



Unified Access Control

Troubleshooting Guide

Release 3.1

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

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986–1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, The Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, E-series, ESP, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, T-series, and TX Matrix. 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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Copyright © 2006–2009, Juniper Networks, Inc.
All rights reserved. Printed in USA.

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.

Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

End User License Agreement

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. The Software. In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- Customer shall use the Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller, unless the applicable Juniper documentation expressly permits installation on non-Juniper equipment.
- Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees.
- Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any "locked" or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even

if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Software on non-Juniper equipment where the Juniper documentation does not expressly permit installation on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; or (k) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. Ownership. Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. Commercial Computer Software. The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language).)

Table of Contents

Unified Access Control Solution Troubleshooting Guide 1

- Troubleshooting the UAC Solution 1
 - Troubleshooting the ScreenOS Enforcer 1
 - Troubleshooting the Infranet Controller 4
 - Troubleshooting Host Checker Policies 10
 - Troubleshooting Layer 2 Connectivity Issues 11
 - Time Limits on RADIUS Authentication and Accounting 12
 - Port Numbers used by the Infranet Controller, Infranet Enforcer, and Odyssey Access Client 13

Unified Access Control Solution Logging and Monitoring Tools for Troubleshooting 15

- Tracking Events 15
 - Tracking Events Using Policy Tracing 16
- Creating Snapshots of the Infranet Controller System State 17
- Creating TCP Dump Files 18
- Testing Infranet Controller Network Connectivity 20
 - Address Resolution Protocol (ARP) 20
 - Ping 20
 - Traceroute 20
 - NSlookup 21
- Running Debugging Tools Remotely 21
- Creating Debugging Logs 22
- Using the RADIUS Diagnostic Log 22
- Monitoring Cluster Nodes 23
- Configuring Group Communication Monitoring on a Cluster 24
- Configuring Network Connectivity Monitoring on a Cluster 26

Unified Access Control Solution Troubleshooting Guide

Troubleshooting the UAC Solution

This section contains topics to help you troubleshoot problems with the configuration of the Infranet Controller.

- “Troubleshooting the ScreenOS Enforcer” on page 1
- “Troubleshooting the Infranet Controller” on page 4
- “Troubleshooting Host Checker Policies” on page 10
- “Time Limits on RADIUS Authentication and Accounting” on page 12
- “Port Numbers used by the Infranet Controller, Infranet Enforcer, and Odyssey Access Client” on page 13

Troubleshooting the ScreenOS Enforcer

If configured correctly, a Juniper Networks security device running an Infranet Enforcer instance sends a connection request to an Infranet Controller at startup. When a connection is successful a message appears on the console and in the **Reports > System Log > Event** page of the Infranet Enforcer WebUI. If success does not occur, this section describes some of the next steps for troubleshooting. To analyze IP traffic you might consider downloading a copy of a software program called *Wireshark* from www.wireshark.org.

Table 1 lists potential problems and a solution to each problem. For hardware or configuration issues and LED meanings, consult the User Guide appropriate to your model of Juniper Networks security device.

Table 1: Infranet Enforcer Problems and Solutions

Problem	Solution
No connection between the Infranet Controller and the Infranet Enforcer	<ul style="list-style-type: none">■ Use the debug auth infranet CLI command to display debugging messages regarding the Infranet Controller connection.■ See the solutions listed in Table 3 on page 6.

Table 1: Infranet Enforcer Problems and Solutions (Continued)

Problem	Solution
Unable to establish connection between the Infranet Enforcer and the Infranet Controller Receiving PKI errors	<p>Ensure that Infranet Enforcer has a valid Root CA certificate of CA which issued SSL webserver certificate to Infranet Controller.</p> <p>If you see “PKI: Failed to obtain CRL for CA issuing cert....” message, check that CRL server of the CA is reachable from Infranet Enforcer. If CRL server is not reachable from Infranet enforcer one alternative to making it reachable is to set the check method to ‘none’ under ‘Certificate Revocation settings’ of the CA certificate that is in use for IC-IE communication.</p> <p>If you see “PKI: Cert is not yet valid”, check whether the CA certificate on Infranet enforcer and SSL webserver certificate on Infranet Controller are valid. If they are valid and you are still getting this error, check the date and time settings on Infranet enforcer and Infranet Controller.</p> <p>If you see “PKI: Cannot build certificate chain for cert with subject name.....” check whether Infranet Enforcer has the correct CA certificate of CA which issued web server certificate to IC and check that same CA certificate is configured as ‘Selected CA’ in Infranet Controller’s configuration in Infranet Enforcer.</p>
Unable to establish SSL	Use the debug ssl all CLI command.
Unable to establish redirect by means of captive portal	Use the debug flow basic CLI command to see redirect messages when traffic starts. Alternately, use the debug auth all command to show redirects in the debug log.
Losing packets in VPN tunnel	Use the get event CLI command. To troubleshoot packet loss with VPN tunnels, use the debug ike CLI command.
Unable to establish connection between the Infranet Controller and Infranet Enforcer in Transparent mode	<p>Transparent mode has no default policies (exception: NS-5GT).</p> <p>Although the Juniper Networks security device is operating in Layer-2 mode, policies are configured with Layer-3 IP addresses.</p> <p>To know if the Juniper Networks security device is operating but is not answering pings, use the get arp CLI command.</p> <p>To view the Layer-2 forwarding table use the get mac-learn CLI command.</p> <p>To manually add a static route mapping use the set mac mac_addr outgoing_interface command.</p>
Dynamic auth table provisioning does not work: auth table entries do not get provisioned.	Dynamic auth table allocation does not work with http traffic if the Infranet Enforcer’s captive portal feature is configured to re-direct traffic to a Web server other than the Infranet Controller.

Recommended CLI Commands for Troubleshooting the Infranet Enforcer

This section contains information about recommended CLI commands to help you troubleshoot the Infranet Enforcer.

