Release Notes

Juniper Networks

Unified Access Control 4.0 (IVE 7.0)
Odyssey Access Client 5.2
UAC Build# 14913
OAC Version 5.20.14913.0
Pulse Version 1.5.0.6541
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper Networks UAC 4.0 New Feature Summary</td>
<td>1</td>
</tr>
<tr>
<td>Junos Pulse 1.0 and UAC</td>
<td>1</td>
</tr>
<tr>
<td>Guest User Account Manager (GUAM)</td>
<td>1</td>
</tr>
<tr>
<td>Captive Portal (Traffic Redirection) with SRX Series Services Gateways</td>
<td>1</td>
</tr>
<tr>
<td>Coordinated Threat Control (CTC) with SRX Series Gateways</td>
<td>1</td>
</tr>
<tr>
<td>Customizable Agentless Web Page</td>
<td>1</td>
</tr>
<tr>
<td>No Separate Coordinated Threat Control License Required</td>
<td>1</td>
</tr>
<tr>
<td>IC4500 UAC Appliance Mixed Mode Configuration</td>
<td>1</td>
</tr>
<tr>
<td>Interoperability and Supported Platforms</td>
<td>1</td>
</tr>
<tr>
<td>Endpoint Security Assessment Plug-in (ESAP) Availability</td>
<td>1</td>
</tr>
<tr>
<td>Supported NSM releases</td>
<td>1</td>
</tr>
<tr>
<td>Upgrading to this Release</td>
<td>1</td>
</tr>
<tr>
<td>IC Series Device Upgrade</td>
<td>2</td>
</tr>
<tr>
<td>Installing Odyssey Access Client (OAC)</td>
<td>2</td>
</tr>
<tr>
<td>UAC Agent (OAC)</td>
<td>2</td>
</tr>
<tr>
<td>Standalone OAC Client</td>
<td>2</td>
</tr>
<tr>
<td>Fixed Bugs and Enhancements for this release (UAC 4.0, OAC 5.20.14877.0)</td>
<td>2</td>
</tr>
<tr>
<td>IC Series Device</td>
<td>2</td>
</tr>
<tr>
<td>Odyssey Access Client (OAC)</td>
<td>2</td>
</tr>
<tr>
<td>Odyssey Access Client (OAC) on Vista</td>
<td>3</td>
</tr>
<tr>
<td>Odyssey Access Client (OAC) on Macintosh</td>
<td>3</td>
</tr>
<tr>
<td>Network and Security Manager (NSM)</td>
<td>3</td>
</tr>
<tr>
<td>Known Issues and Limitations</td>
<td>3</td>
</tr>
<tr>
<td>IC Series Device</td>
<td>3</td>
</tr>
<tr>
<td>Odyssey Access Client (OAC)</td>
<td>5</td>
</tr>
<tr>
<td>Odyssey Access Client (OAC) on Vista</td>
<td>8</td>
</tr>
<tr>
<td>Odyssey Access Client (OAC) on Windows 7 Build 7201</td>
<td>9</td>
</tr>
<tr>
<td>Odyssey Access Client (OAC) on Macintosh</td>
<td>9</td>
</tr>
<tr>
<td>Infranet Enforcer (IE) - ScreenOS</td>
<td>10</td>
</tr>
<tr>
<td>Infranet Enforcer (IE) – JUNOS (SRX and J-series)</td>
<td>11</td>
</tr>
<tr>
<td>JUNOS-EX (EX)</td>
<td>11</td>
</tr>
<tr>
<td>Network and Security Manager (NSM)</td>
<td>11</td>
</tr>
<tr>
<td>Communicating Issues and Bugs</td>
<td>12</td>
</tr>
<tr>
<td>Documentation Errata</td>
<td>12</td>
</tr>
</tbody>
</table>
Juniper Networks UAC 4.0 New Feature Summary

Junos Pulse 1.0 and UAC
Junos Pulse is an integrated, multi-service network client enabling anytime, anywhere connectivity, security, acceleration and collaboration with a simplified user experience. When deployed as the client for UAC, Junos Pulse helps UAC deliver dynamic, granular identity- and role-based local network access control (NAC).

