aaa-reports!

for Cisco Secure ACS & Funk SBR

***the* essential tool for measuring the effectiveness of your security solution**

Deployment FAQ...

Pre-Install Quick Check List

- **Run the Trial Version on a non-production host**
- **Use the *Administrator* account for a *Local* install**
  Do Not just use an account with Admin Rights – this may not be sufficient
  Install locally if possible rather than remotely via Terminal Services
- **View sample reports immediately**

  or
- **Configure your AAA Server's Logging**
- **Tune aaa-reports! to your logs**
- **Report and analyze your own data**
- **Review this document for a smooth deployment and evaluation**

Welcome to aaa-reports!

Thank you for your interest in ***aaa-reports!*** This document discusses the downloadable Trial Version available from our web site, the configuration of your AAA Server and the typical considerations to be made when planning your reporting installation and how to get up and running quickly and smoothly.

Contents:

Which AAA Servers Does aaa-reports! Support?

- Cisco Secure ACS for Windows 3.x (Including ACS Appliances)
- Cisco Secure ACS for Windows 4.x once released
- Cisco Secure ACS for Unix
- Funk Steel Belted Radius

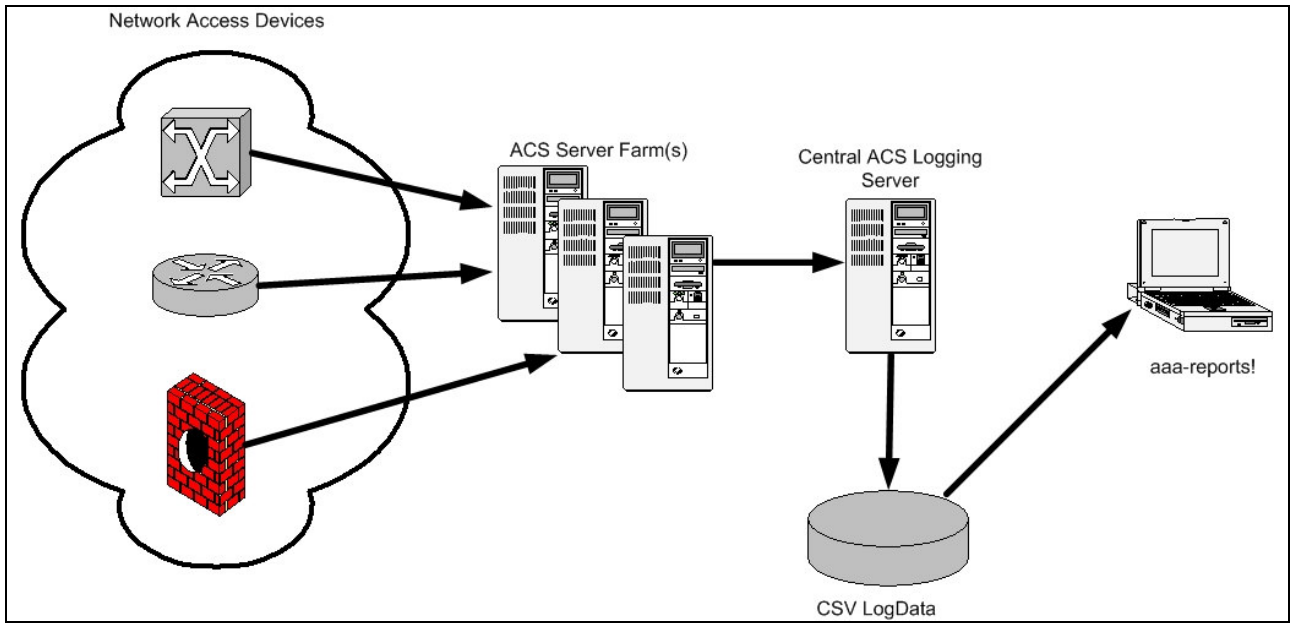
What functionality does the Trial Version of aaa-reports! have?