- If the Infranet Enforcer is not responding, use the following commands to view system usage:

```
get perf cpu
get task
```

- To check current IKE and IPsec configuration, use the following commands to show the IKE phase 1 and phase 2 parameters:

```
get ike gateway
get vpn
```

The dynamic configuration usually has long names. To see the full non-truncated version, use:

```
get -v
```

- To see dynamic IKE information, use this command to show Phase 1 SA:

```
get ike cookie
```

Or, to show Phase 2 SA, use:

```
get sa
```

The output shows both the lifetime and state of SA's. To get more detailed information about a phase 2 SA, use:

```
get sa id
```

- The Infranet Enforcer **debug** CLI commands are in the form of **debug module_name keyword**. Some commonly used commands are:

```
debug flow basic
debug ike basic
debug ike detail
```

All the debug messages output to the debug buffer (dbuf). The commands to manage dbuf are:

To see the message:

```
get dbuf stream
```

To clear the dbuf:

```
clear dbuf
```

To output the message directly to the console:

```
unset console dbuf
```

- If traffic does not go through the Infranet Enforcer, check the VPN, IKE gateway, and Policy first. Make sure the Infranet Controller has sent this information to the Infranet Enforcer. Next, investigate IKE Phase 1 and Phase 2 SA. If they are not up, you need to do IKE debug by using either of these commands:

```
debug ike basic
debug ike detail
```

If the SA is up but the traffic is not going through, you can do use:

debug flow basic

- There is a flow filter (for **debug flow**) and sa filter (for **debug ike**) that you can use to limit the debug information to a specific IP address. Use either of these:

```
set ffilter
set sa-filter
```

- To get debug information when a packet comes in and out of the Infranet Enforcer, use:

```
snoop
```

Use this command to display information about a snoop filter:

```
snoop ?
```

- Table 2 lists some other useful troubleshooting CLI commands:

Table 2: Troubleshooting CLI commands

To	Use
Force the Infranet Enforcer to attempt to connect to the Infranet Controller	exec infranet controller connect (You can also restart the Infranet Enforcer.)
Show interface information	get interface
Show routing information	get route
Show policy information (including dynamic policies that the Infranet Controller generated)	get policy
Show session information	get session
Show tunnel session information (IPsec, L2TP, NAT-Traversal, GRE, and IPv6in4 are implemented as tunnel sessions.)	get session tunnel
Show a list of all Infranet Controller authentication table entries. The output includes an auth-id, source IP address, user name, and role ID for each authentication table entry.	get auth table infranet
Show information about a specific Infranet Controller authentication table entry. Specify the table entry's auth-id for <x>. The output includes a source IP address, user name, role ID(s), and role name(s) for the table entry.	get auth table infranet auth-id <x>
Show system information including the image version	get system
To display the CA certificates available for the Infranet Controller configuration	get ssl cert-list

Troubleshooting the Infranet Controller

If the connection is successful between an Infranet Enforcer and an Infranet Controller, a green dot appears next to the Infranet Enforcer icon under **Enforcer Status** on the **System > Status > Overview** page in the Infranet Controller admin console. The Infranet Enforcer IP address also appears on the **UAC > Infranet Enforcer > Connection** page in the Infranet Controller admin console.

If the connection is unsuccessful, the dot appears white and the IP address does not appear on the **UAC > Infranet Enforcer > Connection** page. To troubleshoot problems with the Infranet Controller, you can:

- Track events when a user signs into a realm by using policy tracing on the **Maintenance > Troubleshooting > User Sessions > Policy Tracing** page. Policy tracing allows you to record a policy trace file for an individual user. The Infranet Controller displays log entries that list the user's actions and indicates which roles each user gets mapped to and why. You can work from the set of roles to figure out why access is allowed or denied for a certain user.
- Refer to the event logs in the **System > Log/Monitoring > Events** page. To configure the event logs to include information related to the Infranet Enforcer, click the **Settings** tab and select the following options:
 - **Enforcer Events**—Select this option to view events pertaining to the Infranet Enforcer.
 - **Enforcer Command Trace**—Select this option to view an event for each command sent to the Infranet Enforcer along with its output. Note that the log lists the newest entries first.
- In Odyssey Access Client, choose **Tools > Logs** to open the OAC Log Viewer which displays the log file. To configure the content and amount of detail in the Odyssey Access Client logs, choose a setting from the drop-down list under **Log Level**. To access the saved log files, click **Browse**. You can then open the log files in a text editor or attach them to an email message. Always set the log level at 5 to get the most useful information.
- In Odyssey Access Client, choose **Tools > Diagnostics**. From the drop-down list under **Select diagnostic function**, choose one of the following:
 - **IPsec Diagnostics**—displays the current IPsec statistics.
 - **IPsec Configuration**—displays IPsec configuration information about all of the Infranet Enforcers to which Odyssey Access Client can connect. Odyssey Access Client downloads this information from the Infranet Controller.
 - **Network Agent Diagnostics**—displays configuration and diagnostic information about the Odyssey Access Client Network Agent.
 - **Host Enforcer Configuration**—displays configuration information about all of the Host Enforcer policies Odyssey Access Client is currently enforcing. Odyssey Access Client downloads these policies from the Infranet Controller.

Table 3 lists potential problems and a solution to each problem. For hardware issues, consult the *Installation Guide*.

Table 3: Infranet Controller Problems and Solutions

Problem	Solution
No connection between the Infranet Enforcer and the Infranet Controller	<ul style="list-style-type: none"> ■ Make sure the date set on the Infranet Enforcer and Infranet Controller are the same. ■ Make sure the following are configured correctly on the UAC > Infranet Enforcer > Connection page of the Infranet Controller: <ul style="list-style-type: none"> ■ NACN password ■ Administrator name and password for signing into the Infranet Enforcer ■ Serial number of the Infranet Enforcer ■ Make sure the signed certificate is assigned to the Infranet Controller interface to which the Infranet Enforcer connects. Also, make sure that the CA that signed the server certificate is properly configured on the Infranet Enforcer. ■ If you changed the webserver certificate and CA certificate that is currently in use by the IC, you may need to disconnect the Infranet Enforcer from the Infranet Controller and reconnect again. You can use the <code>exec infranet controller disconnect</code> and <code>exec infranet controller connect</code> CLI commands for doing this. ■ The Infranet Controller can connect to the Infranet Enforcer only on its internal Ethernet port. Be sure to connect the Infranet Enforcer to a network that is accessible to the Infranet Controller's internal port. ■ Enable SSH management option on the interface that is being used as 'source interface' for IC-IE communication. ■ Ensure that the NACN password and serial number entered on both devices is the same. Check the Infranet Controller event log. ■ Look for ssh password and serial number mismatch between the devices. Check the Infranet Controller event log.
In an Active/Passive High Availability cluster, the Infranet Enforcer can establish communication with individual Infranet Controller IP addresses, but not the VIP.	<ul style="list-style-type: none"> ■ Check in System > Device Certificate to ensure that the certificate is bound to the internal port and the cluster VIP.
A previously-working Infranet Controller and Infranet Enforcer lose the ability to connect.	<ul style="list-style-type: none"> ■ Ensure that the Infranet Controller is included as a managed IP address.

