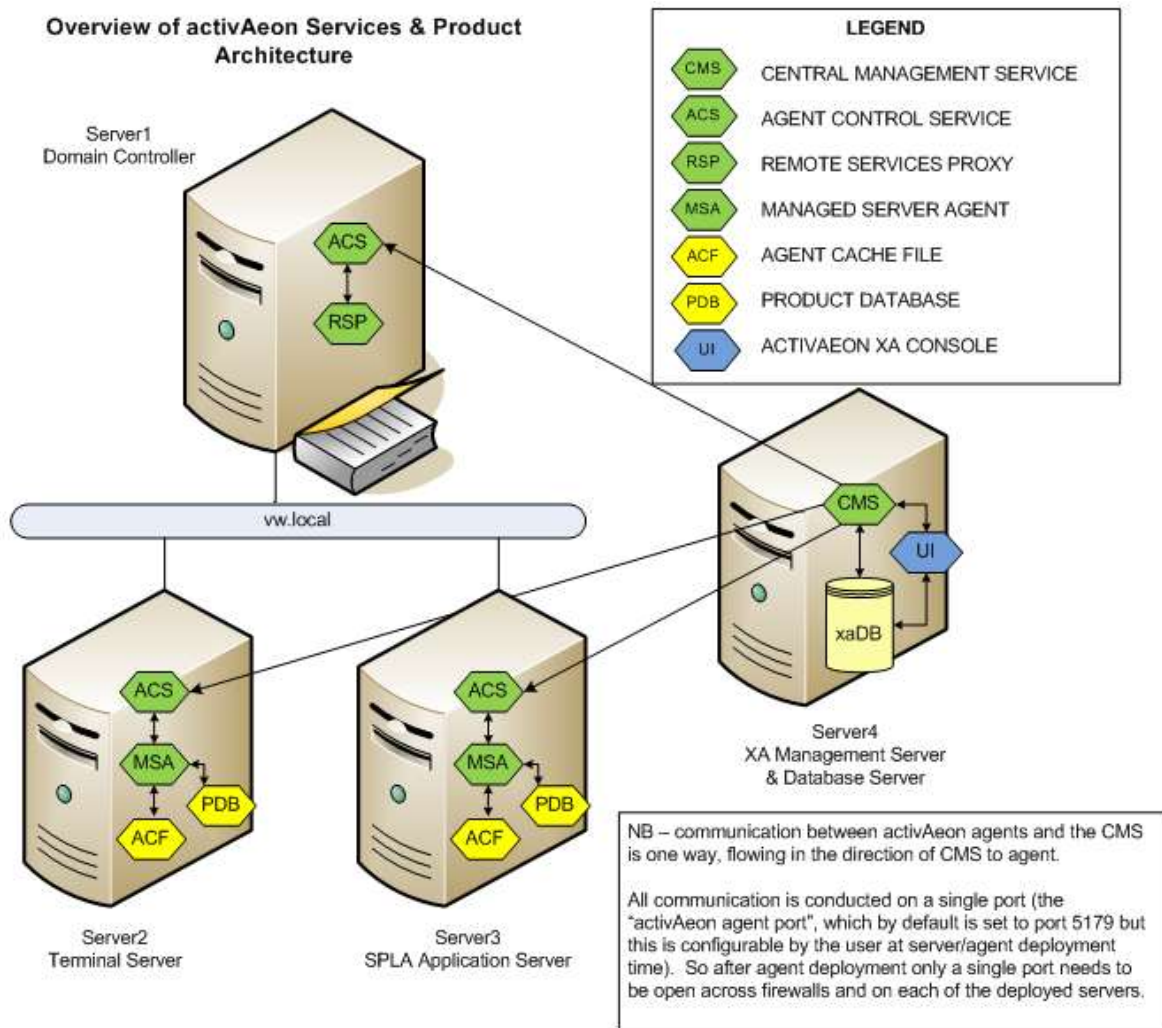
The activAeon XA rules engine is the core mechanism for retrieving and manipulating license utilisation information within the database to facilitate accurate reporting in accordance with the Microsoft Service Provide Use Rights (SPUR).

