

User Guide

activAeon XA

Copyright © activAeon Ltd.
All rights reserved

The software contains proprietary information of activAeon Ltd; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between activAeon Ltd and the client and remains the exclusive property of activAeon Ltd. If you find any problems in the documentation, please report them to us in writing. activAeon Ltd does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of activAeon Ltd.

All brands and product names mentioned herein are trademarks or registered trademarks of their respective companies.

activAeon Ltd
Lugano Building
57 Melbourne Street
Newcastle
NE1 2JQ
UK

E-Mail: support@activaeon.com

<http://www.activaeon.com>

Contents

- activAeon XA 1**
- Contents..... i**
- Introduction 5**
 - Online Help & Technical Support 6**
- Installation Guide 7**
 - System Requirements 9**
 - activAeon XA Installation 11**
 - Select Installation Folder..... 11
 - activAeon XA Configuration..... 12**
 - SQL Server Details 12
 - CMS Details 14
 - Registration and Licensing..... 16**
 - License Requests 16
 - License Expiry 17
 - Removing activAeon XA 19**
- Quick Setup Guide 20**
- Setup Default Customer 21**
- Domain Management 24**
 - Managing a Domain 25**
 - Managing a Non-Trusted Domain 26**
 - Unmanaging a Domain 27**
 - Managed Domain Properties..... 28**
- Managed Device Groups 30**
 - Groups..... 31**
 - Linking a Domain 33**
 - Devices 34**
 - Device Input Information 36
 - Managed Device Properties..... 38
 - Virtualisation 41**
 - Create a Non-Microsoft Virtual Host 41
 - Setup a Virtual Host 41
 - Setup a Virtual Guest 43
 - Application Management 45**
 - Product Inventory Analysis 45
 - Monitoring Non-Supported Applications..... 46
 - Provisioning..... 48
 - SQL Credentials 49

Agent Management	51
Data Transfer.....	52
Desktop Applications	54
Working With Applications	55
Publishers.....	55
Applications.....	56
Suites.....	57
Deployment Groups	60
Creating a Deployment Group	61
Invoking a Deployment Group	65
Handling Failed Deployments	66
Editing a Deployment Group	67
Customers	68
Global Exclusions	69
Setting Up Further Customers	70
Assigning Licenses to a Customer	73
User Association.....	73
Server Association.....	74
Exclusions	77
Exchange	78
Exchange Setup	79
Hosted Exchange Database Settings	80
Hosted Exchange Service Plans	82
Exchange Mapping	84
Central Management Service (CMS)	86
System Log	87
activAeon XA System Updates	88
Update Settings	89
System Updates	90
Update Packages	93
Reports	94
Report Settings for Licensing Reports	95
SPLA Report	97
License Usage Report	98
Customer License Report	99
Microsoft Exchange License Report	100
Microsoft Windows License Report	101
Microsoft Server Products License Report	102
Microsoft Terminal Server License Report	103

Microsoft Desktop Application License Report	104
Terminal Server Session Activity Report.....	105
Desktop Application Usage Report	107
Saved Reports.....	110
Usage Summary.....	111
Index	113

Introduction

License efficiency for greater return on investment.

activAeon XA is an automated license efficiency solution that gives organisations the opportunity to increase revenue and maximise return on investment.

By automating the lengthy process of data collection and applying **Best Value Reporting Technology**, activAeon XA provides an organisation with cost effective decisions that have a positive impact in many areas of the business. This ensures that profits are maximised and costs are reduced, making the most of SPLA.

Online Help & Technical Support

Context Sensitive Help and Manual

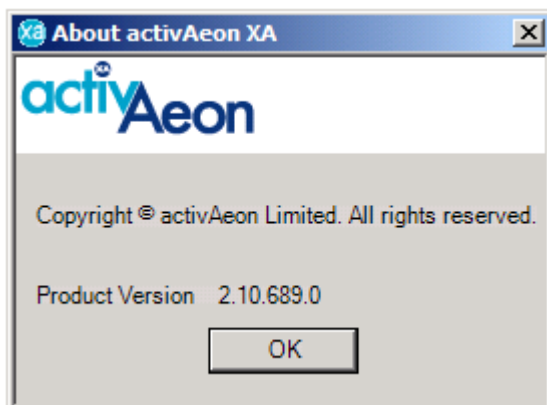
To access the fully integrated online help system provided with activAeon XA, click on the Help menu. From here you may browse or search the contents of the integrated help file which covers all aspects of using the software. Alternatively the relevant help for each dialog can be accessed by pressing F1 whilst the dialog is active.

Support

Support is available from the activAeon XA web site at <http://support.activaeon.com>.

About activAeon XA

Your installed version of activAeon XA is specified under [Help | About activAeon XA](#). Please check and report this number in any technical correspondence with activAeon Ltd.

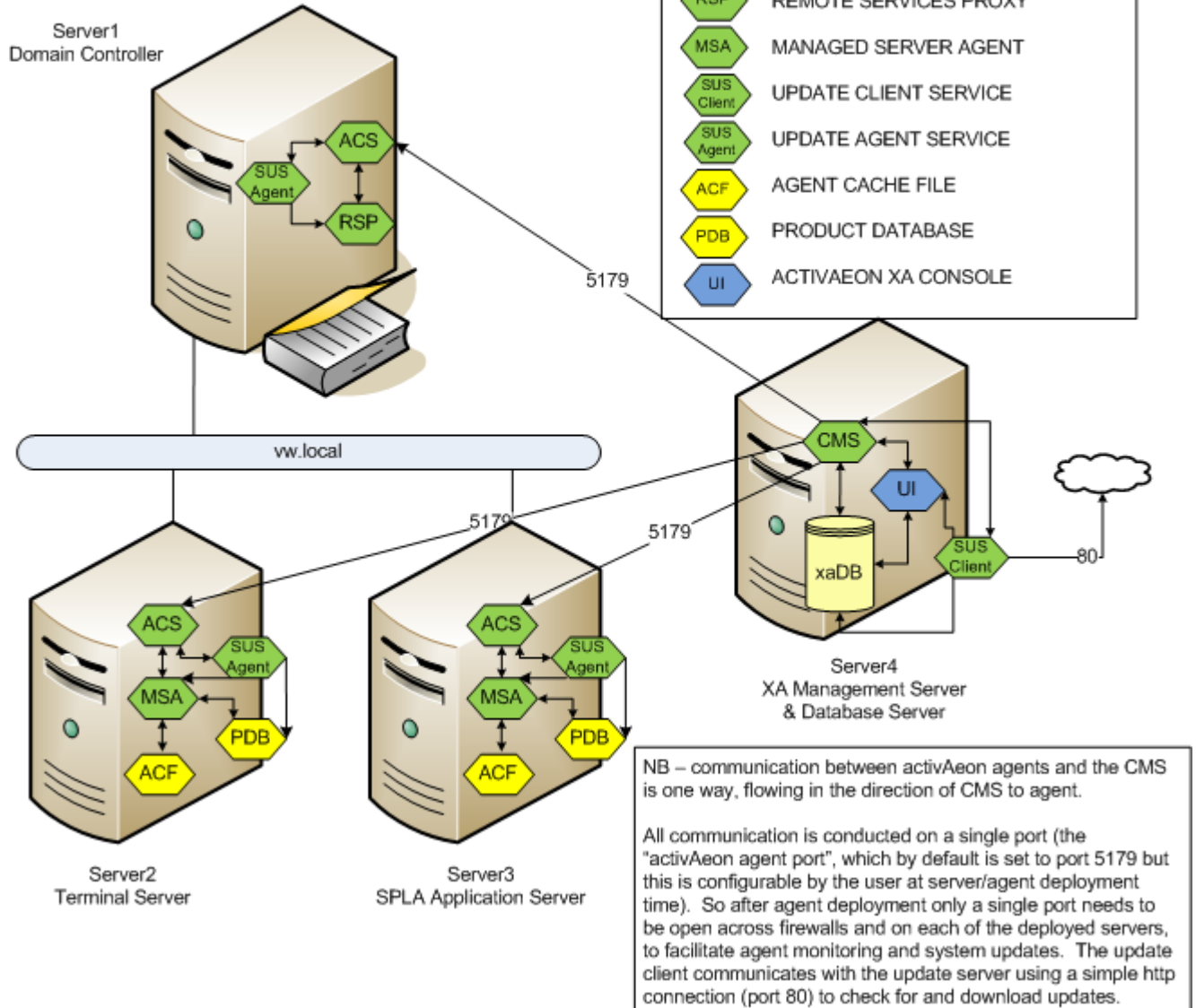


Installation Guide

The activAeon solution is comprised of ten 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 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 utilisation information received from the activAeon XA 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 Server 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 SUS Client Service** - The SUS Client service is a Windows service that is deployed to the AMS to communicate with the activAeon XA SUS Server, using http, allowing it to receive activAeon XA software updates.
- **activAeon XA SUS Agent Service** - The SUS Agent service is a Windows service that is deployed to devices across an enterprise to receive and install activAeon XA software updates from the SUS Client.
- **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 Provider 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.

Overview of activAeon Services & Product Architecture



Note: The installation information given here is for the setup of the AMS. Agents are deployed from within the activAeon XA management console.

System Requirements

Network Configuration

It is recommended that a dedicated device is available to act as the AMS.

The activAeon XA Management Server (AMS)

The AMS must have access to the [SQL Server Host](#). The installation creates an ODBC data source called XAdb to connect to the SQL server.

The AMS requires the following software and hardware:

Device Type	Category	Requirement
Server	Operating system	Windows 2003 Server (Standard/Enterprise/DataCenter), Windows 2003 R2 Server (Standard/Enterprise/DataCenter), Windows 2008 Server (Standard/Enterprise/DataCenter) or Windows 2008 R2 Server (Standard/Enterprise/DataCenter)
	CPU	Pentium III Processor or higher
	Memory	512 Mb RAM minimum
	Disk space	512 Mb Free Disk Space
	Software	.NET Framework 3.5 minimum

The activAeon XA Agent

The activAeon XA agent requires the following software:

Device Type	Category	Requirement
Server	Operating system	Windows 2003 Server (Standard/Enterprise/DataCenter/Web), Windows 2003 R2 Server (Standard/Enterprise/DataCenter/Web), Windows 2008 Server (Standard/Enterprise/DataCenter/Web) or Windows 2008 R2 Server (Standard/Enterprise/DataCenter/Web)

SQL Server Host

The SQL Server host requires the following software:

Device Type	Category	Requirement
Server	Operating system	Windows 2003 Server (Standard/Enterprise/DataCenter), Windows 2003 R2 Server (Standard/Enterprise/DataCenter), Windows 2008 Server (Standard/Enterprise/DataCenter) or Windows 2008 R2 Server (Standard/Enterprise/DataCenter)
	Database software	Microsoft SQL Server 2005 (Express/Standard/Enterprise/Workgroup) or Microsoft SQL Server 2008 (Express/Standard/Enterprise/Workgroup) or Microsoft SQL Server 2008 R2 (Standard/Enterprise/Workgroup/DataCenter)

A regular backup and maintenance routine should be performed to ensure optimum database performance.

Note: These are baseline recommendations to ensure optimum application performance where activAeon XA has been installed on a dedicated device. Where activAeon XA is installed on a device alongside other applications, the system requirements may be higher.

activAeon XA Installation

Before you begin the installation process log on to the machine you wish to use as the main management device for activAeon XA. Log on using an account with administrative privileges.

Extract the software and click on setup.exe to begin the installation.

Click next and work through the installation as follows.

Select Installation Folder

Specify an install folder for activAeon XA and select who can use the software once installed.

Click on the **Next** button to confirm the install folder.

If you are not ready to install the program go back or **Cancel** out of the setup procedure. If you elect to go on then activAeon XA will begin to install components onto your device. You will then need to carry out a full uninstall to remove the program.

To proceed with the installation process, click on the **Next** button.

activAeon XA Configuration

The activAeon XA configuration procedure involves two stages:

Stage 1

SQL Server database setup. This is required to create the system database and ODBC connections, see SQL Server Details (on page 12).

Stage 2

Management Server setup. This will register the account under which the central management service will run and configure the database connection used by the management console, see CMS Details (on page 14).

Note: You must complete the configuration procedure before using the management console to deploy agents.

If you chose to cancel the configuration process, it is possible to run the **XASQLSetup.exe** located in **<InstallDir>\activAeon\activAeon XA** to complete the process.

Click on the **Next** button to proceed.

SQL Server Details

This part of the configuration is used to determine the location of the SQL Server. It is not necessary to have SQL Server on the same machine as the activAeon XA Management Server.

Note: The SQL Server must already be installed and running for the installation to complete successfully.



Database Details

➤ SQL Server

This will default to the name of the device onto which the software has been installed. If you wish to change this installation then enter the name of the target SQL Server host. To use the default instance of a SQL Server installation, enter the name of the **SQL Server**. To use a named instance, enter the name of the **instance** in the format **server\<instance name>**, for example SQLServer\Instance2.

➤ Data Location

This is the location of the SQL Server database. Enter a path or use the Browse button provided, if you wish to change the location.

Note: The data location specified is local to the database server.

Database Connection

The database connection method used to create the database will be dependent on the setup of SQL Server.

➤ **Use Trusted Connection**

This option should be used if SQL Server has been setup using Windows authentication. activAeon XA will then use the current logon credentials to create the database.

➤ **Use the following SQL account**

This option should be used if SQL Server has been setup using SQL authentication. Enter an appropriate login name and password.

Warning: Whichever connection method you choose it is important that the user account has the correct privileges to allow activAeon XA to create and populate a SQL database.

Click on the **Next** button to proceed. This will create the SQL Server database at the specified location immediately.

Note: Please use the backup procedures available as part of SQL Server to ensure that your database is backed up on a regular basis. activAeon XA does not perform this procedure.

CMS Details

These are the specified settings for the CMS and the management console. The settings that you select will depend upon whether the database is local to the AMS or on a remote device.

The screenshot shows the 'activAeon XA Setup Wizard' window with the 'CMS Details' tab selected. The window title is 'activAeon XA Setup Wizard' and it features the 'XA' logo in the top right corner. The main heading is 'CMS Details' with the instruction 'Please enter the settings for the activAeon XA Central Management Service'. The dialog is divided into two sections: 'CMS Service' and 'Database Connection'. In the 'CMS Service' section, the 'Run as Local System Account' radio button is selected, and there are empty text boxes for 'User', 'Password', and 'Domain'. In the 'Database Connection' section, the 'Use Trusted Connection' radio button is selected, and there are empty text boxes for 'User', 'Password', and 'Confirm Password'. At the bottom of the dialog, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

CMS Service

By default, the CMS runs using the local system account. However, by selecting the **Use following account** option it is possible to supply an alternative username and password under which the service will run. The account specified must have the appropriate privileges to interact with the database and have administrative privileges on the AMS.

Database Connection

The database connection method will be dependent on the setup of SQL Server. Whichever connection method is used it is important that the user has the appropriate credentials for interacting with the database.

➤ Use Trusted Connection

This option should be used if SQL Server has been setup using Windows authentication. The interface will then use the current logon credentials to interact with the activAeon XA database and the CMS will connect to the database with the account specified in the previous step.

Note: The use local system account option with the use trusted connection option is only appropriate to local databases.

➤ Use the following SQL account

This option should be used if SQL Server has been setup using SQL authentication. Enter an appropriate login name and password for both the interface and the CMS to interact with the activAeon XA database.

Click on the **Next** button to proceed.

Click on the **Setup** button to complete the configuration process.

Once the setup process has completed, click on the **Finish** button and then **Close** to close the installation wizard.

Note: After setup has complete, if you have chosen to run the CMS using a specified account and chosen to connect using a trusted connection, it is important that this user is granted both public and db_owner privileges on the XAdb database prior to starting the CMS. Also, if the database resides on a remote device, the account used to logon to the AMS must have the appropriate privileges to interact with the database.

Registration and Licensing



Once installation has been completed activAeon XA can be accessed via the [Start menu | All Programs | activAeon | activAeon XA | XA Management Console](#). The first time the program is selected you will be asked to select the license agreement you wish to use.

activAeon XA is protected by a license key. Before you can use the product you will need to register with activAeon Ltd to receive a valid license key.

The following types of license are available.

- **Evaluation License** - This provides a limited deployment of 30 devices, running for fifteen days. The program is fully operational throughout the license period.
- **Non-Perpetual License** - This license is renewable on a yearly basis. This version of the software will only permit activAeon XA agents to be deployed to the number of **devices** specified at registration. It is inclusive of standard support and maintenance.
- **Perpetual License** - This license has no expiry date. This version of the software will only permit activAeon XA agents to be deployed to the number of **devices** specified at registration.

Once you have decided on the type of license, **select the relevant option**. Read through the displayed license agreement. If you agree with the terms select **Accept** to proceed.

License Requests

Selection of the license type and acceptance of the license agreement activates the **License Request** dialog.

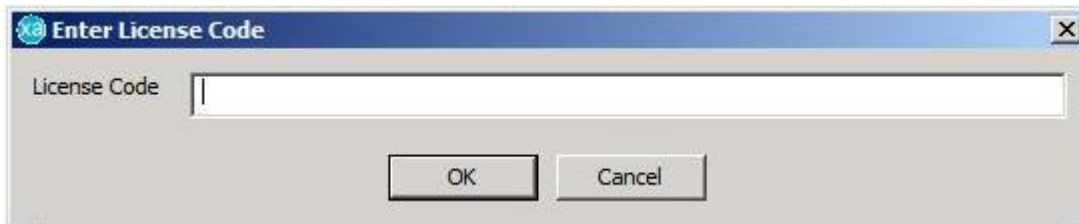
The License Manager generates a unique machine id which must be sent to activAeon Ltd in order to request a license key.

You now have two options for sending the code:

1. If you have an email client enabled on your system then click on the e-mail link to automatically generate a license request.
2. Copy (highlight then Ctrl+C) and paste the code into an e-mail and send it to register@activaeon.com.

Note: In the case of a non-perpetual or perpetual license request please remember to specify the number of devices that require monitoring by activAeon XA agents.

To activate activAeon XA select **Register activAeon XA** from the **Help** menu and click **Enter License Code...**



Copy and paste the code into the box. Then click the **OK** button.

You will now see the expiry date for the license and in the case of a perpetual or evaluation license the number of devices available.

Note: If the CMS is running when you attempt to renew a license for activAeon XA then the License Manager will stop the service and then re-start it once the licensing process has been successfully completed. No data is lost from the agents, which will continue to cache data until the CMS is running again.

A license key can only be used on the machine on which the unique machine id was generated. Therefore, if you relocate the AMS to a new device, you must generate a new machine id in order to request a new license key.

Once activAeon XA has been licensed successfully you will receive a license certificate.

License Expiry

The expiry date of the current license is shown in the License Manager. This can be checked by going to the **Help** menu and then **Register activAeon XA**.

Ten days prior to the expiry of the current license a notification will appear informing you of the need to either upgrade for an evaluation license or renew for a non-perpetual license.

Warning: It is important to ensure your license is renewed prior to expiration as after a license has expired the CMS will stop collecting data from the activAeon XA agents. No existing data will be lost.

Evaluation Licenses - If you have been operating an evaluation license then please contact activAeon Ltd or your reseller to discuss upgrading to either a perpetual or non-perpetual license.

Non-Perpetual Licenses - Select the license option again to generate the machine id and re-submit to activAeon Ltd or your reseller for a new key, see License Requests (on page 16).

Removing activAeon XA

If you need to remove activAeon XA from the management device it is recommended that you delete each device, and thereby its associated agent, from the management console first. For information on deleting devices, see [Devices](#) (on page 34).

Whilst activAeon XA supports the removal of agents during the uninstallation of the software, this will not be possible if an agent cannot be contacted. If during the software uninstall, activAeon XA fails to remove all of the agents, it is possible to remove orphaned agents manually via Add/Remove Programs on the individual devices. However, this is not recommended for an agent still managed by the AMS.

To remove activAeon XA from the AMS use [Start | Control Panel | Add/Remove Programs](#).

Note: All data collected by activAeon XA will remain on the SQL Server host and the ODBC connection to the database will remain on the AMS. This will allow access to the usage data collected even after activAeon XA has been removed.

Quick Setup Guide

Once activAeon XA has been installed it is advised that you complete the following tasks in order.

- Setup your default customer details, see [Setup Default Customer](#) (on page 21).
- Setup the domains that activAeon XA will manage, see [Domain Management](#) (on page 24).
- Create your group structure, see [Groups](#) (on page 31).
- Link the managed device groups created to a domain, see [Linking a Domain](#) (on page 33).
- Deploy your devices (on page 34) and determine requirements for application monitoring, see [Desktop Applications](#) (on page 54).
- Create any further customers, see [Customers](#) (on page 68).
- Setup your associations and exclusions, see [Assigning Licenses to a Customer](#) (on page 73).

The following tasks must also be completed before using the reports section of activAeon XA for the first time.

- Configure activAeon XA to report on your Exchange deployment, see [Exchange](#) (on page 78).

Setup Default Customer

Before you can use activAeon XA for the first time you must setup your details. The customer information provided here is used on the relevant license reports. The information given here will not be passed on to any third party.

MOET

Enter your SPLA (Service Provider license Agreement) details as agreed with Microsoft.

The screenshot shows a 'Customer Details' dialog box with the following fields and options:

- Organization: Smiths Garages
- Agreement Number: 123456789
- Agreement Date: 01 January 2010
- Carrier Code: [Empty]
- Carrier Account No.: [Empty]
- Reference: [Empty]
- Reporting: Generate a Microsoft SPLA Report for this customer

Buttons: OK, Cancel, Help

Contact

Enter your contact details. The contact information will be used in the event of a query.

The screenshot shows a dialog box titled "Customer Details" with three tabs: "MOET", "Contact", and "Address". The "Contact" tab is selected. The form contains the following fields:

- Contact Name: Joe Smith
- Phone Number: 0191 5698745
- Fax Number: 0191 5698746
- Email Address: joe.smith@smiths.com
- Correspondence Language: EN (dropdown menu)

At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

Address

Enter an appropriate invoicing and billing address.