Guest User Account Manager (GUAM)
This feature enables enterprise employees to create guest user accounts dynamically.

Captive Portal (Traffic Redirection) with SRX Series Services Gateways
When an unauthenticated user attempts to access a resource protected by a UAC policy and policy enforcement points, packets are dropped; if a web browser is used, administrators have the option to redirect the user to an IC Series appliance for authentication.

Coordinated Threat Control (CTC) with SRX Series Gateways
Coordinated Threat Control with UAC is now supported with SRX-3000 Series and SRX-5000 Series gateways.

Customizable Agentless Web Page
This feature allows administrators to customize the UAC’s agentless mode web page.

No Separate Coordinated Threat Control License Required
A separate Coordinated Threat Control (CTC) license is no longer required when CTC is implemented with the IDP Series Intrusion Detection and Prevention Appliances, ISG/IDP, or with SRX Series gateways.

IC4500 UAC Appliance Mixed Mode Configuration
A single IC4500 appliance may be used as an Interface Metadata Access Point (IF-MAP) server and UAC policy server simultaneously.

Interoperability and Supported Platforms
- Please refer to the Supported Platforms document for supported versions of Screen OS, JUNOS, browsers, and operating systems in this release: http://www.juniper.net/techpubs/software/uac/4.0.

Endpoint Security Assessment Plug-in (ESAP) Availability
- ESAP packages for UAC 4.0 are available for download from the following URL: http://www.juniper.net/techpubs/software/uac/esap
  Log in with your Juniper support account to download any ESAP packages.

Supported NSM releases
The UAC 4.0 release has been qualified with the following NSM releases:
- 2010.1 and 2010.2.

Upgrading to this Release
IC Series Device Upgrade
1. Automatic updates to this release are supported for all UAC releases after and including UAC 2.2 R1 Build 11657.

Installing Odyssey Access Client (OAC)

UAC Agent (OAC)

The IC Series device is capable of handling 1500 concurrent endpoint upgrades. Anything beyond this may require administrators to upgrade endpoints prior to upgrading the IC Series device using some other mechanism such as Microsoft Systems Management Server (SMS).

Standalone OAC Client

This release also supports the standalone, non-UAC version of Odyssey Access Client. Instructions for installing OAC on standalone clients are contained in Chapter 2, Installing OAC, of the Odyssey Access Client User Guide.

Fixed Bugs and Enhancements for this release (UAC 4.0, OAC 5.20.14877.0)

IC Series Device

- A process snapshot for "radius" was generated if RADIUS requests arrived while the RADIUS server on an IC Series device was shutting down. (461084)
- Group lookup after Kerberos SSO authentication using Active Directory group membership failed if the user was a member of a child domain in the forest for the configured domain controller authentication server. (444375)
- When an un-authenticated user tried to access a web resource which was protected by dynamic IPSec policy, the IC sometimes gave an error: "An error occurred provisioning access for http://<ip-address-of-resource>/ Please contact your administrator". (436724)
- If a sensor reported an event by attaching it to an IP or MAC address in an IF-MAP server, an IC Series device failed to respond to the event. This happens if the IF-MAP client is IC C3.1 or earlier or SSL-VPN 6.1 or earlier and the IF-MAP server is non-Juniper or is IC C4.0 or later. (459067)
- The IF-MAP client can lose communication with the IF-MAP server and incur communication errors very rapidly. The client's event log contains a message like the following, repeatedly: “Error communicating with IF-MAP server ‘https:// ifmap.acme.com/ dana-ws/ soap/ d sifmap: Fatal error:”. Both the client and the server may show high CPU utilization. This problem can occur when the client is IC C3.1 or SSL-VPN 7.1. (462681)
- The IC Series device incorrectly displayed the auto upgrade prompt for previously installed UAC Agents even though the “Enable automatic upgrade of UAC Agent” option was unchecked. (461707)
- When the IC Series device was configured for use with Remote Integrity Measurement Verifiers (IMV), performance of the IC was significantly impacted. (450733)
- The backup RADIUS server is no longer ignored for RADIUS proxy requests. (376583)
- When a custom Radius Dictionary was added, the attributes were not automatically updated to NSM for use in Radius return/request policies and attribute logging. (454722)

