Pulse Secure

Pulse Access Control Service

Release Notes

Pulse Access Control Service version 4.4 R1 Build 20957

Pulse client version 4.0 R1 Build 32327

Odyssey Access Client version 5.6 R1 Build 20957

Version	**4.4 R1, 4.01 R1, 5.6 R1**
Build	**20957, 32327, 20957**
Published	**July 2015**
Revision	**00**

Contents

New Features in this Release

- Please refer to the "What's New" document on the software download site for details about new features. This document will be available in the **http://www.pulsesecure.net/support**

Interoperability and Supported Platforms

- Please refer to the "Supported Platforms" document on the software download site for details about supported versions of the Screen OS Enforcer, the Junos Enforcer, client browsers, client smart phones, and client operating systems. Go to **http://www.pulsesecure.net/support**

Upgrading to Access Control Service 4.4R1

Access Control Service Software Upgrade

- Automatic updates to this release are supported for all UAC releases after and including UAC 3.1 R1.
- This release does not support IC4000 and IC6000 devices. These hardware models have reached end-of-life (EOL).
- When upgrading from version prior to 4.2Rx, upgrade the Access Control Service software before you upgrade the Pulse and OAC clients if predefined Host Checker antivirus, firewall, anti-spyware policies are enforced. This is the opposite of the typical recommended upgrade procedures.

Pulse 4.0R1 Client Software Upgrade

- Please refer to the Pulse Release 4.0 release notes.

Odyssey Access Client Upgrade

UAC Agent (OAC)

- An IC Series device can handle 1500 concurrent endpoint upgrades.

Standalone OAC Client

- This release supports the standalone, non-UAC version of Odyssey Access Client. Instructions for installing OAC on standalone clients are contained in the help guide under the section Getting Started > Initial Configuration.

Endpoint Security Assessment Plug-in (ESAP) Compatibility

- ESAP package version 2.1.9 is the minimum version to be compatible with Access Control Service version 4.4. The default version for ESAP is 2.2.9.

Network and Security Manager (NSM) Compatibility

- Access Control Service 4.4 has been qualified with NSM build 2010.3s9 and the release is 2012.1R3.
- NSM 2011.1S1 and later support MAG Series devices.

Resolved Issues in Release 4.4R1

The following are the issues that have been resolved in 4.4R1 Build 20957.

The identifier following the description is the tracking number in the Pulse Secure Problem Report (PR) tracking system.

- Access Control Service cannot do MAC address authentication with Enterasys switches. For MAC address authentication, Access Control Service requires that the password, username, and MAC address are all the same. When an Enterasys switch does MAC authentication, it uses a MAC authentication password chosen by the administrator. (812204: This issue has been resolved.)
- When Pulse prompts the user to upgrade and a compliance check fails, the upgrade might fail if the remediation window is displayed. Closing the remediation window might allow the upgrade to complete. (809992: This issue has been resolved.)
- Host Checker support of Predefined policies on Windows 8 endpoints is limited to Windows Defender 4.0 only with ESAP 2.2.4. Windows Defender needs to be manually turned off/on once on Windows 8 machines to enable the 'Check RTP status' Host Checker policy. (792564, 802832, 802855, 813340, 815559: This issue has been resolved.)

Pulse 4.4R1- Known Issues

The following issues have been reported for 4.4 features and were not resolved in the released software:

- OAC client is not supported with IC servers with Elliptic Curve Digital Signature Algorithm (ECDSA) certificates. (821109)
- IC with ECDSA certificate cannot communicate with SRX firewall as SRX does not support ECDSA certificates. (821711)
    - On Windows 8, EnableUA value is set to 0 in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System for remediating Windows 8 firewall. (845980)
    - When host check policies are enabled for Pulse with Sophos 8 Anti-Virus installed on Macintosh, the time to complete the checks may take longer than 35 seconds to complete. (827891)
    - To enable Anti-Virus or Firewall predefined host checks on Windows 8 with Pulse, ESAP 2.2.7 is required. (847310)

- In some scenarios if the inbound DMI was already enabled on that node before adding it to a cluster, the inbound DMI must be re-enabled again in that node once the cluster is formed. (840855)
- The configuration item under Configuration > Security > SSL Options > Require client certificate on these ports is not relevant to Access Control, and should not be configured. (845259)
- When <a href> and <script> html tags are used together in GUAM instructions Text box in IC admin UI, the option buttons are not ordered properly in the GUAM admin page (845189)
- In clusters with large configurations, Snapshot might take longer time to complete (842332)

Known Issues (Previous Releases)

The remainder of this document lists known issues from previous release, which are still outstanding in this release.

