Avaya Identity Engines Ignition CASE Administration

Avaya Identity Engines Ignition Server
Release 8.0

Document Status: **Standard**
Document Number: **NN47280-603**
Document Version: **01.01**
Date: **April 2012**

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

CASE example

Troubleshooting

Purpose of this document

The *Avaya Identity Engines Ignition CASE Administration* guide explains how to install, configure, and deploy Avaya Identity Engines Ignition Client for Accessing Secure Enterprise (CASE).

This guide also includes an example of how you can deploy CASE in conjunction with an Avaya wireless controller and Avaya Ignition Access Portal to provide a seamless, automated experience for end-users accessing secure wireless networks.

This guide is written for network administrators who need to install, configure, and deploy CASE.

New in this release

This guide is new and all features are new.

Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Introduction

The Avaya Identity Engines Ignition Client for Accessing Secure Enterprise (CASE) feature grants network access to devices and users. CASE automatically verifies and corrects wired and wireless configuration on endpoint machines, automating the client configuration required to enable 802.1x and Microsoft Network Access Protection (NAP).

CASE components

CASE includes:

- CASE Administrative Console (for the network administrator)
- CASE application (for the end-user)

CASE Administrative Console

The CASE Administrative Console is a web-based application. The network administrator uses the CASE Administrative Console to build a configuration that specifies the end user settings for specific network access. This configuration is called a network profile. Network administrators can define multiple network profiles, each with its own configuration and behavior settings. The network administrator then builds CASE deployment packages that contain one or more network profiles and deploys these packages directly to Avaya Identity Engines Ignition Access Portal (Access Portal).

CASE application

The CASE application is an application that guides a user while it applies the settings the network administrator configured for the network access.The first time the end user connects to the network, they are presented with a link to the CASE application (or the CASE application automatically launches). If the end user agrees to the terms and conditions presented by the Enterprise, the CASE application runs and automatically sets up the end user's network configuration.

