

# Release Notes

## *Juniper Networks*

---

Unified Access Control 3.0 R1 (*IVE 6.4*)

Odyssey Access Client 5.0

UAC Build# 12709

OAC Version 5.00.12709.0



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
408 745 2000 or 888 JUNIPER  
[www.juniper.net](http://www.juniper.net)

March 2009  
Part Number 530-029909-1 Rev 01

---

## Contents

New Features .....	1
UAC - Secure Access (SA) Federation.....	1
IF-MAP Support .....	1
Identity-Enabled Firewalling in the Data Center with SRX and UAC .....	1
Extended Guest Access Support.....	2
Automatic Patch Remediation via SMS.....	2
UAC Agent Upgrade Enhancements .....	2
IC 6500 FIPS Hardware Appliance.....	2
UAC Agent Localization.....	3
Support for 64-Bit Windows Vista .....	3
Extended support for ScreenOS Enforcer's Virtual Systems .....	3
Seamless Layer 2/Layer 3 Re-authentication .....	3
Standards-based Dynamic Policy Re-evaluation .....	4
Endpoint Security Assessment Plug-in (ESAP) Availability .....	4
Upgrading to this Release.....	4
Infranet Controller Upgrade.....	4
Installing Odyssey Access Client (OAC).....	4
Fixed Bugs and Enhancements for this release (C3.0, 5.0.12709.0) .....	4
Infranet Controller (IC).....	4
Odyssey Access Client (OAC) on Vista.....	5
JUNOS-EX (EX) .....	5
Network and Security Manager (NSM) .....	5
Known Issues Fixed for the previous release (C2.2R4, 4.80.12363).....	5
Infranet Controller (IC).....	6
Odyssey Access Client (OAC) .....	6
Known Issues and Limitations .....	6
Infranet Controller (IC).....	6
Odyssey Access Client (OAC) .....	9
Odyssey Access Client (OAC) on Vista.....	11
Infranet Enforcer (IE) - ScreenOS.....	12
Infranet Enforcer (IE) - SRX (JUNOS) .....	12
JUNOS-EX (EX) .....	13
Network and Security Manager (NSM) .....	13
Communicating Issues and Bugs .....	14

## New Features

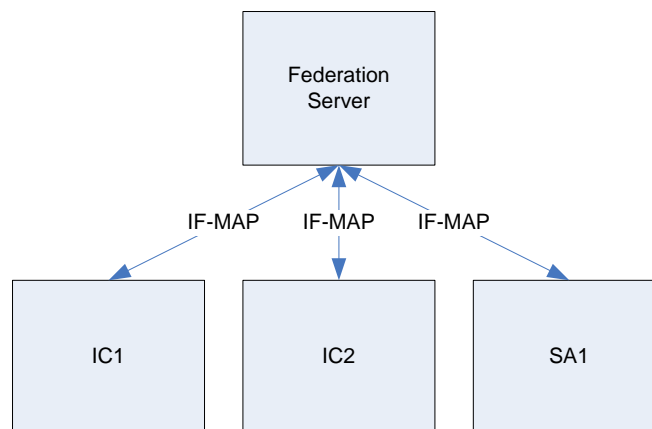
### UAC – Secure Access (SA) Federation

In many organizations, where both a remote access solution and a network access control (NAC) solution have been deployed, remote access users frequently need to authenticate first into remote access, and then again into NAC – or vice versa – in order to access the full range of protected resources.

UAC 3.0 introduces Federation of user sessions between the Juniper Networks Secure Access (SA) SSL VPN and UAC. This adds the ability to seamlessly provision access to UAC resources via SSL VPN, enabling a seamless end user experience in these types of environments.

Similarly users authenticated to one IC appliance can access resources protected by another IC appliance.

As Juniper is committed to supporting industry standards, UAC-SA Federation leverages an open standard from the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) known as Interface for Metadata Access Protocol (IF-MAP).



Federation of the SA and UAC products provides users – whether remote or local – seamless access to corporate resources which are protected by access control policies from UAC or SA. This enables users to access the protected resources with a single login. It is available on all IC and SA platforms.

### IF-MAP Support

As an active participant in and adopter of industry standards, Juniper, in UAC leverages the open standards and specifications of the Trusted Computing Group's (TCG) Trusted Network Connect (TNC). UAC 3.0 adopts and utilizes the TNC's open standard known as the Interface for Metadata Access Protocol (IF-MAP).

Leveraging the TNC's IF-MAP specification enables UAC 3.0 to integrate with third-party network and security devices, which can include virtually any device that collects information about what's happening in or the status of a network. These devices can report back to the IC, serving as an IF-MAP server, enabling UAC to use the collected data to formulate and take the appropriate access actions.

