SOA and EA Installation / Migration Guides

1. Avast! Small Office Administration console (SOA)

NOTE: The SOA console does NOT have to be installed on the server, and does not use conventional SQL (it uses an embedded SQL lite). You may push a deployment from the console for a domain. Workgroups will not deploy, so installs either occur from users or administrators. SOA is limited to 200 users (300 users if you use go ahead and use SQL Express 2008 R2, but this is not usually recommended)

Small Office Administration Console - http://files.avast.com/iavs5x/setup_console_epsp.exe

SOA Quick Start Guide - www.advantage77.com/Files/avast_Quick_Guide_ASOA.pdf

SOA Installation Guide - http://support.avast.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1290

SOA User Manual - http://files.avast.com/files/documentation/small-office-administration-console-user-guide.pdf

SOA with Mirror Console + Client Download - http://files.avast.com/iavs5x/setup_console_epsp_full.exe

SOA Administrator Manual - http://files.avast.com/files/documentation/enterprise-administration-user-guide.pdf

Endpoint Protection Suite Stand Alone Client - http://files.avast.com/iavs5x/setup_av_epsp.exe

Endpoint Protection User Guides - http://www.avast.com/download-documentation#business-products

Endpoint Protection FAQ - https://support.avast.com/index.php?languageid=1&group=eng&_m=knowledgebase&_a=viewarticle&kbarticleid=1291

SOA Migration Steps

1. Please make sure the ports listed below are opened in the network on both the client and server side (you can use the GPO to dispatch on all machines, and make sure to reboot the machines for the changes to be applied) :

avast! Small Office Administration uses the following ports: Service Port Numbers

     Port for Console: 8731

     Secure Port for Console : 8732

     Port for Client : 25322

2. Do a discovery task to find all the machines

3. Create a deployment package for each type of OS (Desktop, server)

A. For servers, I will recommend to create a light installation package for servers OS's which consist on of File System Shield. This is usually the only real protection required for file servers, but this assumes that the File Server not being used as a workstation), and this is an industry standard best practice. NOTE: DO NOT use the Network Shield on servers. Add the SharePoint shield if you are using SharePoint. Add the email server protection (exchange plug-in) if you want to have avast! anti-virus protect the Exchange server Mail store. If servers are to be managed (see below), then each server type will require its own group, separate from the managed client group. If servers are NOT to be managed, then use the custom install feature to select the correct shield/shields for that server type.

B. For desktop installation package, I recommend to remove from it all the server protection so they are not installed on the client. Note: When creating an installation package please be sure to select the server name / address in the installation package for the clients to communicate with the console after deployment.

4. Create a deployment task for each type of OS

5. Start to deploy by group of 10-20 machines at once, make sure to enable the "Reboot the machine" option in the deployment task settings. **Important** - Before sending out an installation please be sure the mirror is up to date which you can check by going to view tab in the console and check mirror status. Once it's up to date then you can send out the installation.

6. After you send out a installation you may receive an error code 0x00000005 which usually means access denied. This is also due when you don't reboot the client after the initial installation so please do so and then refresh the Console. Also be sure to use the network administrative passwords or a password with full administrative rights to push the client through the network.

7. If you find that when you deploy some of your clients license change or remain in the trial mode please check to be sure you're not over your license count in which case you will have a "KEY" icon over the PC. Please note the total sum of your license count is Computers with Agent + Computers without Agent = License Count. So if you have old clients in the Active Directory that will not receive the EPS installation please delete them from your lists and this should resolve your issue.

8. If you find that you will be over your estimated license count or current license please contact us for remedy.

9. WORKGROUP VS ACTIVE DIRECTORY

ACTIVE DIRECTORY
If using Active Directory you can easily create an installation package to push the client remotely through the network with Network Administrating password and in the Deploying Group.

WORKGROUP
If using a Workgroup you can only DEPLOY Remotely and ONLY With the EA Console to one computer at a time because you need to use the local administrative password / rights to push the deployment. We recommend to create the installation package manually and send it via email to each client or install it separately via USB Flash disk to manually install it on each client. Once the client has been installed only then will it be detected in the Enterprise Console.