Access Control Service

- RADIUS proxy event logs log show the default timeout value but not the configured timeout value. (813572)
- IC-VA-SPE is supported beginning with Access Control Service 4.3R1. If you downgrade to an earlier release, the following message is not displayed due to a bug. "lower version of Pulse Access Control Service is not supported".
- If the service package you selected to install is older than the currently installed package, the device cannot preserve system configuration and user account settings. . Please contact Please contact Pulse Secure for support. (812034)
- EAP-TLS based 802.1x certificate authentication doesn't work on Android devices unless a value for 'anonymous identity' is supplied. This is because of a bug in Google Android OS. Please see: **http://code.google.com/p/android/issues/detail?id=36392**. (807883)

  Workaround - In addition to all required parameters for Wifi 802.1x connection, supply a value for 'anonymous identity' field in Android's wifi connection configuration dialog to get EAP-TLS based certificate authentication to work on Android devices.
- Admin user unable to close Task guidance option on the Admin UI of IC from IE9 browser. Work around is to enable the Compatibility view for the IE9. (806372)
- Realm Password Length Restrictions not working for Non JUAC protocols while doing OAC dot1x. (804851)
- The Pulse 8021x module restores the default Microsoft Wired autoconfig profile on uninstall and not the value that existed prior to installation of Pulse. The Pulse 8021x module also does not restore the Microsoft Wired-autoconfig service to the Pulse pre-install state and leaves the Microsoft Wired-autoconfig service "Automatic". (802778)

- IC allows creation of AD Auth server for same domain in both AD and AD Legacy Mode if same computer name in different case is used. (802194)
- Agentless Host Checker is unable to remediate HKLM Registry in Windows 7 and Windows 8 with User Account Control turned on. (787990)
- When Access Control Service is configured as an IF-MAP server employing IF-MAP replication, each IF-MAP server initiates a connection to its replicas. The connection originates from the internal interface. The source IP address of the connection is the address found in the **Access Control Service Network > Internal Port > Settings** page.
- Therefore, the replica IF-MAP servers must be reachable from that address. No attempt is made to initiate a connection from a VLAN port or from the external port. (787348)
- Rapid Configuration of VA-SPE and VA-IC with IPv6 Network Configurations is not supported (812100) When Pulse is configured with Minimal components, the user might be prompted multiple times to upgrade when connecting to a Pulse Secure Access server or Pulse Access Control server configured with either Host check polices or when Enhanced Endpoint Security (EES) is enabled. (802723)
- SCP of system snapshot from serial console is not supported over management port. instead use the internal port. (802265)
- When an ACE auth server is created in IC and if the system is upgraded before any user authentication against the ACE server, there is a possibility of false alarm "ACE Authentication Server internal upgrade failed" popping up during upgrade. (805278)
- In NSM, the error page "java.lang.NullPointerException" might be displayed when you are editing the IC Series device configuration. This happens in rare scenarios. As a workaround, load schema manually after applying it. (810435)
- On Blackberry phones, the IC user login page for Agentless access has very small font size for username and password text boxes. (800080)
- When logging in from a WIndows Mobile device for Agentless connection, the user home page shows a message 'Connection lost-retrying' after logging in. (804172)
- When use Machine Authentication with Pulse and the Odyssey Access Client on Windows 8, a system registry entry must be modified. Please see the Microsoft KB article **http://support.microsoft.com/kb/2743127** for details. (784981)
- L3 Java agent is not supported on Ubuntu 12.04 and OpenSuse 12.1. (804058, 798392)
- When an IC Series device is configured to use an Active Directory authentication server and SSO is enabled for the realm, the username specified in the OAC profile is displayed in the User Access log when a Host Checker policy fails. (512796)
- An Access Control Service device that is configured as an IF-MAP client connects using the internal IP port to the IF-MAP server. The source IP address of the connection is the address found in the **Network > Internal Port > Settings** panel. The IF-MAP server must be reachable from that address. The IF-MAP client does not attempt to connect via a VLAN port or via the external port. (545786)

- When a MAC Address Realm is associated with a MAC Authentication Server without LDAP support, the Administrator UI should not display a choice for any "User Attribute" under the role mapping rule. (555326)
- If you are using IF-MAP federation, an IF-MAP client might get into a state where the Events log fills up with this message:

  Error from IF-MAP server: "Failure: Another connection is already polling this session"

  In addition the client cannot import user sessions from IF-MAP, and both the client and the server might show high CPU usage.

  As a workaround, restart the IF-MAP client. Go to the IF-MAP Federation Overview page, select "No IF-MAP", click "Save Changes", restore the previous selection, and click "Save Changes" again.

  This problem might affect UAC versions 3.0 through 4.0. (526382)
- Coordinated Threat Control is not supported with overlapping IP addresses. (529530)
- The Attributes catalog window requires an LDAP server to be specified in the Mac auth Realm. If no server is specified, a blank window appears. (453246)
- If an auth table mapping policy is configured to always provision auth table entries to VSYS for all devices, Access Control Service provides auth table entry to JUNOS Enforcers as well. The workaround to not select the JUNOS Enforcer in an auth table mapping policy which is configured to provision auth table entries to VSYS for Infranet Enforcers. (424922)
- If you are using an imported root CA certificate, you must re-install the certificate if you restore the system configuration from a system.cfg or XML file. Imported root CA certificates are not properly included in a system restoration. (456144)
- Access Control Service might not send keepalive messages to the Infranet Enforcer while a second Infranet Enforcer is connecting. As a workaround, increase the keepalive timeout. (436732)
- When session extension is enabled, it is only supported by OAC if the EAP-JUAC protocol is enabled. (400631)
- On IC Series 6500, when Active Directory is used as the authentication server, only the domain name should be specified and not the Fully Qualified Domain Name (FQDN). (407271)
- The **IF-MAP Federation > Active Users > Imported** display includes interim sessions that are in the process of being imported. These sessions display with an IP address, but no username or roles. (411678)
- UAC firmware Release 4.0 and above provides additional features on the IC Series device. The additional features use more memory. Total memory usage varies by site and load. You might need to adjust the SNMP memory percentage trap to accommodate the increased memory usage. (382550)
- Active-active and active-passive clustering configurations over a WAN link are not supported.