This feature is available on all IC and SA platforms. IF-MAP Server functionality is available on IC4500, IC6000, IC6500, and IC6500 FIPS platforms.

### Identity-Enabled Firewalling in the Data Center with SRX and UAC

Organizations may now combine the widely adopted, identity-aware capabilities of UAC with the robust networking and security services of the SRX-Series Services Gateways.

With UAC 3.0, the SRX platforms can be employed as UAC Enforcers, allowing organizations to leverage UAC Source IP enforcement in the world's most demanding and high performance data centers.

This feature expands UAC's enforcement capabilities to include the high performing SRX platforms, drastically increasing scale for data center environments.

These capabilities are available on all IC appliances and all SRX-Series Dynamic Services Gateways starting with those running JUNOS 9.4.

## **Extended Guest Access Support**

UAC 3.0 enhances an organization's ability to provide guest user access to their networks.

In addition to providing existing one-time use accounts, UAC 3.0 adds the ability for guest user accounts to be provisioned with a pre-defined expiration. For example, front desk personnel at an organization's site can create accounts that last up to 8 hours, or the duration of a typical workday.

This feature is available on all IC appliances.

## **Automatic Patch Remediation via SMS**

UAC 3.0 leverages existing System Management Server (SMS) deployments by enabling automatic patch remediation.

With this enhancement, when an end user logs into UAC, if their device is missing one or more required patches, the UAC Agent will force the SMS Client installed on the user's device to check for updates on demand. The user's device will be placed into quarantine.

When the device has been patched and is up to date, it will be removed from quarantine and the user and device will be provided their authorized level of network access.

This enables enterprises to automatically remediate and manage patches for endpoint devices, minimizing user interaction, thereby reducing the possibility of a help desk call.

This feature is available on all IC appliances.

## **UAC Agent Upgrade Enhancements**

UAC 3.0 adds several new features that provide additional deployment flexibility for the UAC Agent, and that can allow organizations, their administrators and their end users greater control in the deployment and upgrading of the UAC Agent.

Some organizations would prefer to manage the installation and upgrade of the UAC Agent via SMS or other software distribution mechanism, rather than through the automated means available within the IC. With UAC 3.0, automated upgrade mechanisms for the UAC Agent can be disabled on the IC.

Finally, UAC 3.0 provides the end user with an option to upgrade the UAC Agent when prompted. This capability can be allowed by an administrator.

This feature is available on all IC platforms.

## **IC 6500 FIPS Hardware Appliance**

The industry-leading Juniper Networks UAC now delivers FIPS compatibility with the IC 6500 FIPS platform. This new platform includes the same functionality available on other IC appliances, and adds a dedicated FIPS 140-2 Level 3 certified hardware security module which performs FIPS certified cryptographic operations.

The IC 6500 FIPS is built to meet the needs of the most demanding and complex government agencies and secure enterprise environments.

The IC 6500 FIPS can support up to tens of thousands of simultaneous users as a standalone device, scaling up to support multiple tens of thousands of users in a 3 unit cluster.

The IC 6500 FIPS features:

- dual mirrored, hot swappable power supplies

dual hot swappable fans  
dual redundant hot swappable power-efficient power supplies (second power supply optional, DC power supplies available)  
a four-port 10/100/1000 copper interface card standard

## UAC Agent Localization

UAC 3.0 provides fully localized user interface (UI) and documentation for the UAC Agent, supporting the following languages:

- Chinese (Simplified)
- Chinese (Traditional)
- Japanese
- Korean

Also, UAC 3.0 is available in French, without localized documentation.

These localizations enable organizations with users for whom English is not their native language to effectively use UAC, and enables organizations to deploy UAC across their organizations, regardless of language. These capabilities are available on all IC platforms.

## Support for 64-Bit Windows Vista

UAC 3.0 delivers support for the 64-bit versions of Microsoft® Windows Vista®, providing support for all Windows Vista deployments and environments.

## Extended support for ScreenOS Enforcer's Virtual Systems

This feature extends policy enforcement on a per-VSYS level for those customers that prefer to enable UAC functionality per VSYS.

UAC 3.0 extends enforcement capabilities to include authorization (auth) table entries and UAC's resource access policies on a per-VSYS basis. It enables the IC to provision different auth table entries and resource access policies in different virtual systems on a ScreenOS firewall.

Also, when configuring ScreenOS policies from the IC, the VSYS in which to create the policy and VPN objects may be chosen.

These capabilities are available on all IC platforms and ScreenOS Enforcers running ScreenOS 6.2R1 or later.

