



Juniper Networks
Odyssey Access Client for Windows

Release Notes

Release 4.72.11421.0
May 2008

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: OAC-RN472.R4W

Copyright © 1999–2008 Juniper Networks, Inc. All rights reserved. Printed in USA.

Odyssey Access Client, Juniper Networks, and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. Raima, Raima Database Manager and Raima Object Manager are trademarks of Birdstep Technology. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Revision History

| Date | Description |
|---------------|--------------------|
| November 2007 | FRS release |
| January 2008 | Maintenance update |
| May 2008 | Maintenance update |

Table of Contents

| | |
|---|---|
| Upgrading to this Release..... | 1 |
| Installing Odyssey Access Client | 1 |
| Resolved Issues..... | 2 |
| Odyssey Access Client—Version 4.72.11421.0 for Windows..... | 2 |
| Odyssey Access Client—Version 4.72.11421.0 for Vista..... | 3 |
| Odyssey Access Client—Version 4.72.10945.0 for Windows..... | 3 |
| Odyssey Access Client—Version 4.72.10945.0 for Vista..... | 3 |
| Odyssey Access Client—Version 4.7.10697.0 for Windows..... | 3 |
| Odyssey Access Client—Version 4.7.10697.0 for Vista..... | 4 |
| Odyssey Access Client—Version 4.7.10539.0 for Windows..... | 4 |
| Agentless..... | 4 |
| Known Problems and Limitations | 5 |
| Odyssey Access Client (OAC)..... | 5 |
| Odyssey Access Client (OAC) on Vista | 8 |
| Authentication with Active Directory | 9 |
| Communicating Issues and Bugs..... | 9 |
| Contacting Technical Support..... | 9 |

Release Notes

These release notes accompany Odyssey Access Client (OAC) 4.72.11421.0. Before installing or using your new software, read these release notes in their entirety, especially the “Known Problems and Limitations” section on page 5.

If the information in these release notes differs from the information found in the product documentation, follow the release notes.

You can find release notes in Adobe Acrobat (PDF) format on the Juniper Networks Technical Publications Web page, which is located at <http://www.juniper.net/techpubs>.

Upgrading to this Release

See the *Supported Platforms Guide* for important information pertaining to supported platforms and operating systems. You can access the document at:

https://www.juniper.net/customers/csc/software/ive/releases/enterprise_infranet/2.x/b49455/index.jsp

If you are using OAC in a Unified Access Control (UAC) network, read the release notes for UAC version 2.1.

Installing Odyssey Access Client

Upgrading the Infranet Controller firmware to 2.1 before deploying the OAC 4.72 Enterprise Edition custom installer with a new 4.7 license key may cause some users to fail authentication. In an 802.1X environment, depending on network setup, users who fail to be authenticated by the Infranet Controller may be unable to connect to a network.



NOTE: Upgrading from OAC 4.6 Enterprise Edition to OAC 4.72 Enterprise Edition requires a new license key. If you have a current service contract and have not received a new 4.7 license, contact Juniper Technical Support for the new 4.7 license key.

If you are running OAC 4.6 Enterprise Edition, you must create and deploy a new OAC 4.72 Enterprise Edition custom installer with a new 4.7 license key to all users *before* upgrading the Infranet Controller's firmware to 2.1.

If you are installing OAC in a traditional, non-UAC network, the installation procedure is unchanged.

- The Infranet Controller is capable of handling 1500 active endpoint upgrades. Anything beyond this may require administrators to upgrade endpoints prior to upgrading the Infranet Controller using some other mechanism such as SMS.
- A Java JVM or Active-X must be enabled in order to install OAC through the browser. (51841)
- Unlike previous UAC versions, installation of OAC now occurs as follows:
 - a. The end-user must first sign in to the Infranet Controller via web-browser.
 - b. If the user's role allows OAC installation, the OAC will automatically download and install.

Refer to the installation chapter in the *Odyssey Access Client User Guide* for more details on installation. For more information about Infranet Controller topics, refer to the *Unified Access Control Administration Guide*.