The screenshot shows the same "Customer Details" dialog box, but with the "Address" tab selected. The form contains the following fields:

- Ship-To Address: 1 North Street
- Ship-To City: The City
- State/Province: (empty field)
- Postal Code: SR5 7HD
- Country Code: GB (dropdown menu)

At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

Click **OK** to save the details.

Domain Management

The domain management operations are accessed using the **Domains** node in the tree view.

Domain management is used to configure the list of domains that you wish activAeon XA to manage and interrogate. A Remote Services Proxy (RSP) is placed on a specified device in each managed domain to interface with Active Directory, together with the activAeon XA control service (ACS) for communication with the AMS.

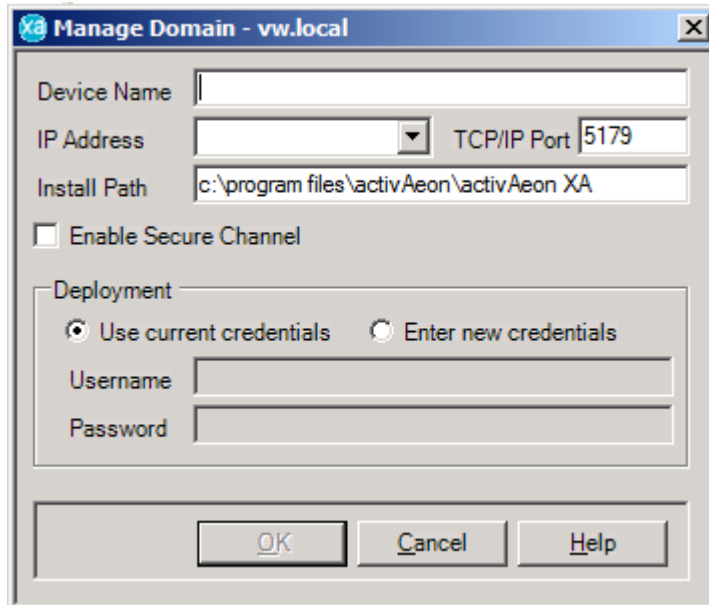
Note: Agents deployed to devices for the sole purpose of managing a domain (RSP) are not billed under the licensing terms of activAeon XA.

The domains currently available to the AMS are shown in the right hand pane when the **Domains** node is selected in the tree.

Domains that are currently managed by activAeon XA have an icon with a green circle and white tick. Unmanaged domains have an icon with a red circle and white cross.

Managing a Domain

1. Select the **Domains** node.
2. In the right hand pane, right click on the domain that you wish to manage and select **Manage...**



3. Complete the **Manage Domain** details dialog
 - a. **Device Name** - enter the name of a device within the selected domain to which you wish to deploy an RSP.
 - b. **IP Address** - select or enter an appropriate IP address for the device.
 - c. **TCP/IP Port** - enter a TCP/IP port that the agent will use to listen on for incoming connections from the AMS.
 - d. **Install Path** - enter the target install directory for the agent.
 - e. **Enable Secure Channel** - check this option to encrypt communications between the device and the AMS.
 - f. **Deployment** - to use the current logon credentials, select **Use Current Credentials**. To specify different credentials for access to the device, select **Enter New Credentials** and enter a **Username** in the format **domain\username** and a **Password**.
 - g. Click **OK** to continue.

Note: The credentials specified must have the appropriate privileges to perform this action.

Managing a Non-Trusted Domain

1. Right click the **Domains** node and select **Add Domain...**
2. Complete the **Manage Domain** details dialog
 - a. **Device Name** - enter the name of a device within the selected domain to which you wish to deploy an RSP.
 - b. **IP Address** - select or enter an appropriate IP address for the device.
 - c. **TCP/IP Port** - enter a TCP/IP port that the agent will use to listen on for incoming connections from the AMS.
 - d. **Install Path** - enter the target install directory for the agent.
 - e. **Enable Secure Channel** - check this option to encrypt communications between the server and the AMS.
 - f. **Deployment** - to use the current logon credentials, select **Use Current Credentials**. To specify different credentials for access to the device, select **Enter New Credentials** and enter a **Username** in the format **domain\username** and a **Password**.
 - g. Click **OK** to continue.

Note: The credentials specified must have the appropriate privileges to perform this action.

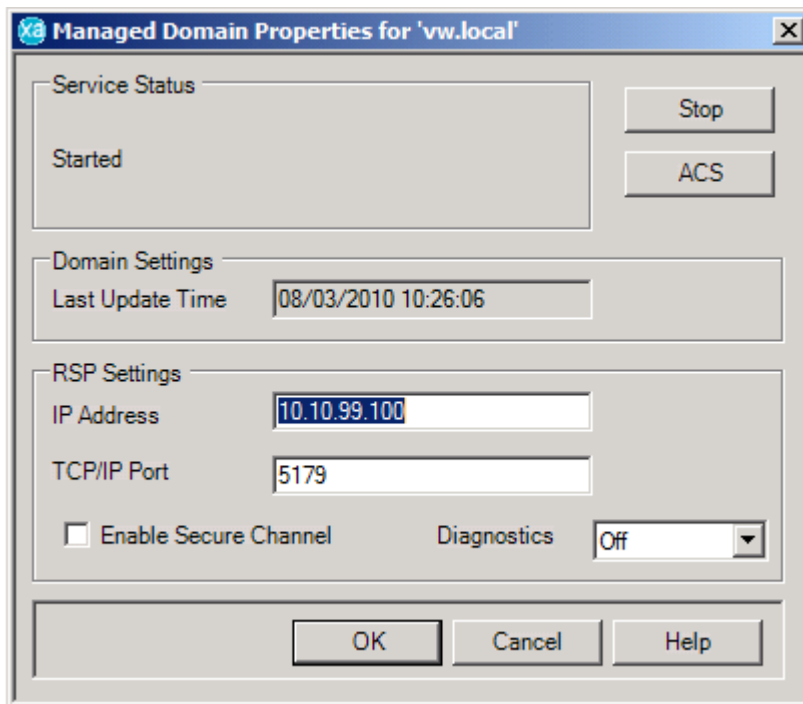
Unmanaging a Domain

1. Select the **Domains** node.
2. In the right hand pane, right click the domain that you no longer wish to manage and select **Unmanage...**
3. A warning will now ask you to enter the credentials required to unmanage the domain, click **OK** to proceed.

Managed Domain Properties

The **Managed Domain Properties** dialog shows the current status and settings of the RSP on the selected domain.

1. Select the **Domains** node.
2. In the right hand pane, right click the appropriate domain and select **Properties....**

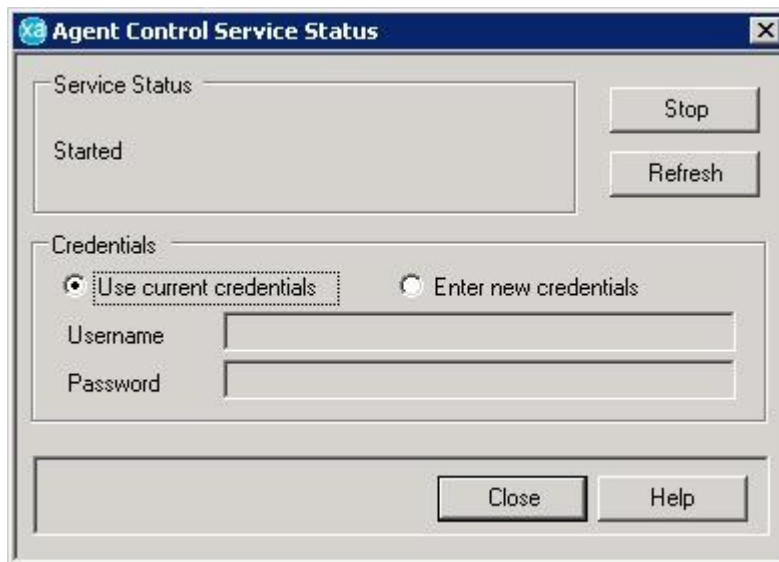


Starting/Stopping the RSP

1. To start the service click **Start**.
2. To stop the service click **Stop**.

activAeon XA Control Service (ACS)

It is possible to interact with the ACS on the remote device by clicking on the **ACS** button. To do so requires administrative privileges for the remote device. To use the current logon credentials, select **Use Current Credentials**. To specify different credentials, select **Enter New Credentials** and enter a **Username** in the format **domain\username** and a **Password**.



Note: If the **Service Status** is set to **Access Denied**, you need to specify a new set of credentials with the relevant administrative privileges.

1. To start the ACS click **Start**.
2. To stop the ACS click **Stop**.

Click on the **Close** button to return to the **Managed Domain Properties** dialog.

Domain Settings

This section shows the time of the last domain update within activAeon XA.

RSP Settings

It is possible to change the **IP address** of the device or the **TCP/IP port** applicable to this device should the need arise.

Check the **Enable Secure Channel** to encrypt communications between the device and the AMS.

The **Diagnostics** setting enables debugging of the agent services. This should be set to **Off** unless otherwise instructed by activAeon XA Technical Support.

Managed Device Groups

The group structure of activAeon XA is used to set up a hierarchy for your device deployment. The hierarchy is depicted using a tree.

The group structure is setup using the following steps:

Managed Device Group Setup

Managed device groups are created to facilitate the organisation of devices in accordance with the network structure of your company, see Groups (on page 31).

Domain Link Setup

Once a managed device group has been created it is recommended that it is linked to a managed domain before you associate devices that belong to the domain, see Linking a Domain (on page 33).

Device Setup

Setup the devices associated with each managed device group. These carry the various desktop and business applications being monitored and licensed, see Devices (on page 34).

Virtualisation Setup

Set-up any non-Microsoft virtual hosts and configure your virtual guests and their associated hosts, see Virtualisation (on page 40).

Application Management

Desktop applications need to be managed for each device. Supported SPLA products are automatically monitored, other applications need to be specified for each device, see Application Management (on page 45).

Groups

Groups are used to link related devices. We therefore recommend that groups are setup in a hierarchy according to the domain structure of your network. Groups can be nested to create subgroups to as many levels as required.

Adding a Group

1. Right click the **Managed Devices** node or an existing managed device group to create a subgroup and select **Create Managed Device Group....**



2. Type in the **Name** of your group.

Note: Group names must be unique within a group. It is not possible to have two groups with the same name within one parent group.

The Device Settings section is disabled during group creation. The settings in this section need to be set using the Properties dialog of the group and only apply to devices currently within the group; new devices added to a group later do not automatically inherit these settings.

3. Click **OK**.

Deleting Groups

1. Expand the **Managed Devices** node.
2. Right click the appropriate managed device group and select **Delete**.
3. If the managed device group contains devices or sub-groups, a warning will now ask you to enter the credentials required to delete all devices that belong to the managed device group and any associated subgroups. If an individual device cannot be deleted the process must be repeated after deleting the individual device.
4. Select **OK** to continue. Select **Cancel** to cancel the deletion.

Note: Deleting a managed device group will not remove the group from the user interface until after the end of the current reporting period. The licenses attributable to any devices within the group will remain valid for the current reporting period only.

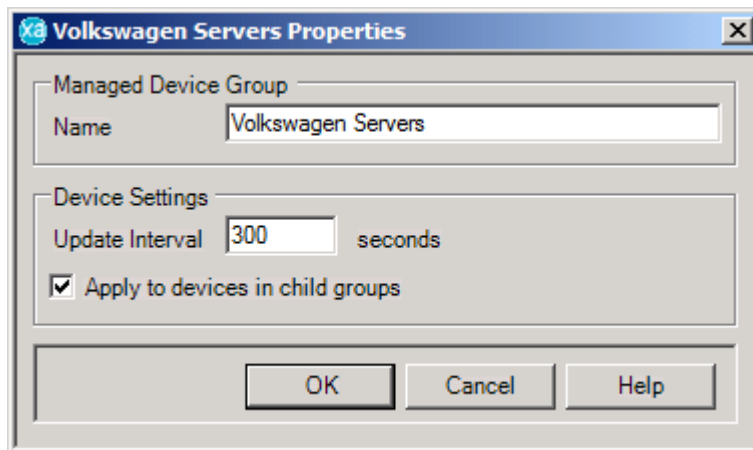
Restoring a Group

1. Expand the **Managed Devices** node.
2. Right click the appropriate managed device group and select **Restore**.

Note: If you choose to restore a managed device group the restore action will only restore the group. To restore any subgroups or devices within the group, right click the object and select **Restore**.

Group Properties

1. Expand the **Managed Devices** node.
2. Right click the appropriate group and select **Properties...**



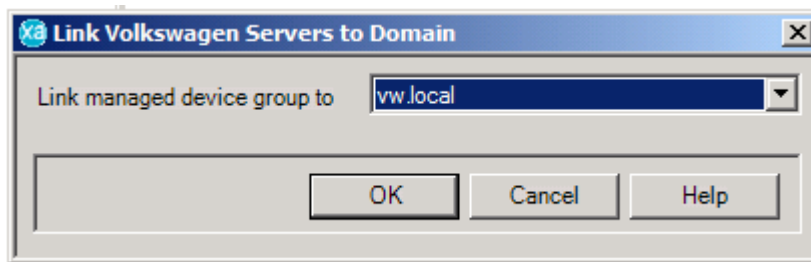
3. Make any changes to the group settings.
 - a. **Name** - if appropriate, give the group a new name.
 - b. **Update Interval** - set the interval for CMS to agent communication for devices already within the group.
 - c. **Apply to devices in child groups** - tick this option to apply the device settings to all sub-groups.
4. Click **OK** to save the changes.

Linking a Domain

The **Link Domain** process is used to associate a managed domain, see [Managing a Domain](#) (on page 25), with a managed device group, this will then provide you with a list of available devices within the **Manage Device** dialog. A domain can be linked to more than one managed device group.

Linking a Domain

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Right click the managed device group and select **Link Domain...**



4. Select the appropriate domain from the list available and click **OK**.

Unlinking a Domain

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Right click the managed device group and select **Unlink Domain...**

Devices

Once you have created your managed device group hierarchy you may start the process of deploying devices to individual groups (on page 31). As part of the device configuration and deployment process the **activAeon XA agent** is installed on each host. The agent consists of two services: the Agent Control Service (ACS), which is responsible for communicating with the AMS, and the Managed Server Agent (MSA), which is responsible for collecting the application license and usage data.

Note: The same device cannot be added to more than one group.

Adding a Device

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Right click the server group and select **Manage Device...**
4. Enter the data. For full details, see Device Input Information (on page 36).
5. Click **OK**.

Deleting a Device

Warning: It is recommended that you **do not** stop the agent prior to deleting a device.

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Delete...**
5. A warning will now ask you to enter the credentials required to delete the device. Click **OK** to proceed.

Note: Deleting a device will remove the agent software from the device, but the device will remain in the user interface until after the end of the current reporting period. The licenses assigned to this device will remain valid for the current reporting period only.

Restoring a Device

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Restore**.
5. Enter the data. For full details, see Device Input Information (on page 36).
6. Click **OK**.

Copying Device Information

If you have several devices with similar specifications in the same group, then you can copy the monitored components and provisioning settings from one device to another device.

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Copy**.
5. Highlight the device requiring the settings, then right click and select **Paste**.
6. Click **OK** to paste the new device configuration and overwrite the existing device configuration.

Moving a Device

It is possible to move a device between groups using drag and drop. Select the device to be moved and then drag it to its new managed device group.

If the destination managed device group is not assigned to the same customer, see Server Association (on page 74), then moving the device will also move any licenses associated with it to the new customer.

Device Input Information

The screenshot shows the 'Manage Device' dialog box. It features a title bar with the 'activAeon' logo and the text 'Manage Device'. The dialog is organized into three main sections: 'Device', 'Windows Licensing', and 'Deployment'.
- The 'Device' section includes a 'Domain' dropdown menu (currently set to '<Workgroup>') with a 'Refresh...' button, a 'Device Name' dropdown menu with an 'Add...' button, an 'IP Address' dropdown menu, a 'TCP/IP Port' text box (set to '5179'), an 'Install Path' text box (set to 'C:\Program Files\activAeon\activAeon XA'), an 'Enable Secure Channel' checkbox, and an 'Update Interval' text box (set to '300') with the unit 'seconds'.
- The 'Windows Licensing' section contains a 'Server Configured for Anonymous Access' checkbox.
- The 'Deployment' section has two radio buttons: 'Use current credentials' (selected) and 'Enter new credentials'. Below these are 'Username' and 'Password' text boxes.
- At the bottom of the dialog are five buttons: 'ACS...', 'Monitor...', 'OK', 'Cancel', and 'Help'.

Device

➤ Domain

When adding a device, this list contains all of the domains currently being managed by activAeon XA. If the current managed device group is linked to a domain, this field will default to the relevant domain. However, this field can be changed to any of the managed domains or to **Workgroup** should you wish to add a workgroup device.

➤ Device Name

When adding a domain device, this list displays all visible devices within the selected domain. Use the drop down list to select the required device. Once a device is deployed it is removed from the list of available devices. Use the **Refresh...** button to update the list of available devices. If your device does not appear in the list of devices it is possible to add the device by selecting the **Add...** button. On the **Add Member** dialog, enter the **Name** and an appropriate **IP Address** for the device, select whether it is a **server** or a **desktop** and then click **OK**.

Note: A device being added in this way must be online, be contactable from the AMS and be a member of the selected domain.

When adding a workgroup device, you may type in an alias for that device and specify its IP address in the **IP Address** field. The alias will be the name of the device used by the interface and the reports to reference the device. Alternatively, you may type in the complete IP address, Fully Qualified Domain Name (FQDN) or NETBIOS name of the device. In the case of IP address, this is automatically copied across into the **IP Address** field.

➤ **IP Address**

This is the IP address of the device. The IP address field will default to the public IP address of the device. It can be altered as necessary as long as the device can be contacted on the new IP address. The IP address can be changed after the agent has been deployed if the device IP address is changed.

➤ **TCP/IP Port**

This is the port number on which the ACS listens for information from the AMS. The default is port 5179.

➤ **Install Path**

The path is the location on the device where the services and collected information cache is stored, prior to uploading to the AMS.

➤ **Enable Secure Channel**

Check the **Enable Secure Channel** to encrypt communications between the device and the AMS.

➤ **Update Interval**

This is the time interval, in seconds, between agent and management server communications. We recommend that the interval is not set to less than 60 seconds to avoid excessive traffic on the system. The default setting is 300 seconds.

Windows Licensing

Note: This section only applies if the device you are adding is a server, this section will be disabled if you are adding a desktop.

➤ Server Configured for Anonymous Access

Indicate whether this device will be accessed by anonymous users. This is then used to determine the correct licensing type for a device.

Deployment

To use the current logon credentials, select **Use Current Credentials**. To specify different credentials for access to the device, select **Enter New Credentials** and enter a **Username** in the format **domain\username** and a **Password**. These new logon details must have administrative privileges over the device on which the agent program is to be installed.

Monitor

To setup a list of monitored components (on page 46) for the device select **Monitor...**

If you wish to leave this until later, or to add or change components in the future then the option can also be reached by

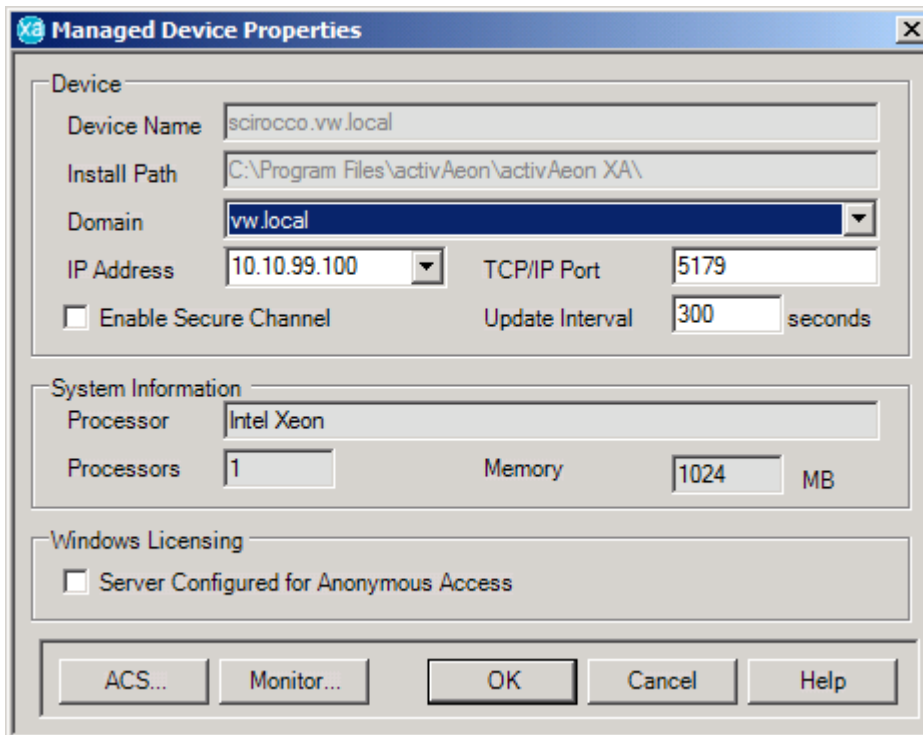
1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Properties**.

Managed Device Properties

The Managed Devices Properties section displays device data which can be altered after a device has been created, see Device Input Information (on page 36). To open the properties:

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.