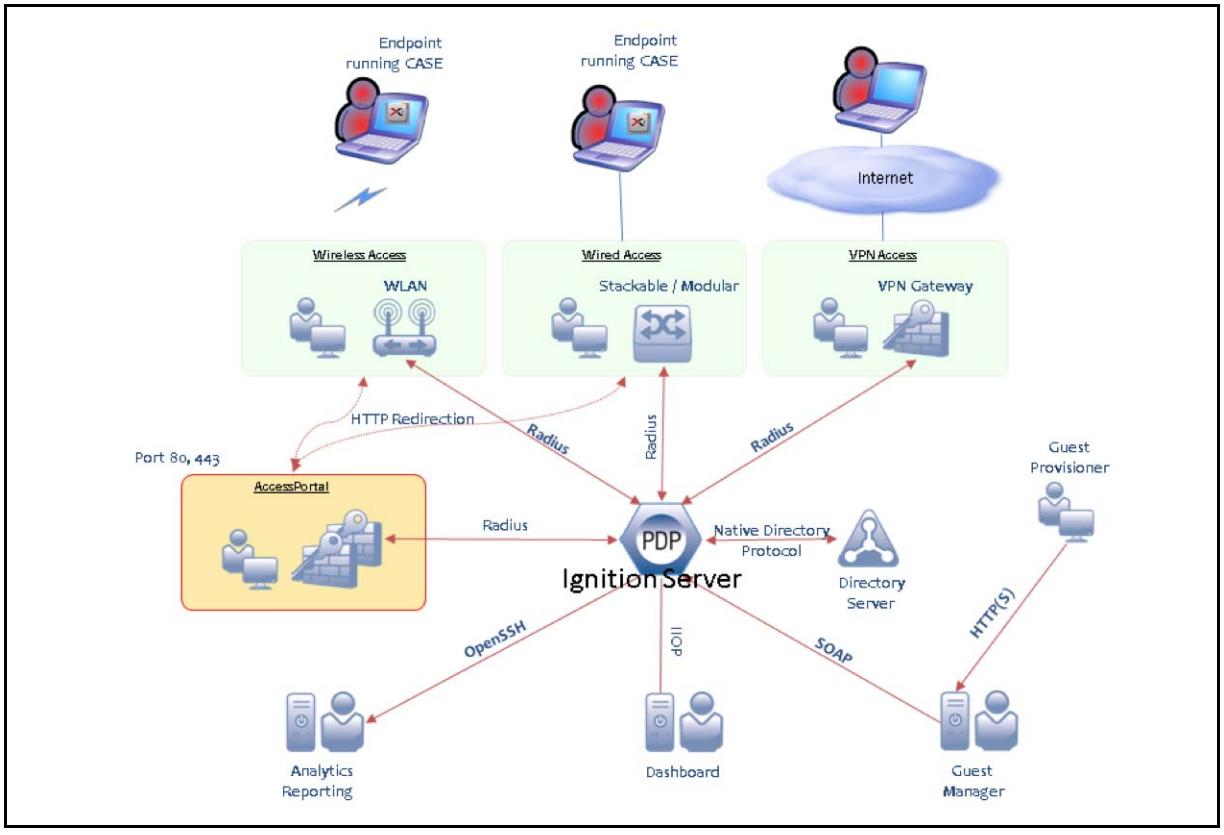
CASE terminology

The following terms are used throughout this document:

- **CASE Administrative Console:** The tool used to create and customize the CASE deployment package.

- **CASE deployment package:** The CASE components, packaged as a web application that you can deploy to Avaya Access Portal. It requires HTML and Java Script.
- **CASE application:** The step-by-step application that guides a user while it configures the network supplicant settings and other client security settings on the user's laptop or desktop computer.
- **CASE network profile:** A CASE network profile is a set of settings that allows a user to connect to a particular defined network. This profile is saved as an XML file and bundled into a CASE package, which in turn applies the settings to the user's computer system. A site can have as many network profiles as it has unique networks to which users may connect. Networks can be grouped into servers.
- **Captive Portal:** A device, usually on an open network, that intercepts a new user's browser traffic and presents a login page. Typically, this login page lets the user authenticate and connect to a secured network. You can deploy the CASE package on a captive portal. Access Portal is a captive portal.

Figure 1 CASE architecture



Installing CASE Administrative Console

Avaya Identity Engines Ignition Client for Accessing Secure Enterprise (CASE) Administrative Console is a web based application similar to Guest Manager that is provided as an installer. You run the installer to deploy the CASE Administrative Console on a tomcat based application server.

This chapter shows you how to install CASE Administrative Console, (and if needed) its required components, Apache Tomcat, and the Sun Java Runtime Environment (JRE). CASE Administrative Console will be installed in your Apache Tomcat installation, in the `webapps` directory.

Note: It is possible to host CASE Administrative Console and Guest Manager on the same Tomcat server.

System requirements

Application server hardware

The application server machine that hosts CASE Administrative Console must meet these minimum hardware requirements:

- Pentium 4, 2.4 GHz or equivalent
- a minimum of 2 GB of RAM

Browser compatibility

The CASE Administrative Console is compatible with the following web browsers:

- Microsoft Internet Explorer, version 6.0 or later, running on Windows.
- Firefox 1.5 or later, running on Windows.

Before you install

To install CASE Administrative Console, you need:

- A PC running Microsoft Windows XP Service Pack 3 (32 bit) or Windows Server 2003 (32 bit and 64 bit) or Windows Server 2008 (32 bit and 64 bit). You will install CASE Administrative Console and its supporting Apache Tomcat server on this PC.

- Administration rights with Windows XP, Windows Server 2003, and Windows Server 2008 enabled. The CASE Administrative Console must be installed by Administrator of the machine.
- The CASE Administrative Console product CD, which contains installers for:
  - Java™ 2 Platform Standard Edition Runtime Environment (JRE) 6,
  - Apache Tomcat 6.0
  - CASE Administrative Console

Running the installer

Follow these steps to install CASE Administrative Console:

1. On the Windows PC that will host CASE Administrative Console, insert the CASE Administrative Console product CD and run the file named **AdminConsoleInstaller-8.0.0<Build Number>.exe**.
2. The installer displays the License Agreement screen. Scroll down to review the entire license agreement. Select the radio button indicating you accept the license agreement, and click **Next**.
3. In the Choose Install Folder screen, specify the directory in which CASE Administrative Console will be installed, and click **Next**.
4. Review the information on the Pre-Installation Summary screen and click **Install**. A Pre install confirmation window appears stating “Confirm Installation. The following tools are necessary for Avaya Admin Console 1.0.0 Java JRE 1.6.0_27 and Apache Tomcat 6.0. These will be selected for installation.”
5. In the Pre install confirmation window, click **OK** to confirm the installation of Java JRE and Apache Tomcat.
6. The installer displays the **Installing** window. If you have the correct version of JRE, a notification appears indicating that JRE is already installed and that the installer will skip the JRE installation. Click **OK** to continue.
7. *If Apache Tomcat is not found on your computer*, the installer displays the **Tomcat Installation** window. If the installer displays this window:
   - Click **OK** to install Tomcat.
   - In the **Choose Components** window, accept the defaults.
   - In the **Choose Install Location** window, use the default or choose your own location.
   - In the **Configuration** window, specify your Tomcat port number, specify a Tomcat administrator account name, and *specify a password*

that is unlikely to be guessed. Make a note of your account name and password.

