



CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

**ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
ForeScout CounterACT v6.3.4.1**

Maintenance Report Number: CCEVS-ACMR-VID10342-0005

Date of Activity: 13 November 2012

References: Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation”, 8 September 2008;
Common Criteria Assurance Maintenance Impact Analysis Report (IAR) ForeScout CounterACT v6.3.4.1

Documentation Updated: (List all documentation updated)

Assurance Family	Title	Version	Date
ASE	ForeScout CounterACT v6.3.3 with Hotfix 6.11070 Security Target	2.1	08/06/2012
AGD	ForeScout CounterACT v6.3.3 with Hotfix 6.11070 CC Supplement	1.1	08/06/2012
AGD	ForeScout Technologies, Inc. CounterACT Installation Guide	6.3.4.1	07/07/2012
AGD	ForeScout Technologies, Inc. CounterACT Console User Manual	6.3.4.1	07/19/2012
AGD	ForeScout Technologies, Inc. CounterACT Release Notes	6.3.3.2	No date
AGD	ForeScout Technologies, Inc. CounterACT Release Notes	6.3.4.0	09/2010
AGD	ForeScout Technologies, Inc. CounterACT Release Notes	6.3.4.1	07/27/2011
ALC	ForeScout Technologies, Inc. TOE Component CI list ForeScout	n/a	07/06/2012
ATE	ForeScout CounterACT v6.3.4.1 CC Test Results	n/a	06/05/2012

Assurance Continuity Maintenance Report

The Corsec Security, Inc., acting for ForeScout technologies, Inc. the vendor of ForeScout CounterACT v6.3.4.1, submitted an Impact Analysis Report (IAR) to CCEVS for approval in August 2012. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation”, 8 September 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes, and the security impact of the changes.

Changes to TOE:

- Total Changes included in IAR – 71;
- Changes with major security relevance – 0;
- Changes with minor security relevance – 17; and
- Changes with no security relevance – 54.

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

Types of Changes:

- System Changes (9) - allow new appliance hardware, modifications to installation packages, support for CAC authentication;
- Display Changes (32) - modifications to how TOE data was organized and displayed;
- Functional Changes (28) – miscellaneous changes to the functional operation of the TOE that did not alter security operation or introduce any new interfaces; and
- Security Changes (2) - changes where existing TOE security mechanisms were extended (e.g., adding password validation to existing command selection) or were outside the scope of the evaluation (e.g., permitting login w/o password, which is not allowed in the evaluated configuration).

TOE Changes with security Significance

Of the 71 changes made to the TOE CCEVS concluded one had greater security impact than was reported in the IAR. That change appears to explicitly modify a Security Functional Requirement (SFR) by either adding or removing specific attributes from that SFR. According to CCEVS Scheme Publication #6, *Assurance Continuity Guidance for Maintenance and Re-evaluation*, those modifications constitute “Changes to the TOE boundary” and are considered to have major security impact. Making a change with major security impact to an evaluated TOE requires re-evaluation of the modified TOE.

The relevant change is indicated in the table below.

Change #	Related SFRs	ST Change Required
67	FIA_ATD.1	Add CAC-related attributes to Table 6-6, 7.1.3.1, and CAC-related description to 7.1.3.2

Conclusion

CCEVS considers change #67 (i.e., the introduction of a CAC-based authentication method) as having a major security impact on the TOE and for that reason the CAC-based authentication mechanism must not be included in the updated TOE. In order for assurance maintenance, the vendor will update all related Common Criteria supplement documents (i.e., *ForeScout CounterACT v6.3.3 Common Criteria Supplement to the Administrative Guidance*) to clearly explain that CAC authentication is not part of the evaluated TOE or its installation and configuration. Further, the vendor will supply that guidance as part of the delivery of the updated TOE.