2. Avast! Enterprise Administration console

The AEA console is required when system count is greater than 200 systems. If you are using ADNM (previous version 4 of the Enterprise console with blue icon), you already know 90% of AEA, as it is the same reliable code from ADNM. There are very few differences from ADNM, such as the combining of Computer Catalog and Task Management modules into the same location. During installation, you are prompted for choice of SQL 2008 R2 Express (to be installed with AEA), or use an existing installation of SQL. If you have either SQL 2005 or SQL 2008, you then can use same SQL instance, but a NEW database will be required. Both ADNM and AEA can coexist simultaneously. During a push Deployment, the Endpoint client installation will uninstall existing avast net clients from avast! version 4 ONLY. If any other version of avast! or other anti-virus is present, then these products will need to be removed prior to an avast! deployment. The Endpoint client will require a reboot after installation, so be prepared for this. The avast! AEA console can support tens of thousands of clients. This is achieved through support of multiple avast! Enterprise Administration Servers (AEAS). The AEAS is a mirror of an avast! update server, and each AEAS can manage up to 1000 systems. The AEA console then can manage many AEAS. However, full SQL is required for the "Replication Service" to support multiple AEAS (to support 1000+ clients) There is no migration path currently that will use the existing database from ADNM.

 Helpful Links

avast! Enterprise Administration console (AEA) installation Guide -
http://forum.avast.com/index.php?topic=110470.msg868790#msg868790

Enterprise Administration Console + Client - http://files.avast.com/iavs5x/setup_enterprise_epsp.exe

Enterprise Administration Console Installation Guide -
http://support.avast.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1289

Endpoint Protection User Guides - http://www.avast.com/download-documentation#business-products

Enterprise Administration Required Ports -
http://support.avast.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1291#idt_18

Enterprise Administration Console User Manual - http://files.avast.com/files/documentation/enterprise-administration-user-guide.pdf

Endpoint Protection Suite Stand Alone Client - http://files.avast.com/iavs5x/setup_av_epsp.exe

Endpoint Protection FAQ -
https://support.avast.com/index.php?languageid=1&group=eng&_m=knowledgebase&_a=viewarticle&kbarticleid=1291

**Installing and configuring Microsoft SQL Server 2008 R2 Express -
http://support.avast.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1286&nav=0,1,23,727

Migration Steps

From avast! ADNM v4.8 to avast! AEA v7

1. Please make sure the ports listed below are opened in the network on both the client and server side (you can use the GPO to dispatch on all machines, and make sure to reboot the machines for the changes to be applied) :

avast! Enterprise Administration uses the following ports: Service Port Numbers
Mirror 16135
Client communication port 16136
Client communication port, push requests 16139
SSL communication port console 16138
UDP information port 16133
Standard RPC, NETBIOS and SMB TCP ports for remote deployment 135, 139, 445
Standard NETBIOS UDP ports for remote deployment 137, 138

2. When installing the Enterprise Administration Console please make sure to **install a MS SQL 2008 R2** as standalone, not from the installation process, so later you can connect the EA to it.

3. Do a discovery task to find all the machines

4. Create a deployment package for each type of OS (Desktop, server)

> A. For servers, I will recommend to create a light installation package for servers OS's which consist on of File System Shield. This is usually the only real protection required for file servers, but this assumes that the File Server not being used as a workstation), and this is an industry standard best practice. NOTE: DO NOT use the Network Shield on servers.   Add the SharePoint shield if you are using SharePoint. Add the email server protection (exchange plug-in) if you want to have avast! anti-virus protect the Exchange server Mail store. If servers are to be managed (see below), then each server type will require its own group, separate from the managed client group. If servers are NOT to be managed, then use the custom install feature to select the correct shield/shields for that server type.

> B. For desktop installation package, I recommend to remove all server packages from the installation package for the client.