4. Right click the device and select **Properties...**

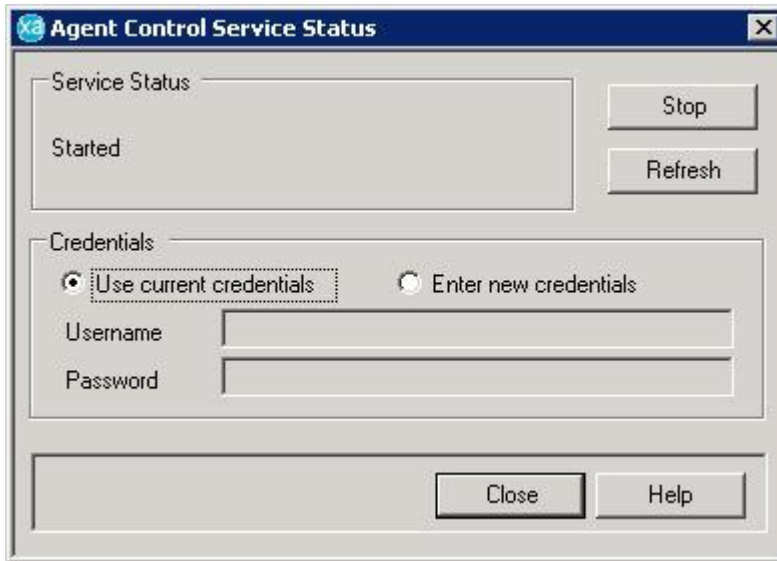


The following options can be amended:

- Domain
- IP Address
- TCP/IP Port
- Enable Secure Channel
- Update Interval
- Windows Licensing
- Monitored Components

activAeon XA Control Service (ACS)

It is possible to interact with the ACS on the remote device by clicking the **ACS** button. To do so requires administrative privileges for the remote device. To use the current logon credentials, select **Use Current Credentials**. To specify different credentials, select **Enter New Credentials** and enter a **Username** in the format **domain\username** and a **Password**.



Note: If the **Service Status** is set to **Access Denied**, you need to specify a new set of credentials with the relevant administrative privileges.

1. To start the ACS click **Start**.
2. To stop the ACS click **Stop**.

Click on the **Close** button to return to the **Managed Device Properties** dialog.

Virtualisation

Note: All servers that must be licensed under SPLA must have an activAeon XA agent deployed to it. Before you can setup virtualisation you must add each server to the activAeon XA console, see Devices (on page 34).

The virtualisation functionality of activAeon XA allows you to associate host servers with their virtual guests to achieve the licensing savings available under SPLA.

Create a Non-Microsoft Virtual Host

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Create Non-Microsoft Virtual Host...** The **Create Non-Microsoft Virtual Host** dialog is displayed.

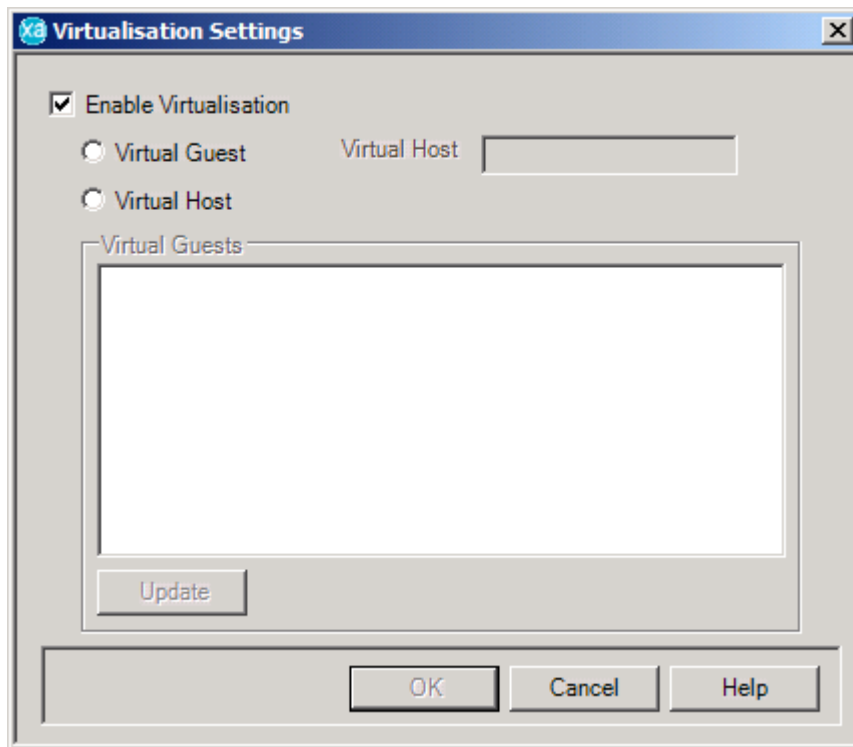


5. Enter a **Name** for the host.
6. Enter the number of **Processors** that the host has.
7. Click **OK** to add the host.

Setup a Virtual Host

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.

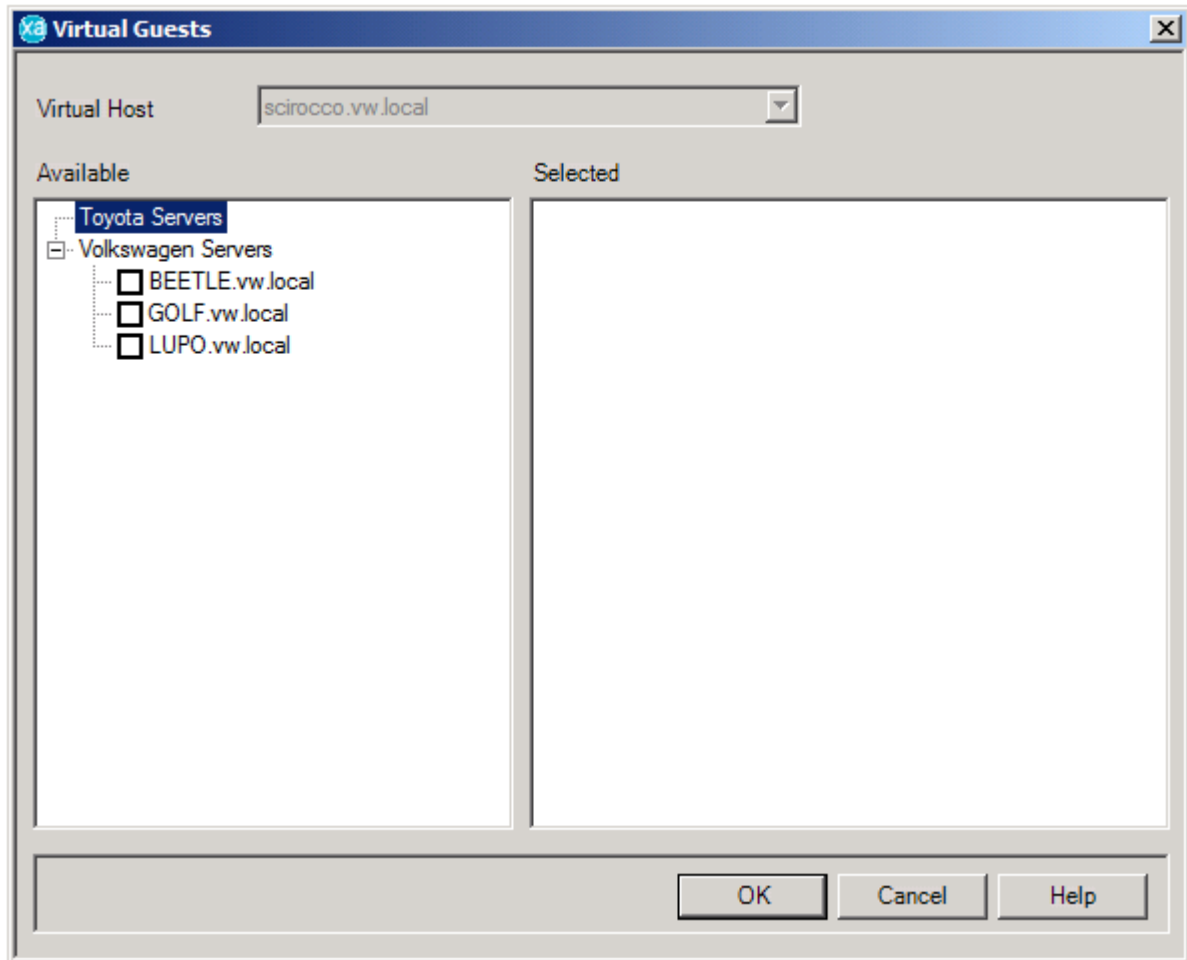
- Right click the device and select **Virtualisation...**. The **Virtualisation Settings** dialog is displayed.



- Check the **Enable Virtualisation** option.
- Check the **Virtual Host** option.

Note: If the device is a non-Microsoft virtual host, this option will be checked by default and cannot be changed.

7. To setup a list of virtual guests associated with the host click **Update**. The **Virtual Guests** dialog is displayed.



- a. Expand the appropriate managed device group(s) in the **Available** list.
- b. Check the devices that are virtual guests. When ticked the devices will appear in the **Selected** list. To select all child devices, right click the managed device group and select **Select All**.
- c. Click **OK** when all virtual guests have been selected to return to the **Virtualisation Settings** dialog.

Note: To remove an associated virtual guest follow the steps above, but in step (b) uncheck the devices that you no longer wish to associate or if appropriate right click the managed device group and select **Unselect All**.

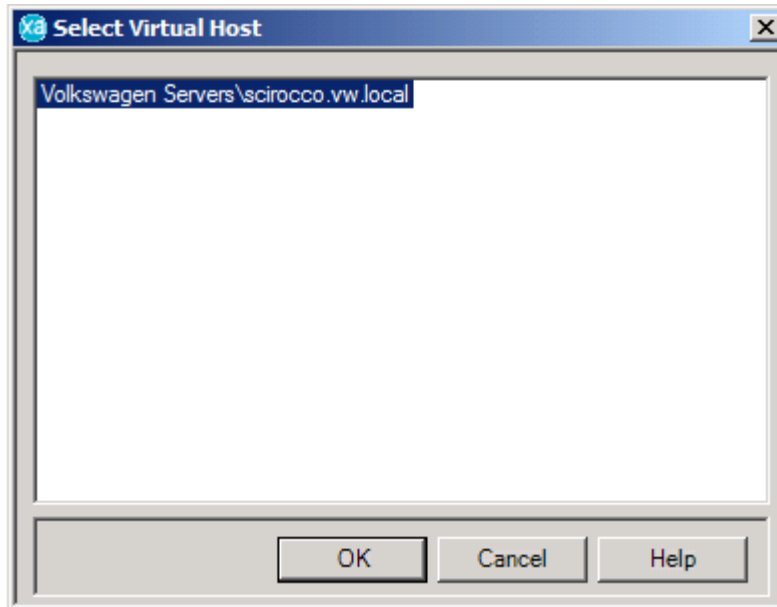
8. Click **OK** to apply the virtualisation settings.

Setup a Virtual Guest

Note: a non-Microsoft virtual host cannot be a virtual guest.

1. Expand the **Managed Devices** node.

2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Virtualisation....**. The **Virtualisation Settings** dialog is displayed.
5. Check the **Enable Virtualisation** option.
6. Check the **Virtual Guest** option.
7. To specify a virtual host for the guest click **...**. The **Select Virtual Host** dialog is displayed.



8. Select a host from the list of servers and click **OK** to return to the **Virtualisation Settings** dialog.
9. Click **OK** to apply the virtualisation settings.

Application Management

Within activAeon XA there are three phases to application management:

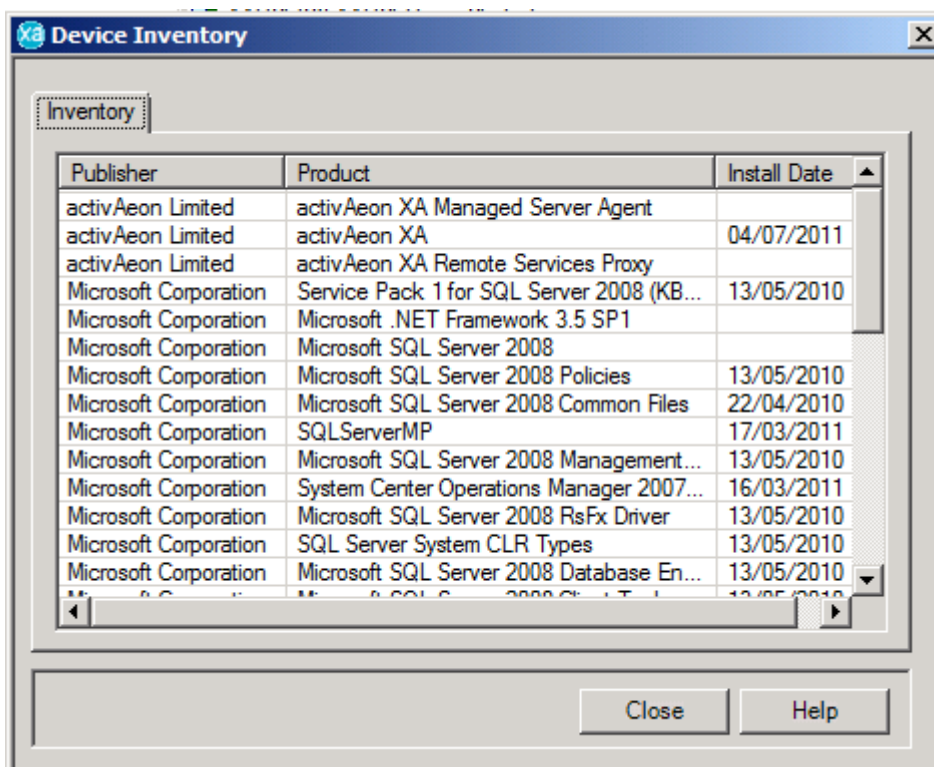
1. Product Inventory Analysis - this is used to determine what products are installed on a device.
2. Monitoring - this is setup automatically for supported SPLA products, but can be configured manually for other applications.
3. Provisioning - this must be setup for all SPLA desktop products to ensure an accurate license count is obtained.

Product Inventory Analysis

When an agent is deployed to a device activAeon XA will perform a product inventory check to establish a list of all products currently installed in the device.

To view the product inventory for a device:

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Products... | Inventory...**

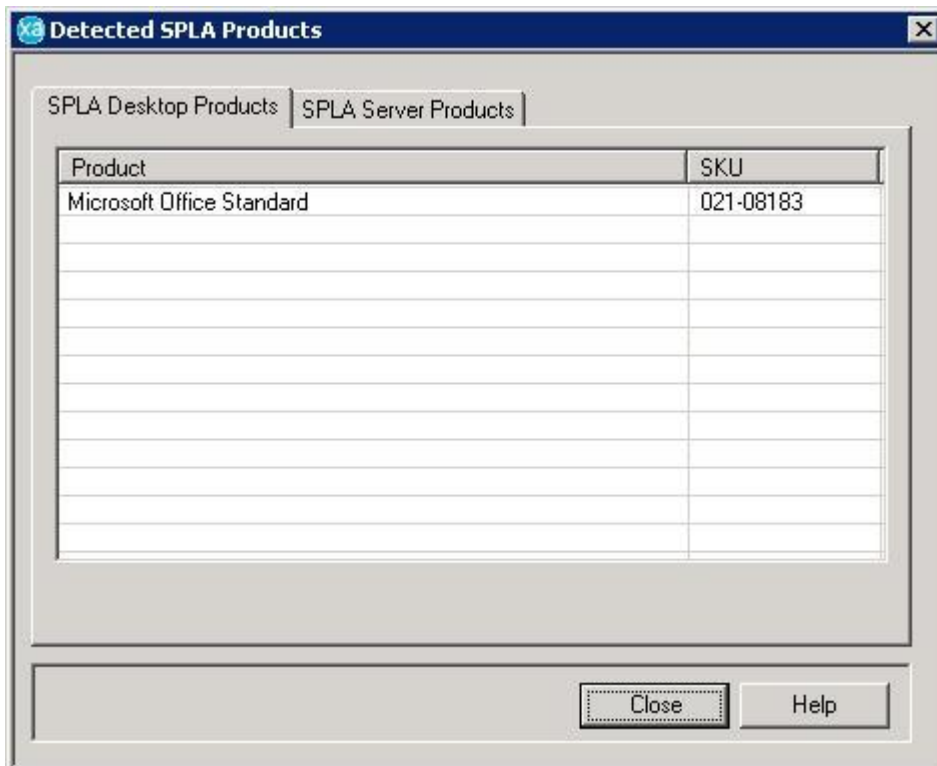


Note: The data displayed is raw product data, no processing or analysis has taken place.

Once the product inventory check has been performed the agent then checks the list of installed products against the activAeon XA Product Database (PDB) to determine the list of supported SPLA products that are installed on the device.

To view the list of detected SPLA products for a device:

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Products... | SPLA | Products...**



This dialog displays any supported **SPLA Desktop Products** and **SPLA Server Products** that are installed on the device.

Note: Any supported SPLA products that are detected on a device are automatically monitored for license and usage analysis. The next step for these products is to setup provisioning (on page 48).

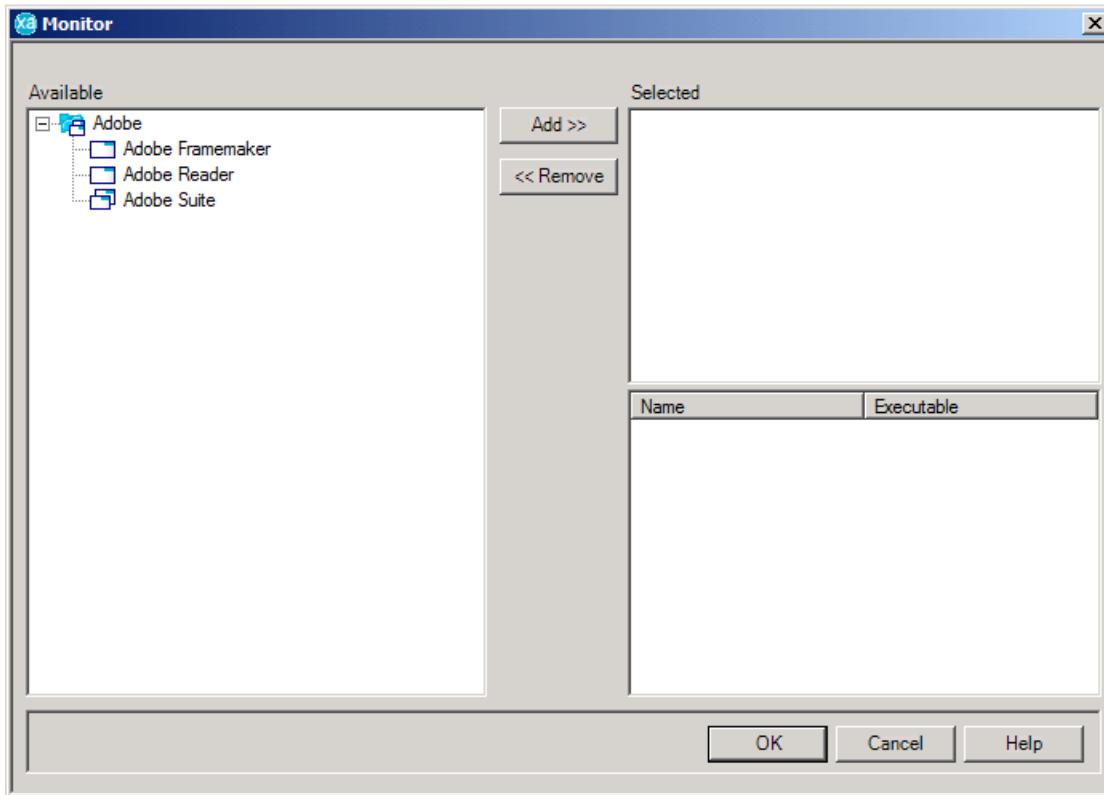
Monitoring Non-Supported Applications

It is possible to monitor other non-supported products on a device using activAeon XA. Once an application is setup to be monitored usage data will be recorded against the device.

Warning: This method should only be used for non-supported products that have not been automatically detected and monitored by activAeon XA.

Application monitoring can be access in the following ways:

- During the device setup process, see Device Input Information (on page 36).
- From the Managed Device Properties (on page 38) dialog.



Note: The global list of available programs is created and managed under the **Desktop Products** node. For further information, see Desktop Applications (on page 54).

The monitoring options are listed in the **left hand window**. On the right hand side are two windows. The **upper window** is used to show your selected applications and suites. The **lower window** shows the application and suite breakdown of your selected programs.

To Monitor an Application

1. Highlight the required application in the left hand window.
2. Click **Add>>**.

Note: It is not possible to monitor two or more applications with the same executable name on a device or an application and a suite containing that application on a device at the same time.

