



## RSA SecurID Ready Implementation Guide

Last Modified: March 27<sup>th</sup>, 2008

### Partner Information

---

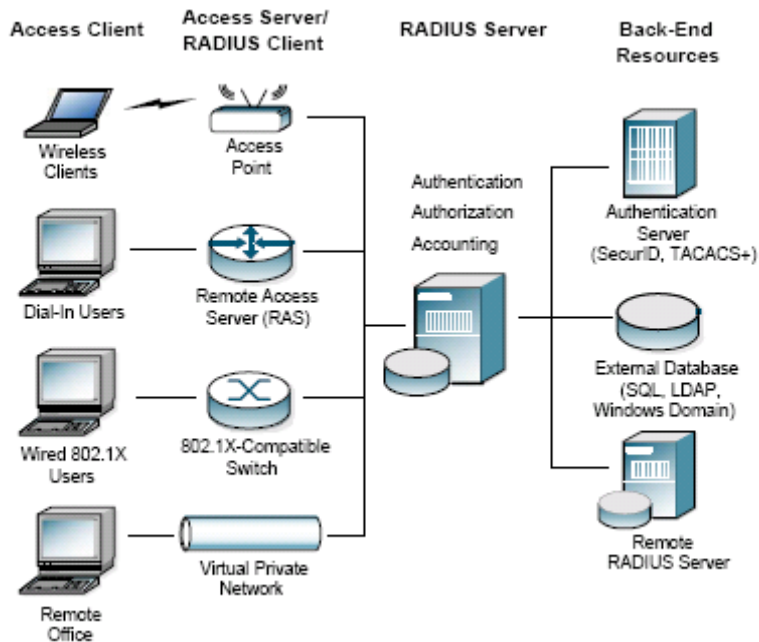
Product Information	
Partner Name	Juniper Networks
Web Site	<a href="http://www.juniper.net">www.juniper.net</a>
Product Name	Odyssey Access Client
Version & Platform	4.6.0 and 4.72
Product Description	Juniper Networks Odyssey Access Client (OAC) is an enterprise-class 802.1X supplicant/access client, offering full support for the advanced protocols required for secure wired and wireless LAN access. OAC ensures that users can connect to authorized networks, where login credentials are not compromised, and data privacy is maintained. OAC is compatible and integrates with Juniper Networks' Unified Access Control (UAC) v2.x, a comprehensive network access control solution that combines powerful, standards-based user authentication and authorization with identity-based policy control and management, ensuring endpoint security intelligence to extend access control across an enterprise network.
Product Category	Networks and Communication





## Solution Summary

The scope of this guide is to show how to setup and configure Odyssey Client 4.6 to be used in RSA SecurID authenticated 802.1x environments. For a more in depth explanation of how to configure your switch/wireless hardware, please refer to the documentation provided by your hardware vendor.



## Product Requirements

Operating System	
Windows XP	SP2 or higher
Windows 2003	SP1 or higher

### Adapter Cards

The Odyssey Client is capable of performing 802.1x authentication through any **wired** or **wireless** adapter card driver that fully supports the 802.11 OIDs defined in NDIS 5.1. Please contact Juniper Networks for the latest list of supported Access Points, Switches, and LAN / WLAN adapter cards.



## Partner Product Configuration

---

### ***Before You Begin***

This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### ***Documenting the Solution***

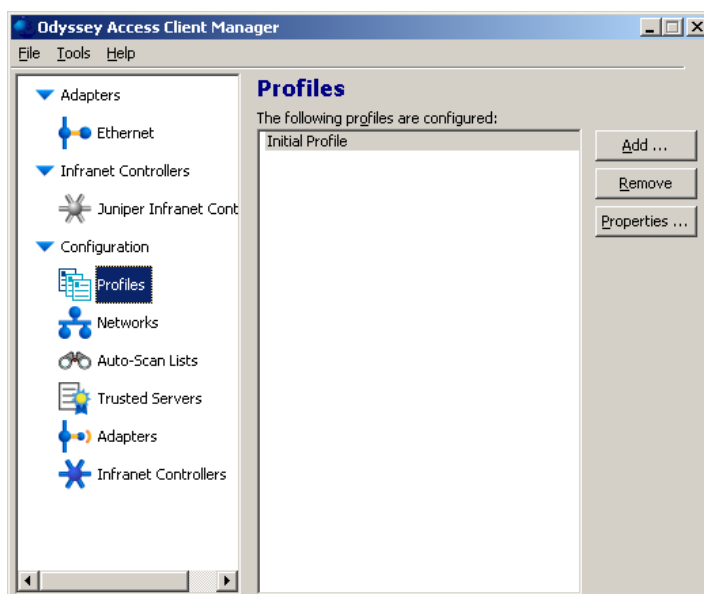
This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### **Odyssey Client Configuration**

1. Install Odyssey Client and start application by navigating to **Start | Programs | Juniper Networks | Odyssey Access Client | Odyssey Access Client Manager**.
2. On the left hand pane, click on **Profiles**.
3. Click **Add** to create new profile and name the profile.
4. Enter the username (optional) of the Authentication Manager user to be authenticated.
5. On the **Password** tab, verify that **Permit logon using password** and **Prompt for login name and password** are selected.