- When upgrading from a previous release, you might see a number of the following entries in the event log:

  store key failed for key vc0/roles/role0000000001.000003.0/meetings/show_meeting_link value 0 created 1

  These entries can be ignored. (385063)

- Authentication fails when the supplicant is Odyssey Access Client, the protocol is non-EAP MS-CHAP-V2 in an EAP-TTLS tunnel, and the username has a decoration containing an @ character. To avoid this problem, change the protocol to EAP-MS-CHAP-V2. (380011)

- The UAC Password Management feature only supports GPO's in the default User container. If you are using authentication servers of the types Active Directory, or LDAP server as type Active Directory, and you have the Password Management features enabled on the realm, you may see errors in the user log. Access Control Service changes the user's password, but is unable to read and enforce other Active Directory password parameters specified by the policies outside of the default location. (372957)

- When defining IP pools, use a large range of IP addresses to avoid running out of IP addresses. (366541)

- Access Control Service does not allow outbound connections on the external interface. (370241)

- Access Control Service cannot process Infranet Enforcer destination zones that contain blank spaces in the zone name. Make sure that the Infranet Enforcer zone names used in IPSec definitions do not contain blank spaces. (361252)

- Access Control Service does not properly handle Infranet Enforcer connections over the VLAN interface. (367599)

- In an Active/Passive clustered configuration, and with multiple device certificates configured, the wrong certificate could be presented to the client during authentication. (370227)

- Location Groups and RADIUS Client configuration are now part of system configuration. As a result, if importing user and system configuration files from prior UAC versions (2.0Rx), you must first import the system configuration (system.cfg) followed by the user configuration (user.cfg). This upgrade procedure is also documented in the Administration guide. (372046)

- When a Host Checker policy fails with auto-remediation enabled, the resulting remediation instructions do not contain information about the action to be taken to auto-remediate the endpoint. (374822)

- The options "User may specify the realm name as a username suffix" and "Remove realm suffix before passing to authentication server" on the sign-in policy configuration do not apply to agentless authentication. (377212)

- In an Active/Passive cluster, if you have RADIUS Attributes Policies with the VLAN option selected, those policies must specify the internal or external interface. If they specify the "Automatic" interface and the active node fails, OAC fails to reconnect to the cluster and the user's session ends. (376451)

- When configuring 802.1X authentication, if the switch/AP does not listen to the session-timeout attributes on challenge response packets to control re-transmission timeouts, you must manually configure the re-transmission timeout on the switch/AP to 30 seconds or longer. (377413)
- Change password using MS-CHAP-V2 against an LDAP server is not supported. (376999)
- The Odyssey Users field on the Status page of Access Control Service depicts the number of OAC clients connected with an EE license. (375685)
- When configuring an Active Directory server on Access Control Service for authentication, note the following points:
    - Ensure that the AD server administrator you specify is a domain administrator in the same domain as the AD server.
    - Do not include a domain name with the server administrator username in the Admin Username field on the Authentication > Auth Servers > Active Directory / Windows NT page in the admin console.
- In agentless mode, new PIN mode does not work against an ACE authentication server when using custom sign-in pages. (377332)
- When an IF-MAP server is reconciling with a replica, you might see incomplete data if you navigate to IF-MAP Federation > This Server > Federation-Wide Sessions. Other IF-MAP clients see the same incomplete data. (396597)
- When a cluster publishes data to Access Control Service acting as an IF-MAP server, the Authenticated-By address viewable in the Federation Wide sessions display is the address of one node of the cluster. However, it is not necessarily the node that actually performed the authentication. (411038)
- When configuring an IF-MAP client and IF-MAP server to use certificate authentication, a device certificate signed by a Certificate Authority (CA) is required to be installed on the IF-MAP client. Please note that the default self-signed device certificate created at installation time cannot be used for this purpose. (413383)
- On the admin UI, under Configuration->User Realms-><REALM NAME>->Role mapping rules, there are three options:

    1. Merge settings of all assigned roles.
    2. User must select among the assigned roles.
    3. User must select sets of merged roles assigned by each rule.

    Of these options, the first one is never exported or imported via XML Export/Import. Instead, the system assumes that the first option applies (i.e. that it needs to Merge Settings for all Roles) if the second and third options are set to <false> in the imported XML document. (382974)