To Stop Monitoring an Application

1. Highlight the required application in the upper right hand window.
2. Click **<<Remove**.

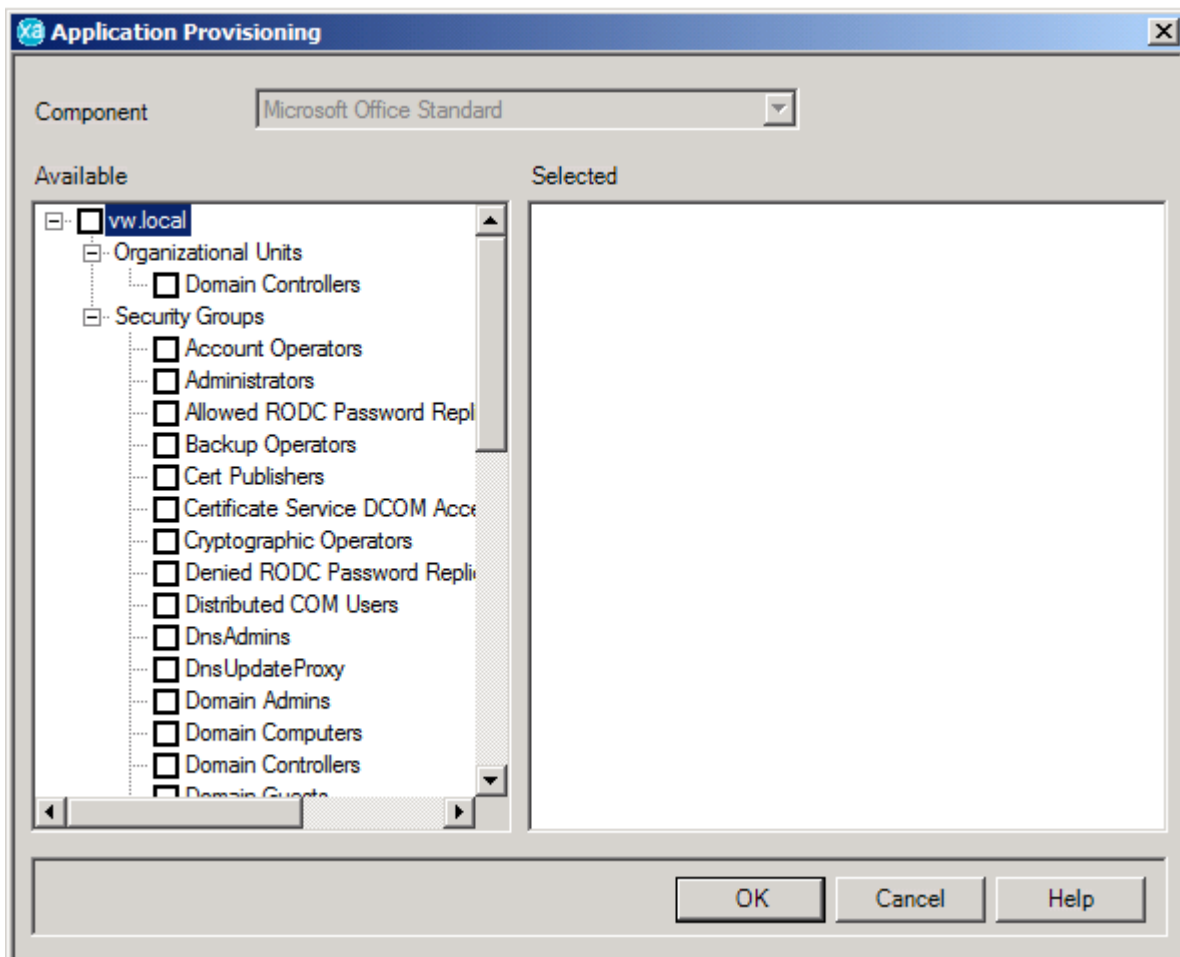
Provisioning

Provisioning is the process of mapping Organizational Units and Security Groups within Active Directory to the Microsoft desktop applications being monitored on a device. The provisioning mechanism is used by activAeon XA to identify which users are permitted to use the applications. The user provisioning information is then used to calculate desktop application license requirements.

Note: Provisioning is only used for Microsoft products available under the SPLA agreement.

Provisioning can be accessed in the following way:

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the server and select **Products... | SPLA | Provisioning...**



Entering Security Groups and Organizational Units

1. Select the application for which you wish to setup provisioning from the **Component** drop down list.

2. Expand the appropriate domain node(s) in the **Available** list.
3. Expand the **Organizational Units** and/or **Security Groups** node(s).
4. This will open a list of all security groups or organizational units in the current domain.
5. Check the organizational units or security groups that you wish to provision. When ticked the Active Directory objects will appear in the **Selected** list. To select all child organizational units or security groups, right click the object and select **Select All**.
6. Click **OK**.

Removing Security Groups and Organizational Units

To remove a security group or organizational unit find the security group or organizational unit name as before and remove the tick or if appropriate right click and select **Unselect All**.

SQL Credentials

In order to determine the correct number of SALs for Microsoft Office SharePoint Portal Server, Microsoft Systems Management Server, Microsoft Operations Manager and Microsoft CRM, the activAeon XA agent must interrogate the appropriate database.

If activAeon XA cannot interrogate the SQL database, you must enter into the activAeon XA management console account credentials that have sufficient rights to access the required database and tables.

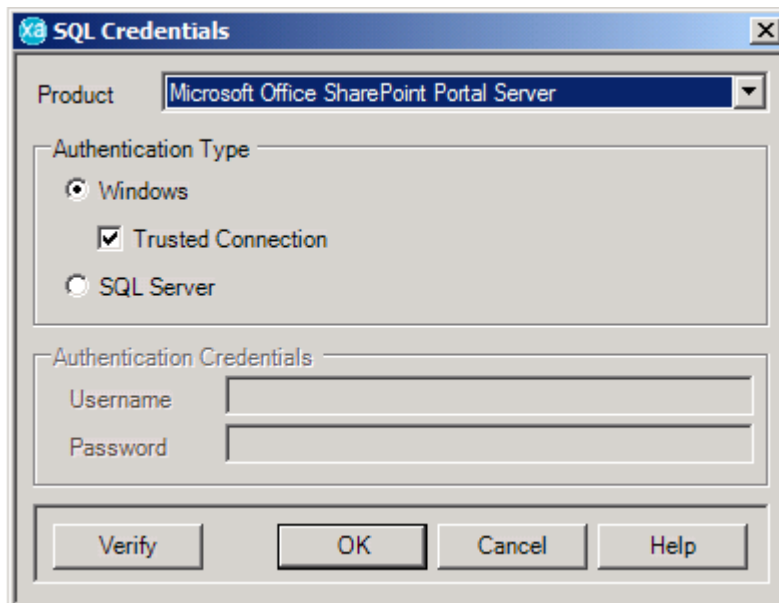
The activAeon XA management console indicates that the activAeon XA agent is unable to successfully connect to the database by displaying an error message in the System Log (on page 87).

Warning: No licenses will be allocated to these products if they are not fully configured.

To configure these settings:

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.

- Right click the computer and select **Products | SPLA | Server Product Configuration...**



- Select the product which requires further setup from the **Product** drop down list.
- Select the **Authentication Type** and specify credentials:
 - Windows** - select to use **Trusted Connection** or specify an appropriate Windows username and password in the **Authentication Credentials** section, this option only applies if the SQL database is local to the product installation.
 - SQL Server** - specify an appropriate SQL username and password in the **Authentication Credentials** section.
- Click **Verify** to check that the information provided is correct.
- Click **OK** to confirm the settings.

Agent Management

The activAeon XA agent is a program installed on a device which collects, stores and sends information to the AMS. The agent consists of two services: the Agent Control Service (ACS) which is responsible for communicating with the AMS; and the Managed Server Agent (MSA) which is responsible for collecting the application license and usage data.

License information is stored in a cache and then transferred to the AMS at the specified update interval. For information on the location of the agent and cache and the specified update interval, see Device Input Information (on page 36).

Once the information has been transferred to the AMS, the cache is cleared.

Starting and Stopping the Agent

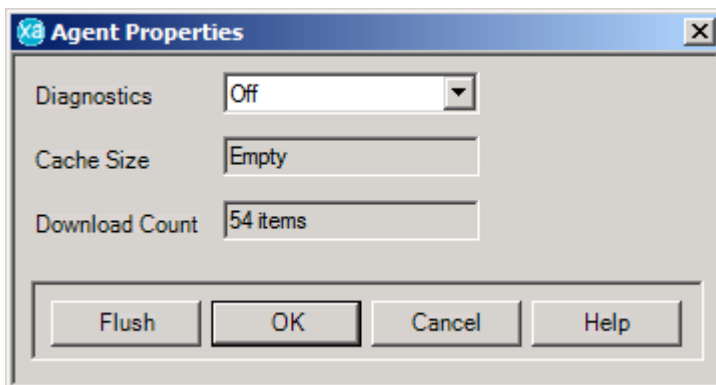
1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Agent | Start**.

You can the stop an agent in the same way by selecting **Agent | Stop** from the context menu.

Warning: If you decide to **STOP** an agent, then any sessions initiated during the stop period will not be logged.

Agent Properties

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Agent | Properties....**



➤ **Diagnostics**

This setting enables diagnostic logging of the agent services. This should be set to **Off** unless otherwise instructed by activAeon XA Technical Support.

➤ **Cache Size**

Displays the number of items currently in the agent cache waiting to be downloaded to the central server.

➤ **Download Count**

Displays the number of items that have been downloaded to the central server.

➤ **Flush**

To download the items in the agent cache before the next update interval, click **Flush**.

Deleting Agents

Agents are deleted by removing the device from the activAeon XA management console, see [Devices](#) (on page 34).

Note: It is recommended that you **do not** stop the agent prior to deleting the device.

Data Transfer

The agent monitors the use of the specified programs and captures all licensing information relating to that computer.

This information is stored in a cache and then transferred via the ACS to the AMS at the specified update interval. For information on the location of the agent and cache and the specified update interval, see [Device Input Information](#) (on page 36).

Query Cache

If you wish to check the current number of items held in a cache, then you can do this by running a query.

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Agent | Query**.

This gives the number of items currently held in the cache.

Flush Cache

If you wish to download the cache, before the next update interval, then you can do this by flushing out the cache.

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Agent | Flush**.

Refresh Agent

If you wish to update the device details displayed in the user interface, you can do this by refreshing the device.

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Locate the appropriate device in the right hand pane.
4. Right click the device and select **Refresh**.

Desktop Applications

activAeon XA enables you to monitor application usage on devices. activAeon XA installs an agent program on the device, which logs an event each time someone **Logs On** or **Off** and **Opens** or **Closes** an application that is being monitored on the device.

Working With Applications

Applications are created and setup under the **Products** node.

The **Products** node is used to add further applications and application groups to the list. These will not be submitted for invoicing under SPLA, but can be monitored to gain information about usage.

The applications are added in a hierarchy as follows.

Publishers

Publishers provide a mechanism for you to group applications and suites.

Applications

Applications are individual programs or packages. These can be added to a publisher and then selected to be copied into a **suite**.

Suites

Suites are groups of applications (programs or packages), which are commonly loaded together on your devices and need to be monitored as a unit. This may include a specific group of Microsoft products or a specific set of programs for a company or office. The advantage of a suite is that it can be selected as a complete entity, when creating the list of monitored components. This prevents the need to repeatedly copy each individual application for each computer.

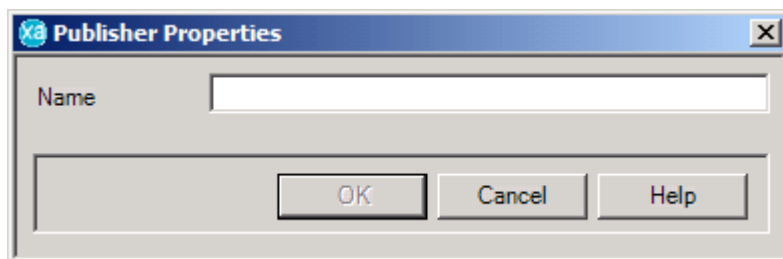
Publishers

Publishers are added under the **Products** node.

Note: Publishers cannot be copied, as a complete entity, for monitoring on a device.

Creating a Publisher

1. Right click the **Products** node and select **Create Publisher...**

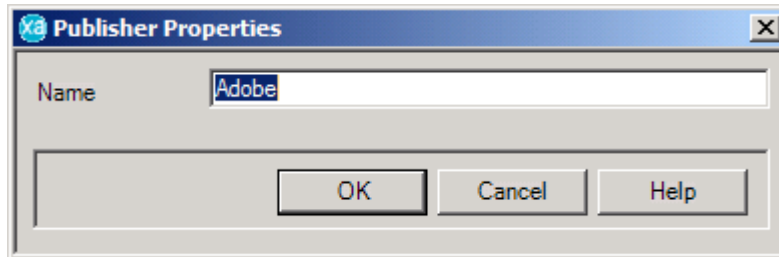


2. Enter the **Name** of the publisher.
3. Click **OK**.

The new publisher will now be listed under the **Products** node.

Renaming Publishers

1. Right click the **Products** node.
2. Right click the appropriate publisher and select **Properties**.



3. Enter the new **Name** for the publisher.
4. Click **OK**.

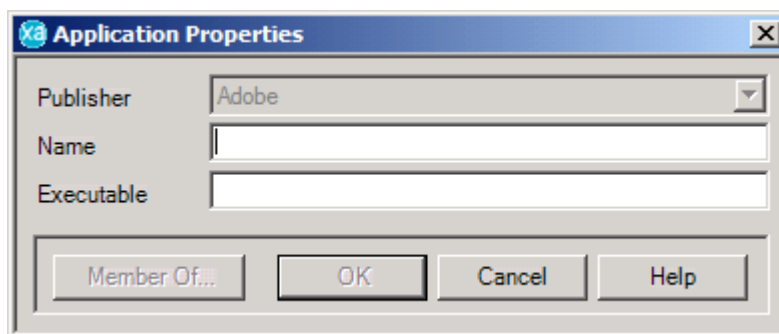
Warning: Only those publishers which have been added manually can be amended.

Applications

Applications are added to publishers under the **Products** node. Once created they can also be copied into suites.

Adding an Application

1. Expand the **Products** node.
2. Right click the appropriate publisher and select **Create Application...**

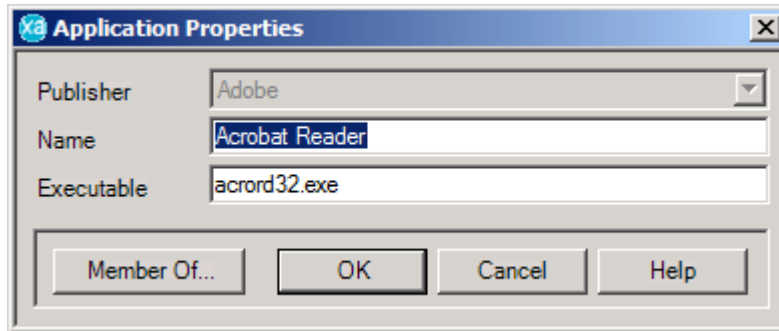


3. Enter the **Name** of the application, e.g. Adobe Acrobat.
4. Enter the **Executable** e.g. acro32.exe.
5. Click **OK**.

Note: The **Member of...** button is disabled when a new application is added. This option can be accessed from the application's **Properties** dialog.

Editing an Application

1. Expand the **Products** node.
2. Locate the appropriate publisher in the tree.
3. Locate the appropriate application in the right hand pane.
4. Right click the application and select **Properties....**



5. The **Member of** button is used to provide a list showing which suites the application has been assigned to. For information on how to add an application to a suite, see suites (on page 57).
6. Make any necessary changes and click **OK**.

Renaming an Application

1. Expand the **Products** node.
2. Locate the appropriate publisher in the tree.
3. Locate the appropriate application in the right hand pane.
4. Right click the application and select **Properties....**
5. Enter the new **Name** for the application.
6. Click **OK**.

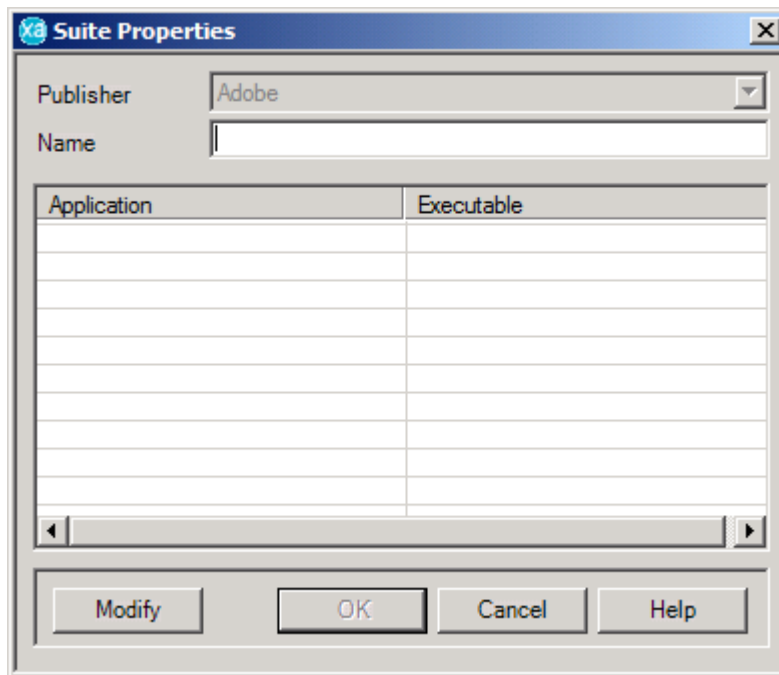
Suites

Suites are added to publishers under the **Products** node.

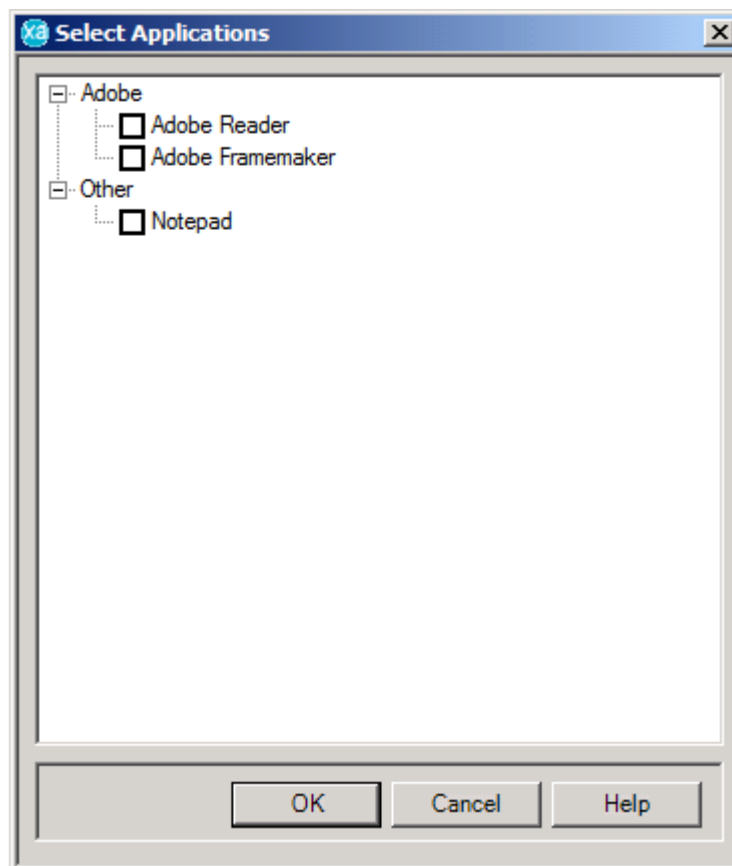
Creating a Suite

1. Expand the **Products** node.

2. Right click the appropriate publisher and select **Create Suite...**



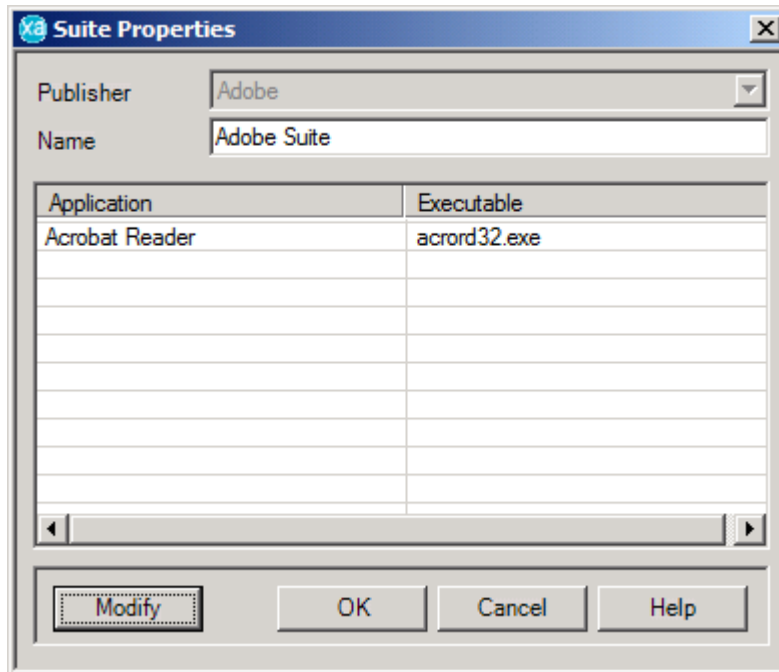
3. Enter the **Name** of the suite, e.g. Adobe Suite.
4. Click **Modify**. This will open a window displaying the full tree of current publishers and applications.



5. Tick the applications you wish to add to the suite and then click **OK**.
6. Click **OK** to finish.

Editing a Suite

1. Expand the **Products** node.
2. Locate the appropriate publisher in the tree.
3. Locate the appropriate suite in the right hand pane.
4. Right click the appropriate suite and select **Properties...**



5. You can now **Modify** the applications assigned to the suite as before, click **OK** to save the changes.

Renaming Suites

1. Expand the **Products** node.
2. Locate the appropriate publisher in the tree.
3. Locate the appropriate suite in the right hand pane.
4. Right click the appropriate suite and select **Properties...**
5. Enter the new **Name** for the suite.
6. Click **OK**.

Deployment Groups

Deployment groups provide a mechanism for deploying a group of devices in a single batch. A deployment group contains a set of devices and all of the settings required to deploy those devices. To deploy the devices in a deployment group, the deployment group is **invoked**. This is done by associating the deployment group with a managed device group, into which the devices are added after deployment.