**Add Profile**

Profile name: Authentication Manager

User Info | **Authentication** | ITLS | PEAP | QUAC

Login name: cyork

Password | Certificate | Soft Token | SIM Card

Permit login using password

Use Windows password

Prompt for password

Prompt for login name and password

Use the following password:

Unmask

OK Cancel

## Connecting and Authenticating in a 802.1x environment

1. On the left hand pane, click on **Ethernet** and verify **Connect to the Network** is checked.

**Odyssey Access Client Manager**

File Tools Help

Adapters  
Ethernet

Infranet Controllers

Configuration  
Profiles  
Networks  
Auto-Scan Lists  
Trusted Servers  
Adapters  
Infranet Controllers

**Ethernet**

Adapter: Intel(R) PRO/1000 MT Network Connection

Use Odyssey to operate this adapter

Profile: Authentication Manager

Connect to the network Scan ...

**Connection Information**

Status: authenticating

Elapsed time:

Network (SSID):

Access point: switch

IP address:

Packets in/out:

**Infranet Controller**

Status:

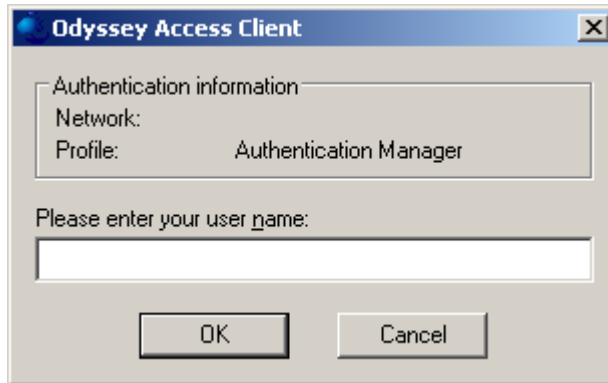
Server:

Compliance:


Reconnect Regenerate



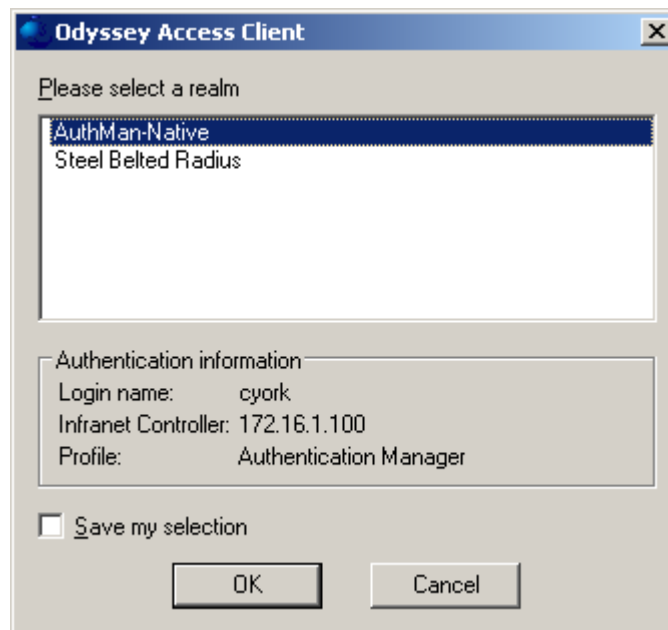
2. Enter the RSA Authentication Manager username when prompted for authentication information.




---

 Depending on the configuration of the Unified Access Control Server (UAC), you may or may not be prompted to select a particular realm. If prompted, select the appropriate realm when logging on. This information can be provided by your Help Desk or the UAC device administrator.

---



---

 To connect and authenticate directly to a Unified Access Server (non-802.1x authentication), please refer to the Appendix for additional configuration information.