- IF-MAP might decrease the number of Coordinated Threat Control attack alerts received by an IF-MAP client due to batching of events within IF-MAP that is done to address performance concerns. In this case, a sensor event policy that is configured with an attack count greater than 1 might not to be triggered if all of the events are included in a single batch. (407232)
- In the IF-MAP Federation-Wide Sessions display, sessions without a signed-in IP Address are not shown when sorting by IP Address. (405919)
- When IF-MAP server is enabled on an IC6000, limit the size of log files to ensure that the total size of the log files is not larger than 500MB. (430784)
- CIDR notation is not a supported format for location awareness rules. The help text has been updated to reflect this. (PR 688155)
- The admin UI shows the wrong version when there is a version mismatch while joining a cluster. (700437)
    - When the client sends a TLS 1.2 ClientHello with no 'signature_algorithms' extension, then the IVE will not negotiate any cipher and the handshake will fail (837406)
    - A system configuration which contains an ECC certificate should not be imported into a platform which does not support ECC certificates. (834217)
    - After a TCP Dump capture of traffic on the device, when you select SSLDump to view the resulting traffic, application traffic cannot be deciphered with either ECDH or ECDHE based cipher suites. This will be true when ECC certificates are used on the network port. As a workaround, install an RSA certificate to another (for example, virtual) network port. Accessing the device with that network port will negotiate a cipher where the application data can be deciphered. (848061)
    - Apple OSX 10.8 (Mountain Lion) with Safari will not access an IVE interface associated with an ECC certificate. This issue is acknowledged by Apple (821519)
    - Certificate authentication doesn't work on Internet Explorer version 8, 9 and 10 if the browser's option "SSL 2.0" is enabled along with other SSL and TLS versions. Workaround is to disable SSL 2.0 in the browser (828640). This issue is acknowledged by Microsoft.
    - Admin should refrain from changing the cluster name when a cluster has been bound to a license server because the name change will not be propagated properly to the server. If the cluster name needs to be changed after binding a cluster to a server, the client configuration at the license server for each cluster node involved will have to be deleted and installed again after the cluster name change. (596739)
    - The configuration item under Configuration > Security > SSL Options > "Require client certificate on these ports" is not relevant to Access Control, and should not be configured. (845259)

Active Directory Authentication

- An XML import of Active Directory Legacy mode Active Directory authentication server configuration that was exported from an IC Series device cluster is not supported (676300)
- Creating two separate Active Directory authentication servers for same Active Directory domain either in Active Directory mode or in Active Directory legacy mode is not supported.
- The LDAP group search fields in Active Directory Legacy mode Active Directory auth server creation page does not appear as read-only for a read-only administrator. (711789)
- When SPNEGO SSO fails, the username is shown as 'System'. The username is normally retrieved from the Kerberos ticket. If decryption fails, this information is not available (732207)
- When the 'Enable periodic password change of machine account' setting for 'Active Directory' mode Active Directory authentication server is enabled after Access Control Service changes the computer account password in Active Directory, user authentication is disrupted for a brief period(few seconds) after which Access Control Service begins processing authentication and authorization requests using Active Directory. (737408)
- The use of groups from domains that are trusted by the Access Control Service domain via external one-way trusts, in IC's role mapping rules is not supported for 'Active Directory' mode Active Directory authentication server. (739825)
- If an 'Active Directory' mode Active Directory authentication server is in a realm, when the administrator is performing 'search groups' using a role mapping rule 'server catalog' window to build a groups catalog, the group search could fail with 'Error 1' if the Active Directory domain has more than 10000 groups. As a workaround, attempt the group search again. (745867)
- User login attempt fails with 'You are not allowed to sign-in' error and Access Control Service logs an '0xC00000B5' error in the user access log during group lookup if the realm uses the 'Active Directory' mode Active Directory authentication server for authentication and group lookup. As a workaround, attempt the authentication again. (746467)

Agentless Layer 3 Authentication with Smartphones

- With some non-multitasking operating systems, for example iOS on the iPhone, the browser session might get terminated after a heartbeat timeout. The browser on the device goes to sleep mode if it is not the front-most application, and it does not send a heartbeat to the server. As a result, the server terminates the session after the heartbeat timeout. As a workaround, enable "Allow VPN through Firewall" on User Role's Session Options. This allows traffic between the device and Enforcers to act as heartbeat. (670646)

EX Series Integration

- An 802.1x port might be left open despite failing authentication. This has been observed using JUNOS 9.1R1.8. To workaround this issue, upgrade to Release 9.1R2.10 or later. (298587)

- On an 802.1x enabled port with accounting enabled, Class attributes are not part of the Accounting start or stop requests. The Class attribute is necessary for correctly correlating the Accounting request with the session established on a UAC or an SBR RADIUS server. As a result, the session on the Access Control Service is not terminated. (299740)
- It has been reported that after a switch is rebooted, it might take up to 10 minutes to re-establish connectivity with the RADIUS server (IC). (300721)
- When COA Disconnect Messages are enabled on Access Control Service and 802.1 x-based authentications is configured using an EX Series switch, configuration changes on Access Control Service .resulting in a VLAN change on the switch port might not cause the UAC Agent to obtain an IP Address on the new VLAN until re-connecting via the UAC Agent. (417206)
- Reauthentication does not work with the EX Series switch when the EX Series switch is configured as a Junos Enforcer on Access Control Service. (742347)

Enterprise Guest Access License

- NSM does not support the EGA license version of the Access Control Service. (525179)
- If a bridge is enabled, and the management interface is also enabled, the event log periodically reports that the management interface gateway is unreachable, eventhough it is reachable. This log can be ignored. (733367)

Host Checker

- When a Host Checker policy fails using agentless authentication, the TRY AGAIN button might not cause the Host Checker policy to rescan the system after the remediation steps have been taken. (530449)
- Access Control Service Release 4.2 or higher does not support access from a Pulse 2.1 or earlier client with 'Any AV' OPSWAT policy. You must define a specific set of AVs, one or more of which you expect to be installed on the endpoints in the OPSWAT policy. (723968)

IC6500 FIPS

- During bootup, sometimes the FIPS card does not respond because the driver fails to load. FIPS related errors are displayed in the serial console, and the administrator cannot access the device. When this happens, the administrator should reboot the device, or remove the power from the device for 5 minutes and apply power again to resolve the issue. (679624)
- When a realm is using an 'Active Directory' mode Active Directory authentication server for authenticating and authorizing users, custom expression based role mapping rule that uses Active Directory user's group membership(groups and group.<group-name> variables) to determine roles does not work. (700122).