Creating a Deployment Group

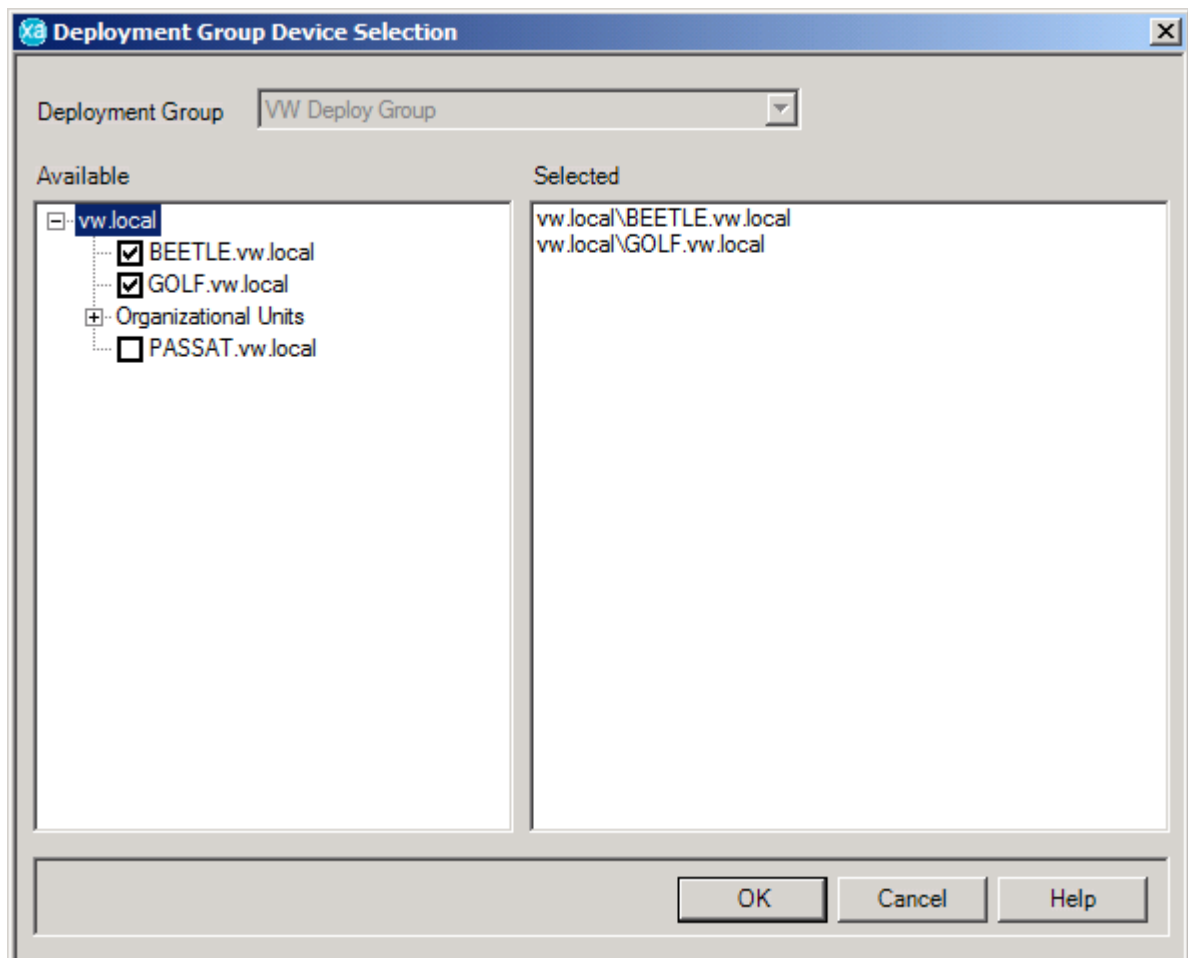
Creating a deployment group involves the following steps:

- Define the set of devices to be deployed.
- Specify the settings required to deploy the devices.

Define Deployment Group Devices

This step enables you to define which devices you want to manage within activAeon XA. When you create a deployment group you typically want to group together devices that have similar properties. For example, all the devices in one domain that require the same set of user credentials; or a group of terminal servers on which you will be monitoring the same set of applications.

1. Right click the **Deployment Groups** node and select **Create Deployment Group...**
2. Enter a **Name** for the deployment group and select **OK**. The **Deployment Group Device Selection** dialog is displayed.

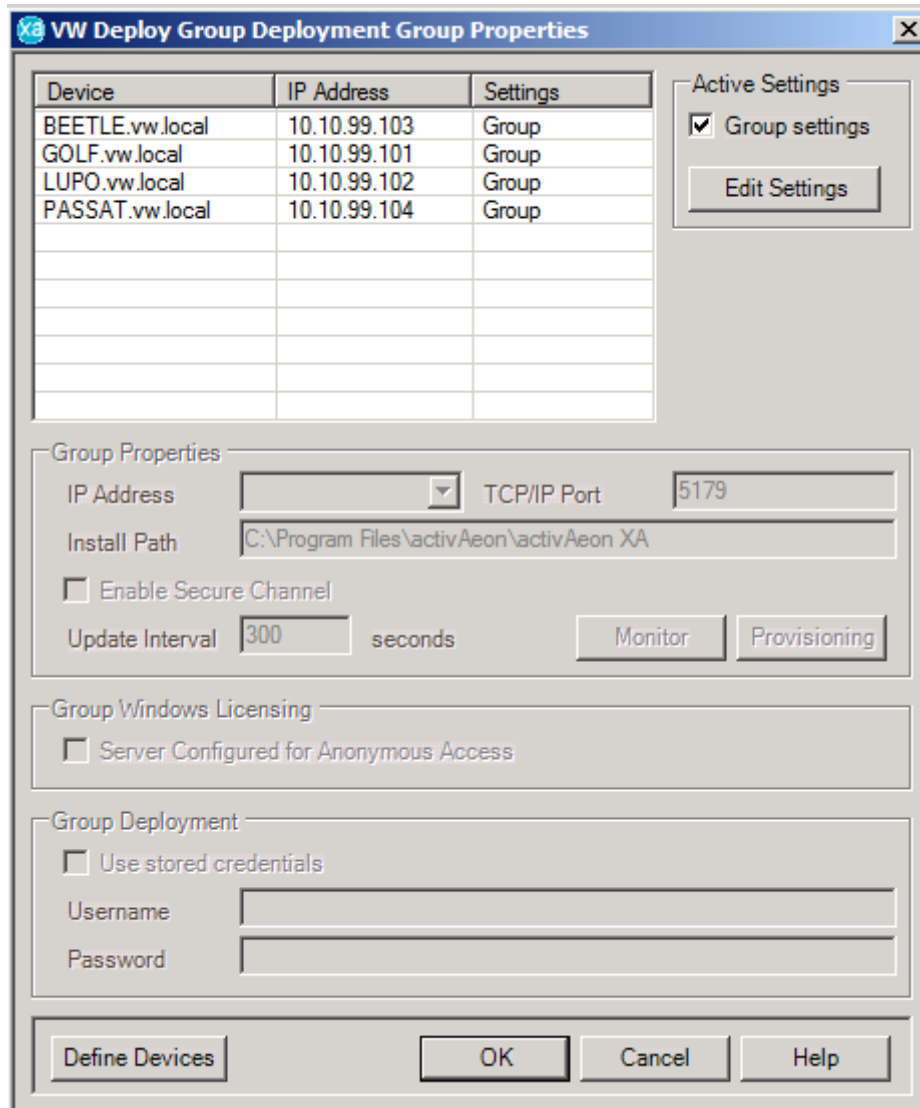


Note: The left hand pane lists all domains managed by activAeon XA and all workgroups that are visible from the activAeon XA management device.

- Expand the domains in the **Available list** and locate the devices that you wish to add to the deployment group. Place a tick next to the appropriate devices and they will appear in the **Selected list**. To select all devices within a domain, right click the domain and select **Select All**.

Note: To remove a device from the deployment group follow the steps above, but in step 3 unchecked the devices that you no longer wish to deploy or if appropriate right click a domain and select **Unselect All**.

- Select **OK**. The **Deployment Group Properties** dialog is displayed.

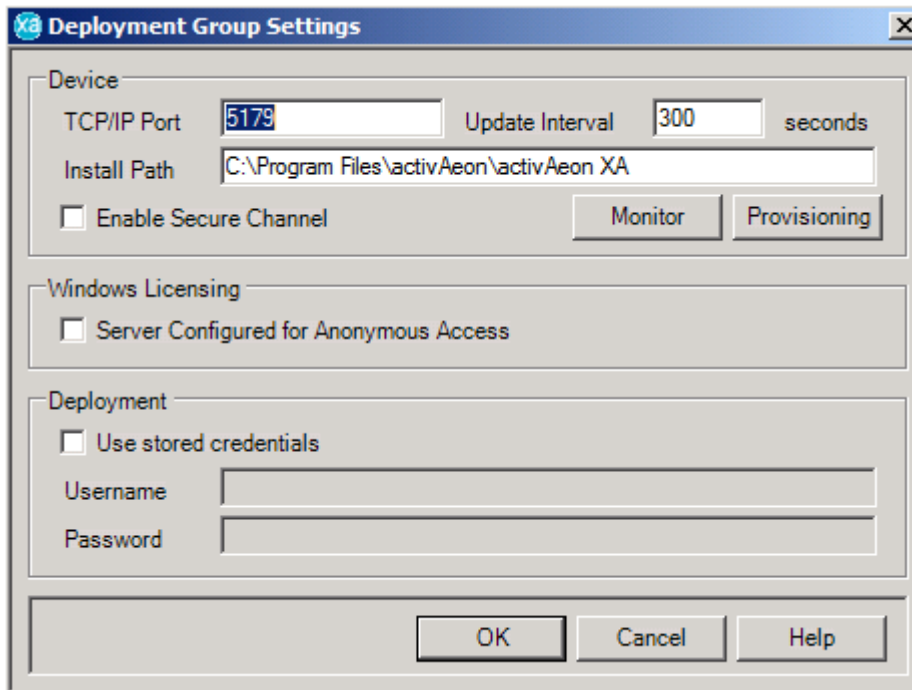


Define Deployment Group Settings

The **Deployment Group Properties** dialog shows the list of devices chosen in the previous steps. It is possible to change this list by clicking the **Define Devices** button.

By default, each device shares the same common settings. To change the settings for an individual device, uncheck the **Group Settings** option, select the relevant device and then make any necessary

changes within the **Deployment Group Properties** dialog. To change the settings for all devices in the group, check the **Group Settings** option and select **Edit Settings**. When you choose to edit the group settings the **Deployment Group Settings** dialog is displayed.



Device

➤ TCP/IP Port

This is the port number on which the ACS listens for information from the AMS. The default is port 5179.

➤ Update Interval

This is the time interval, in seconds, between agent and management server communications. We recommend that the interval is not set to less than 60 seconds to avoid excessive traffic on the system. The default setting is 300 seconds.

➤ Install Path

The path is the location on the device where the services and collected information cache is stored, prior to uploading to the AMS.

➤ **Enable Secure Channel**

Check the **Enable Secure Channel** to encrypt communications between the device and the AMS.

➤ **Monitored Components**

To setup a list of monitored components (on page 46) for the device select **Monitor**.

➤ **Provisioning**

To setup provisioning (on page 48) for the list of monitored components select **Provisioning**.

Windows Licensing

➤ **Server Configured for Anonymous Access**

Indicate whether this device will be accessed by anonymous users. This is then used to determine the correct licensing type for a device.

Deployment

To specify a new set of credentials for the deployment group tick the **Use stored credentials** option.

Enter a **username** and **password** which has the appropriate privileges to deploy to the devices within the deployment group.

Select **OK** to continue. The settings you have just entered now appear in the **Deployment Group Properties** dialog.

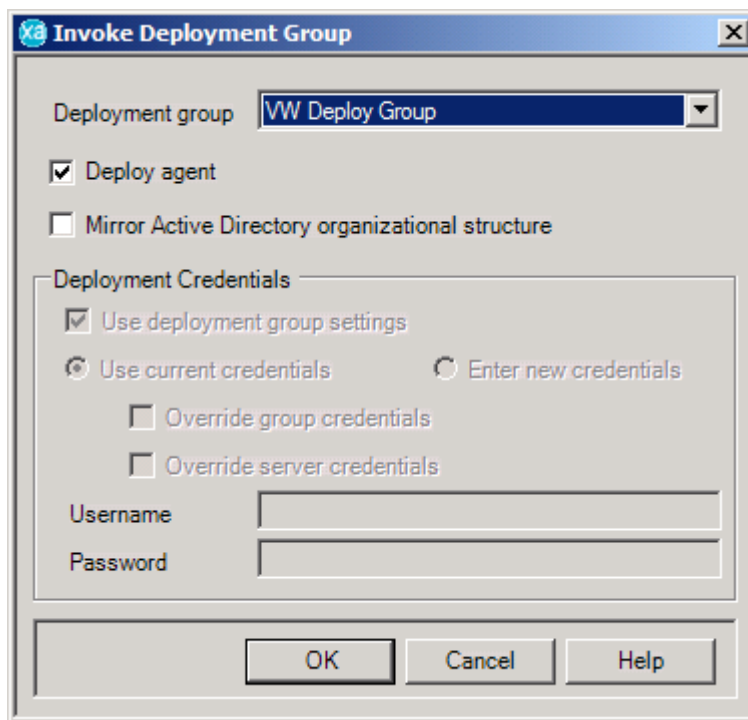
Select **OK** to finish creating your deployment group.

Invoking a Deployment Group

In order to deploy all of the devices within a deployment group, you need to associate the deployment group with a managed device group. When activAeon XA deploys the devices in the deployment group they become members of the managed device group. activAeon XA logs any devices that could not be deployed.

You can re-associate a deployment group with a managed device group and activAeon XA will attempt to deploy any devices that have not already been deployed.

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree.
3. Right click the managed device group and select **Invoke Deployment Group....** The **Invoke Deployment Group** dialog is displayed.



4. Select the appropriate **Deployment Group** from the drop-down list.
5. Check the **Deploy Agent** option to install activAeon XA to all devices within the deployment group.
6. To create your device structure to mirror Active Directory, that is to create a managed device group container for each appropriate Active Directory organizational unit, check the **Mirror Active Directory organizational structure** option. To create a flat device structure with all devices under the one managed device group leave this option unchecked.

7. Choose your **Deployment Credentials**. To use the credentials setup when you created the deployment group check the **Use deployment group settings** option. Otherwise, uncheck this option and specify new credentials.
8. Select **OK** to invoke the deployment group.

It is also possible to invoke a deployment group using drag and drop.

1. Expand the **Deployment Groups** node.
2. Locate the appropriate deployment group in the tree and drag it over the appropriate managed device group and drop it. The **Invoke Deployment Group** dialog is displayed.
3. Follow steps 4-7 above to invoke the group.

Handling Failed Deployments

When you invoke a deployment group it is possible that some devices will not deploy successfully; this may be due to transient connectivity issues, credential issues or other causes. It is possible to remedy this situation in one of two ways:

- You can simply re-invoke the deployment group. This causes activAeon XA to attempt to deploy to any devices that failed to deploy the last time the deployment group was invoked.
- You can remove the devices that failed to deploy from the original deployment group and place them into a separate deployment group. This will allow you to change the settings for those devices before you try to invoke the new deployment group. When you remove the devices that failed to deploy from a deployment group, only the successfully deployed devices will be left in the original deployment group.

Editing a Deployment Group

Updating a Deployment Group

You can update a deployment group at any time. The **Deployment Group Properties** dialog is displayed, which enables you to change the settings for the deployment.

1. Expand the **Deployment Groups** node.
2. Locate the appropriate deployment group in the tree.
3. Right click the deployment group and select **Properties....**
4. Make the necessary changes and select **OK**.

Renaming a Deployment Group

1. Expand the **Deployment Groups** node.
2. Locate the appropriate deployment group in the tree.
3. Right click the deployment group and select **Rename....**
4. Enter a new **Name** and select **OK**.

Deleting a Deployment Group

1. Expand the **Deployment Groups** node.
2. Locate the appropriate deployment group in the tree.
3. Right click the deployment group and select **Delete**.
4. A warning dialog is displayed, select **OK** to delete the deployment group.

Customers

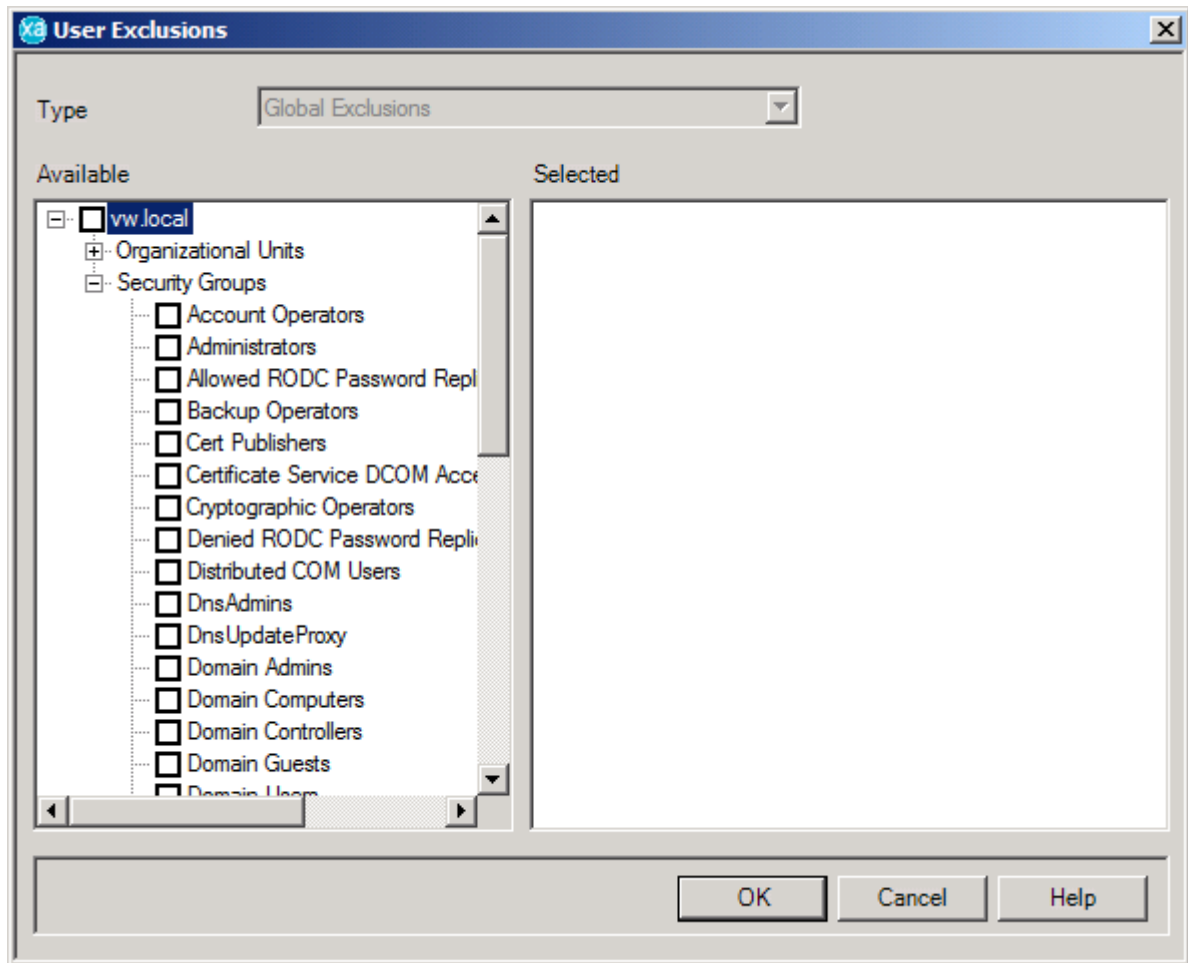
Customers are the main activAeon XA reporting entity. You can use activAeon XA to generate a number of different licensing reports for customers. activAeon XA is installed with a single customer. You can change the name and details of this customer. If you are hosting for a number of different customers and you want to create reports that show the licenses assigned to those customers, then you can create additional customers. You only need to create customers if you want to view customer-specific licenses.

You create customers within a tree structure under the **Customers** node. Customers can contain other customers, so you can build a hierarchy of customers that reflect how you may need to view or report licenses.

Global Exclusions

Global exclusions are used to setup any users that are to be excluded from all reports over your entire activAeon XA setup.

1. Expand the **Customers** node.
2. Right click on the **Global Exclusions** node.
3. Select **Properties...**



4. Expand the appropriate domain(s) in the **Available** list.
5. Check the organizational units or security groups that you wish to exclude. When ticked the Active Directory objects will appear in the **Selected** list. To select all child organizational units or security groups, right click the object and select **Select All**.
6. Click **OK** to apply the settings.

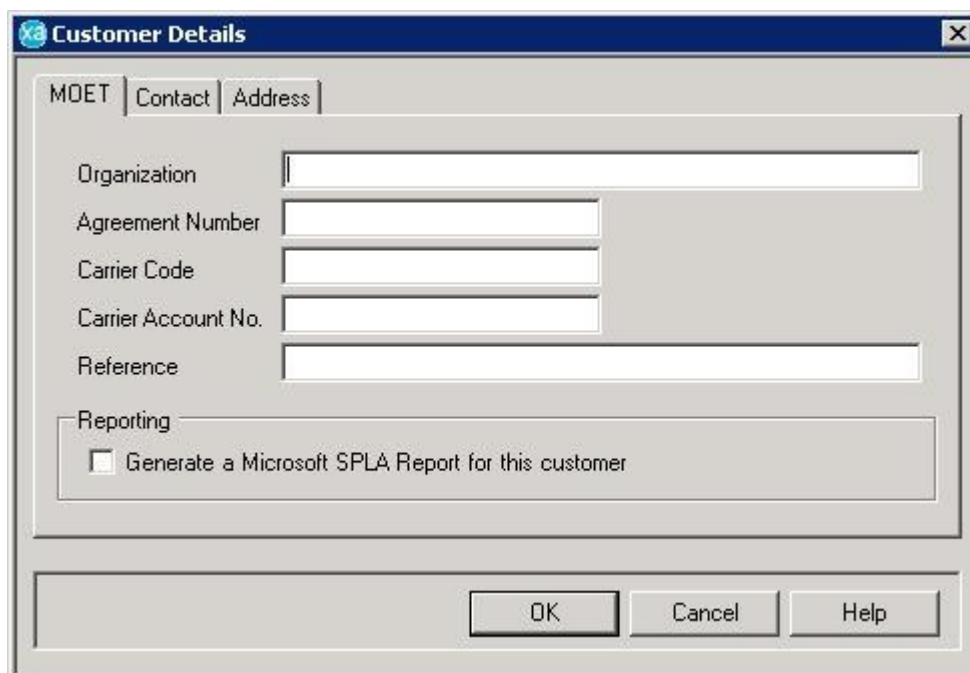
Note: To remove a global exclusion follow the steps above, but in step 5 uncheck the objects that you no longer wish to exclude or if appropriate right click and select **Unselect All**.

