



Pulse Access Control Service

Release Notes

Unified Access Control 4.4R4

OAC Version	5.60.22403
Build	22403
Published	July 2015

This is an incremental release notes describing the changes made from C4.4R1 release to C4.4R4. The C4.4R1 GA release notes still apply except for the changes mentioned in this document. Please refer to C4.4R1 GA release notes for the complete version.

Contents

Noteworthy Changes:	3
NSM Schema for C4.4 R4	3
Known Issues/Limitations Fixed in C4.4R4 Release	3
Known Issues/Limitations Fixed in C4.4R3 Release	3
Known Issues/Limitations Fixed in C4.4R2 Release	4

Noteworthy Changes:

1. The IKE Phase 1 soft rekeying doesn't work properly, and it causes packets dropping while rekeying. It results most TCP applications disconnected.
The IKE Phase 1 soft rekeying is temporary disabled. After Phase1 lifetime is reached, a new phase1 can be triggered by a tunnel traffic packet or by a Persistent Tunnel trigger. The gap is small, and most TCP application connections will stay.
The IKE Phase 1 soft rekeying is fixed in a later version.

NSM Schema for C4.4 R4

The NSM schema for this software version will not be published.

Known Issues/Limitations Fixed in C4.4R4 Release

1. aaa-local - Start Time for a system local user doesn't get exported when an XML export of the IC configuration is done. (870404)
2. ifmap-client - Infranet Controller allows roles to be deleted, even if they are used in session import/export policies. (884343)
3. uac-auth - Mac authenticated users are counted against the license preventing the user session login. (883552)
4. uac-gateman - Gateman cores intermittently while communicating with two Netscreen firewalls configured in NSRP A/A mode. (880527)
5. uac-sbr - Radius request attributes does not show realm attached to it on Admin UI. (853429)
6. uac-sbr - Occasionally authentication is slow on IC and SA. (861011)
7. uac-sbr - Radius sometimes crashes in association with concurrent TLS authentications. (896214)
8. uac-other - IC sends CoA/Disconnect message when it receives accounting stop message causing Machine to User login failure. (852392)

Known Issues/Limitations Fixed in C4.4R3 Release

1. ifmap-server - Fed server crashes when MAG profiler as a Fed client tries to connect. (867088)
2. pulse-other - Certificate trust popup appears when Pulse L3 connection fails over to another node in a cluster. (860555)
3. system-dspar - RADIUS requests dropped during heavy RADIUS utilization and reported in the events log. (661192)

4. uac-admin - Realms with the apostrophe character cannot be assigned to a sign-in policy. (858472)
5. uac-auth - IC does not send MAC address which it receives as “:callingStationID” attribute during authentication to SQL server for authorization. (877594)
6. uac-other - Post-Auth Sign-In Notification causes Native Windows supplicant to fail authentication. (852780)
7. uac-other - HTTP to HTTPS redirect does not happen during captive portal for IC landing page. (859287)

Known Issues/Limitations Fixed in C4.4R2 Release

1. pulse-ive-cm – When the option, “Between endpoints and the Pulse Access Control Service” is not selected, in some instances the IC doesn’t send the list of ICs in the cluster for Pulse to failover. (851615)
2. pulse-connmgr - With DNS load balancer configured, Pulse will not get a new IP list from DNS by clicking on retry button when connection to an invalid IC fails. (840939)
3. pulse-tunnelmgr-ike - The IKE Phase 1 soft rekeying doesn’t work properly and packets are dropped while rekeying which can result in TCP applications getting disconnected. In this release, the IKE Phase 1 soft rekeying is temporary disabled. After Phase1 lifetime is reached, a new phase1 can be triggered by a tunnel traffic packet or by a persistent tunnel trigger. The gap is small and most TCP applications will stay connected. The IKE Phase 1 soft rekeying is fixed in a later version. (853698)
4. sa-sbr - When a user logs onto the SA that has a certificate restriction or certificate authentication configured then a process on the SA can go into an infinite loop if the following conditions are met:
 - a. The realm you are signing into has a certificate restriction or is configured for certificate authentication.
 - b. The client you are using is OAC or Pulse 3.0 or earlier.
 - c. There is no certificate on the endpoint that the client can select. (867048)
5. uac-admin - The maximum session length for a user role cannot be modified when Radius Server only license is installed on the IC. (845597)
6. uac-other – On the serial console, when entering a string for <path>, after generating a system snapshot, the system used the input as a filename instead of a directory location. (810209)
7. uac-other - SSO does not show up under Realm->Authentication Policy for a realm with AD authentication enabled when MAGX600-UAC-SRX license is installed. (858894)
8. uac-xmlimport - XML import of the config fails if an Enforcer on an IC with the serial number is configured in the second line by keeping the first line empty. (842698)