As a workaround, perform the following steps:

1. Navigate to the Realm's role mapping rules page, and click on the 'New Rule' button to create a new rule.
2. Select the 'Group Membership' option from the 'Rule Based On.' menu and click the 'update' button.
3. Click the 'Groups' button.
4. In the 'Server Catalog' window, click 'search' to search Active Directory for groups..
5. When the search returns the groups, select all groups and click 'Add', and then click 'OK' in the Server Catalog window.
6. Select the 'Custom Expressions' option from the 'Rule Based On.' menu and click the 'update' button.
7. Next, configure a custom expression based role mapping rule that uses Active Directory group memberships for mapping users to roles on Access Control Service.

Infranet Enforcer – Junos

- If an auth table mapping action is configured as "provision auth table as needed", Access Control Service terminates the existing sessions after RE failover. You must initiate new sessions. Existing sessions are not be affected after RE failover if the auth table mapping action is configured as "Always provision auth table". (416843)
- MAC address based authentication against Access Control Service does not work with J-series devices. (431595)
- The Infranet Enforcer does not perform CRL checking against the configured certificate profile. (451820)
- It was erroneously reported in previous UAC and Pulse documentation that using IPsec VPN required the establish-tunnels immediately option to be enabled. This is not a requirement, and is not recommended. (581360)
- An A/A cluster failover stops the access to resources for dynamically discovered sessions that are authenticated through an SRX Series device configured as a Layer 2 authenticator. (671481)
- IC-SRX takes10 minutes to establish communication after you reboot an SRX Series device configured in transparent mode. (672724)
- Captive portal redirection happens twice when you explicitly configure a redirect-URL on the SRX Series device. (677905)
- The SRX100 does not support Dynamic VLAN assignment. (694609)

Infranet Enforcer – ScreenOS

- When the X-auth server setting in a ScreenOS Infranet Enforcer is changed from NSM and updated, during IPSec resource access from the endpoint, IPSec access might not resume just by "Refreshing policy Actions" from the Admin UI. Issue the "exec infranet controller disconnect/exec infranet controller connect" command from the ScreenOS Firewall CLI to regain access. (516799)
- After completing a successful Authentication Request, the ScreenOS Enforcer does not send the Accounting Request. (458403)
- The ScreenOS Enforcer does not support IP address ranges that cross over class C, even though resource access policies defined on Access Control Service allows it. (385537)
- If you change the interface to which Access Control Service communicates, you must either restart the device or execute the following CLI commands on the Infranet Enforcer:
  - exec infranet controller disconnect
  - exec infranet controller connect
- Access Control Service sends a "set console page 0" command to the Infranet Enforcer, which disables console paging on the firewall. (369666)
- Do not create phase 2 proposals with spaces in the names. Access Control Service does not allow this. (373330)
- We suggests that DPD (Dead Peer Detection) should be enabled on policies defined in the ScreenOS Policy UI. (376385)
- If NSRP A/P cluster is running ScreenOS 5.4R8, Infranet auth table entries are not deleted from backup members of the NSRP A/P cluster when primary member disconnects from Access Control Service. (271375)
- If NS5400 is running ScreenOS 6.0R2, sometimes the Infranet Enforcer might stop processing traffic and might crash if the number of Infranet auth table entries on the device is greater than 2000. (259452)
- If NS5400 is running ScreenOS 6.0R2, the Infranet Enforcer could fail if the device has more than 5000 Infranet auth table entries and Access Control Service attempts to delete the Infranet auth table entries on the Infranet Enforcer. (255318)
- IPSec Policies are not supported in ScreenOS if the source zone of the IPSec policy is shared between ScreenOS Enforcer's Virtual Systems. (390805)
- IPSec is not supported if the source zone and destination zone are in a non-root VSYS of a Transparent mode ScreenOS Enforcer. (421126)
- If the ScreenOS Enforcer is running ScreenOS6.2R1,in NSRP L2 mode, and also configured to connect to Access Control Service using MGT interfaces, you might see continuous failures on both the back and the master NSRP members while a hardware session for traffic is being created in ScreenOS Enforcer. To resolve this issue, upgrade to ScreenOS 6.2R2. (413796)

- When an ISG-2000 running ScreenOS6.2R1 is configured with multiple virtual systems (VSYS) and UAC support is enabled for VSYS, the Firewall could crash while traffic is going through the Enforcer. (400899)
- If a ScreenOS Enforcer with VSYS configuration is in an NSRP cluster, and if auth table entries are deleted in one member of NSRP cluster, the other member does not delete the auth table entries. As a workaround, use ScreenOS 6.2R2. (401896)
- Occasionally, event logs might display messages like "Connection from IP 10.204.90.54 not authenticated yet (URL=/dana/js?prot=1&svc=1)" when ISG-IDP detects an attack from an authenticated user and Access Control Service terminates the user session as sensor action post attack notification. (682819)

MAG Series

- On MAG-SM160 or MAG-SM360 service modules, in the user interface under Maintenance and then System, the hard disk locations are reported opposite of actual placement in the chassis. Care should be taken when identifying the disk that has failed and requires removal. A failed disk in a RAID volume is properly identified by a red LED next to the failed drive in the rear of the chassis. (585496)
- The attempt to install multiple 'Role based firewall licenses' on MAG platforms using the download licenses feature gives 'Failed to install new license key' errors in the first attempt and installs only one license key. As a workaround, attempt the operation again. (747369)