---



## Client Login Screens

New PIN – System Generated - #1	New PIN – System Generated - #2
<p><b>Odyssey Access Client</b></p> <p>Message from server: Enter empty PIN to generate a new PIN and display it on the screen, or Press &lt;Cancel&gt; to cancel the New PIN procedure:</p> <p>Please enter response:</p> <p><input type="checkbox"/> unmask</p> <p>Authentication information Login name: cyork Infranet Controller: 172.16.1.100 Profile: Authentication Manager</p> <p>OK Cancel</p>	<p><b>Odyssey Access Client</b></p> <p>Message from server: ARE YOU PREPARED TO HAVE THE SYSTEM GENERATE A PIN? (y or n) [n]:</p> <p>Please enter response:</p> <p><input type="checkbox"/> unmask</p> <p>Authentication information Login name: cyork Infranet Controller: 172.16.1.100 Profile: Authentication Manager</p> <p>OK Cancel</p>

New PIN - System Generated #3	Force Authentication with New PIN
<p><b>Odyssey Access Client</b></p> <p>Message from server: PIN: qoa1x Remember PIN and enter empty PIN to continue.</p> <p>Please enter response:</p> <p><input type="checkbox"/> unmask</p> <p>Authentication information Login name: cyork Infranet Controller: 172.16.1.100 Profile: Authentication Manager</p> <p>OK Cancel</p>	<p><b>Odyssey Access Client</b></p> <p>Message from server: Wait for the code on your card to change, then log in with the new PIN Enter PASSCODE:</p> <p>Please enter response:</p> <p><input type="checkbox"/> unmask</p> <p>Authentication information Login name: cyork Infranet Controller: 172.16.1.100 Profile: Authentication Manager</p> <p>OK Cancel</p>



### User Defined 4-8 Alphanumeric

**Odyssey Access Client** [X]

Message from server:  
Enter your new PIN, containing 4 to 8 characters, or  
Press <Cancel> to cancel the New PIN procedure: Enter your  
new PIN or  
Press <Cancel> to cancel the New PIN procedure:

Please enter response:  
[ ]

unmask

Authentication information  
Login name: cyork  
Network:  
Profile: Authentication Manager

OK Cancel

### User Defined 5-7 Numeric

**Odyssey Access Client** [X]

Message from server:  
Enter your new PIN, containing 5 to 7 digits, or  
Press <Cancel> to cancel the New PIN procedure: Enter your  
new PIN or  
Press <Cancel> to cancel the New PIN procedure:

Please enter response:  
[ ]

unmask

Authentication information  
Login name: cyork  
Network:  
Profile: Authentication Manager

OK Cancel

### New PIN - User Selectable 4-8 Alphanumeric

**Odyssey Access Client** [X]

Message from server:  
Enter your new PIN, containing 4 to 8 characters, or  
Enter empty PIN to generate a new PIN and display it on the  
screen, or  
Press <Cancel> to cancel the New PIN procedure:

Please enter response:  
[ ]

unmask

Authentication information  
Login name: cyork  
Infranet Controller: 172.16.1.100  
Profile: Authentication Manager

OK Cancel

### New PIN - User Selectable 5-7 Numeric

**Odyssey Access Client** [X]

Message from server:  
Enter your new PIN, containing 5 to 7 digits, or  
Enter empty PIN to generate a new PIN and display it on the  
screen, or  
Press <Cancel> to cancel the New PIN procedure:

Please enter response:  
[ ]

unmask

Authentication information  
Login name: cyork  
Infranet Controller: 172.16.1.100  
Profile: Authentication Manager

OK Cancel



### Deny 4 and 8 PIN length

**Odyssey Access Client** [X]

Message from server:  
PIN rejected: invalid length. Please try again.

Enter PASSCODE:

Please enter response:

unmask

Authentication information  
Login name: cyork  
Infranet Controller: 172.16.1.100  
Profile: Authentication Manager

OK Cancel

### Deny Alphanumeric PIN

**Odyssey Access Client** [X]

Message from server:  
PIN rejected: invalid format. Please try again.

Enter PASSCODE:

Please enter response:

unmask

Authentication information  
Login name: cyork  
Infranet Controller: 172.16.1.100  
Profile: Authentication Manager

OK Cancel

### Next TokenCode

**Odyssey Access Client** [X]

Message from server:  
Please Enter the Next Code from Your Token:

Please enter response:

unmask

Authentication information  
Login name: cyork  
Infranet Controller: 172.16.1.100  
Profile: Authentication Manager

OK Cancel

# Certification Checklist For RSA Authentication Manager 6.1

Date Tested: September 7, 2007

Certification Environment		
Product Name	Version Information	Operating System
<b>RSA Authentication Manager</b>	6.1	Windows 2003
<b>Juniper Odyssey Client</b>	4.6.0.49455	Windows XP
<b>Unified Access Control (UAC)</b>	2.0 (build 49383)	Proprietary
<b>Steel Belted RADIUS</b>	V6.10.4280	Windows 2003 (SP2)