Setting Up Further Customers

The customer information provided is used on the relevant license reports. The information given here will not be passed on to any third party.

New Customer

1. Expand the **Customers** node.
2. Right click a customer and select **Create Customer...**
3. **MOET** - Enter your SPLA (Service Provider License Agreement) details as agreed with Microsoft. If you wish to create a separate SPLA report entry for this customer, check the **Reporting** field.



The screenshot shows a dialog box titled "Customer Details" with a close button (X) in the top right corner. The dialog has three tabs: "MOET", "Contact", and "Address". The "MOET" tab is selected. The dialog contains the following fields and controls:

- Organization: A wide text input field.
- Agreement Number: A text input field.
- Carrier Code: A text input field.
- Carrier Account No.: A text input field.
- Reference: A wide text input field.
- Reporting: A section containing a checkbox labeled "Generate a Microsoft SPLA Report for this customer".
- Buttons: "OK", "Cancel", and "Help" buttons are located at the bottom of the dialog.

4. **Contact** - Enter your contact details. The contact information will be used in the event of a query.

The screenshot shows a dialog box titled "Customer Details" with a close button (X) in the top right corner. It has three tabs: "MOET", "Contact", and "Address". The "Contact" tab is selected. The form contains the following fields:

- Contact Name: A single-line text input field.
- Phone Number: A single-line text input field.
- Fax Number: A single-line text input field.
- Email Address: A single-line text input field.
- Correspondence Language: A dropdown menu.

At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

5. **Address** - Enter an appropriate invoicing and billing address.

The screenshot shows the same "Customer Details" dialog box, but with the "Address" tab selected. The form contains the following fields:

- Ship-To Address: A multi-line text input field consisting of four stacked boxes.
- Ship-To City: A single-line text input field.
- State/Province: A single-line text input field.
- Postal Code: A single-line text input field.
- Country Code: A dropdown menu.

At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

6. Click **OK** to save the details.

Customer Details

1. Expand the **Customers** node.
2. Locate the appropriate customer in the tree.

3. Right click the customer and select **Customer Details...**
4. Enter or change the information as above.
5. Click **OK** to save the details.

Delete a Customer

1. Expand the **Customers** node.
2. Locate the appropriate customer in the tree.
3. Right click the customer and select **Delete**.
4. A warning dialog will be displayed, click **OK** to delete the customer.

Note: When a customer is deleted it remains in the interface until the end of the current reporting period. The licenses associated with that customer will remain valid for the current reporting period only. Once the customer has been removed from the interface it is still possible to report on that customer for previous reporting periods.

Restoring a Customer

1. Expand the **Customers** node.
2. Locate the appropriate customer in the tree.
3. Right click the customer and select **Restore**.

Moving a Customer

It is possible to move customers using drag and drop.

1. Expand the **Customers** node.
2. Locate the customer that you wish to move in the tree.
3. Drag the customer to where you wish to move it and then drop it.

Assigning Licenses to a Customer

activAeon XA automatically calculates the licenses that you must report to Microsoft under the terms of SPLA. If you want to create reports for specific customers, or you are required by Microsoft to report a particular customer as a separate MOET entry, then activAeon XA enables you to do so by associating licenses to customers. When you have done this, a customer report contains only the licenses required by that customer.

There are two types of association:

- **User associations.** These are used to assign subscriber access licenses to customers, see User Association (on page 73).
- **Server associations.** These are used to assign processor licenses to customers, see Server Association (on page 74).

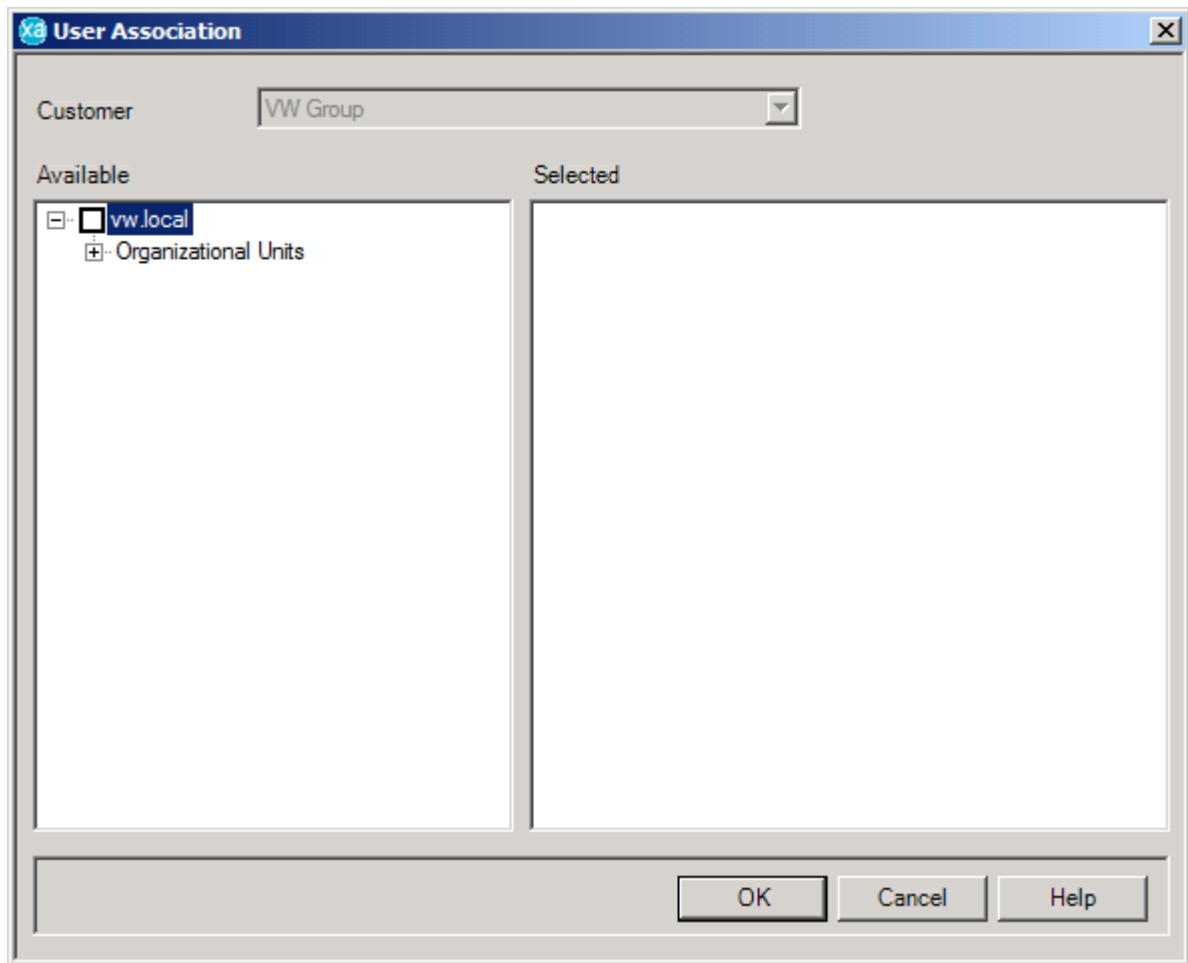
Note: Any users or devices that are not explicitly associated with a customer are associated with the default customer.

User Association

You use user associations to assign subscriber access licenses to customers. You can assign local users and Active Directory domains and organizational units. If you associate a domain with a customer then subscriber access licenses required for all users in the domain are assigned to the customer. If you associate an organizational unit then all users in the organizational unit are assigned to the customer. If you associate local users then the individual users are assigned to the customer. Subscriber access licenses required for users added to an associated domain or organizational unit are automatically assigned to the customer.

1. Expand the **Customers** node.
2. Locate the appropriate customer in the tree.

3. Right click the customer and select **User Association...**



4. Expand the appropriate domain(s) in the **Available** list.
5. Check the organizational units that you wish to associate. When ticked the Active Directory objects will appear in the **Selected** list. To select all child organizational units, right click the object and select **Select All**.
6. Click **OK** to apply the settings.

Note: To remove a user association follow the steps above, but in step 5 uncheck the objects that you no longer wish to associate or if appropriate right click and select **Unselect All**.

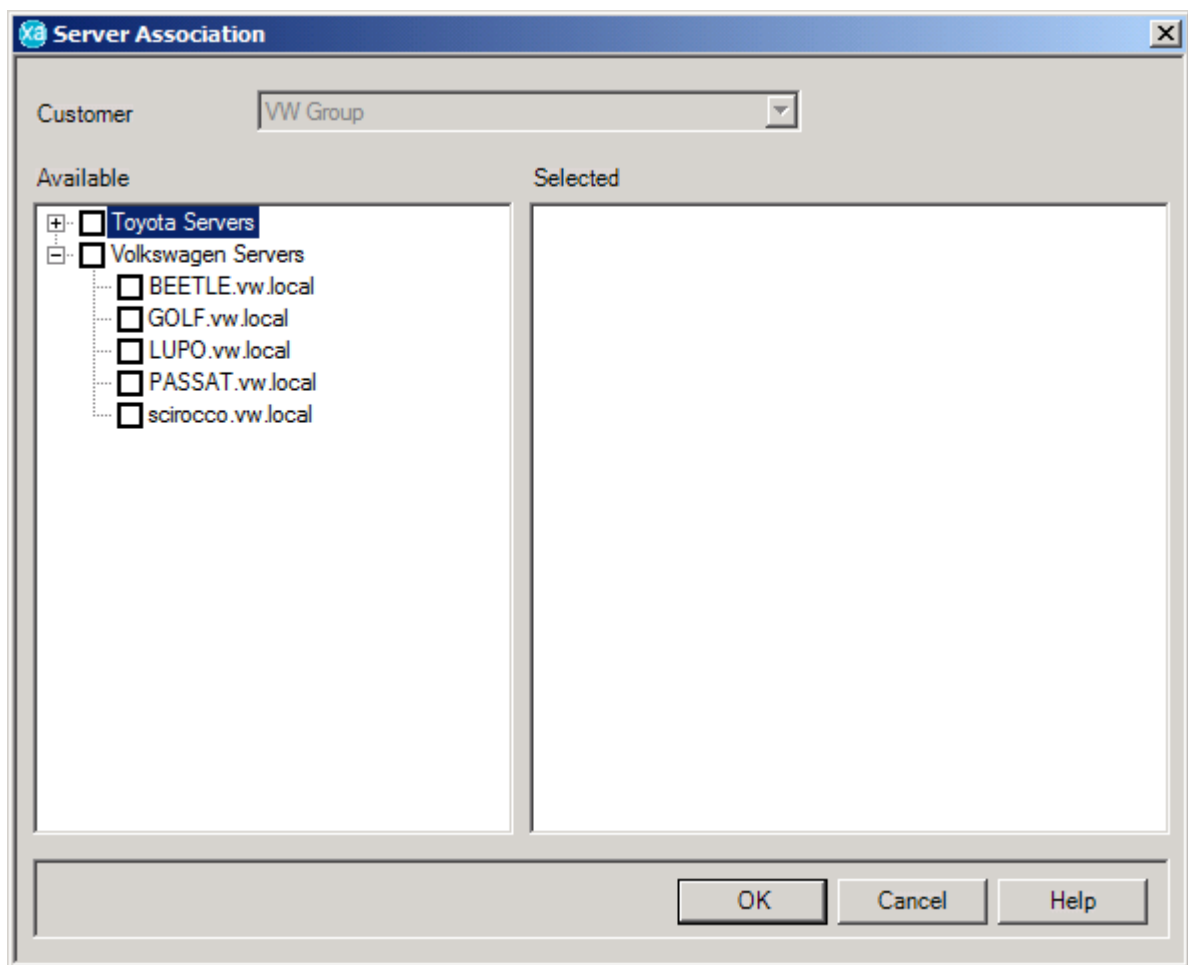
Server Association

You use server associations to assign processor licenses to customers. You can assign an individual device or managed device group. If you assign a managed device group then processor licenses required for all devices in that group are assigned to the customer. Processor licenses for devices added to the managed device group are automatically assigned to the customer; processor licenses for devices removed from the managed device group are automatically unassigned from the customer.

A device can only be associated with one customer; a managed device group can only be associated with a customer if none of its devices and none of its sub-groups are associated with a different customer.

activAeon XA reports licenses required for all devices to which an agent has been deployed. If a device or managed device group is deleted, then the licenses required for the device or devices in the managed device group are reported for the current and past reporting periods, but not future reporting periods. The device or managed device group is displayed in the user interface until the end of the reporting period.

1. Expand the **Customers** node.
2. Locate the appropriate customer in the tree.
3. Right click the customer and select **Server Association...**



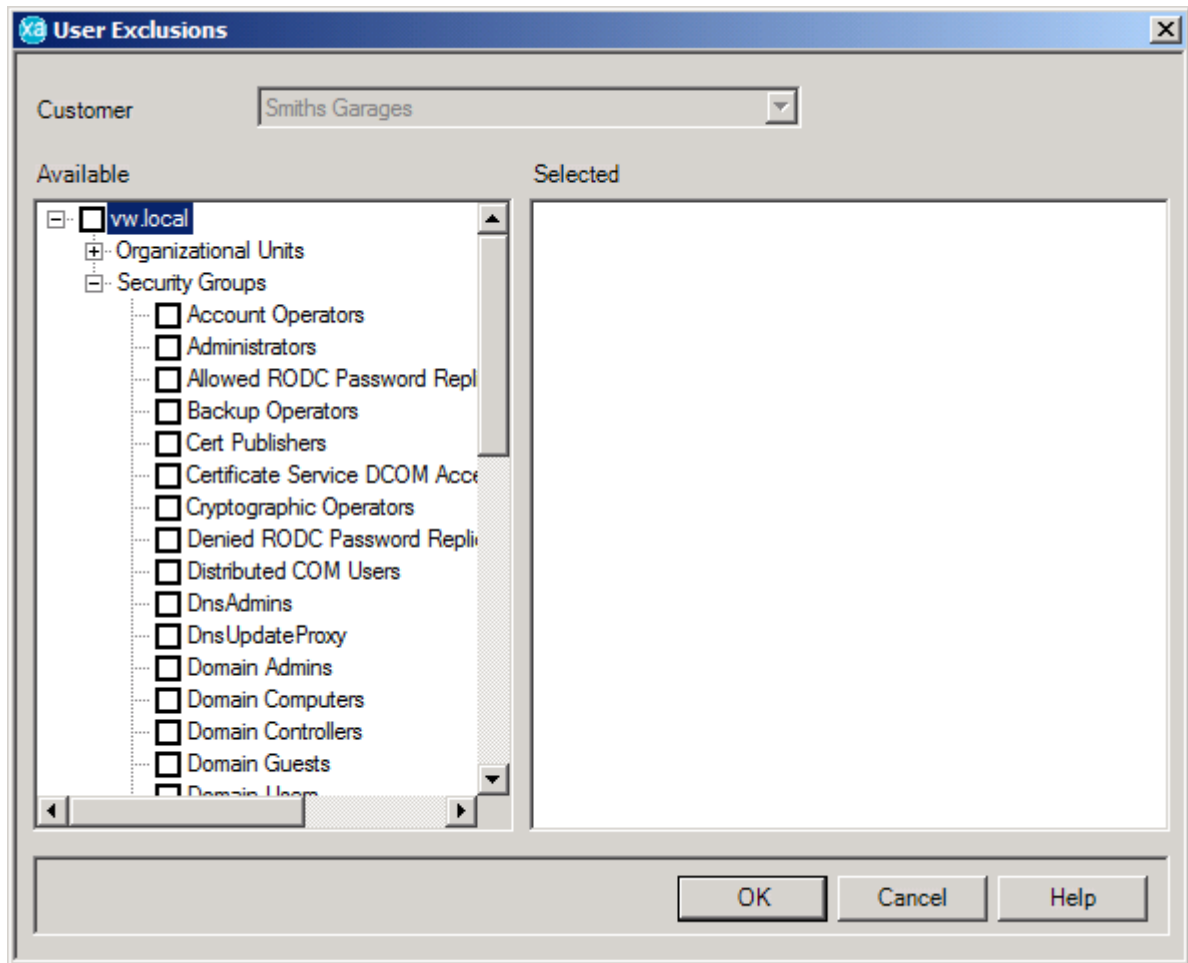
4. Expand the appropriate managed device group(s) in the **Available** list.
5. Check the devices and/or managed device groups that you wish to associate. When ticked the objects will appear in the **Selected** list. To select all child devices or managed device groups, right click the object and select **Select All**.
6. Click **OK** to apply the settings.

Note: To remove a server association follow the steps above, but in step 5 uncheck the objects that you no longer wish to associate or if appropriate right click and select **Unselect All**.

Exclusions

Exclusions can also be setup at the customer level. Exclusions setup here will only apply to the current customer, the exclusions will not apply to any of its sub-customers.

1. Expand the **Customers** node.
2. Locate the appropriate customer in the tree.
3. Right click the customer and select **Exclusions...**



4. Expand the appropriate domain(s) in the **Available** list.
5. Check the Organizational Units and/or Security Groups that you wish to exclude. When ticked the Active Directory objects will appear in the **Selected** list. To select all child organizational units and/or security groups, right click the **Organizational Units**, the **Security Groups** node or an individual object and select **Select All**.
6. Click **OK** to apply the settings.

Note: To remove an exclusion follow the steps above, but in step 5 uncheck the objects that you no longer wish to exclude or if appropriate right click and select **Unselect All**.

Exchange

activAeon XA can be used to submit licensing reports on any of the following forms of Exchange:

1. Hosted Exchange
2. Exchange 2000/2003/2007/2010

The setup wizard can be accessed via the context menu of a managed domain under [Microsoft Exchange | Microsoft Exchange Settings...](#)

Exchange Setup

Note: The following steps are only required for Exchange Server 2000, 2003 or 2007, if you have Exchange Server 2010 installed this will be automatically detected and licensed.

This section is used to specify your Exchange configuration for a domain.

1. Select the **Domains** node.
2. Locate the appropriate domain in the right hand pane.
3. Right click the domain and select **Microsoft Exchange | Microsoft Exchange Settings...**

If you offer an Exchange service check the **Microsoft Exchange Installed** option and then go on to specify the version of Exchange you offer.



Hosted Exchange

activAeon XA supports the standard Microsoft implementation for Hosted Exchange, i.e. HMC 3.5 or 4.0. If you offer such a Hosted Exchange service, check the **Microsoft Hosted Exchange with HMC 3.5/4.0** option and then click **OK**.

You must now go on to provide further information about your Hosted Exchange setup, see Hosted Exchange Database Settings (on page 80) and Hosted Exchange Service Plans (on page 82).

Standard Exchange

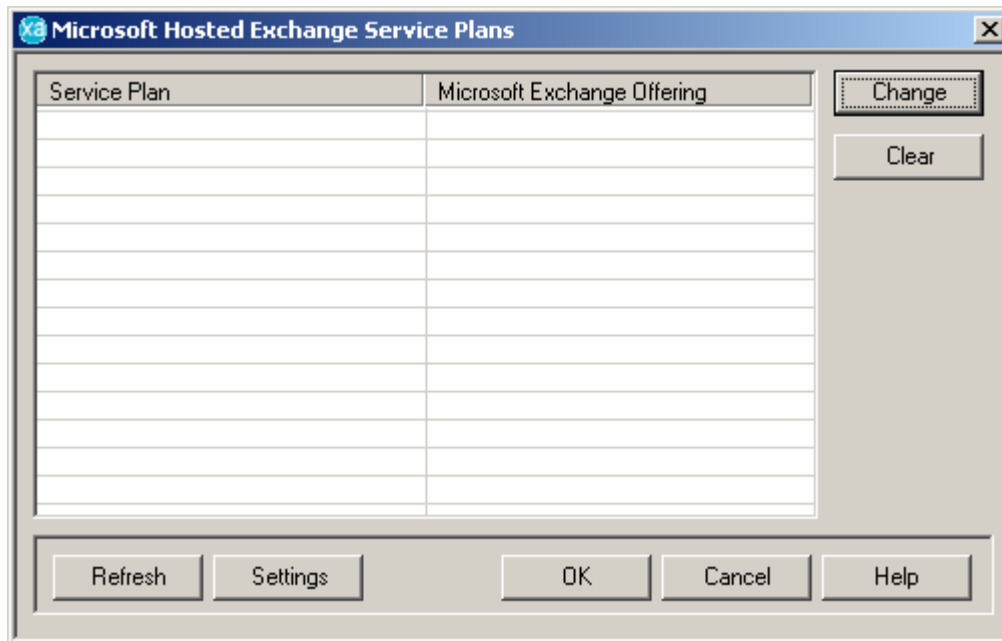
If you are not operating a Hosted Exchange environment, check the **Microsoft Exchange** option and then click **OK**.

Once you have completed the Exchange setup you must map Active Directory security groups and organizational units using **Microsoft Exchange | Active Directory Microsoft Exchange User Mappings...** from the context menu of the appropriate domain, see Exchange Mapping (on page 84).

Hosted Exchange Database Settings

This section is used to determine the database details of your Hosted Exchange deployment.

1. Select the **Domains** node.
2. In the right hand pane, right click the appropriate domain and section **Microsoft Exchange | Microsoft Hosted Exchange Service Plans...**
3. The **Microsoft Hosted Exchange Service Plans** dialog is displayed.



4. Click **Settings**, the **Microsoft Hosted Exchange Database Settings** dialog is displayed.



Server

Enter the name of the SQL Server on which the Hosted Exchange database is stored.

Database

Enter the name of the Hosted Exchange database. The default name is "HECustomerDB" for HMC 3.5 or "PlanManager" for HMC 4.0.

Authentication Type

Select the authentication type and specify credentials.