Table 3: Infranet Controller Problems and Solutions (Continued)

Problem	Solution
Users are unable to sign into the Infranet Controller.	<ul style="list-style-type: none"> ■ Close all Web browser windows, and try using a different Web browser application. ■ Try using a different endpoint to determine if the problem occurs only on that particular endpoint. ■ If you are using an external authentication server, create a local user account on the Infranet Controller and try to sign in using that account to determine if the problem is in the authentication server configuration. ■ If you are using Kerberos single sign-on, make sure: <ul style="list-style-type: none"> ■ The clocks on the Infranet Controller and the Windows Active Directory authentication server are synchronized to within two minutes of each other. ■ The Windows endpoint computers are joined to the same domain as the domain controller that you use for user authentication with the Infranet Controller. Alternatively, make sure the Windows endpoint computers are joined to a domain with a domain controller that has a trust relationship with the domain controller for the Infranet Controller. ■ Kerberos single sign-on is configured correctly. ■ Uninstall Odyssey Access Client from the endpoint and access the Infranet Controller again to reinstall Odyssey Access Client. ■ Reboot the endpoint computer. ■ If a user with Odyssey Access Client connected to Infranet Controller loses the connection, If you are using IPsec, make sure you have specified an exception in the IPsec routing policy for the IP address assigned to the Infranet Controller if it is located in a subnet the Infranet Enforcer is protecting. ■ Ensure that you can ping the IC from the endpoint, and you can ping the endpoint from the IC. ■ If the endpoint's IP address is being NATed before it reaches the IC, you must use IPsec enforcement: Source IP will not work.
User auth table entries don't show up on the Infranet Enforcer.	<ul style="list-style-type: none"> ■ Verify that the connection is up between the Infranet Enforcer and the Infranet Controller. ■ Check the active users table or user access logs to ensure that the user is authenticated to the role you expect. If not, turn on policy tracing and attempt to determine why. ■ Turn on ScreenOS command tracking in the event log, ask the user to reauthenticate again and ensure that the auth table entries are being sent to the firewall. If not, the Resource Access > Network > Auth Table Mapping and ensure that either the default policy is in place, or there is a policy mapping that role to that firewall.

Table 3: Infranet Controller Problems and Solutions (Continued)

Problem	Solution
<p>Users are unable to access protected resources through the Infranet Enforcer</p>	<ul style="list-style-type: none"> ■ The Infranet Controller does not support Web rewriting from a Juniper Networks SSL VPN appliance. If you deploy the Infranet Controller and Infranet Enforcer in a network where remote users sign into a Juniper Networks SSL VPN appliance and those remote users request access to protected resources behind the Infranet Enforcer, the Infranet Enforcer will block the requests from the Juniper Networks SSL VPN appliance by default. <p>To solve this problem, you can instruct users to use Network Connect on the SSL VPN appliance. To accommodate users who are using the SSL VPN appliance rewriter, JSAM, or WSAM features, you must create a policy on the Infranet Enforcer that permits traffic directly from the SSL VPN appliance to the protected resources. Note that since the SSL VPN appliance traffic is by-passing the Infranet Controller, you should configure the SSL VPN appliance to provide equivalent security by doing the following:</p> <ul style="list-style-type: none"> ■ Assign the proper roles to users before allowing them to sign in to the SSL VPN appliance and access the protected resources. ■ Configure Host Checker policies on the SSL VPN appliance that are equivalent to the Host Checker policies on the Infranet Controller. ■ If you are using IPsec, make sure you have specified an exception in the IPsec routing policy for the IP address assigned to the Infranet Controller if it is located in a subnet the Infranet Enforcer is protecting. ■ If you are using IPsec in a Network Address Translation (NAT) environment, be sure to configure IP address pool policies.
<p>After configuring a cluster of Infranet Controller systems, you (as Administrator) or end users are unable to sign in or access protected resources.</p>	<ul style="list-style-type: none"> ■ To simplify troubleshooting, delete the cluster and then troubleshoot the problem on a stand-alone Infranet Controller. ■ Delete the NSRP cluster of Infranet Enforcer systems and then troubleshoot the problem on a stand-alone Infranet Enforcer. ■ Check in System > Device Certificate to ensure that the certificate is bound to the internal port and the cluster VIP.
<p>It takes a long time to sign into the Infranet Controller.</p>	<ul style="list-style-type: none"> ■ Ping the Infranet Controller. If the response takes a long time, determine if the number of hops is causing the delay. ■ Restart services on the Infranet Controller by using the Maintenance > System > Platform page in the admin console. ■ Determine if the DNS server is causing the delay. Try using the Infranet Controller IP address in the Web browser URL and see if the response from the Infranet Controller is faster. ■ Connect the endpoint to the subnet where the Infranet Controller is installed, or directly to an external port of the Infranet Controller. ■ If you are using an external authentication server, create a local user account on the Infranet Controller and try to sign in using that account to determine if the problem is in the authentication server configuration. ■ If you are using Kerberos single sign-on, make sure the endpoint computer is in the correct domain and that Kerberos single sign-on is configured correctly.