## Seamless Layer 2/Layer 3 Re-authentication

Organizations, in many cases, want to allow employees to extend their network sessions, provided they re-authenticate after a pre-determined time period (Max Session Timeout). Previously, UAC would drop the existing session and establish a new session. Though the loss of network connectivity experienced by users when UAC would drop the existing session and establish a new session was extremely short in duration, it could create problems for many applications.

UAC 3.0 allows re-authentication without losing network connectivity, ensuring that connectivity-dependent applications continue to function throughout the re-authentication.

This capability works with 802.1X-based enforcement as well as firewall-based enforcement, on both UAC Agent and agent-less sessions.

This capability allows organizations to comply with their corporate security policies for user authentication without interrupting user productivity.

It is available on all IC platforms.

---

## Standards-based Dynamic Policy Re-evaluation

UAC 3.0 supports the Internet Engineering Task Force (IETF) RFC 5176 RADIUS Disconnect Messages standard, enabling standards-based support for dynamic policy re-evaluation on 802.1X switches serving as UAC enforcement points.

Should an end user's role changes in the middle of a network session, UAC can send a RADIUS Disconnect Message to the 802.1X capable switch, forcing a re-authentication.

By supporting IETF RFC 5176, UAC delivers dynamic policy re-evaluation through support of industry accepted open standards.

This capability is available on all IC platforms.

## 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:

[https://www.juniper.net/techpubs/software/uac/3.0xrelnotes/Unified\\_Access\\_Control\\_SupportedPlatforms\\_3\\_0\\_R\\_1.pdf](https://www.juniper.net/techpubs/software/uac/3.0xrelnotes/Unified_Access_Control_SupportedPlatforms_3_0_R_1.pdf).

## Endpoint Security Assessment Plug-in (ESAP) Availability

ESAP packages for UAC 3.0 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.

## Upgrading to this Release

### Infranet Controller Upgrade

1. Please refer to the *Supported Platforms* document for important information pertaining to supported platforms and operating systems.
2. Automatic updated to this release is supported from all UAC releases after and including UAC 2.1 R1.1 Build 105359.

### Installing Odyssey Access Client (OAC)

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

## Fixed Bugs and Enhancements for this release (C3.0, 5.0.12709.0)

### Infranet Controller (IC)

When configured to use LDAP for authentication, users no longer experience very long delays while logging in prior to completing authentication. (385641)

Importing System Snapshot options via XML (Maintenance > Troubleshooting > System snapshot) no longer causes a commit failure as follows:

```
Commit failed
Failure...
[/system/maintenance/system-snapshot/periodic-snapshot]
```

Workaround is no longer required. (385108)

Creating an IPSec policy with 0.0.0.0/0 as resource does not fail with an error when there is a dynamic IPSec policy on IC. (385140)

After changing the certificate on the internal port, TLS protocols work (TTLS, PEAP and TLS). The workaround is no longer required. (385166)

Communication with IDP could take several minutes to fail over to the second node in an IC cluster if the primary node of the cluster drops out of the network. (375213)

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

The OAC option “Override default settings for Windows logon” does not work on Vista. (376230)

If using Internet Explorer 7 on Vista, make sure to enable Active-X delivery. Java delivery does not install the UAC agent. (383796)

When installing OAC on 64-bit Vista systems with User Account Control enabled, be sure to select “Install Anyway” if prompted during the installation. (401633)

### **JUNOS-EX (EX)**

On occasion, during dynamic VLAN assignment, an 802.1x enabled port may not always switch to the requested VLAN. This has been observed on JUNOS 9.1R2.10. Resolved in JUNOS R2.15 (301748)

EX does not send the RADIUS attribute “Calling-Station-Id. As a result, the Mac address cannot be displayed in the user access log. Resolved in JUNOS 9.4. (303419)

An 802.1x enabled port does not reset to its statically configured VLAN when the IC is configured not to send a VLAN id. Workaround is to configure a RADIUS attribute policy with the desired VLAN. Resolved in JUNOS R2.15 (298609)

### **Network and Security Manager (NSM)**

Using NSM, if the administrator wants to remove an outer authentication protocol from an existing authentication protocol set, it is not necessary to remove the inner authentication protocols of the respective outer authentication protocol. Removing the inner authentication protocols along with the outer authentication protocols no longer causes the device update from NSM to fail. (386166)

When using NSM to update a device while specifying a DMI backup port, the NSM log no longer indicates that the device returned a null rpc reply for the Edit-config message even though the update was successful. (386092)

When defining a ‘Require and Enforce’ Host Checker restriction on the user realm, it is not necessary to specify ‘Evaluate policies’ also. NSM client now automatically selects this option as the IC admin UI does. (383765)