➤ Windows

Select to use **Trusted Connection** or specify an appropriate Windows username and password in the **Authentication Credentials** section, this option only applies if the SQL database is local to the hosted exchange installation.

➤ SQL Server

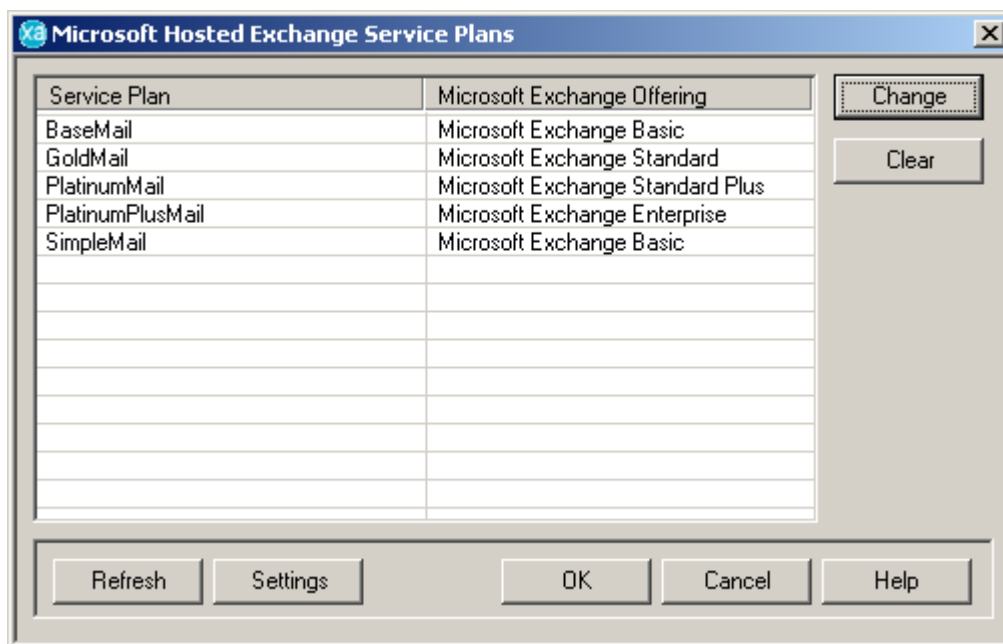
Specify an appropriate SQL username and password in the **Authentication Credentials** section.

Click **Verify** to check that the information provided is correct and then click **OK** to confirm the settings.

Hosted Exchange Service Plans

This section is used to link the various Hosted Exchange service plans configured within your environment with the associated Microsoft products reported under SPLA.

1. Select the **Domains** node.
2. In the right hand pane, right click the appropriate domain and section **Microsoft Exchange | Microsoft Hosted Exchange Service Plans...**



The service plans configured within your Hosted Exchange environment appear in the left hand column. Standard service plans are:

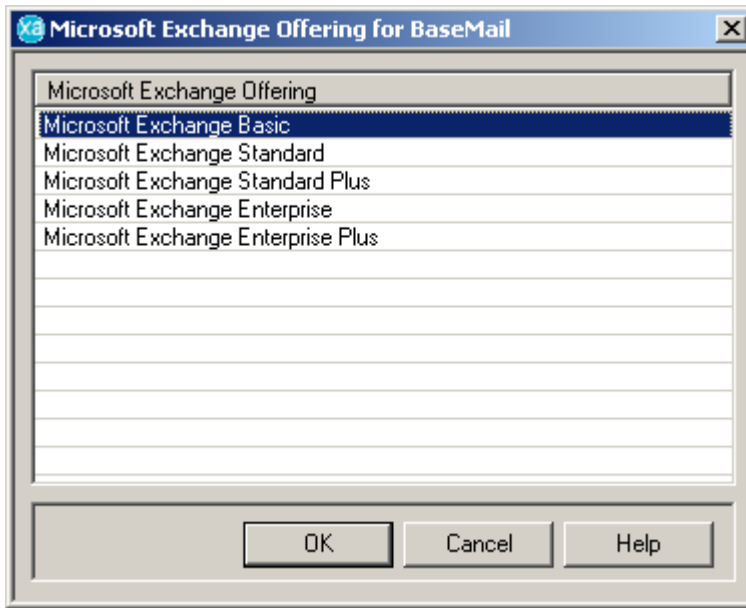
1. Basemail
2. Goldmail
3. Platinummail
4. Platinumplusmail

Other company specific plans will also appear.

To link the plans

1. Highlight the service plan you wish to link.

2. Click **Change** and the **Microsoft Exchange Offering** dialog is displayed.



3. Select the corresponding Microsoft product.
4. Click **OK**.

Repeat this process for all plans.

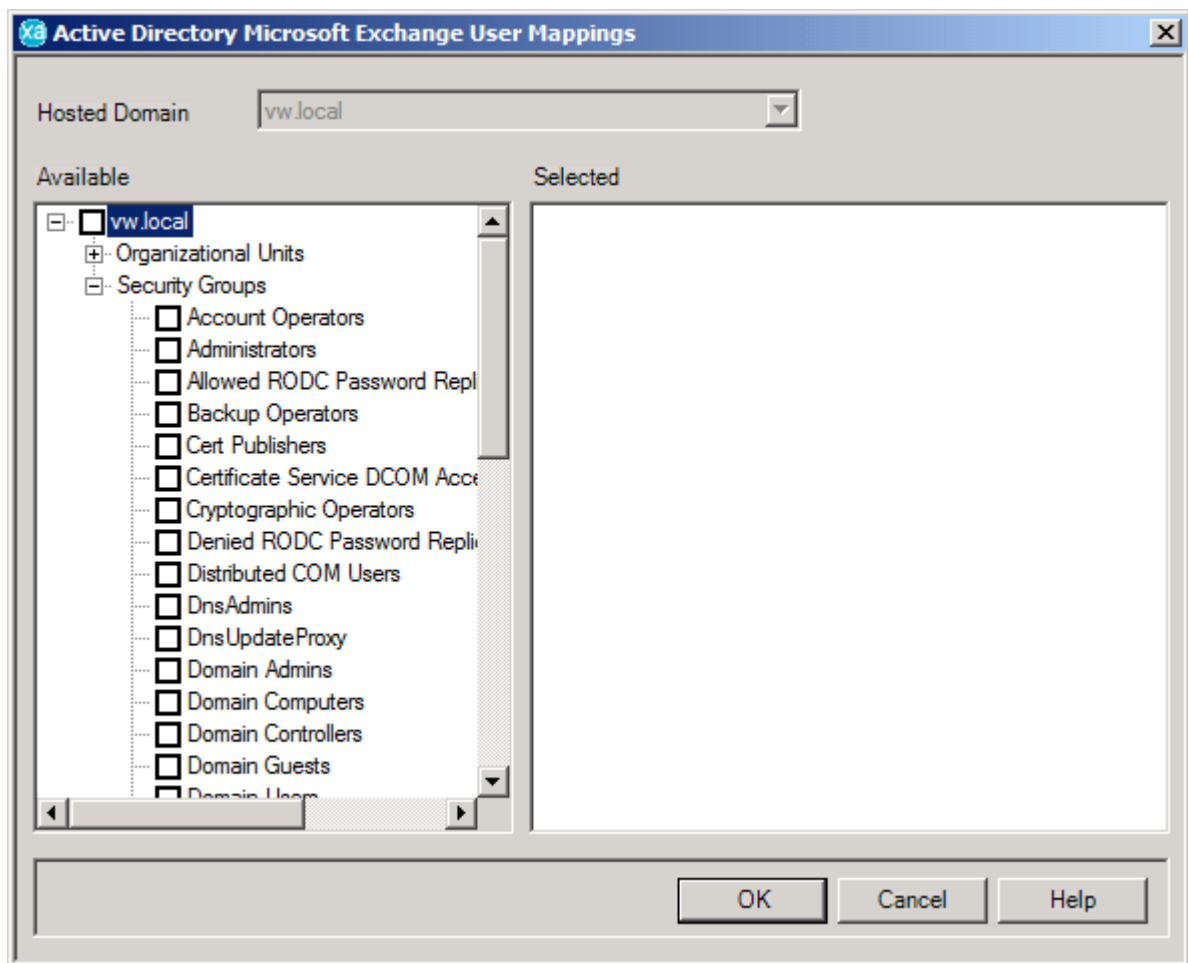
Click on **OK** to confirm the settings.

Exchange Mapping

Exchange mapping is used to link objects in Active Directory. activAeon XA will then use these mappings at report time to calculate your Exchange licensing requirements.

Mapping Active Directory Objects

1. Select the **Domains** node.
2. In the right hand pane, right click the appropriate domains and select **Microsoft Exchange | Active Directory Microsoft Exchange User Mappings...**



3. Expand the domain Active Directory object.
4. Select either the **Organizational Units** or **Security Groups** option.
5. Check each Active Directory object you want to map in the **Available** list. The mappings selected are then displayed in the **Selected** list. To select all child organizational units, right click the object and select **Select All**.
6. Click **OK** to finish.

Note: To remove a mapping follow the steps above, but in step 5 uncheck the objects that you no longer wish to map or if appropriate right click and select **Unselect All**.

Central Management Service (CMS)

The CMS can be started and stopped from within activAeon XA.

If the CMS is stopped then it is unable to collect any data from the deployed agents. This information is not lost. It will merely be held on each agent device until the CMS is running again.

Starting and Stopping the CMS

1. Select the **CMS** menu.
2. Click on the **Start** or **Stop** option as required.

Update

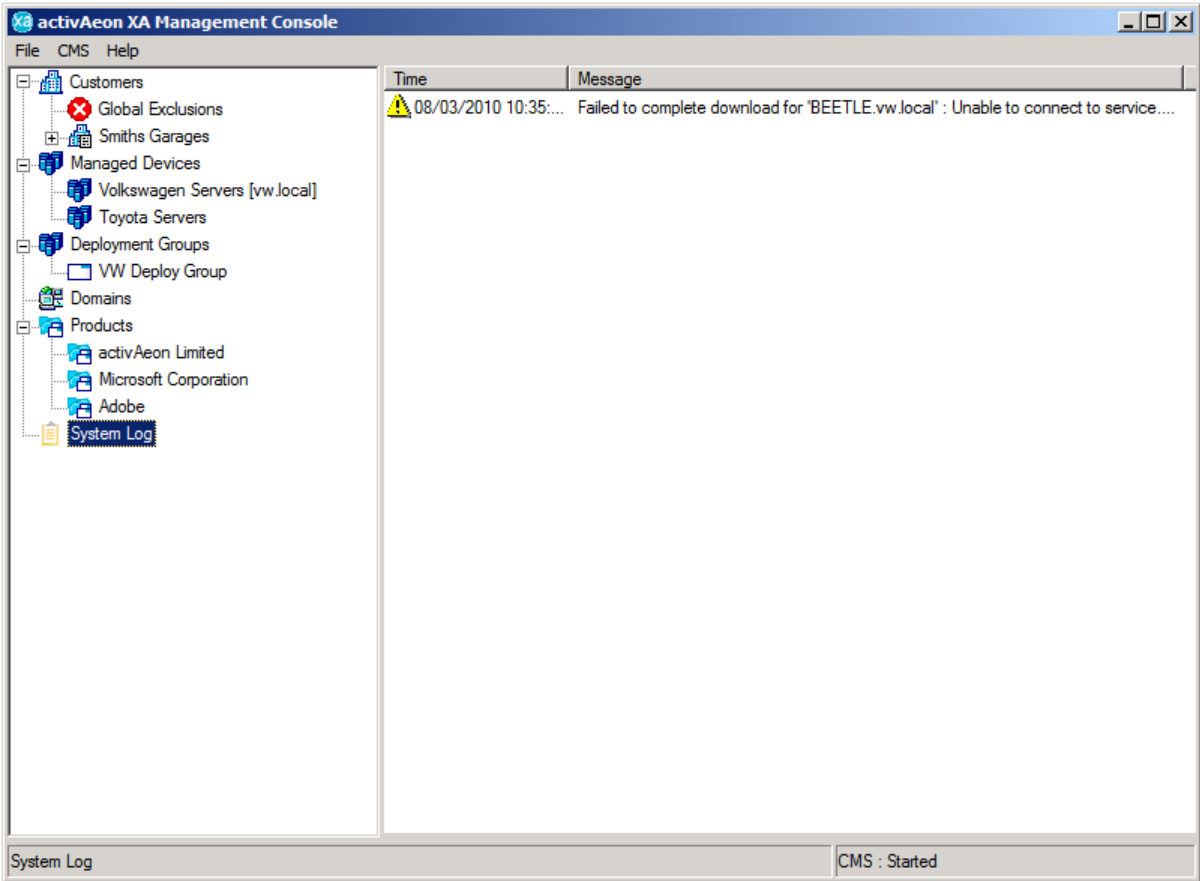
This menu option is used to trigger an Active Directory objects update within the activAeon XA software. The update process commences immediately but may take time to complete.

Diagnostics

The **Diagnostics** setting enables diagnostic logging of the CMS. This should be set to **Off** unless otherwise instructed by activAeon XA Technical Support.

System Log

The **System Log** provides important information about activAeon XA which may indicate that you need to provide additional configuration information. For example, the System Log will notify you if activAeon XA is unable to access any of the databases that it requires to determine licensing information. The System Log also provides useful system diagnostics messages.



activAeon XA System Updates

activAeon XA provides a mechanism to update itself. The updates will make changes to the different components of activAeon XA as and when appropriate.

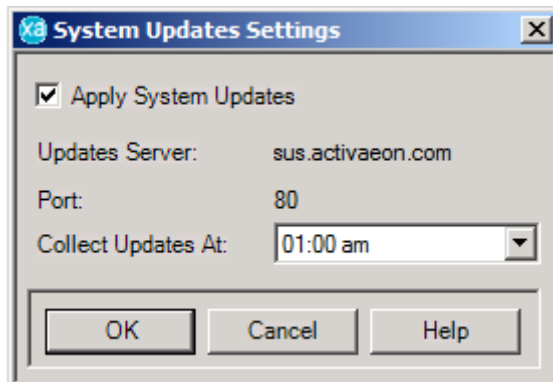
Updates are created on an **Update Server** hosted by activAeon Ltd and are passed down to an **Update Client** which is located on the activAeon XA Management Server. The update client communicates with the update server using a simple http connection (port 80) to check for and download new updates. When an update is available within your environment it will then be passed down to the **Update Agent** on every server that has an activAeon XA agent installed. An update will only be applied to the relevant activAeon XA component.

Updates are applied automatically each day at a defined time, see Update Settings (on page 89), or can be applied manually when required, see System Updates (on page 90).

If for some reason the activAeon XA Management Server cannot connect to the update server, each of the software updates will also be created as a stand-alone package which can be downloaded from the activAeon XA ftp site and then installed from the management server, see Updates Packages (on page 93).

Update Settings

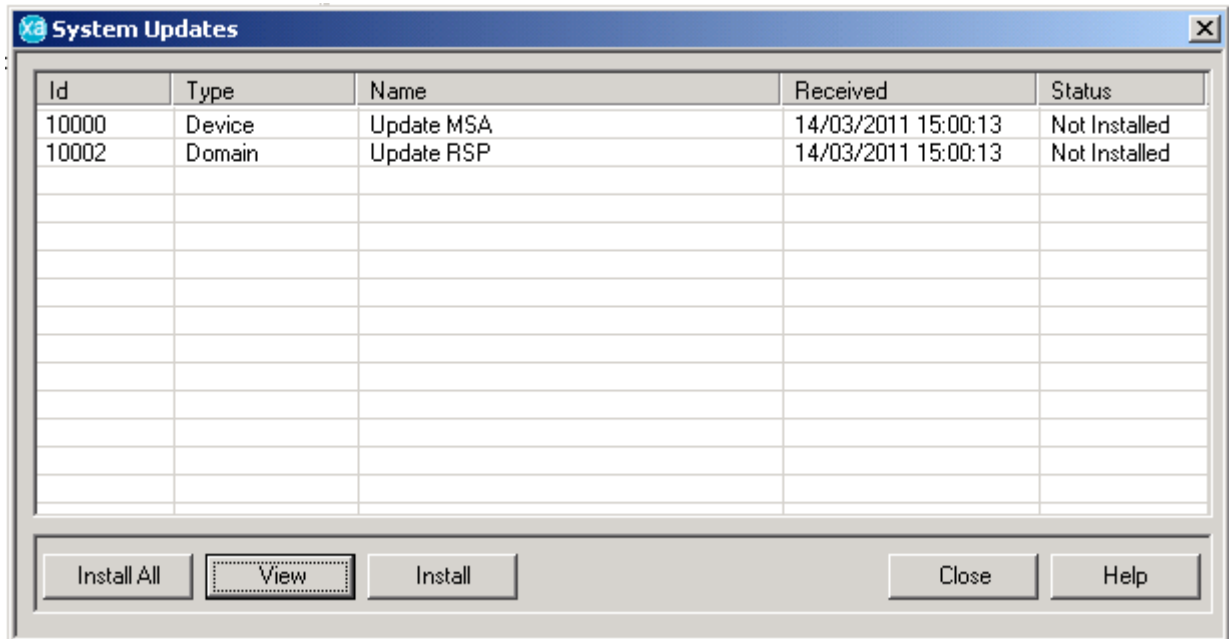
1. Select the **Help** menu.
2. Click on the **System Updates** option.
3. Click on the **Update Settings...** option, the **System Update Settings** dialog is displayed.



4. Complete the dialog as follows:
 - a. **Apply System Updates** - tick this option to install activAeon XA updates automatically when received from the update server. System or console updates are applied immediately upon download, device or domain updates are applied 30 minutes later. If this option is not ticked, updates will be downloaded from the update server but will then need to be installed manually, see System Updates (on page 90).
 - b. **Collect Updates At** - set the time when you want the update client to communicate with the update server to receive updates, the default time is 1.00am.
5. Click **OK** to save the changes.

System Updates

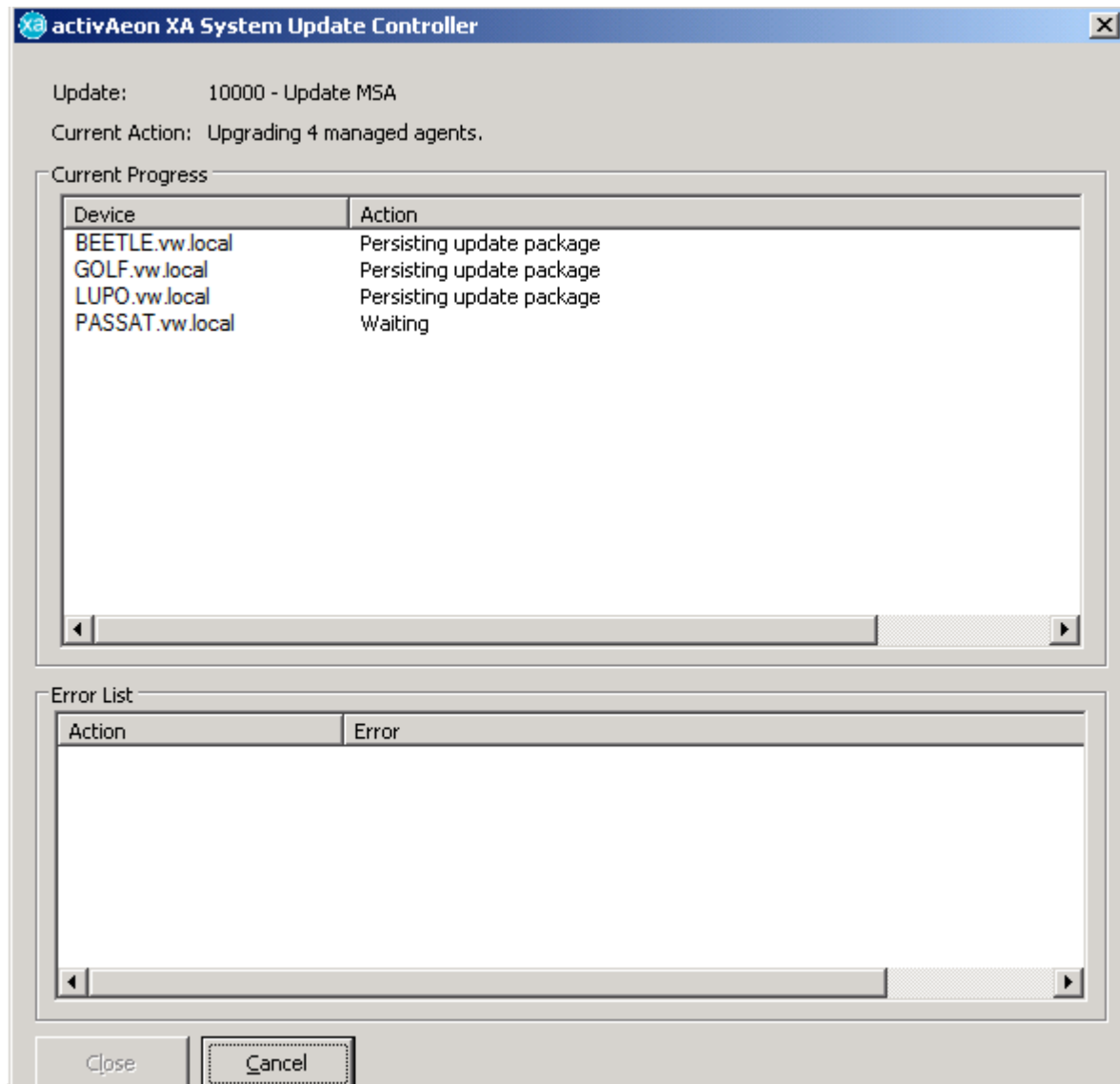
1. Select the **Help** menu.
2. Click on the **System Updates** option.
3. Click on the **Updates...** option. The **System Updates** dialog is displayed, showing a summary of the activAeon XA software updates that have been downloaded from the update server.