## activAeon XA Management Console

The activAeon XA management console allows administrators to manage and control the operation of activAeon XA. It is primarily used to deploy, configure and manage activAeon XA agents and to access the reporting functionality of activAeon XA.

## activAeon XA Component Overview

The following diagram shows the main components that comprise activAeon.



## Data Collection

Data is collected by two components: the Remote Services Proxy (RSP), and the Managed Server Agent (MSA).

### Remote Services Proxy

The RSP collects information from Active Directory (AD). It collects information about the devices in AD, and information about users that must be covered in some way by a SPLA licence (for example, a Windows operating system licence or a Terminal Server licence).

## Device information

- NetBios name
- Fully qualified domain name
- IP address (if operating in a static IP address environment)
- Device role (e.g. domain controller, terminal server)
- Device's organisational unit (if it is contained in one)

## User information

- User name (common name, UPN, SAM)
- Email address
- Existence of mailbox
- User's organisational unit (if it is contained in one)

## Other Information

- List of security groups
- Organisational unit structure

This information is used to associate SPLA licenses with specific users in security groups or organisational units.

## Data Storage

The RSP does not store any data locally.

## Managed Server Agent

The MSA collects license and usage information, and stores it locally until the data is requested by the CMS.

## Device Information

The MSA collects:

- Operating system information
- Processor information
- SPLA product information

## User Information

The MSA collects user information for users that:

- Authenticate on the device
- Conduct a terminal server session on the device
- Run a monitored application on the device

Depending on the nature of the user interaction with the device, the MSA stores the SAM name of the user (e.g. domain\username) or the UPN for the user (e.g. [username@domain.local](#)).

## Data Storage

All data collected by the MSA is stored in a local file cache until the CMS requests the data. The MSA removes the data from the cache only when the CMS confirms that it has committed the data to the database.

## Data Communication

### CMS Initiated Communication

The CMS initiates communications to the RSP (to collect AD-related information) and to the MSA (to collect device information).

The CMS initiates communication to the RSP on a daily basis, to ensure the local copy of Active Directory information is current, and that any changes in that data are recorded.

The CMS initiates communication to the MSA at a frequency defined on a per-device basis. The default frequency is every five minutes. The CMS also initiates communication to the MSA on a daily basis, to collect additional product specific licence information.

The CMS initiates communication to the RSP and MSA using TCP/IP, on a port defined on a per-device basis. The default port is 5179. This is the only port that must be open for activAeon to collect licensing data reliably.

### MSA Initiated Communication

The MSA initiates communication to the RSP to request the resolution of user names in Active Directory. It does this in response to the CMS request that the MSA's cache should be emptied.

The MSA initiates communication to the RSP using TCP/IP, on a port defined by the user. The default port is 5179. The MSA must be able to connect to the RSP using this port.

### activAeon Secure Communications Protocol

Message requests from the CMS to the RSP and MSA, and from the MSA to the RSP, and their responses, are defined by the proprietary activAeon Secure Communications Protocol (SCP). The SCP can run in one of two modes: simple or secure.

In simple mode, data passed in message requests and message responses is not encrypted. This is appropriate for private networks where the data is not transmitted publically.

In secure mode, message requests and message responses are both encrypted, using 128-bit Blowfish encryption. This is appropriate for public networks. An RSP or MSA running in secure mode will drop and report any requests that are not encrypted. Encryption and decryption of data has a negligible impact on data throughput, nor on data volumes: in real-time there is no discernable effect on system performance.

## Firewall Issues

Installation of the RSP and MSA software from the CMS typically requires SMB port access from the CMS to the RSP or MSA. This is used to install the software on the target device. These ports are routinely blocked in many organisations, as they pose significant security risks. If it is not possible to open these ports (even temporarily for the duration of the installation process) then a local installation procedure is possible. This involves running an installation process locally on each device, which installs an Agent Control Service (ACS) on the device. This service

enables the rest of the agent software (RSP or MSA) to be installed centrally from the CMS without requiring SMB access.

Any firewalls between the CMS and the target device must permit connections from the CMS to that device using the specified port (by default 5179). This is required to complete the installation of the agent software on the device, and to collect data from the device.