Odyssey Access Client (OAC)

- When a proxy was configured in the user’s browser and AED was enabled, OAC could not download AED signature updates. (460534)
- The OAC adapter icons appeared grayed out during long host check scans. (459087)
- When used with Internet Explorer 7, host check scans took a long time to complete. (444181)

**Odyssey Access Client (OAC) on Vista**
- When attempting to install the Advanced Endpoint Defense (AED) either from Internet Explorer 8 or from an already installed OAC client, the following error may occur: “AED failed to initialize. Contact system administrator”. (448121)

**Odyssey Access Client (OAC) on Macintosh**
- When importing a script from Windows with an IC Series device profile, OAC display an error: “This file could not be opened because it could not be accessed, or is not a valid Odyssey script”. (438977)
- Safari 4 is supported in this release. (446272)
- When connecting to an IC Series device with a profile that has server verification enabled, the “Verify Certificate” windows appeared hidden behind the Odyssey Access Client Manager windows. (451365)

**Network and Security Manager (NSM)**
- A major alarm for “long re-join time” was sent incorrectly by IC cluster members to NSM, and displayed in the NSM UI. (465880)

**Known Issues and Limitations**
The following lists known issues which are still outstanding in this release:

**IC Series Device**
- Given a configuration with 2 federation clients, one federation client may incorrectly grant the other one access to a protected resource in some cases when it should not. This is possible since the federation clients are assumed to be trust worthy. Workaround is to deny federation client access to connect to federation server. (492596)
- Sessions exported to IF-MAP solely for session migration do not appear in the "Federation-Wide Sessions” view on the IF-MAP server. To work around this issue, configure an IF-MAP Session-Export Policy on the IF-MAP client device. (522469)
- Although a particular username may have two or more sessions at a time, keep the number of sessions per username per realm under 4000. With more sessions, internal errors may happen and be logged as critical events in the system event log. (515306)
- The Attributes catalog window requires an LDAP server to be specified in the Mac auth Realm. If no server is specified, a blank window will appear. (453246)
- If an auth table mapping policy on the IC Series device is configured to always provision auth table entries to vsys for all Infranet Enforcers, the IC will provide auth table entry to JUNOS Enforcers as well. The workaround is not to 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 on the IC Series device, 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)
- The IC Series device may miss sending keepalive messages to the Infranet Enforcer while a second Infranet Enforcer is connecting. The workaround is to increase the IC Series device keepalive timeout. (436732)
- When session extension is enabled on the IC Series device, it is only supported by OAC with the EAP-JUAC protocol enabled. (400631)
- On the IC Series 6500, when an Active Directory is used as the Authentication Server, only the domain name should be specified and not the Fully Qualified Domain Name. (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 4.0 and above provides additional features on the IC Series device. The additional features will use more memory. Total memory usage will vary by site and load, but you may need to adjust your 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 may 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 safely 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 auth servers of type 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 IC User log. The IC will change the user’s password, but will be unable to read and enforce other Active Directory password parameters specified by the policies outside of the default location. (372957)
- When defining IP pools in the IC Series device, use a large range of IP addresses to avoid running out of IP addresses in IP pools. (366541)
- The IC Series device does not allow outbound connections on the external interface. (370241)
- The IC Series device cannot process Infranet Enforcer destination zones that contain blank spaces in the zone name. Make sure the Infranet Enforcer zone names used in IPsec definitions do not contain blank spaces. (361252)
- The IC Series device does not properly handle Infranet Enforcer connections over its 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 resultant remediation instructions do not contain any information about what action will 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 any RADIUS Attributes Policies with the “VLAN” option selected, those policies should specify the “Internal” or “External” interface. If instead they specify the “Automatic” interface and the active node fails, OAC will fail to reconnect to the cluster and the user’s session will end. (376451)
- When configuring 802.1x authentication, in case 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 the IC Series device depicts the number of OAC clients connected with an EE license. (375685)