Native iOS and Android Supplicant for 802.1x

- RSA SecurID authentication for Google Android and Apple iOS 802.1x supplicants is not supported with EAP-PEAP/EAP-GTC because of issues in Android and iOS. (678661)

Network and Security Manager

- Please note that NSM-related issues for UAC 4.0 are documented in the NSM 2008.2 release notes.
- When creating a new or modifying an existing sign-in policy from NSM, a trailing '/' must be appended to the sign-in URL. For example, '/test-url/' instead of '/test-url' as would be entered in the web admin UI. (442853)
- The user expiration field should come after the password field for Local authentication of new users in NSM UI. (411366)
- When creating new Sign In pages from NSM for IC Series device, the Default Portal name is "Secure Access SSL VPN" instead of " IC Series device ". (440128)
- The 'Current preconfiguration file' under Role's Agent->Odyssey Settings->Preconfigured installer tab should specify a file name to ensure that the IC Series device associates the preconfiguration file with that role. (441804)
- The log viewer does not show all the roles in 'roles' field for traffic log from ScreenOS FW if there are 200 roles in role's field. (441370).
- When configuring a sensor from NSM, you must assign a One Time Password. (417136)

- When importing an IC Series device Active/Active cluster into NSM, log synchronization should be enabled to ensure logs are properly sent. (386132)
- Using NSM, applying a template promoted from one cluster to another might fail if the Sensor OTP field is left blank. (385985)
- No validation exists in the NSM client when entering a value for System->Configuration->Global security->settings->Lockout period. As a result, updating the device fails if you enter an invalid value. Valid range is 1 – 10081 minutes. (384524)
- The default NSM Agent configuration port should be set to 7804. This setting is found on the Configuration > NSM Agent > NSM Settings > Primary port page. (380220)
- If a device is added to NSM and the platform is not specified correctly (e.g. adding an IC4000 as an IC4500), the device could cause high CPU utilization. As a workaround, specify the correct platform when adding the device to NSM. (385121)
- The option 'Bandwidth Management' under System->Network->Overview for an IC device should be ignored. This option does not apply to the IC Series device. (384786)
- Host Checker Statement of Health rule types are visible within NSM client even if SOH license not installed on IC. (384841)
- When configuring RADIUS Parameters within NSM, there is no option for creating "Custom challenge expressions". (383475)
- When configuring RADIUS Attribute Policies within NSM, it is not possible to modify the values of existing attributes. Attributes should be deleted and re-created if changing the value within NSM is required. (406154)
- Management of 'Active Directory' mode AD auth server configuration from NSM is not supported. (747864)

OAC (Vista Only)

- On Vista and Windows 7, OAC's setting "After Windows logon, before the desktop appears" connection setting does not work. Due to Microsoft's implementation of Session 0 Isolation in Windows Vista and beyond, it is not possible to display prompts or perform authentication operations requiring a user mode process after the Credential Provider but before OAC's desktop application is started. This mode is not supported on Windows Vista and Windows 7 and further versions of Windows. If connectivity is required prior to the users desktop appearing, install and configure the OAC Credential Provider (Odyssey Access Client Administrator / Connection Settings / GINA). (503819)
- The OAC Manager icon for Vista64 is located in the Control Panel under the following location:
    1. Open the Control Panel.
    2. Click "Control Panel Home".
    3. Click the "Additional Options" icon
    4. Click "View 32-bit Control Panel"

5. Close OAC Manager.
6. Double click the OAC Manager Icon in the Control Panel and the OAC Manager should be displayed. (404289)Close OAC Manager.

- After upgrading from 2.1R5 to 2.2, on some machines, OAC might display the following status "ERROR(UNKNOWN)". This is caused by the following Microsoft bug: **http://support.microsoft.com/?kbid=905238**
  As a workaround, upgrade to Windows Vista SP1. (385084)
- Although multiple static WEP keys can be configured, only the highest ordinal key is used. (379577)
- 'Survey Airwaves' in OAC does not retrieve the list of networks for some models of network adapters. This can be resolved by upgrading the wireless NIC driver from the NIC manufacturer. (375258, 375260)
- OAC on Vista does not support WPA2 Fast Roaming. (374454)
- OAC does not recognize that a wireless card has been removed for about 30 seconds. (374875)
- Static keys with open/WEP (authentication) and MD5 (encryption) do not succeed in providing network connectivity on Vista. (377446)
- If User Account Control is enabled on Vista, auto-remediation to enable the Microsoft firewall does not work. (377596)
- Certain applications running on Vista (for example,. Lenovo's ThinkVantage Access Connections software) might cause OAC to not work properly when configuring peer-to-peer wireless networks. In addition, ad-hoc WPA/WPA2 is not supported on Vista. (376485)
- Some auto-remediation actions do not work on Vista as they require the service to interact with the desktop. (375842)
- Registry auto-remediation does not work on Vista. (375612)
- On certain Cisco access points, it has been observed that if an invalid password is entered during authentication, OAC continues to attempt to connect, and no failure is reported. Ensure that the password entered is correct. (375268)
- License keys cannot be added to OAC if User Account Control is enabled on Vista. As a workaround, use Odyssey Client Administrator to enter the license keys. (375317)
- When upgrading OAC from UAC 2.2R5, the installation might not complete once the message "Installing UAC agent. Please wait" is displayed. As a workaround, cancel the installation and download and install the MSI. (462875)