Update Properties

1. Select the appropriate update from the list.

The **activAeon XA System Update Controller** dialog will be displayed.



The update will be installed, if the update controller encounters any problems during the update the errors will be displayed in the **Error List**. These errors will need to be corrected before the update can be re-tried.

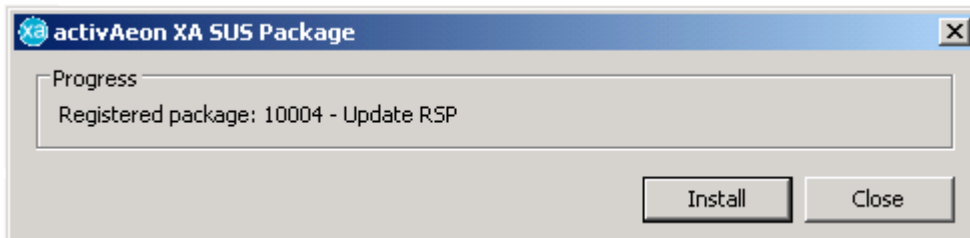
3. Click **Close** when the update is complete.

Update Packages

activAeon XA software updates are also available as stand-alone packages. These are created on the [Update Server](#) and are to be used if the [activAeon XA Management Server](#) cannot communicate with the update server directly.

When a software update becomes available the package will be placed on the activAeon XA FTP site. You will then be notified by email that such an update exists and will be prompted to download the package. The update package can be downloaded to any server but must be installed from the management server.

Once downloaded and placed on the management server, run the package executable to extract the update. The [activAeon XA SUS Package](#) dialog is displayed.



Once extracted the hoster can choose to install the update immediately by selecting [Install](#), or can [Close](#) this dialog and use the install functionality of the activAeon XA user interface, see System Updates (on page 90).

Reports

Reports are accessed via the context menu of a customer or a managed device group. Right click to open the context menu and then select **Reports**.

activAeon XA provides the following licensing reports for a customer:

- SPLA Report (on page 97)
- License Usage Report (on page 98)
- Customer License Report (on page 99)
- Microsoft Exchange License Report (on page 100)
- Microsoft Windows License Report (on page 101)
- Microsoft Server Products License Report (on page 102)
- Microsoft Terminal Server License Report (on page 103)
- Microsoft Desktop Application License Report (on page 104)
- activAeon XA also provides the following reports for a managed device group or device:
- Terminal Server Session Activity Report (on page 105)
- Desktop Application Usage Report (on page 107)

Note: It is not possible to print any of the reports directly from your web browser, please use the appropriate print options provided with each report.

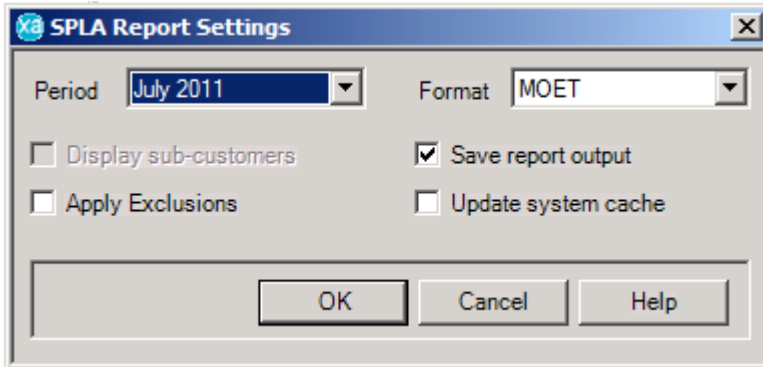
Before running an activAeon XA report it may be necessary to adjust the security settings of Internet Explorer in order to view the report output correctly.

1. Set Internet Explorer as the default web browser.
2. In Internet Explorer, select **Tools | Internet Options...**
3. Click on the **Advanced** tab, in the **Security** section of the list, check the box to **Allow active content to run in files on My Computer** and then click on the **OK** button. Alternatively, if this option is not available, click on the **Security** tab, click on the **Custom Level...** button, in the **Scripting** section select the **Enable** option for **Active Scripting** and then click on the **OK** button. Click **OK** to finish.

Report Settings for Licensing Reports

Before running a report you must select the customer for which you wish to run the report. Data will then be collected from any devices associated with that customer and any sub-customers.

1. Expand the **Customers** node.
2. Locate the appropriate customer in the tree.
3. Right click and select **Reports**.
4. Select the report you wish to run, the **Report Settings** dialog is displayed.



Reporting Period

Select the period for which you wish to run the report, this will default to the current reporting period.

Format

Select the appropriate output option for the report. The options available will depend on the report selected.

➤ MOET

Microsoft Order Entry Template, only available as an output format for the SPLA report. This option creates a report using the standard MOET template issued by Microsoft.

➤ HTML

This is a dynamic HTML format. It will allow you flexibility in both viewing and searching the data. Information can be sorted on an individual column on most reports. Click on one of the highlighted headings to sort the data in ascending order for that column.

➤ XML

The XML report provides the list of raw data in XML format. This can be read by most browsers and manipulated outside activAeon XA.

Display Sub-customers

Check this option to produce reports for all sub-customers associated with the selected customer as well as a report for the customer itself.

Apply Exclusions

It is possible to exclude users from a report, for example administrative or demo users, see Global Exclusions (on page 69) or Exclusions (on page 77). To apply exclusions to a report check this option.

Save Report Output

It is possible to save the output of a report to file; the report will be saved in [\[InstallDir\]\Reports\Repository](#). To save the report to file check this option, see Saved Reports (on page 110).

Update System Cache

Check this option to update the system cache. The system cache is ordinarily updated automatically each night.

To run the report click **OK**.

SPLA Report

The SPLA report provides licensing information for all Microsoft products configured and reported within activAeon XA.

This report can only be run from the main **Customers** node or from an individual customer for which you have selected to create a separate SPLA entry. A new entry in the report will be created for each customer that you have chosen to generate a separate SPLA report for, see Setting Up Further Customers (on page 70).

Report Formats

- **MOET**

This option creates a report using the standard MOET template issued by Microsoft. In order to use this option you must have Excel installed on the activAeon XA Management Server (AMS) from where the reports are created and run. Once the report has been created, carry out the following steps to prepare the report for submission to Microsoft or your reseller.

1. Check the address details. These have been generated from your customer details.
2. Change the title to **Microsoft Volume Licensing Order Sheet**.
3. Insert a unique **Purchase Order Number**.
4. Remove the disclaimer.
5. Save the file to a different name.

- **HTML**

- **XML**

License Usage Report

This report provides a detailed breakdown of the licensed Microsoft products.

This report can be run from the main [Customers](#) node or from any individual customer. A separate report entry will be created for each appropriate customer detailing their licensing requirements.

Report Formats

- [HTML](#)
- [XML](#)

Customer License Report

This report provides a detailed breakdown of the licensing requirements for a customer.

If the report is run for a customer with sub-customers, use the [Customer](#) drop-down list on the report to view the license requirements for the sub-customers.

The report displays the list of licensing requirements by product in the upper window, with details of the licenses for the selected product in the lower window.

To print out the summary information displayed in the upper window select [Print Summary](#), to print out the full detailed report select [Print All](#).

Report Formats

- [HTML](#)
- [XML](#)

Microsoft Exchange License Report

The Exchange report uses the Hosted Exchange database or Active Directory and the user group mappings to provide details for each Exchange license type.

If the report is run for a customer with sub-customers, use the **Customer** drop-down list on the report to view the license requirements for the sub-customers.

The report displays a list of each license type required in the upper window, with the associated user information for the selected license type in the lower window.

To print out the summary information displayed in the upper window select **Print Summary**, to print out the full detailed report select **Print All**.

Report Formats

- **HTML**
- **XML**

Microsoft Windows License Report

This report provides Microsoft Windows licensing information.

The information provided shows the best value option for processor (PL) and subscriber access (SAL) licensing.

If the report is run for a customer with sub-customers, use the [Customer](#) drop-down list on the report to view the license requirements for the sub-customers.

The report displays a list of each license type required in the upper window, with details of the associated servers (for PL licenses) or users (for SAL licenses) for the selected license type in the lower window.

To print out the summary information displayed in the upper window select [Print Summary](#), to print out the full detailed report select [Print All](#).

Report Formats

- [HTML](#)
- [XML](#)

Microsoft Server Products License Report

This report provides a detailed breakdown of the licensed Microsoft server products. This report does not include desktop applications.

If the report is run for a customer with sub-customers, use the [Customer](#) drop-down list on the report to view the license requirements for the sub-customers.

The report displays a list of each license type required in the upper window, with details of the associated servers (for PL licenses) or users (for SAL licenses) for the selected license type in the lower window.

To print out the summary information displayed in the upper window select [Print Summary](#), to print out the full detailed report select [Print All](#).

Report Formats

- [HTML](#)
- [XML](#)

Microsoft Terminal Server License Report

This report provides information about Microsoft Windows Terminal Server license requirements.

If the report is run for a customer with sub-customers, use the [Customer](#) drop-down list on the report to view the license requirements for the sub-customers.

The report displays a list of licenses required in the upper window, with details of the associated users in the lower window.

To print out the summary information displayed in the upper window select [Print Summary](#), to print out the full detailed report select [Print All](#).

Report Formats

- [HTML](#)
- [XML](#)

Microsoft Desktop Application License Report

The desktop application license report provides a license count for the different Microsoft desktop applications.

If the report is run for a customer with sub-customers, use the **Customer** drop-down list on the report to view the license requirements for the sub-customers.

The report displays a list of each license type required in the upper window, with the associated user information for the selected license type in the lower window.

To print out the summary information displayed in the upper window select **Print Summary**, to print out the full detailed report select **Print All**.

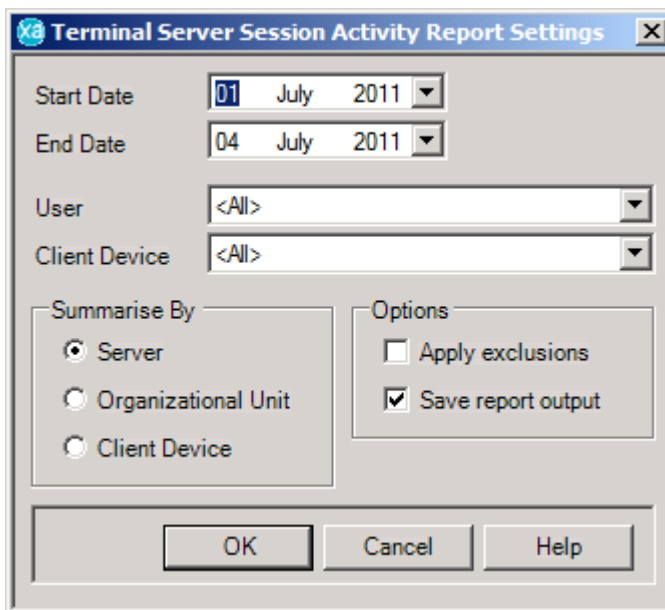
Report Formats

- **HTML**
- **XML**

Terminal Server Session Activity Report

Before running the report you must select the device or managed device group for which you wish to run the report. Data will be collected for any devices associated with a managed device group.

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree, or device in the right hand pane.
3. Right click the managed device group or device and select **Reports**.
4. Select **Terminal Server Session Activity Report**. The **Terminal Server Session Activity Settings** dialog is displayed.



The screenshot shows the 'Terminal Server Session Activity Report Settings' dialog box. It features a title bar with a close button. The main area contains several controls: 'Start Date' and 'End Date' are date pickers set to '01 July 2011' and '04 July 2011' respectively; 'User' and 'Client Device' are dropdown menus both set to '<All>'. Below these are two sections: 'Summarise By' with radio buttons for 'Server' (selected), 'Organizational Unit', and 'Client Device'; and 'Options' with checkboxes for 'Apply exclusions' (unchecked) and 'Save report output' (checked). At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Start Date

Select the start date for the report data.

End Date

Select the end date for the report data.

User

Select the user for which you wish to view the session data, or select **<All>** to run the report for all users.

Client Device

Select the client device for which you wish to view the session data, or select **<All>** to run the report for all devices.

Summarise By

It is possible to organize the report data by server, organizational unit or client device. Select the appropriate option here.

Options

➤ Apply Exclusions

It is possible to exclude users from a report, for example administrative or demo users, see Global Exclusions (on page 69) or Exclusions (on page 77). To apply exclusions to a report check this option.

➤ Save Report Output

It is possible to save the output of a report to file; the report will be saved in [\[InstallDir\]\Reports\Repository](#). To save the report to file check this option, see Saved Reports (on page 110).

To run the report click **OK**.

If the report is run for a managed device group with sub-group(s), use the managed device group drop-down list on the report to view the license requirements for the sub-group(s).

It is then possible to change how the report is summarised by using the **Summary** drop-down list, you can summarise by server, organizational unit, user or client device.

The upper window of the report displays the summarised option information. The lower window displays the individual session information.

To print out the detailed report select **Print View**.

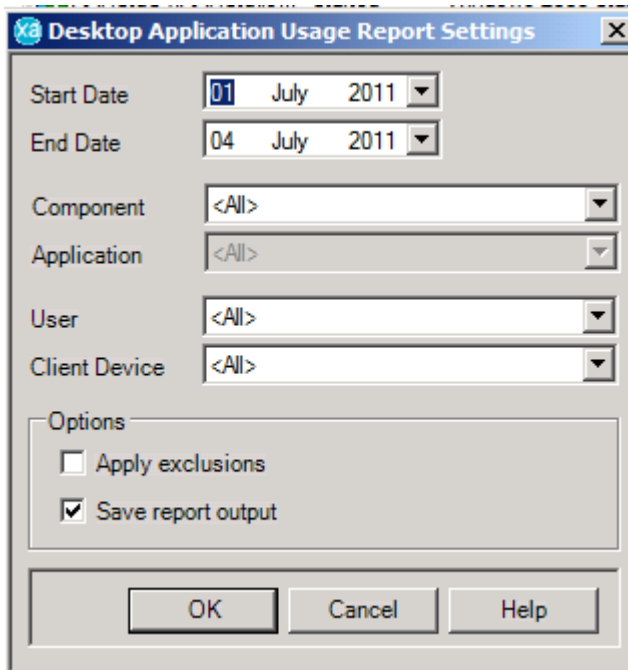
Report Formats

- **HTML**

Desktop Application Usage Report

Before running the report you must select the managed device group or device for which you wish to run the report. Data will be collected for any devices associated with a managed device group.

1. Expand the **Managed Devices** node.
2. Locate the appropriate managed device group in the tree, or device in the right hand pane.
3. Right click the managed device group or device and select **Reports**.
4. Select **Desktop Application Usage Report**. The **Desktop Application Usage Settings** dialog is displayed.



The screenshot shows a dialog box titled "Desktop Application Usage Report Settings". It contains several fields and options:

- Start Date:** A date picker set to 01 July 2011.
- End Date:** A date picker set to 04 July 2011.
- Component:** A dropdown menu set to <All>.
- Application:** A dropdown menu set to <All>.
- User:** A dropdown menu set to <All>.
- Client Device:** A dropdown menu set to <All>.
- Options:** A section containing two checkboxes:
 - Apply exclusions
 - Save report output
- Buttons:** OK, Cancel, and Help buttons at the bottom.

Start Date

Select the start date for the report data.

End Date

Select the end date for the report data.

Component

Select the desktop product for which you wish to view the usage data, or select **<All>** to run the report for all desktop products.

Application

If the component selected above is a suite it is possible to select the individual application for which you wish to view the usage data, or select **<All>** to run the report for all applications in the suite.

User

Select the user for which you wish to view the usage data, or select **<All>** to run the report for all users.

Client Device

Select the client device for which you wish to view the usage data, or select **<All>** to run the report for all devices.

Options

➤ Apply Exclusions

It is possible to exclude users from a report, for example administrative or demo users, see Global Exclusions (on page 69) or Exclusions (on page 77). To apply exclusions to a report check this option.

➤ Save Report Output

It is possible to save the output of a report to file; the report will be saved in **[InstallDir]\Reports\Repository**. To save the report to file check this option, see Saved Reports (on page 110).

To run the report click **OK**.

If the report is run for a managed device group with sub-group(s), use the managed device group drop-down list on the report to view the license requirements for the sub-group(s).

To change how the report is summarised use the **Summary** drop-down list, you can summarise by host or user.

The component for which you chose to run the report is displayed in a drop-down box, if this component is a suite it is then possible to select a sub-component for which to view usage data. If a sub-component is not defined then you will see basic usage data for the suite as a whole, if a sub-component is selected you will see basic usage data for the selected sub-component of the suite only.

The upper window of the report provides summary information. The lower window displays individual usage information based on the report type selected.

To print out the detailed report select [Print View](#).

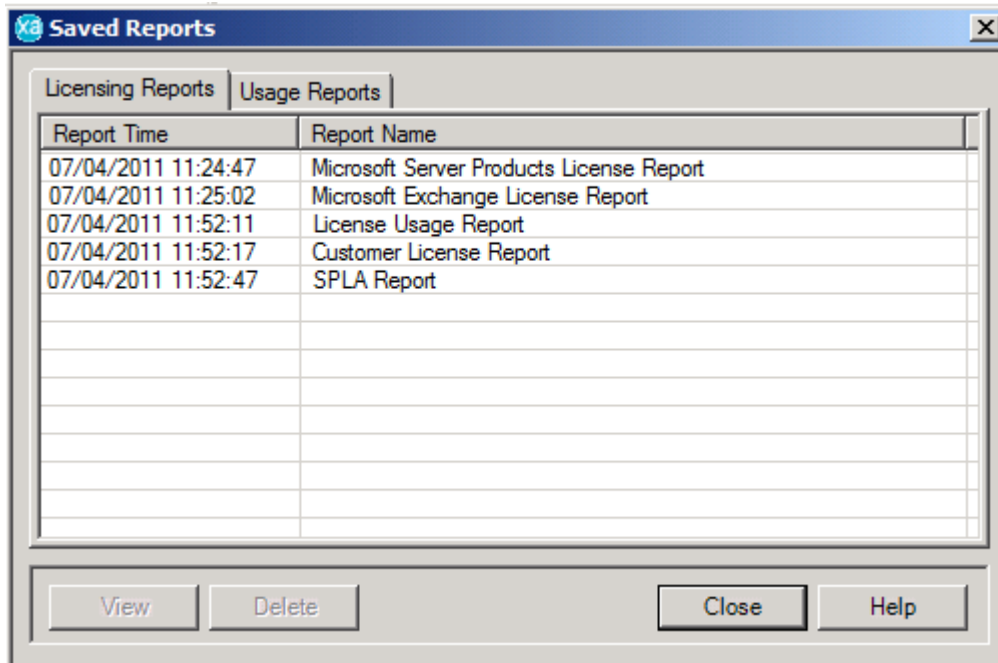
Report Formats

- [HTML](#)

Saved Reports

activAeon XA provides the ability to save reports to an archive directory when they are executed. If you choose the **Save Report Output** option at report runtime, the report will be saved in **[Install Dir]\Reports\Repository**. The reports can also be accessed from with the user interface the following methods:

1. Right click the **Customers** node or the **Managed Devices** node, select **Reports** and then select **Saved Reports**.



To view a report, select either the **Licensing Report** tab or the **Usage Reports** tab, double-click the individual report or select the individual report and then select **View**.

To delete a report that is no longer required, select the individual report and then select **Delete**.

Usage Details [X]

Customer: Smiths Garages

SKU: D75-00274

Product: Microsoft BizTalk Server Standard PL

Associated Item	Quantity
scirocco.vw.local	1

Close Help

Index

A

activAeon XA Configuration • 12
activAeon XA Installation • 11
activAeon XA System Updates • 85
Agent Management • 50
Application Management • 44
Applications • 55
Assigning Licenses to a Customer • 72

C

Central Management Service (CMS) • 83
CMS Details • 14
Create a Non-Microsoft Virtual Host • 40
Creating a Deployment Group • 60
Customer License Report • 96
Customers • 67

D

Data Transfer • 51
Deployment Groups • 59
Desktop Application Usage Report • 104
Desktop Applications • 53
Device Input Information • 35
Devices • 33
Domain Management • 23

E

Editing a Deployment Group • 66
Exchange • 76
Exchange Mapping • 82
Exchange Setup • 77
Exclusions • 75

G

Global Exclusions • 68
Groups • 30

H

Handling Failed Deployments • 65
Hosted Exchange Database Settings • 78
Hosted Exchange Service Plans • 80

I

Installation Guide • 7
Introduction • 5
Invoking a Deployment Group • 64

L

License Expiry • 17
License Requests • 16
License Usage Report • 95
Linking a Domain • 32

M

Managed Device Groups • 29
Managed Device Properties • 37
Managed Domain Properties • 27
Managing a Domain • 24
Managing a Non-Trusted Domain • 25
Microsoft Desktop Application License Report • 101
Microsoft Exchange License Report • 97
Microsoft Server Products License Report • 99
Microsoft Terminal Server License Report • 100
Microsoft Windows License Report • 98
Monitoring Non-Supported Applications • 45

O

Online Help & Technical Support • 6

P

Product Inventory Analysis • 44
Provisioning • 47
Publishers • 54

Q

Quick Setup Guide • 20

R

Registration and Licensing • 16
Removing activAeon XA • 19
Report Settings for Licensing Reports • 92
Reports • 91

S

Saved Reports • 106

- Select Installation Folder • 11
- Server Association • 73
- Setting Up Further Customers • 69
- Setup a Virtual Guest • 42
- Setup a Virtual Host • 40
- Setup Default Customer • 21
- SPLA Report • 94
- SQL Credentials • 48
- SQL Server Details • 12
- Suites • 56
- System Log • 84
- System Requirements • 9
- System Updates • 87

T

- Terminal Server Session Activity Report • 102

U

- Unmanaging a Domain • 26
- Update Packages • 90
- Update Settings • 86
- Usage Summary • 107
- User Association • 72

V

- Virtualisation • 40

W

- Working With Applications • 54