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
<b>Passcode</b>			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input checked="" type="checkbox"/>
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
<b>Load Balancing / Reliability Testing</b>			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>

Additional Functionality			
<b>RSA Software Token Automation</b>			
System Generated PIN	<input type="checkbox"/>	System Generated PIN	<input type="checkbox"/>
User Defined (8 Digit Numeric)	<input type="checkbox"/>	User Defined (8 Digit Numeric)	<input type="checkbox"/>
User Selectable	<input type="checkbox"/>	User Selectable	<input type="checkbox"/>
Next Tokencode Mode	<input type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/>
<b>RSA SecurID 800 Token Automation</b>			
System Generated PIN	<input type="checkbox"/>	System Generated PIN	<input type="checkbox"/>
User Defined (8 Digit Numeric)	<input type="checkbox"/>	User Defined (8 Digit Numeric)	<input type="checkbox"/>
User Selectable	<input type="checkbox"/>	User Selectable	<input type="checkbox"/>
Next Tokencode Mode	<input type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/>
<b>Credential Functionality</b>			
Determine Cached Credential State	<input type="checkbox"/>	Determine Cached Credential State	<input type="checkbox"/>
Set Credential	<input type="checkbox"/>	Set Credential	<input type="checkbox"/>
Retrieve Credential	<input type="checkbox"/>	Retrieve Credential	<input type="checkbox"/>

CMY

✓ = Pass ✗ = Fail N/A = Non-Available Function

# Certification Checklist For RSA Authentication Manager 7.1

Date Tested: March 27, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003
Juniper Odyssey Client	4.72.10945	Windows XP
Cisco ACS RADIUS	4.2	Windows 2003 (SP2)
Cisco AiroNet Wireless	12.3(7) JA2	Proprietary

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✗
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Deny Numeric PIN	N/A	Deny Numeric PIN	✓
PIN Reuse	N/A	PIN Reuse	✓
<b>Passcode</b>			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Fixed Passcode	N/A	4 Digit Fixed Passcode	✓
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
<b>Load Balancing / Reliability Testing</b>			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓
Additional Functionality			
<b>RSA Software Token Automation</b>			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
<b>RSA SecurID 800 Token Automation</b>			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

CMY

✓ = Pass ✗ = Fail N/A = Non-Available Function



## Known Issues

---

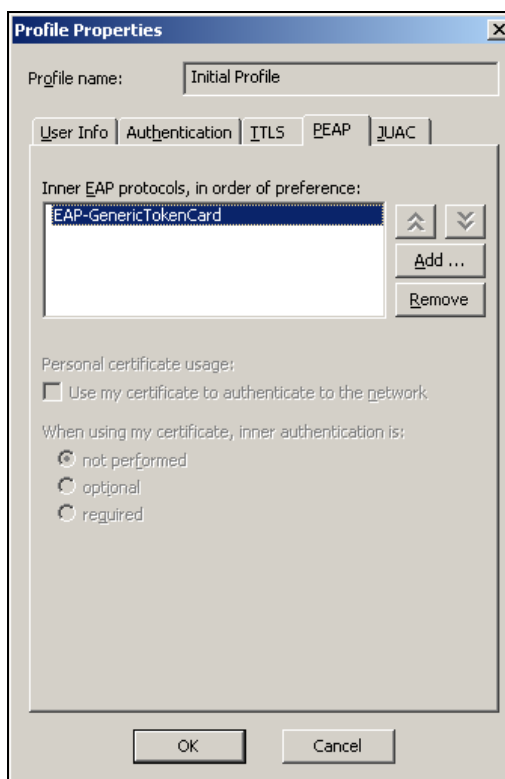
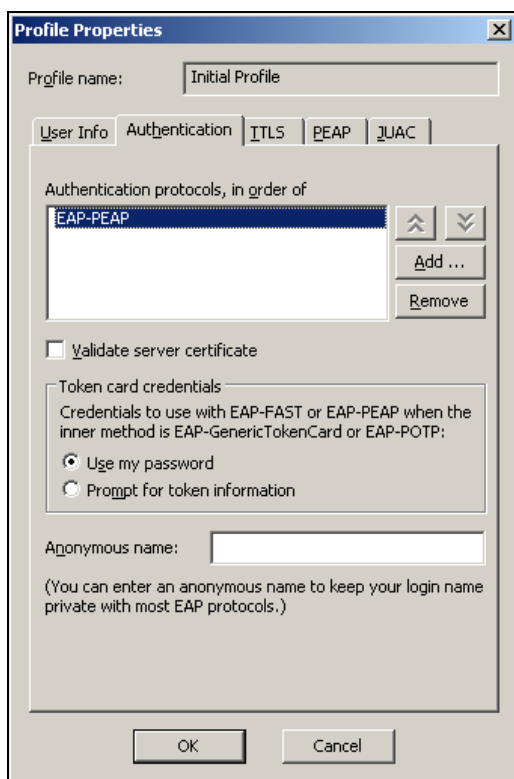
3. When authenticating via the RADIUS protocol and using Cisco ACS RADIUS server as used in the above **Wireless** testing, **Force Authentication after New PIN** does not occur. This is the current behavior of Cisco ACS RADIUS not the Odyssey Client. Cisco has been informed of the matter.