Table 3: Infranet Controller Problems and Solutions (Continued)

Problem	Solution
No connection between Odyssey Access Client and the Infranet Controller	<ul style="list-style-type: none"> ■ Make sure the Infranet Controller is accessible on the network to Odyssey Access Client. ■ Make sure there is no IPsec routing policy that prevents Odyssey Access Client from connecting to the Infranet Controller. ■ Attempt to access the IC sign-in page with a Web browser.
Odyssey Access Client users report that they are disconnected frequently	<ul style="list-style-type: none"> ■ Increase the amount of time specified for the Timeout option on the Users > User Roles > RoleName > Agent page. ■ If users are connecting with Layer 2: <ul style="list-style-type: none"> ■ Determine if the machine is dropping packets. ■ Check the switch timers. ■ Send back “terminate-action = 1” as a RADIUS attribute. ■ For wireless, check roaming aggressiveness on the wireless radio settings (device manager).
When attempting to sign into the Infranet Controller for the first time, the Windows user sees the following message and is unable to install Odyssey Access Client on the endpoint: “You do not have the proper privileges to install the application.”	<ul style="list-style-type: none"> ■ To install Odyssey Access Client, the user must have Administrator privileges. For users with restricted privileges, the local administrator can install Odyssey Access Client using Remote Login or an automated push system such as SMS. For more information, see the <i>Client-side Changes Guide</i> on the Juniper Networks Customer Support Center. ■ As an alternative, you can configure agentless access for the endpoint.
During remediation, users are unable to access a resource that you refer to in your custom instructions, such as a server to obtain antivirus software.	<ul style="list-style-type: none"> ■ If the resource is behind the Infranet Enforcer, make sure you create an Infranet Enforcer resource access policy to allow access to that protected resource when the user’s computer is in a non-compliant state. ■ If the DNS server is behind the Infranet Enforcer, make sure you create an Infranet Enforcer resource access policy to allow access to the DNS server.

Troubleshooting Host Checker Policies

Host Checker policies are the front line for determining the health and security status of endpoints. If a user cannot access a role or realm, the issue is potentially due to a Host Checker misconfiguration.

Table 4: Troubleshooting Host Checker

Problem	Solution
Host Checker is configured with a Statement of Health (SOH) rule, and client cannot log in (third-party supplicant).	<ul style="list-style-type: none"> ■ Ensure that the NAP Agent Service is running on the client. for instructions for Windows Vista: http://thelazyadmin.com/blogs/thelazyadmin/archive/2008/02/21/configuring-the-vista-nap-client.aspx for instructions for Windows XP: http://thelazyadmin.com/blogs/thelazyadmin/archive/2008/02/11/configuring-the-nap-client-in-xp-sp3.aspx ■ Ensure that EAP-SOH is selected as the authentication protocol in an authentication protocol set that is associated with the realm to which the user is trying to authenticate. ■ Client Windows Security Center (WSC) and the IC's WSC panel can display different status. Toggle WSC elements and re-attempt. ■ Using Odyssey Access Client, after disconnecting and reconnecting login may fail. The IC thinks the client is still connected.
Linux or Solaris endpoints cannot download Host Checker application.	Linux or Solaris endpoints must use the Firefox browser.
Macintosh, Linux, or Solaris endpoints fail Host Checker policy.	You must explicitly create policies for each operating system you want to allow. Macintosh, Linux, or Solaris endpoints cannot access resources if the Host Checker policy is for a Windows machine.
Client receives no indication of Host Checker failure.	You must explicitly enable endpoint Host Checker logging from the System > Log Monitoring > Client Logs > Settings page of the admin console.

Troubleshooting Layer 2 Connectivity Issues

Layer 2 connectivity issues usually involve miscommunication between the Infranet Controller and the switch.

Table 5: Layer 2 Connectivity

Problem	Solution
Connectivity issues between the Infranet Controller and the switch.	<ul style="list-style-type: none"> ■ Check the event logs on the Infranet Controller to ensure that the switch is added as a RADIUS client and has the correct shared secret. ■ Check the RADIUS request status on the switch. For example, on the Juniper Networks EX series switch: EX-Switch > show network-access aaa statistics authentication Authentication module statistics Requests received: 91 Accepts: 3 Rejects: 44 Challenges: 44 Requests timedout: 2 ■ Check the status of dot1x timers on port. For example on the EX series switch: root@UAC-Hurricane-Switch > show dot1x interface ge-0/0/1.0 detail Role: Authenticator Administrative state: Auto Supplicant mode: Single Number of retries: 3 Quiet period: 60 seconds Transmit period: 30 seconds Reauthentication: Enabled Reauthentication interval: 3600 seconds Supplicant timeout: 30 seconds Server timeout: 30 seconds Maximum EAPOL requests: 2 Guest VLAN member: < not configured > Number of connected supplicants: 0 ■ Check the RADIUS parameters sent by the Infranet Controller by enabling tcpdump on the Infranet Controller and ensure that attributes are received on the switch. (Capture the traffic on the switch port connected to OAC). ■ Check to ensure that the Vendor-Specific Attributes (VSA) are sent, and ensure that the proper make is configured. Check the RADIUS dictionary for the vendor to ensure that the VSA exists in the RADIUS dictionary.
Connectivity issues between the supplicant (OAC or 3rd party) and the Infranet Controller.	<ul style="list-style-type: none"> ■ Ensure that OAC or 3rd-party supplicant and the Infranet Controller have a common set of authentication protocols. ■ If the wrong authentication protocol is chosen, check the order of authentication protocols on the Infranet Controller,

Table 5: Layer 2 Connectivity (Continued)

Problem	Solution
Authentication of endpoint fails.	<ul style="list-style-type: none"> Some Host Checker rules require a component to be downloaded to the endpoint. A Layer 2 connection with an IP address will not permit the download. Configure a role with no restrictions to allow the endpoint to authenticate and get an IP address, then the user can access the role with Host Checker restrictions.

Time Limits on RADIUS Authentication and Accounting

All requests for authentication have a time limit. Depending on the endpoint, the authentication protocols used, the network access device (NAD) settings, and the Host Checker policies configured at the role and realm level, RADIUS time limits could affect the success or failure of authentication and the performance and memory allocation of the RADIUS server.

You can use this information along with the RADIUS Diagnostic Log and User Log as a guide for troubleshooting the Infranet Controller.