5. Create a deployment task for each type of OS

6. Start to deploy by group of 10-20 machines at once, make sure to enable the "Reboot the machine" option in the deployment task settings. *Important* - Before sending out an installation please be sure the mirror is up to date which you can check by going to view tab in the console and check mirror status. Once it's up to date then you can send out the installation.*[/color]

*Basically the deployment will detect the old 4.8 version and remove it automatically before installing the new version 7 (avast! End Point Protection/Plus/Suite/Suite Plus)

7. After you deploy the installation you may receive an **error code 0x00000005** which usually means access denied. This is also due when you don't reboot the client after the initial installation so please do so and then refresh the Console. Also be sure to use the network administrative passwords or a password with full administrative rights to push the client through the network.

8. If you find that when you deploy some of your clients license change or remain in the trial mode please check to be sure you're not over your license count in which case you will have a "KEY" icon over the PC. Please note the total sum of your license count is Computers with Agent + Computers without Agent = License Count. So if you have old clients in the Active Directory that will not receive the EPS installation please delete them from your lists and this should resolve your issue.

9. If you find that you will be over your estimated license count or current license please contact us at edu-support@avast.com and we can have your license regenerated to accommodate the new number of licenses you may need.

10. If you need to install or update to a 2008 R2 SQL please click on the link below.
http://support.avast.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1286&nav=0,1,23,727

11. The DEFAULT PASSWORD for the EA Console is ADMIN. This of course can be changed after installing.

12. We recommend using a Full SQL 2008 R2 per EAS Server and to choose the CUSTOM installation using the SQL that you recently installed, if the express install did not work properly.

13. WORKGROUP VS ACTIVE DIRECTORY

ACTIVE DIRECTORY
If using Active Directory you can easily create an installation package to push the client remotely through the network with Network Administrating password and in the Deploying Group.

WORKGROUP
If using a Workgroup you can only DEPLOY remotely and ONLY With the EA Console to one computer at a time because you need to use the local administrative password / rights to push the deployment. We recommend to create the installation package manually, then send the executable via email to each client or install it separately via USB Flash disk to manually install it on each client. Once the client has been installed only then will it be detected in the Enterprise Console.

14. Finally remove the ADNM v 4.8 and its database

Migration Scenarios

A. From avast! ADNM v4.8 to avast! AEA v7

In this scenario, as the AEA v7 is NOT using the same database NOR the same installation folder as the ADNM v4.8, you just need to:

- Install the AEA v7 Console on the same machine or on another one.
- Do a discovery task to find the machines which are already running the v 4.8 managed clients
- Do a remote deployment on these machines *(Basically the deployment will detect the old 4.8 version and remove it automatically before installing the new version 7)
- Finally remove the ADNM v 4.8 and its database

B. From avast! ADNM v4.8 to avast! ASOA v7

This scenario is similar to the scenario ADNM v4.8 to AEA v7 so, you just need to:

- Install the ASOA v7 Console on the same machine or on another one.
- Do a discovery job to find the machines which are already running the v 4.8 managed clients
- Do a remote deployment on these machines *(Basically the deployment will detect the old 4.8 version and remove it automatically before installing the new version 7)
- Finally remove the ADNM v 4.8 and its database

C. From avast! BP/BPP v6 to avast! ASOA v7

Here you can decide to install the ASOA v7 console on the same machine as the BP/BPP v6 Console or install it on another one.

- If you decide to install the ASOA v7 on the same machine as the previous BP/BPP v6
- The installer will just upgrade the BP/BPP v6 to the ASOA v7
    • Note that in this choice the same database will be used instead of the integrated one which comes with the ASOA v7.
- The clients with BP/BPP v6 installed will be connected automatically to the console
- Run a deployment job to upgrade the clients to the version 7

D. From avast! ADNM v4.8 to avast! ASOA v7

This scenario is similar to the scenario ADNM v4.8 to AEA v7 so, you just need to:

- Install the ASOA v7 Console on the same machine or on another one.
- Do a discovery job to find the machines which are already running the v 4.8 managed clients
- Do a remote deployment on these machines (Basically the deployment will detect the old 4.8 version and remove it automatically before installing the new version
- Finally remove the ADNM v 4.8 and its database