- In the **Java Virtual Machine** window, accept the default JRE path.
- In the **Completing the Apache Tomcat Setup Wizard** window, tick **Run Apache Tomcat** and untick **Show Readme**, and click **Next**.

8. The Install Complete screen appears with a “Congratulations” message and states that the Admin Console installer has increased Tomcat’s memory allocation limit. Click **Done** to quit the installer. The installation of Tomcat, Java, and CASE Administrative Console is now complete.

Setting up Tomcat to require HTTPS connections

Avaya recommends that you set your Tomcat server to require HTTPS browser connections for all users of the CASE Administrative Console application. This section explains how to do this.

To set Tomcat to require HTTPS connections, perform the steps below.

1. Open Tomcat’s `server.xml` file in a text editor. By default, it should reside in the install directory for Tomcat (`<tomcat_install>\conf\server.xml`).
2. Locate the block of settings associated with port 8443. This is the https configuration block — the second connector entry in the `server.xml` file, which starts with the text `Connector port="8443"`. The block of code looks like this:

```
<!--
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS" />
-->
```

3. Remove the HTML comment tags around the https configuration block in the `server.xml` file. (i.e. Remove the **<!--** at the beginning and remove the **-->** at the end.) When you remove the comment tags you have the following block:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS" />
```

4. In the “Connector” block, add the “keystoreFile” parameter to specify the location of your keystore. You may use the default keystore shipped with CASE Administrative Console or you may use your own keystore. In a typical CASE Administrative Console installation on Windows, the default keystore is saved as `C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\AdminConsole\WEB-INF\ksTomcat`. To use the default keystore, add the following line to the Connector block:

   ```
   keystoreFile="webapps/AdminConsole/WEB-INF/ksTomcat"
   ```

   After you make the addition, the https configuration block in `server.xml` reads:

   ```
   <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
              maxThreads="150" scheme="https" secure="true"
              keystoreFile="webapps/AdminConsole/WEB-INF/ksTomcat"
              clientAuth="false" sslProtocol="TLS" />
   ```

5. Comment out the “Connector” block for port 8080. This prevents users from loading CASE Administrative Console over a cleartext connection.
6. Close and save the `server.xml` file, and restart Tomcat.

Now that you have set up your Tomcat server to require SSL, the default URL for CASE Administrative Console will take the form (assuming an example host name of *pluto*): **https://pluto:8443/AdminConsole/admin** instead of the non-SSL URL (**http://pluto:8080/AdminConsole/admin**).

Launching Tomcat

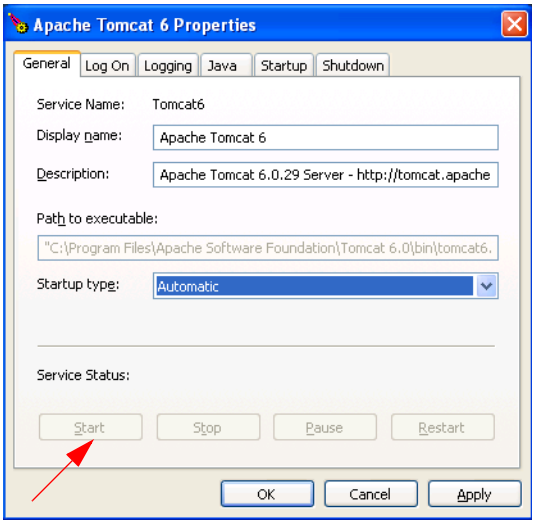
To run CASE Administrative Console:

1. Open the Apache Tomcat Properties window on your PC that hosts CASE Administrative Console. In Windows, click **Start > Programs > Apache Tomcat 6.0 > Configure Tomcat**.

Hint: If the Start menu fails to launch the window, look in the system tray for an icon that looks like the one shown below. Double-click it to open the Properties window.

Tomcat icon in the Windows system tray

Windows displays the Apache Tomcat Properties screen. The **Service Status** field indicates whether the Tomcat Server is running.



2. Click **Start** to start Tomcat; click **OK** to close the Apache Tomcat Properties window.

Launching CASE Administrative Console

In this section you will launch CASE Administrative Console to check that it has been installed correctly.

Connect to the CASE Administrative Console as follows:

1. Open a web browser and point it at the **AdminConsole/admin/** application on your Tomcat server. If you have a default installation of Tomcat running on machine *pluto*, the URL is typically: **https://pluto:8443/AdminConsole/admin/**.

   Note that the URL may be **http://pluto:8080/AdminConsole/admin/** if you are not using a secure port to host **AdminConsole**. Avaya strongly recommends that you set up your Tomcat Server to require SSL connections.

2. Enter the login credentials of the CASE Administrative Console administrator. By default, these are:

   - User ID: **admin**