Resolved Issues

The following issues from previous releases have been resolved in Odyssey Access Client Release 4.72.11421.0. Subsequent sections identify issues resolved in previous releases.

The identifier following the description is the tracking number in our bug database.

Odyssey Access Client—Version 4.72.11421.0 for Windows

- When using Windows Remote Desktop, the user should no longer be prompted for their password after logging into Windows. (56439)
- When using a merge rule to modify an existing Network, changes should now be made to the user settings after installing the settings update file when encrypted data such as passwords, passphrases or PINS are specified in the initial settings. (56435)
- Authentication should not fail when Gina is used with a smart card to authenticate with an IC configured for certificate based login. (55207)
- Session resumption should work correctly when used with machine authentication. (55117)
- OAC should display the prompt for login name and password if the user clicks on OK with a blank username. (53922)
- The Trusted Network Connect (TNC) service should not exit with an error. (56771)
- When the GINA Initial Settings profile is saved with a password that is different from the Windows password, authentication should not fail. (56954)

- OAC on Windows 200 should not fail authentication when changing the domain password. (54058)

Odyssey Access Client—Version 4.72.11421.0 for Vista

- OAC on Vista should now work correctly when used with Broadcom wireless chipsets. (54120)

Odyssey Access Client—Version 4.72.10945.0 for Windows

- The first time a Configuration Profile is used to prompt for login name and password, the dialog box will now be in focus for the user to provide the username and password. (51600)
- The Trusted Network Connect (TNC) service should not crash after upgrading to OAC 4.7R1. (52519)
- The user should not encounter an upgrade dialog message when upgrading from OAC 4.50 to 4.7. (53119)
- When OAC is configured for Machine Authentication and Gina, the machine should now be reachable while the user is prompted for the password. (52912)
- On machines with only one network adapter, OAC should display the IP address when the wireless 802.1X connections is open and authenticated. (52517).
- A license warning dialog message should not appear when trying to create a Silent Custom Installer. (52437)
- The "Bluetooth LAN Access Server Driver" has been added to the Virtual Adapter list. (52109)
- OAC should display the certificate chain correctly from the Infranet Controller. (51599)
- The outer identity of an encrypted tunnel can now be replaced with the Login name used for the inner identity when the anonymous name is cleared. (51396)
- Upgrading OAC from a user account with restricted privileges with the Juniper Installer service should now work correctly. (51877)

Odyssey Access Client—Version 4.72.10945.0 for Vista

- After installing OAC, wireless connection status should not stay in "Searching for network". (51443)
- Connecting to a machine using RDP should not cause the Odyssey 802.1x connection to be reset. (50979)

Odyssey Access Client—Version 4.7.10697.0 for Windows

-

- A UE-edition Custom Installer should now correctly create the configuration as specified in the 'Initial Settings'. (52398)
- OAC installer should now correctly upgrade the client. (52513)

Odyssey Access Client—Version 4.7.10697.0 for Vista

- OAC on Vista should no longer fail to associate with AP when multiple association modes are configured on the AP. (52426, 52431)

Odyssey Access Client—Version 4.7.10539.0 for Windows

- The "reload and execute initial settings" menu item in the Initial Settings applet of the Odyssey Access Client Administrator should now close the Odyssey Access Client Manager application. (43955)
- Users can view debug logs by using the "Browse" button in the log viewer and opening the debuglog.log using a text editor. When reporting issues, users should package all log files by clicking the "Save all logs" button and sending the ZIP file to Juniper Support. (44306, 44370)
- Endpoints previously installed with earlier (Beta) versions of OAC should not encounter problems when installing the final OAC version shipped with UAC 2.0r1. If uninstalling and re-installing does not work, please consult Knowledge Base ID KB9350 (<http://kb.juniper.net/>) for help restoring the endpoint. (44504)
- Odyssey Access Client should now install the Juniper Installer Service delivered via SSL-VPN (IVE) appliances. New MSI functionality has been added to support the Odyssey Access Client package, and thus Odyssey Access Client software will need to be provisioned as a standalone MSI via SMS or an automated Software Delivery system for the first time. A new version of Installer Service is bundled as part of the Odyssey Access Client package. This new version of Installer Service is backward compatible with SSL-VPN clients such as Network Connect and Windows Secure Application Manager (WSAM).
- The correct folder is: system_volume: % APPDATA % \Funk Software\Odyssey Client\newScripts
- The Odyssey Access Client UAC Edition initial software install will no longer add a wireless adapter, if available, when no adapter is configured on the Infranet Controller OAC Configuration or Initial Settings page. (52061)