Enabling the ‘Kill Processes’ Remediation option on a Host Checker policy with MD5 checksums no longer works for only a single process. Ordering is preserved within the NSM UI. (384890)

When configuring localization options via NSM, there may be some options present in NSM which aren’t supported by the IC. (398045)

Adjust OS version feature not working correctly with the NSM 2008.2 Beta Release. Please delete and re-add the device if you experience this issue. (311578)

User sessions may expire prematurely when roles are created via NSM. Workaround is to go to the User Role configuration page in the Admin Console, and re-save the “Session Options” selections. (398077)

### **Known Issues Fixed for the previous release (C2.2R4, 4.80.12363)**

### **Infranet Controller (IC)**

netshim-ipsec-uac - Blue screen issues during IPSec usage have been fixed. (382914-1)

uac-admin - User access warning log is no longer counting MAC address users towards license maximum. (403576-4)

uac-other - When using agentless access, users are no longer seeing "You have not purchased this feature" after login. (384775-1)

uac-sbr - Inner Proxy now works when you have multiple authentication protocol sets configured along with multiple realms on the sign-in policy. (395776-2)

### **Odyssey Access Client (OAC)**

uac-oac-client-installer - Upgrading with a pre-configuration file no longer causes odgina to chain to itself (393175-3)

uac-oac-client-ocm - Cancelling out of an RDP session to a PC running Odyssey no longer breaks Odyssey Client Manager. (386383-1)

uac-oac-client-gina - Using the OAC hidden registry keys for nwgina works (386250-1)

uac-oac-client-gina - Auto-scan list with GINA is now working on Vista. (409258-3)

uac-oac-client-gina - On Vista 32-bit Operating Systems, Odyssey Access Client was disconnecting after GINA login and reconnecting when the desktop appeared. This issue has been resolved. (403168-3, 411599)

## **Known Issues and Limitations**

The following lists known issues which are still outstanding in this release:

### **Infranet Controller (IC)**

UAC firmware 2.2 and above provides additional features on the Infranet Controller. 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. (56778)

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)

After making certain configuration changes (such as changing the authentication server on the realm), the following message may be seen in the user access log "No EAP protocol was agreed on" and OAC never authenticates. Workaround is to restart services on the Infranet Controller. (384093)

After a change of cluster state, IC may retain defunct layer-2 sessions. If an IC cluster has a member whose original factory image was UAC 2.1R2 or earlier and another member whose original factory image was UAC 2.1R3 or newer, then when a NAD closes a session, the cluster may fail to recognize that the session is gone.

The administration console will list the session and it will count against the licensed session limit, until it expires.

This happens if with both active-active and active-passive clusters if:

1. a non-Juniper endpoint makes a layer-2 connection to a network access device, and the network access device (using RADIUS) has one of the ICs in the cluster authenticate the user
2. a change in cluster state causes RADIUS requests from the NAD to go to a different cluster member
3. the endpoint later disconnects from the network access device, which sends a RADIUS Accounting-Stop request to the different cluster member

The problem happens because of an error in the RADIUS dictionary in versions 2.1R2 and earlier, an error that is not fixed by upgrading to 2.2. To correct the problem, if you have not changed radius.dct yourself, do the following once for the entire cluster:

1. In the administration console, go to Network Access > RADIUS Dictionary.
2. Click radius.dct. Click Restore Factory Default Dictionary.

This sends the corrected dictionary to all members of the cluster. Sessions that exist at this moment may not be removed from IC when they end, but sessions created after this will be.

If you have changed radius.dct yourself, do the following once for the entire cluster. Connect your browser to a cluster member whose original factory image was UAC 2.1R2 or earlier. Download and edit radius.dct. Look for this line:

```
ATTRIBUTE Funk-User-UID-of-Session SBR-VSA(30, string) cr
```

Change the 30 to 31. Exit the editor after saving the file. Return to your browser and click Save Changes. This will send the corrected dictionary to all members of the cluster. (376804)

Adding a RADIUS client with an IP address of 127.0.0.1 will cause the following event log to be generated: "RADIUS: There is more then 1 client with an IP Address of 127.0.0.1" and cause SBR to re-start periodically. Do not add a RADIUS client with an IP address of 127.0.0.1. (58154)

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)

Authentication may fail after the user changes password when OAC is configured to use TTLS and non-EAP MS-CHAP-V2. (380579)

When defining IP pools in the Infranet Controller, use a large range of IP addresses to avoid running out of IP addresses in IP pools. (366541)

The Infranet Controller does not allow outbound connections on the external interface. (370241)

The Infranet Controller 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 Infranet Controller does not properly handle Infranet Enforcer connections over its VLAN interface. (367599)

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 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)

The backup RADIUS server is ignored for RADIUS proxy requests. (376583)

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 Infranet Controller depicts the number of OAC clients connected with an EE license. (375685)

When configuring an Active Directory (AD) server on the Infranet Controller for authentication, note the following points:

- a. Ensure that the AD server administrator you specify is a domain administrator in the same domain as the AD server.
- b. 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 Infranet Controller Web console.