## Appendix

---

### Configuring Odyssey Access Client to use EAP-PEAP for two factor authentication.

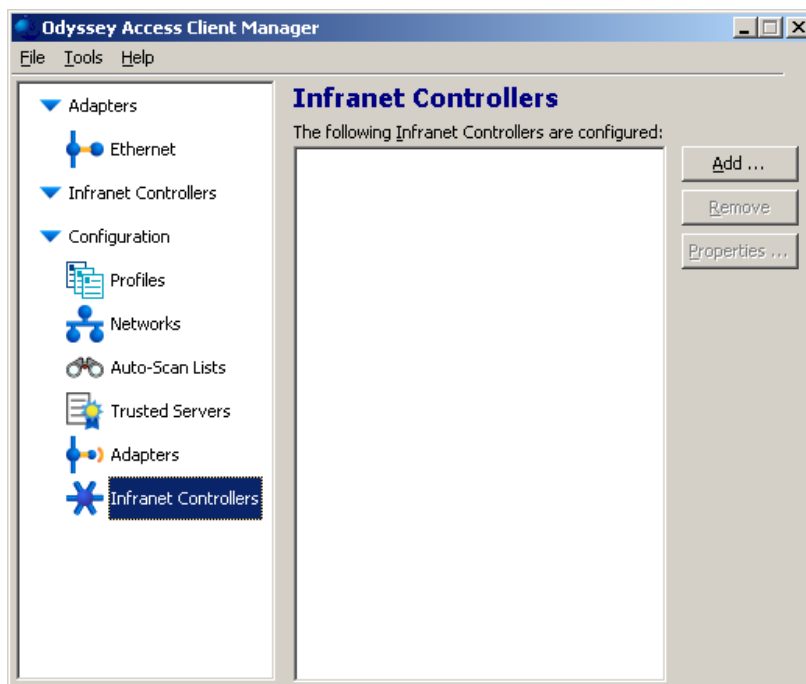
1. Launch the Odyssey Client and click on **Profiles** from the left hand pane.
2. Click on the Properties of the **Profile** being used.
3. Click on the **Authentication Tab** and **Add EAP-PEAP**.
4. Click on the **PEAP Tab** and **Add EAP-GenericTokenCard**.
5. Click OK to Save.



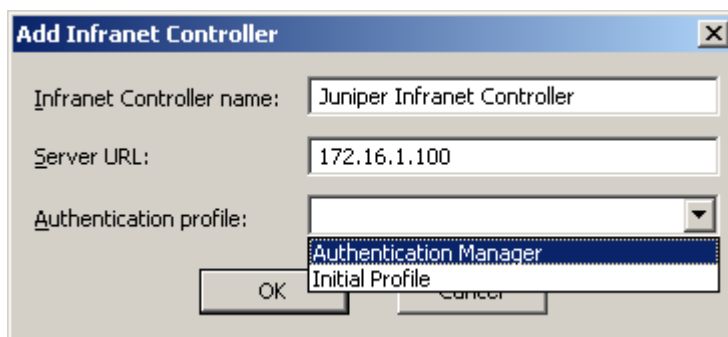


## Configuring the Odyssey Client to connect directly to a Unified Access Control (UAC) server. (non 802.1x authentication)

1. On the left hand pane of the Odyssey Client, select **Infranet Controls**.
2. On the right hand pane, click **Add**.



3. Enter a name and either the IP Address or fully qualified domain name of the Infranet Controller.



4. Select a profile previously configured and click OK.
5. On the Left hand pane, under Infranet Controllers, click on the name created in previous step.
6. On the right hand pane, click in the box Connect to the Infranet Controller.
7. Follow the authentication prompts as instructed.