The Trial Version is **fully functional for 60 days** during which time you can import and analyze your own data or experiment with the **demonstration data** supplied. You can **Activate** your Trial Version for continued use by purchasing a **License Key**.

How does aaa-reports! Integrate with the AAA Server?

aaa-reports! does not directly integrate with your AAA software, it **imports** the various CSV Logs generated by the server. No re-configuration of the AAA Server is required other than to ensure all the necessary attributes are being logged.

Fig 1: ***aaa-reports!*** only requires access to AAA Server log data



Do I Need to Configure My AAA Server's Logging to Run the Trial Version?

Yes, if you want to evaluate the reports against your own data. ***aaa-reports!*** requires a "Core" set of attributes in each log type for the reports to be produced. Once ***aaa-reports!*** is installed you can **print** the **Configuration Report** from the **Tools** menu to see exactly which attributes are required for your AAA server.

Advanced **Tracking Options** in ***aaa-reports!*** allow you to import additional attributes and even User Defined Attributes (UDAs) for analysis with the **Query Builder** facility.

You can safely configure your AAA server to log more attributes than ***aaa-reports!*** requires as it will only import the Core attributes plus any others you specifically need. (Please see the User Guide for more details.)

Where should aaa-reports! be installed?

aaa-reports! does not have to be installed on the same system as ACS but it does need access to the CSV log files. By default ***aaa-reports!*** will look for log files in the "CSVLogs" folder in its own install path, e.g. C:\Program Files\aaa-reports\CSVLogs. You can either copy/write your logs to this folder or point ***aaa-reports!*** to look in another folder. For best performance import the logs from a folder local to ***aaa-reports!***. (See the User Guide for more details on how log files are managed.)

Can I Import Logs From Multiple AAA Servers?

If you have multiple AAA Servers then the simplest method is to have the AAA software centralize your logging. ***aaa-reports!*** will then import the aggregated data contained in the single set of logs.

If it is not practical, or you do not wish to centralize your logging then you will need to collect your logs from multiple AAA servers into a central location for analysis by ***aaa-reports!***. Note that each server will be creating logs with identical filenames so you must also modify the log file names to include a unique AAA server identifier. For example;

Rename	"RADIUS Accounting 2005-10-25.csv"
to	"RADIUS Accounting 2005-10-25 AAA-Server1.csv"

*Make sure any suffix is added after the date part of the filename or **aaa-reports!** will not recognise it as a valid log file.*

For details on our **CSVSync tool** that can be scheduled to collect and re-name logs from multiple ACS servers (including ACS Appliances) visit http://www.extraxi.com/utils.htm

There are scenarios where it may not be desirable to consolidate logs; see the section "Can I Report on Multiple Service Types?" below for details.

Can I Report on Multiple Service Types (Dial, VPN, WLAN & VoIP, For Example) With a Single Copy of the Software?

If you authenticate a specific service type with one or more AAA servers dedicated to that particular service then you may not want to aggregate those logs with logs from other AAA servers authenticating different service types. For example, you may have AAA servers dedicated to Dial/VPN and want to report on this service in complete isolation from other AAA servers authenticating a different service, such as VoIP or NAC perhaps.

Combining logs from multiple service types into the same reporting database is possible by may make it difficult (or not possible, in some cases) to separate out reports and analysis for the individual service types, depending upon the mix of services you have.

It is recommended that organisations authenticating services separately consider reporting them separately also with dedicated copies of ***aaa-reports!.***

Do I Need to Import All Mv AAA Server's Different Log Types?

No. In fact you should only import the log types for the specific service type(s) you want to report on as this will maximize database efficiency.

Where Should aaa-reports! Be Installed?

We recommend you install the Trial Version to a non-production system for evaluation. When you license the trial version for permanent use you can install to your AAA server or to any convenient workstation. ***aaa-reports!*** does not require direct access to your AAA Server, it only needs access to the log files or copies of the logs.