Table 6: RADIUS Event Time Limits

Interval Starts:	Interval Ends:	Limited by:	Effect of Timeout
when the NAD sends a single RADIUS request to the Infranet Controller	when the NAD receives the RADIUS response	NAD: sometimes five seconds, usually configurable	NAD resends an exact copy of the RADIUS request (if it is configured to do so) RADIUS diagnostic log indicates that a duplicate was received
when the NAD sends the first copy of a RADIUS request to the Infranet Controller.	when the NAD receives the RADIUS response	NAD: (the timeout interval above) x (the maximum number of retries + 1) The maximum number of retries is typically 2 or 3 and is usually configurable	The NAD assumes a communication failure with the RADIUS server. It may record the event in the log and report it to the endpoint. The Infranet Controller RADIUS diagnostic log shows turnaround times longer than the NAD's limit.
when NAD forwards an EAP request from the Infranet Controller to an endpoint	when the NAD receives an EAP response from the endpoint	NAD: (this may be limited by a configuration setting on the NAD, or the NAD may honor the Session Timeout attribute that the Infranet Controller included in the Access-Challenge packet - see next row)	The Infranet Controller user log reports timeout while waiting for a RADIUS continuation request.

Table 6: RADIUS Event Time Limits

Interval Starts:	Interval Ends:	Limited by:	Effect of Timeout
when the Infranet Controller sends the first EAP message of an EAP exchange to the NAD for forwarding to the endpoint	when the Infranet Controller receives the last EAP response	Infranet Controller: This limit was two minutes and has been increased to four minutes	The Infranet Controller user log reports timeout while waiting for a RADIUS continuation request.
”	“	NAD: Some NADs limit this. The limit is not always configurable	“
when the Infranet Controller sends a RADIUS Access-Accept packet to the NAD and the NAD lets the endpoint onto the network.	The NAD takes the endpoint off the network unless it has been reauthenticated.	NAD: This may be fixed in the NADs configuration or controlled by the Session Timeout attributes that the sends as part of the Access-Accept packet. The Session-Timeout attribute is set by the roles assigned to the user, or by the RADIUS attributes policy.	Endpoint loses network connectivity. NAD sends a RADIUS Accounting-Stop packet (if configured to do so). The Infranet Controller records in the user log.
when the Infranet Controller finishes authenticating Odyssey Access Client using EAP-JUAC.	Odyssey Access Client automatically initiates reauthentication.	Odyssey Access Client: the Infranet Controller sends a time limit equal to the session timeout fixed by the roles assigned to the user minus two minutes	Odyssey Access Client automatically initiates reauthentication. User intervention is typically needed for a SecureID card only. If reauthentication succeeds, the endpoint retains network access.

Port Numbers used by the Infranet Controller, Infranet Enforcer, and Odyssey Access Client

TCP and UDP port numbers used by UAC are listed in “Port Numbers used on the Infranet Controller” on page 13. The list indicates the direction from which the traffic is initiated.

If you are not using IPsec then the ports listed for IKE or NAT/IKE do not pertain to your configuration.

Table 7: Port Numbers used on the Infranet Controller

Direction	Port and Service	Event
IC -> ScreenOS Enforcer	TCP port 22	IC connects to ScreenOS Enforcer
ScreenOS Enforcer -> IC	TCP port 11122	ScreenOS Enforcer tells IC it wants IC to connect

Table 7: Port Numbers used on the Infranet Controller

Direction	Port and Service	Event
ScreenOS Enforcer - > IC	UDP port 1812 RADIUS	ScreenOS Enforcer authenticates XAUTH user (could be 1645)
ScreenOS Enforcer - > IC	UDP port 1813 RADIUS	ScreenOS Enforcer sends RADIUS accounting (could be 1646)
OAC -> IC	TCP port 443 SSL	ScreenOS Enforcer authentication, control channel
OAC -> ScreenOS Enforcer	UDP port 500 IKE	
OAC -> ScreenOS Enforcer	UDP port 4500 NAT T	ScreenOS Enforcer IKE/IPsec
JUNOS Enforcer > IC	port 11123	JUNOS Enforcer communicates with IC
IF-MAP Federation Server > IC	port 443	Federation server communicates with Federation client

You can have others from the IC depending on the service (LDAP, RSA, etc).

Unified Access Control Solution Logging and Monitoring Tools for Troubleshooting

The Infranet Controller provides several troubleshooting utilities that enable you to monitor the state of your system, including clusters, if you use them. This section provides an overview of the various troubleshooting tasks that are available by using the Infranet Controller:

- “Tracking Events” on page 15
- “Creating Snapshots of the Infranet Controller System State” on page 17
- “Creating TCP Dump Files” on page 18
- “Testing Infranet Controller Network Connectivity” on page 20
- “Running Debugging Tools Remotely” on page 21
- “Creating Debugging Logs” on page 22
- “Using the RADIUS Diagnostic Log” on page 22
- “Monitoring Cluster Nodes” on page 23
- “Configuring Group Communication Monitoring on a Cluster” on page 24
- “Configuring Network Connectivity Monitoring on a Cluster” on page 26

Tracking Events

You can determine why your Infranet Controller does not allow you to accomplish a task that you desire by tracking problematic Infranet Controller events using settings in the **Maintenance > Troubleshooting > User Sessions > Policy Tracing** page of the admin console. This page guides you through all the realms, roles, and policies that are currently configured in the Infranet Controller and print log messages at various steps of the authentication, authorization, and access process.

The events in question are related to authentication, authorization, and access for a particular user. They are entirely driven by what happens during a user session.



NOTE: The events that are captured do not include any other system related events. The Infranet Controller merely uses the events as a filtering mechanism to reduce the number of logs and highlight the problem.

Tracking Events Using Policy Tracing

The Infranet Controller allows you to troubleshoot problems by tracking events when a user signs into a realm. The **Maintenance > Troubleshooting > User Sessions > Policy Tracing** page allows you to record a policy trace file for an individual user. The Infranet Controller displays log entries that list the user's actions and indicates why they are allowed or denied access to various functions.



NOTE: User access logs are only reported for policies that are checked under **Events to Log**.

Use this tab if your users are having problems accessing functions they expect to use in their roles. The events logged in the policy trace file may help you diagnose these problems.