• When configuring an Active Directory (AD) server on the IC Series device for authentication, note the following points:
  1. Ensure that the AD server administrator you specify is a domain administrator in the same domain as the AD server.
  2. 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 IC Series device Web 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 may see incomplete data if you navigate to IF-MAP Federation > This Server > Federation-Wide Sessions. Other IF-MAP clients will see the same incomplete data. (396597)

• When an IC or SA cluster publishes data to an IC acting as an IF-MAP server, the Authenticated-By address viewable in the Federation Wide sessions display will be 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 IC device web admin UI, under Configuration->User Realms-><REALM NAME>->Role mapping rules, there are three options: (radio buttons)
  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 may 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 attack count greater than 1 may not 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)

Odyssey Access Client (OAC)

• During Odyssey upgrade, you may see an error popup that says:

  "OdTray.exe failed to stop. Would you like to retry? If you choose Cancel a reboot will be required at the end of the install."

  Click Cancel to allow upgrade to proceed.

  After upgrade, you will see another popup that says:
"A reboot is required to finish this install. Do you want to reboot your computer? Click Yes to reboot now or No to reboot later."

Click Yes.

During reboot, you will see another popup:
"The application failed to initialize because the window station is shutting down"

You can either ignore this or click OK.

After your machine reboots, Odyssey will be successfully upgraded. (547906)

- The Odyssey Access Client and CheckPoint’s VPN do not interoperate when using ‘UDP encapsulation’ on the IPSec routing policy. Workaround is to unbind “CheckPoint Secureremote” IM driver from your physical adapter. (522200)

- When installing OAC on a system with the Deterministic Network Enhancer (DNE) installed, you may 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 via Network Connect and AED on the client requires updating, the OAC connection status "Odyssey is not running" may appear. (452778)

- When attempting to authenticate to an IC Series device with Kaspersky Anti-Virus for Windows Workstations 6.0 installed, the client will be remediated with the following message: “Kaspersky Anti-Virus for Windows Workstations 6.0.2.700 does not comply with policy. Compliance requires real time protection enabled.”. (445289)

- OAC may 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 IC must be installed in the certificate store of the endpoint. The initial configuration script will install this certificate if the certificate is installed on the IC in "Trusted Server CAs". (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 may have been starting the connection before the desktop appeared. If customers were satisfied with the old behavior, then they can select "After Windows logon, before the desktop appears" to get the old behavior back. (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" will be used. Workaround is to enter a login name in the profile used. (385169)

- Microsoft Windows XP SP3 Enhanced Cryptographic Provider (RSAENH) is still under evaluation. As a result, enabling FIPS on XP SP3 will cause authentication failures. (383527)

- 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 user chooses not to upgrade OAC and subsequent re-authentication attempts occur. (383822)

- Kaspersky anti-virus web scanner can cause OAC to fail to connect to the IC. If you are running Kaspersky anti-virus, and after successfully authenticating an interface via 802.1x, the " IC Series device " status is "terminated", disable the web-scanner (port 443) in Kaspersky anti-virus. (381018)
While upgrading to OAC 5.x, long delays may occur attempting to replace certain OAC components that are in use by other services. In these cases, after upgrading a reboot may 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 will be upgraded with a 5.0 EE license. (377672)

In some circumstances, the Juniper Networks network driver cannot be uninstalled correctly. This can hang the installer, and/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", one of the following two steps may clear up the problem.