By default ***aaa-reports!*** will look for log files in the "CSVLogs" folder in its own install path, e.g. C:\Program Files\aaa-reports\CSVLogs. You can either copy/write your logs to this folder or point ***aaa-reports!*** to look in another folder. For best performance import the logs from a folder local to ***aaa-reports!***. (See the User Guide for more details on how log files are managed.)

For details on our **CSVSync tool** that can be scheduled to collect and re-name logs from multiple ACS servers (including ACS Appliances) visit http://www.extraxi.com/utils.htm

Why Is My Computer's Locale Setting Important?

Cisco Secure ACS uses the comma (,) as the list separator in its log files which causes a conflict in the Microsoft Jet Text Driver if your computer's locale uses the comma as the decimal character.

Can I Install To A Locale That Is Affected By The List Separator Conflict?

Yes, you can still install and run ***aaa-reports!*** to a locale that uses the comma as the decimal character but you must temporarily change the locale to US or UK before running the data import process. Once your data is imported you can switch back to your native locale to run reports and analysis with appropriate formatting.

What Are The Minimum System Requirements For aaa-reports!

System Requirements

Pentium 4, 1Gb RAM, 4Gb hard disk space
Microsoft Windows NT / 2000 / 2003 / XP with an installed printer driver (any).

Cisco Secure ACS Version Support

Version 1.x supports log files for Cisco Secure ACS 3.x for Windows NT/2000 only.
A separate version also supports logs from ACS Unix.

How Do I Install aaa-reports!?

Full Product:

Full product for first time installation.
Download and run AAARx.xx.EXE to start the installer. Follow the on-screen prompts.

Minimum Install (Patch Update):

Zip file containing just the files required to update a previous installation.
Download the zip file AAARx.xx Minimum.zip
Carefully review the ReadMe instructions in the zip file to determine suitability before proceeding.

NOTES:

- Always uninstall any earlier trail version and ensure all application files and folders are removed before attempting a fresh install of the full product.
- You should be logged in as administrator to run the installation. Just being a member of the administrators group may not be sufficient, particularly if using terminal services or other remote access solution.
- The install may require a re-boot.
- Temporarily disable anti-virus software prior to installation and re-enable once complete.

First Time Use

The first time you launch ***aaa-reports!*** the **Configuration Wizard** will guide you through the few simple steps to configure the software.

Immediate Evaluation of Sample Reports Against Demo Data

The quickest way to review the potential of ***aaa-reports!*** is to select the "Demo Data" option at the end of the Configuration Wizard. This allows you to immediately run example reports for most service types against demonstration data without the need to generate and import your own logs.

Detailed Evaluation of Reports Against Your Own Data

Running reports against your own data requires the following steps;

- Review the ***aaa-reports!*** Configuration Report (Tools, Config Report) for details on the log types required and the Attributes each log type should contain
- Check your AAA Server's logging settings and add any required Attributes not already included. Wait for new logs to be generated with all the required Attributes.
- Run a test import using a single log file and review any messages before proceeding to import the full volume of logs. (See "Fine Tuning" section below.)
- Start evaluating the Reports and Query Builder

Fine Tuning aaa-reports! to Suit Your Data

To maximize database efficiency ***aaa-reports!*** employs three strategies that may require some fine tuning to match your data;

1. Only those Attributes required for reports are imported by default. Other Attributes in the log are ignored. If **aaa-reports!** requires Attributes the logs do not contain they are reported as "Missing" and you will need to change your AAA Server settings to start logging them.

   Note: You can force the import of additional Attributes, including User Defined Attributes, from Options.

2. The internal database has default text field sizes based on typical Attribute values. If your logs have values larger than the defaults the import process will truncate your data and report the Attribute(s) affected. You can easily accommodate longer values by increasing the field sizes in Options. Conversely, you can reduce field sizes to increase performance and capacity.