To create a policy trace file:

1. In the admin console, choose **Maintenance > Troubleshooting > User Sessions > Policy Tracing**.
2. In the **User** field, enter the Infranet Controller username of the user you want to trace. Note that you may use a wildcard character (*) in place of a username.
3. In the **Realm** field, select the user's realm. Note that the Infranet Controller does not allow you to select a realm that maps to an anonymous authentication server.
4. Under **Events to log**, select the types of events you want to write to the policy tracing log file.
5. Click **Start Recording**. Ask the user to sign into the Infranet Controller after you have started recording.
6. Click **View Log** to see the log entries.
7. Click **Stop Recording** when you have obtained enough information.
8. Review messages in the log file to determine what is causing the unexpected behavior. If you cannot determine and fix the problem, click **Save Log As** to save a copy of the log file to a location on your network. Then, send the file to Juniper Networks Support for review.
9. Click **Clear Log** to clear the contents of the log file, or click **Delete Trace** to clear the contents of the log file and to remove the default entries from the username and realm fields.

Creating Snapshots of the Infranet Controller System State

The **Maintenance > Troubleshooting > System Snapshot** tab allows you to create a snapshot of the Infranet Controller system state. When you use this option, the Infranet Controller runs various utilities to gather details on the Infranet Controller system state, such as the amount of memory in use, paging performance, the number of processes running, system uptime, the number of open file descriptors, and the ports in use.

You can choose to include or exclude system configuration and debug logs. However, debug logs are particularly important in the event of a problem. You will need to set the debug log at a certain level and add the events list as directed by your Support representative. Recreate the problem or event and then take a snapshot and send it to Support. The debug log is encrypted; you cannot view it.

**NOTE:**

- The Infranet Controller stores up to ten snapshots, which are packaged into an encrypted “dump” file that you can download to a network machine and then email to Juniper Networks Support. If you take more than ten snapshots, the Infranet Controller overwrites the oldest snapshot file with the new snapshot. If the Infranet Controller runs out of disk space, the Infranet Controller does not store the newest snapshot and logs a message in the Event log. We recommend that you download the snapshots to a network machine in a timely manner to avoid losing them.
- In a cluster, the snapshot occurs on a individual node basis only. That is, the snapshot settings you specify are *not* synchronized in all nodes of the cluster.

To take a snapshot of the Infranet Controller system state:

1. In the admin console, choose **Maintenance > Troubleshooting > System Snapshot**.
2. Select the **Include system config** checkbox to include system configuration information in your snapshot (optional).
3. Select the **Include debug log** checkbox to include log file created through the **Debug Log** tab in your system snapshot. For more information, see “Creating Debugging Logs” on page 22.
4. Click **Take Snapshot** to manually take a snapshot immediately.
5. To automatically take a snapshot at regular intervals:
 - a. Select **Schedule automatic snapshots**. Additional configuration items appear.
 - b. Specify how often you want to take a snapshot (in hours).

- c. Specify the maximum file size of each snapshot (in MB).



NOTE: If the size of the snapshot exceeds the maximum file size you specify, the snapshot will fail and the Infranet Controller will log a message in the Event log.

- d. (Optional) If you want to stop taking snapshots at a particular time, specify a date and time. Otherwise, the periodic snapshots continue until you manually stop them.
 - e. If you want to disable debug logs at the stop time you specified, select **Disable debug logs at stop time**.
6. Click **Save Changes**.
 7. When the Infranet Controller finishes taking the snapshot, click the link for the snapshot listed under **Snapshot**, click **Save**, navigate to the folder where you want to store the snapshot file, and then click **Save**.
 8. Email the file to Juniper Networks Support for review.
 9. When you are finished, select the snapshot listed under **Snapshot** and then click **Delete** to delete the snapshot.



NOTE: You can also take a system snapshot from the serial console. This method is useful if you cannot get to the admin console and need to save the system configuration.

Creating TCP Dump Files

The **Maintenance > Troubleshooting > Tools > TCP Dump** tab allows you to sniff network packet headers and save the results in an encrypted “dump” file that you can download to a network machine and then email to Juniper Networks Support.

This feature uses the TCP/IP network stack to capture packets at the TCP layer. It captures all communication that passes through the Infranet Controller. However, certain encrypted higher level protocols cannot be decrypted. This feature is useful for troubleshooting common customer problems. A TCP dump file helps the Juniper Networks Support team observe the communication protocols used between Infranet Controller and any other intranet server and how the intranet server responded to requests from the Infranet Controller.

On the admin console, you can select which interface you want to capture packets from, whether internal or external, you can select promiscuous mode, which increases the level of detail in the dump file, and you can specify a filter.

To sniff network packet headers:

1. In the admin console, choose **Maintenance > Troubleshooting > Tools > TCP Dump**.

2. Select the Infranet Controller port on which you want to sniff network packet headers.
3. Turn off **Promiscuous mode** to sniff only for packets intended for the Infranet Controller.
4. Create a custom filter using TCPDump Filter Expressions (optional). This option provides the ability to filter the sniffed network packets so that the resulting dump file contains only the information you require. See Table 8 below for examples.
5. Click **Start Sniffing**.
6. Click **Stop Sniffing** to stop the sniffing process and create an encrypted file.
7. Click **Download** to download the file to a network machine.
8. Email the file to Juniper Networks Support for review.

Table 8: Examples of TCPDump Filter Expressions

Example	Result
tcp port 80	Sniffs packets on TCP port 80.
port 80	Sniffs packets on TCP or UDP port 80.
ip	Sniffs the IP protocol.
tcp	Sniffs the TCP protocol.
dst #.#.#.#	Sniffs the destination IP address specified, where #.#.#.# is a valid IP address.
src #.#.#.#	Sniffs the source IP address specified, where #.#.#.# is a valid IP address.
port 80 or port 443	Sniffs on port 80 or port 443.
src #.#.#.# and dst #.#.#.#	Sniffs the source and destination IP addresses or hosts specified, where each #.#.#.# represents a valid IP address.
tcp port 80 or port 443 and dst #.#.#.# and src #.#.#.#	This example shows how to specify multiple parameters to create a filter that sniffs on TCP port 80, or on TCP or UDP port 443, and on the destination and source ports, where each #.#.#.# represents a valid IP address.

