extraxi

The aaa-reports! Product Family

Executive Summary

Extraxi was formed by several ex-Cisco personnel who, after initially creating and selling the *Cisco Secure ACS for Windows* product (to Cisco) decided there was a sizeable gap in the market for an Authentication, Authorisation & Accounting (AAA) reporting product. While there are large and very expensive solutions that take the form of network-wide event monitoring platforms there was not an out-of-the-box "install it and go" reporting product – the initial philosophy for *Cisco Secure ACS* itself! Moreover, real-time event monitoring and audit reporting are not the same thing; reporting requires complex offline queries run across multiple logs to unlock their true value.

Introducing the **aaa-reports!** reporting and analysis tool for *Cisco Secure ACS* – the essential reporting tool for your network security solution.

Whatever the function of the network being secured, its security protocol or the number of users and devices, **aaa-reports!** can import the device generated session accounting, the ACS generated security audit logs and even the ACS user/group database itself! This combined with the power of a modern relational database and report generator allow for an un-paralleled view of the policies defined and their operational effectiveness. Out of the box there are reports for:

- Network device capacity planning
- Security exception detection and diagnosis
- Network service usage & simple billing
- Network device management auditing
- ACS database user account status tracking
- ACS database policy documentation & effectiveness auditing

In addition, Extraxi offer various other products and consultancy services – from remote log collection tools, product installation & configuration to customisation and migration services from Cisco Secure ACS for UNIX to Windows.

Extraxi is a member of the *Cisco Development Technology Partner* program and aaa-reports! has been tested and awarded with *Cisco Compatible* status for Cisco Secure ACS v3.x & v4.x.

Why Do Reporting?

The answers are numerous and for many organisations the answer is simply that it's now a legal requirement to produce audit documentation for network access – particularly for network device administrators. Other driving factors are to:

- Provide enhanced management information
- Allow for "post mortem" analysis of network/access failures or security breaches
- Generate additional revenue from commercially hosted AAA services
- Monitor the operational effectiveness of ACS server deployment