3. "Pre-Filtering" is a powerful, flexible feature to allow you to filter out log records matching any one of an arbitrary number of specific criteria. Whilst primarily designed to strip out the huge volumes of data generated by automated "Robot" processes the feature can be used to exclude rows for any purpose.

Fine Tuning Procedure

Because default AAA Server logging settings do not include all the attributes used for reporting it is quite possible that any historical log data you try to import will have core attributes "missing". The following procedure will help identify what logging changes are required to your AAA server and identify the attributes who's field sizes need increasing to accommodate longer than average values;

1. Place a single example of each log type you want to import into the Import Folder specified in Options and run the Data Import.
2. Note the messages during the Import and refer to the Event Log for more specific details.

3. Use the "Undo Last Import" feature on the Data Import screen to remove the data just imported then re-start ***aaa-reports!***
4. Adjust ***aaa-reports!*** field sizes where "Attribute Data was Truncated" (See user guide for details.)
5. Update your AAA server logging to include any "Missing" Attributes.
6. Run the Data Import again, still using a single example of each log, and check that your configuration changes were successful. Repeat steps 1 to 6 if necessary.
7. Once you are satisfied fine tuning is complete, go ahead and import your remaining log files. If you plan to import a large backlog of logs we recommend importing them in monthly batches.
8. Switch to "Silent Import" mode (Import Options) to suppress further messages and allow the import to run unattended. Any message details will be written straight to the Event Log.

If you plan to use the Pre-Filter facility then apply the same principle as above to fine tune your search strings and filter out as much unwanted data as possible;

1. Enter or modify pre-filter search strings
2. Run a test Data Import
3. Review the imported data in ***aaa-reports!*** and the excluded (flagged) data in the log files.
4. If the desired result is not obtained then Undo Last Import and repeat steps 1 to 3.

Running Reports

To run reports, open the **Reports** form and select the reports you want to run.
Specify your desired output and click **Execute Reports**.
If you chose **'File'**, use Explorer to open and view the **Snapshot** or **PDF** files created in **...\Snapshots**. (See the User Guide section "Viewing Report Snapshot Files" for more information.)

Creating Custom Reports

Open the **Query Builder** form to apply simple or complex queries, sort, search and export consolidated data for most types of logs. You can save and recall your queries and export the results to a number of formats.

Filtering Out Unwanted Log Data from Automated Processes (Pre-Filter)

aaa-reports! provides a powerful feature to allow users to filter any log records matching one of an arbitrary number of particular criteria. Whilst simple in operation, the tool provides two key benefits:

- Reports are free of the irritating and distorting effect of the mass of 'bot' generated data. This is particularly useful for those reports that analyze activity where the 'bot' users would generate masses of virtually useless records.

- The reporting database is kept to a more reasonable size thereby conserving system resources and keeping performance high (our research indicates that for the average site using TACACS+ Device Administration between 85-90% of TACACS+ audit records are 'bot generated).

Useful Links

Extraxi Home Page
http://www.extraxi.com

Sample Reports
http://www.extraxi.com/reports.htm

aaa-reports! for TACACS+ Device Administration
http://www.extraxi.com/TDA.htm

aaa-reports! for Sarbanes-Oxley (SOX)
http://www.extraxi.com/SOX.htm

aaa-reports! for Network Admission Control (NAC)
http://www.extraxi.com/NAC.htm

aaa-reports! for VoIP
http://www.extraxi.com/PDFs/VOIP.pdf

A Sample of aaa-reports! Customers
http://www.extraxi.com/customers.htm

Cisco's ACS FAQ Page
http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_qanda_item09186a0080124e7c.shtml

Cisco Documentation on ACS Logging
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs32/user/r.htm#958586

ACS User Group
http://groups.yahoo.com/group/CiscoSecure_ACS_UG/

ACS Log Collection Tool
http://www.extraxi.com/utils.htm