1) Reboot, if this does not clear up the problem then
2) Uninstall OAC and reinstall.

If the above steps do not fix the problem, please contact Juniper Networks TAC for assistance. (378397)

If Odyssey Access Client is installed over Network Connect, the installer will attempt to shut down Network Connect and the Network Connect session will be disconnected. You must manually re-start 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 may take up to 15 seconds. (369746)

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 to the
IC Series device will take longer and consume more CPU on the client machine. (375897)

- Certain versions of the SHUNRA networks WAN emulator driver may not be compatible with the Juniper Network Agent. You may experience a system crash. Disable the SHUNRA driver. (374274)

- Odyssey may not be able to connect to IC’s properly when running Windows XP SP2 and you have multiple network adapters present. Users who experience this issue should install the following patch from Microsoft: http://support.microsoft.com/kb/913522/en-us (399168)

- The text displayed during the OAC installation may not be displayed in the local language. (399004)

- When prompted to reboot during a new install/upgrade, IC Access settings will not be applied if you answer 'Yes' to the reboot prompt. Suggest answering 'No' and reboot after install has completed. (417225)

**Odyssey Access Client (OAC) on Vista**

- On Vista and Win7, 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. Thus, this mode is not supported on Windows Vista and Windows 7 and further versions of Windows. If connectivity is required prior to the user's 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)

- After upgrading from 2.1R5 to 2.2, on some machines, OAC may display the following status “ERROR(UNKNOWN)”. This is caused by the following Microsoft bug: http://support.microsoft.com/?kbid=905238
  The workaround is to upgrade to 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 (e.g. Lenovo's ThinkVantage Access Connections software) may 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 will 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’s been observed that if an invalid password is entered during authentication, OAC will keep trying and no failure will be reported. Ensure that the password entered is correct. (375268)
• License keys cannot be added to OAC if User Account Control is enabled on Vista. Workaround is to use Odyssey Client Administrator to enter the license keys. (375317)
• Credential Provider is not supported on 64-bit Vista (400640)
• When upgrading OAC from UAC 2.2R5, the installation may not complete once the message “Installing UAC agent. Please wait” is displayed. To workaround this issue, cancel the installation and download and install the MSI. (462875)

**Odyssey Access Client (OAC) on Windows 7 Build 7201**

• Attempting to download OAC from an IC Series device with Internet Explorer 8, the “Program compatibility Assistant” message may appear stating that the Juniper setupclientinstaller might not have installed correctly. (450412)

**Odyssey Access Client (OAC) on Macintosh**

• OAC on Macintosh only supports Apple Macintosh integrated Airport wireless adapters.
• The Odyssey Access Client and the Apple 802.1x client do not interoperate. To resolve this interoperability issue, do the following:
  • On Mac OS X 10.5:
    1. Open AirPort Network configuration from 'System Preferences'.
    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. Open AirPort Network configuration from 'System Preferences'.
    2. Change '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 already installed, the Dock may contain have 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 will appear for a moment and then disappear. 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 will display “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 will not work correctly invoked from a shortcut. (418319)

• When the client receives a Coordinated Threat Control message from an IC Series device, the remediation message shown may 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 will fail. (442042)

**Infranet Enforcer (IE) - ScreenOS**

• The ScreenOS Enforcer doesn’t support IP address range cross over class C, even though resource access policy defined on an IC Series device allows it. (385537)

• If you change the interface to which the IC Series device 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"

• The IC Series device sends a “set console page 0” command to the Infranet Enforcer which will disable console paging on the firewall. (369666)

• Do not create phase 2 proposals with spaces in the names. The IC Series device will not handle this properly. (373330)

• It is suggested that DPD (Dead Peer Detection) be enabled on policies defined in the ScreenOS Policy UI. (376385)