Agentless

- If a realm is configured to evaluate Host Checker policies and an endpoint with a browser that is unsupported for Host Checker attempts to authenticate agentlessly, the authentication should no longer fail. (43988)
- Agentless users using Firefox 2.0 browsers should no longer have to click the Remediation Page's 'Try Again' button multiple times before the Infranet Controller recognizes that the endpoint is compliant. (44414)

Known Problems and Limitations

The following lists known issues which are still outstanding in this release. The version of Odyssey Access Client shipped with UAC 2.1 is 4.72.11421.0.

Odyssey Access Client (OAC)

- The version of Odyssey Access Client (OAC) shipped with UAC 2.1 is 4.7.10539.0
- Intermittently and without warning, OAC may crash for no apparent reason (55348).
- 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. (55246)
- While upgrading to OAC 4.72, 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. (54442)
- Extended characters cannot be used in the "Role message" displayed to users for CTC. (54008)
- Odyssey Access Client UAC Edition, when not installed from a pre-configured installer, does not copy configuration information on a workstation to new users from either the initial user install or from OAC Administrator "Initial Settings". In order for new users to get a copy of the configuration information, it is necessary to configure and install an Odyssey Access Client pre-configured MSI. (53698)
- If there is an OAC 4.6 EE license installed in the client and a connection is made to an Infranet Controller, the client will be upgraded with a 4.7 UE license. (51900)
- 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.
 - a. Reboot, if this does not clear up the problem then
 - b. Uninstall OAC and reinstall.
- If the above steps do not fix the problem, please contact Juniper Networks TAC for assistance. (52625)
- When the force VA option is enabled on or when behind a NATed firewall, sometimes, OAC Client Service and Juniper Unified Network Service need to be restarted in order to get access to protected resources. (53626)

- Online help states that the debug level range is 0-9, however the actual range is 0-5. (54956)
- When upgrading OAC, the Juniper Unified Network Service may not suspend. (52687)
- Deleting debuglog.log from the installation may cause OAC to stop logging until the Juniper OAC Service is restarted. (51701)
- 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. (41485)
- If the Infranet Controller specification contains a URL prefix (such as "https://"), OAC can become unresponsive. To fix the problem, remove the "https://" prefix. (44271)
- 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. (41912)
- When the virtual adapter is used, the first TCP connection may take up to 15 seconds. (43974)
- 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. (43458)
- See the Supported Platforms Guide for a list of 3rd party VPN clients that were tested with the OAC. (42834, 42872)
- The NAT-T Status information displayed in the OAC IPsec Configuration window should be ignored. (42155)
- An expired 30-day trial will prevent installation of UAC edition of OAC. The workaround is to uninstall the trial software, and then navigate to the Infranet Controller URL (using a browser) which will start an auto-installation of the latest OAC software. (42954)
- Users upgrading a UAC 1.x Infranet Agent may encounter a jpaService.exe crash while upgrading to the UAC 2.1 Odyssey Access Client. (43223)
- 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. (43913)
- Wireless suppression may not work with some versions of VMware. (44438)
- Customers running OAC 4.52 in FIPS mode should uninstall 4.52 prior to upgrading to the 4.7 client. (44553)
- Endpoint Session scripts can be configured for each user role on the Infranet Controller. The OAC can execute at most one End Session script on the endpoint. (44527)