OAC (Macintosh Only)

- OAC on Macintosh only supports Apple Macintosh integrated Airport wireless adapters.
- OAC and the Apple 802.1x client do not interoperate. To resolve this interoperability issue, do the following:
- On Mac OS X 10.5:
    1. From 'System Preference,' open AirPort Network configuration.
    2. Disable the check box for 'Ask to join new networks.'
    3. Click 'Advanced...' to view Advanced settings of Airport.
    4. Remove all networks from 'Preferred Networks' and uncheck "Remember any network this computer has joined". Click 'OK' and then click 'Apply'.
    5. If OAC still does not connect with status showing: adapter not available, then reboot the system.
- On Mac OS X 10.4:
    1. From 'System Preference,' open AirPort Network configuration.
    2. Change the 'By default, join' setting to 'Preferred networks' and remove all of the networks from the list below.
    3. Click 'Options' button and ensure that 'Keep looking for recent networks' is enabled.
    4. Uncheck 'Automatically add new networks to the preferred networks list'. Click 'OK' and then 'Apply Now'.
    5. Open 'Internet Connect' in 'Applications' and click on the '802.1X' icon.
    6. Click 'Disconnect' (if you are not currently connected, the button shows 'Connect', and you can skip this step.)
- After installing OAC on a system that has OAC 4.3 installed the Dock might contain two Odyssey Access Client Manager icons. To resolve this issue, uninstall OAC 4.3 prior to installing OAC. (417980)
- When a Host Check policy fails compliance on OS X 10.4 and the user clicks the "How do I resolve this problem?" link, the remediation information appears for a moment and then disappears. To redisplay the remediation information, either maximize or re-size the remediation windows. (438311)
- When OAC is configured for EAP-FAST and the user responds to the acquire new credentials prompt, the connection status displays "Requesting authentication" indefinitely. To successfully establish the network connection, click the "Reconnect" button or uncheck/recheck the connection checkbox. (451119)
- Do not create a shortcut to the installed Odyssey application. The OAC application is dependent on the directory structure created during installation and does not work correctly if invoked from a shortcut. (418319)

- When the client receives a Coordinated Threat Control message from an IC Series device, the remediation message shown might contain an invalid link for more information. (437516)
- When an environment variable is used in a Host Checker policy such as <%user.home%>, the Host Check policy fails. (442042)

OAC (Windows 7 Only)

- Attempting to download OAC from Access Control Service with Internet Explorer 8, the "Program compatibility Assistant" message might appear stating that the pulsesetupclientinstaller might not have installed correctly. (450412)

Odyssey Access Client

- When Odyssey Access Client (OAC) is configured to use a certificate for authentication using automatic certificate selection and no user certificates are available, we expect a successful TTLS/PEAP authentication session that does not require a certificate to resume upon re-authentication. The feature does not behave as expected. (558243)
- When creating a profile intended for a Layer 2 connection with EAP-GTC as the only protocol in the inner set, that profile should not be used for a Layer 3 connection. The username/password prompt occurs at the start of the connection, and the inner protocol might or might not require a password to succeed. (509017)
- When configuring or using smart card certificates whose Cryptographic Service Provider or middleware automatically registers the certificate with the operating system, you might receive a warning that some certificates cannot be listed and/or the smart card reader cannot be found. Insert the smart card and retry the operation, or select a different certificate. (506963)
- When upgrading OAC from an IC with the end-user localization option set to automatic, the upgrade prompt is displayed in English. As a workaoround, set the end-user localization option to a specific language. (420032)
- The OAC and the CheckPoint VPN services do not interoperate when using 'UDP encapsulation' on the IPsec routing policy. As a workaround, unbind the "CheckPoint Securemote" IM driver from your physical adapter. (522200)
- When installing OAC on a system with the Deterministic Network Enhancer (DNE) installed, you might encounter the error "An error has occurred while installing the IM driver. Installation will not continue." To resolve this problem, uninstall DNE and then install OAC. (432886)
- When OAC is installed and the user attempts to connect to Secure Access SSL VPN with AED policy enabled using Network Connect and AED on the client requires updating, the OAC connection status "Odyssey is not running" might appear. (452778)
- When attempting to authenticate to Access Control Service with Kaspersky Anti-Virus for Windows Workstations 6.0 installed, the client is remediated with the following message: "Kaspersky Antivirus for Windows Workstations 6.0.2.700 does not comply with policy. Compliance requires real time protection enabled." (445289)