• When configuring a new master in a ScreenOS NSRP setup, you may see errors such as: “Failed command - set auth-server "$infranet" account-type xauth 802.1X”. The error is harmless and will not affect functionality. (376255)

• If NSRP A/P cluster is running ScreenOS 5.4R8, Infranet auth table entries are not deleted from back up member of NSRP A/P cluster when primary member disconnects from the IC Series device. (271375)

• If NS5400 is running ScreenOS 6.0R2, sometimes the Infranet Enforcer might stop processing traffic and might crash if infranet auth table entries on the device are more than 2000. (259452)

• If NS5400 is running ScreenOS 6.0R2, sometimes the Infranet Enforcer might crash when device has more than 5000 infranet auth table entries and IC Series device tries to delete the infranet auth table entries on Infranet Enforcer. (255318)

• IPSec Policies are not supported in ScreenOS if source zone of the IPSec policy is shared between ScreenOS enforcer’s Virtual Systems. (390805)

• IPSec is not supported if source zone and destination zone are in non-root vsys of a Transparent mode ScreenOS Enforcer. (421126)

• If the ScreenOS enforcer is running ScreenOS6.2R1, configured in NSRP L2 mode, and is configured to connect to the IC Series device using MGT interfaces, you might see continuously crashes on both back and master NSRP members while a hardware session for traffic is being created in ScreenOS enforcer. Resolution is to use 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 might 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 won’t delete the auth table entries. Work around is to use ScreenOS6.2R2. (401896)

**Infranet Enforcer (IE) – JUNOS (SRX and J-series)**

- IPsec resource access through SRX/J-series does not work if destination is from an address book. The workaround is to use the ‘Any’ destination in the configuration. (503067)
- If an IC auth table mapping action is configured as "provision auth table as needed", UAC will terminate the existing sessions after RE failover. User needs to initiate new sessions. Existing sessions will not get affected after RE failover if IC auth table mapping action is configured as "Always provision auth table". (416843)
- MAC address based authentication against an IC Series device does not work with J-series. (431595)
- An Infranet Enforcer will not connect to the IC Series device if certificate is signed by an intermediate CA and the Infranet Enforcer is configured to perform CA certificate verification. Workaround is to request a certificate from a root CA. (451859)
- The Infranet Enforcer does not perform CRL checking against the configured certificate profile. (451820)

**JUNOS-EX (EX)**

- An 802.1x port may be left open despite failing authentication. This has been observed using JUNOS 9.1R1.8. Suggest using 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 IC is not terminated. (299740)
- It has been reported that after a switch is rebooted, it may take up to 10 minutes to re-establish connectivity with the RADIUS server (IC). (300721)
- When COA Disconnect Messages are enabled on the IC, and 802.1x based authentication is configured using an EX Switch, configuration changes on the IC resulting in a VLAN change on the switch port may not cause the UAC Agent to obtain an IP Address on the new VLAN until re-connecting via the UAC Agent. (417206)

**Network and Security Manager (NSM)**

- Please note that NSM-related issues for UAC 4.0 are documented in the NSM 2008.2 release notes.
- 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 will be "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 doesn't 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 sensor from NSM, need to 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 may 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 will fail if you enter an invalid value. Valid range is 1 – 10081 minutes. (384524)

- The default NSM Agent configuration port (Configuration > NSM Agent > NSM Settings > Primary port) should be set to 7804. (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. The workaround is to 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)

**Communicating Issues and Bugs**

To open a case or to obtain support information, please visit the Juniper Networks Support Site: [http://www.juniper.net/support](http://www.juniper.net/support).

**Documentation Errata**

In the UAC Administration Guide, Enhanced Endpoint Security (EES) is referred to as Advanced Endpoint Security (AED). Additionally, please refer to the .pdf version of the Administration Guide, as the most current information about this feature is not included in the online help version.