- 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: (43253)
 - a. Uninstall Odyssey Access Client.
 - b. Upgrade Network Connect by accessing any of the following versions of the SSL-VPN (IVE) appliance: IVE 5.2R7 or later, IVE 5.3R7 or later, or IVE 5.4R1.
- 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 2nd time. Session resumption does not work in this case and two sessions will be created on the Infranet Controller. (48616)
- If NAT-T has been configured on the Infranet Controller, connecting and disconnecting the client a number of times may result in the virtual adapter being installed. (49579)
- Failure to configure EAP-JUAC as the inner authentication protocol will cause L3 connections to the Infranet Controller to fail. Workaround is to configure any profile used by L3 connections to use EAP-JUAC. (49654)
- The realm and role selection is not saved during authentication at Gina time. (51111)
- Auto-remediation to run Live Update for Symantec 8.1 may not trigger. Ensure that the registry value "HKLM\Software\Symantec\LiveUpdate\Preferences\HALIndex" is not present. (50504)
- Shavlik 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. (50125)
- Earlier versions of OAC for Mac, Linux, and Windows CE will not accept the new 4.7 license. Contact technical support to get a license key for these platforms. (51148)
- When installing OAC on a Windows XP system, you may encounter the error: "The installer has insufficient privileges to access this directory: C:\Config.Msi.". The workaround is to select Retry rather than Cancel in the error dialog. The installer continues to install OAC correctly. (44506)
- 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. (48502)
- Machine authentication using machine credentials is not supported when using EAP-JUAC. (51432)
- If using a Predefined Firewall rule for the Microsoft Windows Firewall, the reason string may be shown twice in the remediation dialog on OAC. (50568)

Odyssey Access Client (OAC) on Vista

- Although multiple static WEP keys can be configured, only the highest ordinal key is used. (53805)
- If the Access Point is not broadcasting the SSID, OAC on Vista it will never get authenticated when the GINA wizard is used. (53693)
- It has been reported on some endpoints that the OAC client download may not occur automatically via the browser. The workaround is to download the client using the manual installation link or click on the "retry" link. (49762)
- 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. (49486, 49488)
- OAC on Vista does not support WPA2 Fast Roaming. (48682)
- OAC does not recognize that a wireless card has been removed for about 30 seconds. (49103)
- Static keys with open/WEP (authentication) and MD5 (encryption) do not succeed in providing network connectivity on Vista. (51674)
- If UAC (User Access Control) is enabled on Vista, auto-remediation to enable the Microsoft firewall does not work. (51824)
- In the Windows event viewer, the following warning will appear "The Juniper OAC Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly." The warning can be ignored as it does not impact functionality. (49485)
- The OAC option "Override default settings for Windows logon" does not work on Vista. (50458)
- 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. (50713)
- Some auto-remediation action will not work on Vista as they require the service to interact with the desktop. (50070)
- Registry auto-remediation does not work on Vista. (49840)
- 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. (49496)
- License keys cannot be added to OAC if UAC is enabled on Vista. Workaround is to use Odyssey Client Administrator to enter the license keys. (49545)

Authentication with Active Directory

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

1. Ensure that the AD server administrator that 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 Infranet Controller Web console.

For agentless clients, new PIN modes does not work against an ACE/Secure ID authentication server when you are using custom sign-on pages. [51560]

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>

Contacting Technical Support

For technical support, contact Juniper Networks at support@juniper.net, or at 1-888-314-JTAC (in the United States) or 408-745-9500 (outside the United States).

Check our Web site (<http://www.juniper.net>) for additional information and technical notes. You can also go to **Help > Odyssey Access Client User Page** in OAC.

When you call technical support, please have the following at hand:

- Your Odyssey Access Client edition and the release number.
- Information about the server configuration and operating system, including any OS patches that have been applied.
- For licensed products under a current maintenance agreement, your license or support contract number.
- Question or description of the problem, with as much detail as possible.
- Any documentation that may help in resolving the problem, such as error messages, memory dumps, compiler listings, and error logs.