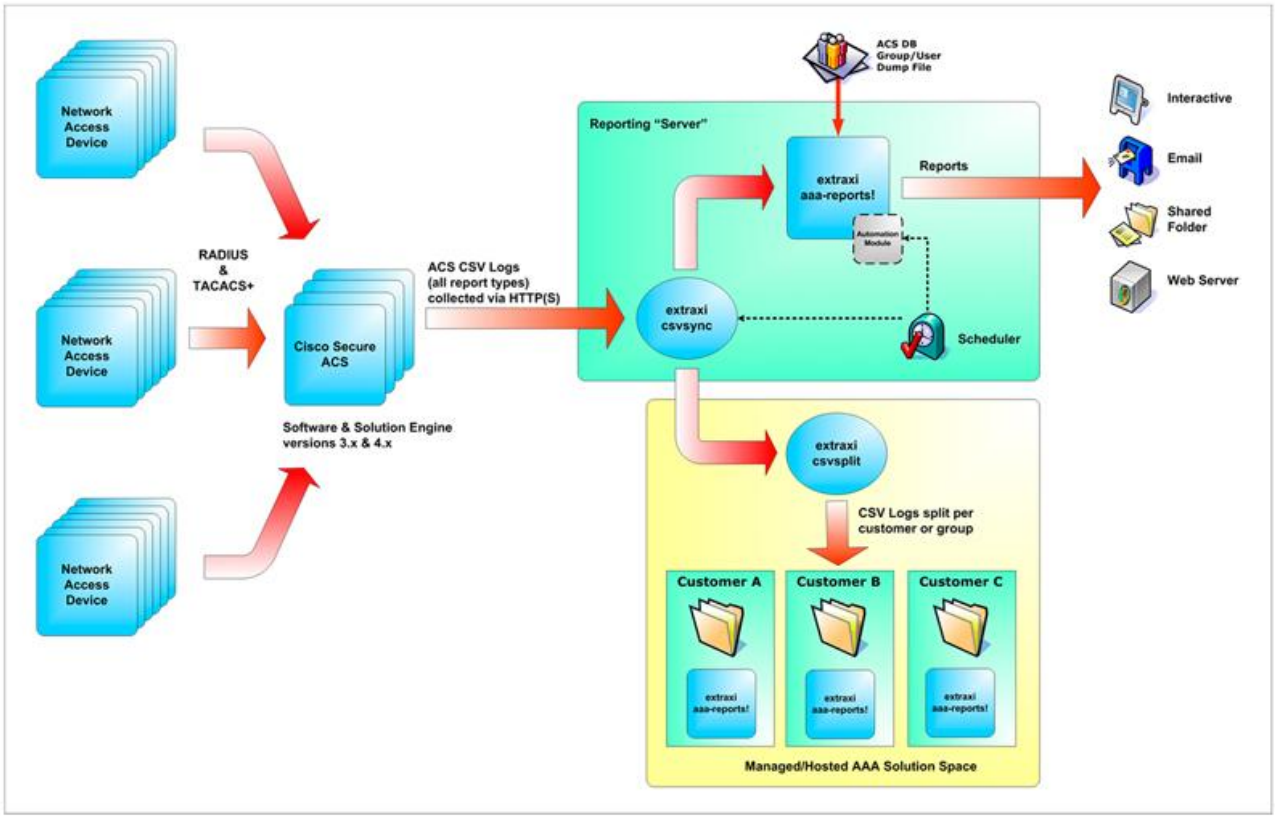
Extraxi Product Family

There are three products in the Extraxi product line-up:

aaa-reports! is a Windows-based reporting application that utilises the full power of a relational database to deliver a feature rich set of canned reports, custom reports, data filtering and much more.

csvsync is a Windows command line tool that enables the downloading of CSV log files directly from any number of ACS servers (windows & appliance) via the ACS Admin HTTP(S) service.

csvsplit is a Windows command line tool that supports the splitting of CSV log files based on any criteria (eg Group-Name) to facilitate revenue generating services such as client reporting in Managed AAA deployments.



Extraxi product family deployment

aaa-reports!

aaa-reports! provides a comprehensive reporting solution for both network service access control by RADIUS and network device management by TACACS+ (with the latter supported both by activity and policy auditing) via *Cisco Secure ACS*.

End User Network Access Control

To assist in the RADIUS network access control role, **aaa-reports!** provides a full set of trend, summary and detailed reports that allow the enterprise to best understand how their service is really being used, such as:

- Usage reports for the overall installation and individual devices
- Usage summary reports by group, user or device
- Failure/problem reporting by group, user and by device
- Excessive use by groups or users.
- Out of hours usage and excessive short sessions

Network Device Management

To assist in the TACACS+ network device administration role, **aaa-reports!** provides a comprehensive set of reports focused on delivering detailed tracking of command line administration activity by system administrators on the network device infrastructure. **aaa-reports!** provides numerous ways to track the activities of network device administrators. These include:

- Activity of specified administrator over a specified time period
- All administrative session activity on a specified device over a specified time period
- Failed command execution attempts by all administrators or by a specified administrator
- Failed login attempts by all administrators or a by a specified administrator and the reasons for failure
- All instances of the execution of any specified command over a network device infrastructure

For many organisations documenting the policy locked within their ACS Server database has become a real issue when faced with the likes of Sarbanes-Oxley regulations. Taking screenshots of the ACS Admin user interface has (until recently) been the de-facto solution. aaa-reports! imports the configuration exported from ACS (including user accounts, group configurations and network device database) to report on:

- Network Access Restrictions (NAR)
- TACACS+ Device Command Authorisation Sets (DCS)
- User group membership, password & account statuses
- IOS Shell service configuration (session & command authorisation)
- Network Device Group (NDG)

As well as simply documenting the configuration in place, **aaa-reports!** can help answer the two key questions faced during an audit:

1. Which groups/users can access device XYZ?
2. What commands can a group/user issue on access device XYZ?

General Features

To support the application areas above **aaa-reports!** provides an ever growing list of features:

- **Automation**. A new "add on" module that allows for logs to be imported and report batches to be executed on a schedule.
- **Report batches**. These comprise any number of canned/custom reports (with parameters) with the resulting saved in PDF or exported to Word/Excel/Html/Txt
- **SMTP Support**. Have PDF reports emailed directly to any number of recipient lists.
- **Custom Reports**. In addition to the canned reports the Query Builder allows the end-user to take either raw log data or canned report datasets and add extra filtering, sorting, grouping and totalling – all with no previous SQL knowledge!
- **ACS Active Log Support**. **aaa-reports!** is able to import active ACS files multiple times a day without creating duplicate records. This is crucial for ACS appliance support where log file rollover is hard-coded to 10MB
- **Multi ACS platform/version support**. ACS versions 3.x and 4.x, software and appliance types supported.