For more information about TCPDump Filter Expressions, visit the following Web site:
http://www.tcpdump.org/tcpdump_man.html

For more information on using TCP Dump, see “Creating TCP Dump Files” on page 18.

Testing Infranet Controller Network Connectivity

The **Maintenance > Troubleshooting > Tools > Commands** tab allows you to run UNIX commands such as arp, ping, traceroute, and NSlookup to test Infranet Controller network connectivity. You can use these connectivity tools to see the network path from the Infranet Controller to a specified server.

Address Resolution Protocol (ARP)

Use the arp command to map IP network addresses to the hardware addresses. The Address Resolution Protocol (ARP) allows you to resolve hardware addresses.

To resolve the address of a server in your network, a client process on the Infranet Controller sends information about its unique identify to a server process executed on a server in the intranet. The server process then returns the required address to the client process.

Ping

Use the ping command to verify that the Infranet Controller can connect to other systems on the network. In the event of a network failure between the local and remote nodes, you will not receive a reply from a pinged device. In that case, contact your LAN administrator for help.

The ping command sends packets to a server and returns the server response, typically a set of statistics including the target server's IP address, the time spent sending packets and receiving the response, and other data. You can ping unicast or multicast addresses, and you must include the target server name in the request.

Traceroute

Use the traceroute command to discover the path that a packet takes from the Infranet Controller to another host. Traceroute sends a packet to a destination server and receives an ICMP TIME_EXCEEDED response from each gateway along its path. The TIME_EXCEEDED responses and other data are recorded and displayed in the output, showing the path of the packet round-trip.

To run a UNIX command to test Infranet Controller network connectivity:

1. In the admin console, choose **Maintenance > Troubleshooting > Tools > Commands**.
2. From the **Command** list, select the command to run.
3. In the **Target Server** field, enter the IP address of the target server.
4. Enter other arguments or options.
5. Click **OK** to run the command.

NSlookup

Use NSlookup to get detailed information about a name server on the network. You can query on several different types of information, including a server's IP address, alias IP address, start-of-authority record, mail exchange record, user information, well-known services information, and other types of information.

To run NSlookup to test name server connectivity:

1. In the admin console, choose **Maintenance > Troubleshooting > Tools > Commands**.
2. From the **Command** list, select **NSlookup**.
3. Select the **Query Type** from the drop down menu.
4. Enter the query, which is a host name, an IP address, or other information, depending on your selection of query type.
5. Enter the DNS server name or IP address.
6. Enter other options.
7. Click **OK** to run the command.

Running Debugging Tools Remotely

The Juniper Networks Support team can run debugging tools on your production Infranet Controller if you configure it to do so through the **Maintenance > Troubleshooting > Remote Debugging** page. To enable this option, you must work with Juniper Networks Support to obtain a debugging code and host to which your Infranet Controller connects.

To enable remote debugging:

1. Contact Juniper Networks Support to set up the terms of a remote debugging session.
2. In the admin console, choose **Maintenance > Troubleshooting > Remote Debugging**.
3. Enter the debugging code provided by Juniper Networks Support.
4. Enter the host name provided by Juniper Networks Support.
5. Click **Enable Debugging** to allow the Juniper Networks Support team to access the Infranet Controller.
6. Notify Juniper Networks Support that your Infranet Controller is accessible.
7. Click **Disable Debugging** when Juniper Networks Support notifies you that the remote debugging session is over.

Creating Debugging Logs

If you have a problem, a Juniper Networks Support representative may ask you to create debugging logs to assist with debugging Infranet Controller internal issues. When you enable logging, the Infranet Controller records certain events and messages based on event codes you enter into admin console on the **Maintenance > Troubleshooting > Monitoring > Debug Log** tab. Using the debug log that results, the support team can identify the code flow for any discrepancies. Your support representative gives you all of the information you need to create the log file, including the debug detail log level and the event codes.



NOTE: Running debug logging can impact your system performance and stability. You should only generate debug logs when directed by your Juniper Networks Support representative.

To enable the debug log:

1. In the admin console, choose **Maintenance > Troubleshooting > Monitoring > Debug Log**.
2. Select the **Debug Logging On** checkbox.
3. Enter the log size, detail level, and event code specified by Juniper Networks Support.



NOTE: Setting the detail level to 0 displays only Critical messages, it does not disable logging completely.

4. Click **Save Changes**.
5. Choose the **Maintenance > Troubleshooting > System Snapshot** tab.
6. Check the **Include debug log** checkbox.
7. Click **Take snapshot** to create a file that contains the debug log.
8. Click **Download**.
9. Attach the snapshot file an email message and sent it to Juniper Networks Support.

Using the RADIUS Diagnostic Log

The RADIUS Troubleshooting Log allows you to view the full suite of RADIUS logging features, including traffic trace and debug-level messages. In releases prior to 2.2 these logs were only available in an encrypted format that required decryption by Juniper Networks.

The RADIUS Troubleshooting Log monitors all requests that the Infranet Controller receives from RADIUS clients. RADIUS requests that the Infranet Controller initiates do not appear in the log.

Raw traffic is not available in the log. To view raw traffic, use the tcpdump feature. See “Creating TCP Dump Files” on page 18.

You can configure the maximum size of the log. When the log fills up, logging stops. You can resume logging by clearing the log.

All events that appear in the log have an ID code, and all messages in a thread are tagged with the same ID. This allows you to track individual logins or login attempts.

The RADIUS Troubleshooting Log is secure, as passwords are suppressed and do not appear in the logs.

Performance of the Infranet Controller is affected with RADIUS logging turned on.

Source IP addresses are represented in the RADIUS Troubleshooting Log as 127.0.0.1 (the loopback address). To determine the real IP address, refer to the Funk-Source-IP-Address for Layer 3 connections. For Layer 2 connections, the calling station ID is the MAC address of the endpoint.

Please refer to <http://www.iana.org/assignments/radius-types> and <http://www.iana.org/assignments/eap-numbers> for information to help you understand RADIUS logs. When referring to external information, note that EAP-JUAC is a Juniper Networks protocol. External references do not mention EAP-JUAC.