- OAC might display the error string “Error (other JUAC failure)” when using a revoked client certificate. (376112)
- For certificate checking to work, the root CA of the chain that signed the server certificate of the Access Control Service must be installed in the certificate store of the endpoint. The initial configuration script installs this certificate if the certificate is added to the Access Control Service Trusted Server CAs certificate store. (367923)
- In some cases, selection of “After my desktop appears” in the “Connection Settings” of the OAC Administrator may not have been effective, and OAC might have been starting the connection before the desktop appeared. If you are satisfied with the old behavior, select “After Windows logon, before the desktop appears” to restore the original behavior. (384280)
    - Some RADIUS servers fail to authenticate when an empty EAP-Response/Identity is sent. If no login name is configured in a profile and the anonymous identity does not apply, or if other methods such as GINA or automatic certificate selection have not located an appropriate login name, “none” is used. As a workaround enter a login name in the profile used. (385169)
- After configuring a machine account and saving the settings in a .MSI file, a reboot is required once the configuration settings have been installed on the client machine. (384095)
- Multiple prompts to upgrade OAC can occur if a user chooses not to upgrade OAC and subsequent re-authentication attempts occur. (383822)
    - The Kaspersky antivirus web scanner can cause OAC or Pulse to fail to connect. If you are running Kaspersky antivirus, and after successfully authenticating an interface using 802.1x, the IC Series device status is “terminated”, disable the web-scanner (port 443) in Kaspersky antivirus. (381018)
    - While upgrading to OAC 5.x, long delays might occur attempting to replace certain OAC components that are in use by other services. In these cases, after upgrading a reboot might be required. (380214)
    - Extended characters cannot be used in the “Role message” displayed to users for coordinated threat control (CTC). (379780)
    - If there is a previous version of OAC with an EE license installed in the client and a connection is made to an IC Series device, the client is upgraded with a 5.0 EE license. (377672)
    - In some circumstances, the Pulse Secure network driver cannot be uninstalled correctly. This can hang the installer or make the installation of the new version fail. If the installation of OAC hangs for more than 5 minutes, or if after upgrading OAC, you receive the message “Unable to load module jnprnaapi.dll”, reboot. If rebooting does not resolve the issue, you must uninstall and then reinstall the OAC software. (378397)
- If Odyssey Access Client is installed over Network Connect, the installer attempts to shut down Network Connect and the Network Connect session is disconnected. You must manually restart Network Connect after the OAC upgrade has completed. (367257)
- If the Nortel Contivity client is installed after the Odyssey Access Client is installed, the endpoint must be rebooted to ensure proper installation of Nortel Contivity. (367684)

- When the virtual adapter is used, the first TCP connection might take up to 15 seconds. (369746)
- If an endpoint has multiple interfaces, and the route to the protected resource is different from the route to the Infranet Enforcer, the endpoint cannot access the resource. (369230)
- See the Supported Platforms Guide for a list of 3rd party VPN clients that were tested with the OAC. (368606, 368644)
- The NAT-T Status information displayed in the OAC IPSec Configuration window should be ignored. (367927)
- Pre-configuration of the Odyssey Access Client MSI invalidates the signature. Administrators must re-sign the new MSI with their own certificate before deploying to their users. (369685)
- Wireless suppression might not work with some versions of VMware. (370210)
- Customers running OAC 4.52 in FIPS mode should uninstall 4.52 prior to upgrading to the 5.x client. (370325)
- Endpoint Session scripts can be configured for each user role on the IC Series device. However, OAC can execute at most one End Session script on the endpoint. (370299)
- If Network Connect version 5.3R6 or older is installed on the endpoint, installing OAC causes Network Connect to malfunction by remaining in the "Connecting" state. To fix this problem, the user must do the following: (369025)

    1. Uninstall Odyssey Access Client.
    2. Upgrade Network Connect to IVE version 5.4 or later.

- The installation of OAC using a web browser requires the user to sign in. When OAC starts, the user is prompted to sign-in again a second time. Session resumption does not work in this case and two Access Control Service sessions are created. (374388)
- If the IC Series device is configured to support NAT Traversal for IPSec traffic, connecting and disconnecting the OAC client a number of times might result in the virtual adapter being installed. (375351)
- The realm and role selection is not saved during authentication at Gina time. (376883)
- Patch assessment compliance checks can take nearly 20 seconds to complete. As a result, authentication takes longer and consumes more CPU on the client machine. (375897)
- Certain versions of the SHUNRA networks WAN emulator driver might not be compatible with the Pulse Secure Agent. You might experience a system crash. Disable the SHUNRA driver. (374274)
- The text displayed during the OAC installation might not be displayed in the local language. (399004)
- When prompted to reboot during a new install/upgrade, IC Access settings are not applied if you answer 'Yes' to the reboot prompt. We suggest answering 'No', and then reboot after the installation has completed. (417225)

- OAC does not support Mac OS X 10.7 (Lion) and 10.8 (Mountain Lion). (658607)
- OAC on Mac OS X does not support configuring a Wi-Fi network for 802.1x with WEP. Configure the AP for WPA or WPA2 instead. (613664)
- Assigning a device certificate to a VLAN interface is not supported in this release. (705493)
- With SUSE 11.4 and Firefox 4 and above, agent heartbeats are sent to IC but the icon is not displayed on the client end. Java SE JRE should be used instead of OpenJDK as the SE version is more stable for the L3Agent applet. (718396)
- When attempting to install OAC on a non-English version of Windows, all the MSI command prompts appear in English (548674).
- The user from a client machine can connect to Access Control Service using both OAC and Pulse if Kaspersky is installed. This has been tested with Kaspersky Anti-Virus 6.0 for Windows Workstation MP4 and Kaspersky Internet Security 2011. (698440)

SQL Authentication Server

- When trying to populate the server catalog attributes for the SQL server, you must enter data into all columns of interest for a particular record. Columns that are not assigned data are ignored during the lookup and are therefore not added appropriately to the server catalog. (670775)

Requesting Technical Support

To open a case or to obtain support information, please visit the Pulse Secure Support Site: **http://www.pulsesecure.net/support.**