In agentless mode, new PIN mode does not work against an ACE authentication server when using custom sign-in pages. (377332)

IF-MAP replicas may take considerable time to synchronize when first connecting if there are a large number of sessions. (388580)

When the IF-MAP server purges data it has received from a particular client or replica, the purging can take several minutes. During this time 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 role changes result in session extension being dynamically disabled or enabled for a particular endpoint, the status of the "extend session" button within the UAC agent or within the browser isn't updated correctly. (422187)

When an IF-MAP client is disconnected, or removed from the configuration of an IF-MAP server, data published by that client may remain for several minutes. (393149/428536)

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)

IC devices acting as IF-MAP Replicas may not display the correct connection status in the Administrator UI initially when one of the devices is in an Idle state. This will not impact functionality of IF-MAP Replication. (413893)

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 Server capabilities are not currently available on Active-Active cluster configurations. If the IF-MAP Server is enabled on an Active-Active cluster, the event log can be flooded with error messages. (413176)

IF-MAP may decrease the number of Coordinate 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 enabling IF-MAP client on a SA device, existing sessions matching the configured session export policy will not be exported to the IF-MAP Server. All sessions created after IF-MAP client is enabled will be exported per the configured export policy. (427843)

If a cluster split occurs between any two nodes of a cluster, duplicate sessions may be created. If this occurs, make sure to delete all sessions from the active users page. (427702)

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)

Enabling the IF-MAP client feature on an IC or SA Device, may cause memory and device resources to be consumed if there are issues establishing a connection to the IF-MAP Server. Be sure to disable the IF-MAP functionality when not in use and ensure connectivity problems are resolved when IF-MAP is enabled. (430487)

### **Odyssey Access Client (OAC)**

OAC may display the error string "Error (other JUAC failure)" when using a revoked client certificate. (376112)

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 "Infranet Controller" status is "terminated", disable the web-scanner (port 443) in Kaspersky anti-virus. (381018)

While upgrading to OAC 5.0, 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 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 Infranet Controller, the client will be upgraded with a 5.0 UE 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)

If an endpoint has multiple interfaces, and the route to the protected resource is different than the route to the Infranet Enforcer, the endpoint will not have access to the resource. (369230)

See the *Supported Platforms Guide* for a list of 3<sup>rd</sup> 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 will invalidate the signature. Administrators should re-sign the new MSI with their own certificate before deploying to their users. (369685)

Wireless suppression may 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 5.0 client. (370325)

Endpoint Session scripts can be configured for each user role on the Infranet Controller. However, the 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 Odyssey Access Client will cause 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, you will be prompted to sign-in again a 2<sup>nd</sup> time. Session resumption does not work in this case and two sessions will be created on the Infranet Controller. (374388)

If the Infranet Controller is configured to support NAT Traversal for IPSec traffic, connecting and disconnecting the OAC client a number of times may 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 to the Infranet Controller 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**

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 UAC (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 ad-hoc 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)

### **Infranet Enforcer (IE) - ScreenOS**

If you change the interface to which the Infranet Controller 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 Infranet Controller 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 Infranet Controller 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 Infranet Controller. (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 Infranet Controller 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 Infranet controller 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) – SRX (JUNOS)**

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)

If a network interface on the IC does not have a certificate configured on the interface, the SRX firewall may hang while the IC attempts to connect to the SRX device. (410989).

## **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)

RADIUS Proxy realms may not work correctly when realm names contain spaces. (421758)

## **Network and Security Manager (NSM)**

Please note that NSM-related issues for UAC 3.0 are documented in the NSM 2008.2 release notes.

When importing an Infranet Controller 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)

After configuring or editing an IDP sensor from NSM, the IC may not re-establish a connection to IDP. Check the One-Time-Password on the IDP to make sure it is set and matches the IC. (58666)

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 Infranet Controller. (384786)

When configuring the System Local authentication server via NSM, there is no option to create User Admins. Please use the IC admin console to perform this task. (392055).

Hostchecker 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>.

The URL for product documentation is incorrect in the help file. Please go to  
<http://www.juniper.net/techpubs/software/uac> to access all product documentation.