NOTE: In an active-active cluster, logs are not synced.

To configure the RADIUS Troubleshooting Log:

1. Select **Troubleshooting > Monitoring > RADIUS** from the left navigation bar of the admin console.
2. Select the **RADIUS Diagnostic Log On** check box.
3. Enter the maximum log size (up to 1,000 MB) in the **Max Diagnostic Log Size** box.
4. Click **Save Changes**.

Monitoring Cluster Nodes

If you have a problem with a cluster, a Juniper Networks Support representative may ask you to create a snapshot that includes node monitoring statistics to assist with debugging the cluster problem. When you enable the node monitor on the **Maintenance > Troubleshooting > Monitoring > Node Monitor** tab, the Infranet Controller captures certain statistics specific to the cluster nodes on your system. Using the snapshot that results, the support team can identify important data, such as network statistics and CPU usage statistics.

To enable node monitoring:

1. Enter the maximum size for the node monitor log.
2. Enter the interval, in seconds, at which node statistics are to be captured.
3. Select the **Node monitoring enabled** checkbox to start monitoring cluster nodes.
4. For **Maximum node monitor log size**, enter the maximum size (in MB) of the log file. Valid values are 1-30.
5. Specify the interval (in seconds) that defines how often nodes are to be monitored.
6. Select the commands to use to monitor the node.

If you select **dsstatdump**, enter its parameters as well.
7. Click **Save Changes**.
8. If you want to include the node monitoring results in the system snapshot, choose **Maintenance > Troubleshooting > System Snapshot**, and select the **Include debug log** checkbox.
9. Take a system snapshot to retrieve the results. For more information, see “Creating Snapshots of the Infranet Controller System State” on page 17.

Configuring Group Communication Monitoring on a Cluster

If you have a problem with a cluster, a Juniper Networks Support representative may ask you to create a snapshot that includes group communication statistics to assist with debugging the cluster problem. When you enable the group communication monitor on the **Maintenance > Troubleshooting > Monitoring > Cluster > Group Communication** tab, the Infranet Controller records statistics related to all of the cluster nodes on your system. As the local node communicates with other nodes in the cluster, the Infranet Controller captures statistics related to intra-cluster communication. The **Maintenance > Troubleshooting > Monitoring > Cluster > Group Communication** tab appears only when you enable clustering on your system. On a standalone Infranet Controller, you do not have access to the **Maintenance > Troubleshooting > Monitoring > Cluster > Group Communication** tab.

You can also enable the cluster networking troubleshooting server on the **Maintenance > Troubleshooting > Monitoring > Cluster > Network Connectivity** page. For more information, see “Configuring Network Connectivity Monitoring on a Cluster” on page 26.

**NOTE:**

- Performing excessive node monitoring can impact your system performance and stability. You should only perform extensive monitoring when directed by your Juniper Networks Support representative.
 - Performing log synchronization across cluster nodes can impact your system performance and stability.
-

To enable group communication monitoring:

1. Enter the maximum size for the statistics log.
2. Enter the interval, in seconds, at which events are to be logged.
3. If you want to monitor all cluster nodes from the current local node, select the **Monitor all cluster nodes from this node** checkbox. If you do not check this option, the group communication monitor gathers statistics only for the local node.



NOTE: If you select the **Monitor all cluster nodes from this node** option, the cluster nodes must be able to communicate over UDP port 6543.

4. Select the **Enable group communication monitoring** checkbox to start the monitoring tool.
5. Click **Save Changes**.
6. If you want to include the node monitoring results in the system snapshot, choose **Maintenance > Troubleshooting > System Snapshot**, and select the **Include debug log** checkbox.
7. Take a system snapshot to retrieve the results. For more information, see “Creating Snapshots of the Infranet Controller System State” on page 17.

Configuring Network Connectivity Monitoring on a Cluster

If you have a problem with a cluster, a Juniper Networks Support representative may ask you to enable the cluster node troubleshooting server. When you enable the server on the **Maintenance > Troubleshooting > Cluster > Network Connectivity** tab, the Infranet Controller attempts to establish connectivity between the node on which the server resides and another node you specify. As the nodes communicate, the Infranet Controller displays network connectivity statistics on the page. The **Maintenance > Troubleshooting > Cluster > Network Connectivity** tab appears only when you enable clustering on your system. On a standalone Infranet Controller, you do not have access to the **Maintenance > Troubleshooting > Cluster > Network Connectivity** tab.

Use the Network Connectivity page to enable the cluster node troubleshooting server and to select a node on which to perform troubleshooting tasks. The troubleshooting tool allows you to determine the network connectivity between cluster nodes.

The server component of this tool runs on the node to which connectivity is being tested. The client component runs on the node from which connectivity is being tested. The basic scenario for testing connectivity is this:

- The administrator starts the server component on the passive node.
- The administrator then tests the connectivity to the server node from the Active node, by starting the client component on the Active node and contacting the Passive node running the server component.



NOTE: The server component must be run on nodes that are configured as either standalone, or in a cluster but disabled. Cluster services cannot be running on the same node as the server component.

1. Select the **Enable cluster network troubleshooting server** checkbox to enable the server component.
2. Click **Save Changes**.
3. On another machine, select **Maintenance > Troubleshooting > Cluster > Network Connectivity**.
4. Perform one of the following steps:
 - Select a node from the drop down menu.
 - Enter the IP address of the server node.
5. Click **Go** to begin troubleshooting the machine on which the server component is running.
6. Click the **Details** link that appears on the page below the fields, to view the results.

C

CLI commands for Infranet Enforcer
troubleshooting commands 2

D

diagnostic log, RADIUS 22

I

Infranet Controller
events log 5
policy tracing 5
troubleshooting 4

Infranet Enforcer
troubleshooting 1

L

logging
policy tracing 16

P

Policy Tracing subtab 16

R

RADIUS diagnostic log 22
recording user sessions 16

S

system
snapshot 24, 25

T

troubleshooting the Unified Access Control initial configuration 1
troubleshooting, RADIUS diagnostic log 22

U

Unified Access Control solution
troubleshooting 1