csvsync

csvsync allows you to download CSV reports files directly from any number of ACS servers (windows & appliance versions) via the HTTP(S) ACS Admin service. It connects to the ACS Server in much the same way as your web browser and therefore is very simple to deploy with no agent software to install on the ACS server. All you need do is create an ACS admin user account for **csvsync**.

csvsync is a simple to use windows command-line executable that will pull down the CSV files for one or more ACS report types (eg Failed Attempts, RADIUS Accounting etc) into the desired location onto the user's computer. **csvsync** only pulls down CSV files that are new - this prevents it from downloading the same files multiple times and keeps the execution time to a minimum. When downloading from multiple ACS servers, **csvsync** can optionally add the server name or other reference as a suffix to the filename. This avoids issues with clashing filenames and aids in general file management.

csvsync is the perfect companion for **aaa-reports!** allowing for fast, secure and automated download of your ACS log data. However, **csvsync** can still be used stand-alone for the purposes of automated log retrieval and archiving.

csvsplit

csvsplit is a simple to use windows command line program that allows any number of csv files to be split into separate file sets based upon a specified match criteria. For example, splitting accounting data based on the values within the "Group" column - a new csv file is created for each unique value found in the Group column (eg admins, sales, engineering).

In case there is some sensitive data that must be removed from the split csv file set, **csvsplit** also provides for simple filtering whereby rows can be excluded based on simple pattern matching. **csvsplit** works in several modes:

- **autosplit mode**. In autosplit mode csvsplit automatically creates a new csv file for each unique value found in the "split field". So, if the "Group" column was set as the split column and a csv file contained rows with 10 different values of "Group", the result would be 10 separate split csv's
- **configured mode**. In configured mode, you specify which values of the split column you are interested in. csvsplit splits out any rows that match and ignores any others.

csvsplit is the perfect companion for **csvsync** & **aaa-reports!** as shown in the example deployment below where "Managed AAA" services are hosted by a provider. CSV data (such as passed authentications, failed attempts, RADIUS/TACACS accounting etc) is downloaded automatically (via csvsync) then split out into a file set per-customer.

Sales & Licensing Model

All Extraxi software is available for download from Extraxi.com as a fully functional 60 day trial version. Conversion to full retail version is simple - by the installation of an activation key typically supplied upon receipt of an authorised Purchase Order. Physical boxed copies of software or documentation is not available.

All Extraxi software is licensed based on the number of ACS servers being reported on with Single Host Copy, Site and Enterprise licensing available.

In addition to software, Extraxi offers consultancy and customisation services.

Support and Maintenance

Customers are encouraged to take up annual support and maintenance contracts which offer the following benefits:

- FREE minor upgrades and patch releases
- Unlimited email technical support
- Telephone based support during UK office hours (subject to availability)

Benefits

As a whole the Extraxi **aaa-reports!** product family offers a totally unique set of benefits to new and existing users of *Cisco Secure ACS*:

- Solution tightly focused on *Cisco Secure ACS* featuring support for ACS specific logs and data formats. Built by the original designers of ACS!
- End to end automation supported – from log collection, import, report generation and publishing via email. Configure it once then sit back and read the reports as they arrive!
- Scheduled "bulk pull" of log data – with **csvsync** you can retrieve CSV logs from **any** version of ACS (software **and** appliance) making efficient use of network bandwidth.
- Policy audit support – be ready when asked questions such as "When was this change implemented?" and "Which devices did user XYZ touch on this date?" and "What commands can group ABC execute on this device?"
- Report on the users whose accounts are expired or who didn't change their passwords according to the aging policy in place.
- Spend a minutes (instead of days) each month creating reports for management.
- Report on every aspect of your *Cisco Secure ACS* deployment – usage & policy
- Play with the data – using the Query Builder drill down into the raw data or report datasets for ad-hoc investigations to scheduled custom reports.
- Split out and push "relevant" log data to groups within the organisation or external clients using **csvsplit**. Generate extra revenue from your hosted AAA services.

Value Proposition

In short there isn't another reporting application available that comes close to **aaa-reports!:**

- In-depth "developer level" knowledge of ACS "designed in".
- Works "out of the box" - no agents to deploy
- Low entry cost – single copy of **aaa-reports!** for 1 ACS server only US$1800
- Low TCO – does not mandate the use of a Windows Server OS
- Large and ever increasing set of standard reports
- Annual support & maintenance contracts ensure FREE minor upgrades
- Vastly reduced effort required to meet regulatory audit & management information requirements