   - Password: **admin**

   A note on password retention: If your browser asks whether you want it to remember your password, you must choose the option that prevents

the browser from storing passwords for the site. On most browsers, you will choose the option, “Never for this site.” Allowing the browser to retain passwords for the CASE Administrative Console application is not secure, and it may cause your browser to display misleading “password update” messages when you edit users.

3. Click **Login**. The CASE Administrative Console displays the following message on the main CASE Administrative Console screen: “You are successfully signed in as administrator”.

Figure 2 Successfully signed in as Administrator

Important!

When using the CASE Administrative Console, do not use your browser’s Refresh command to update a page. Instead, click on the left side of the window to reload the page.

Deploying CASE

This chapter describes Avaya Identity Engines Ignition Client for Accessing Secure Enterprise (CASE) deployment, basic CASE configuration, and CASE verification tasks. This chapter assumes you are familiar with web site creation and deployment, and have experience setting up and maintaining networks and network security.

Before you begin

To create CASE network profiles using the CASE Administrative Console, you need the information and items described in the following sections.

Planning your deployment

The following is a summary of the process to get up and running with CASE.

Determine what kinds of SSIDs exist on your wireless network

Is there a single, secure service set identifier (SSID) for everyone, or are there multiple SSIDs? If there are multiple SSIDs, you can define the SSIDs as different (physical) networks within CASE, and you can deploy them in separate profiles to direct each user to the appropriate SSID.

Determine how user authentication will be handled

Are the requirements the same for everyone, or do they differ from one group to another? If groups have different needs, you can define each group as a different profile, so that each group gets its own CASE network profile that makes settings appropriate for that group only.

Decide how your users will run CASE

CASE deployment is only supported as a web application. If you deploy the CASE package to a web server, you must provide a way for users to access the web server. Typically, the user connects an open SSID on a wireless access point or plugs into a network jack that places the user in a default VLAN. When the user opens a web browser, the user views the CASE link in one of the following ways:

- **Automatically**: A captive portal (for example, the Ignition Access Portal) redirects the user to the CASE link; or
- **Manually**: The user types a published URL to view the CASE link.

Network environment requirements

To deploy CASE, you will need the following:

- At least one of the following edge devices:
  - A switch capable of guest/default VLAN
  - An access point capable of multiple SSIDs
- A configured web server, such as Apache Tomcat or Microsoft IIS. For the best end-user experience, use the Avaya Ignition Access Portal.
- A configured Ignition Server providing RADIUS authentication.
- A network configuration in which the guest/default VLAN has access to the web server that hosts the CASE deployment package.
- For testing, you will need a laptop (running Windows XP SP3 or later) with wired and wireless NICs.

Once the network is configured, Avaya recommends that you walk through the process manually to verify that the configuration is correct. Before you start creating your network profiles, use your wireless-equipped laptop to run the following tests:

1. Connect to the open SSID or guest VLAN. Verify that the laptop receives an IP address from DHCP.
2. Manually configure secure SSID and 802.1X supplicant settings.
3. Connect to the secure SSID. Verify that authentication is successful. Verify that the laptop receives an IP address from DHCP.

CASE configuration information requirements

Collect the following information before you start creating CASE Profiles:

- IP address of Access Portal that will host the CASE deployment package: _____
- Subnet of guest VLAN: _____
- Subnet of authenticated VLAN: _____

For 802.1X environments, you need the following additional information:

- Valid user name and password in RADIUS: _____ / _____
- RADIUS server certificate type: ___ self-signed ___ commercially signed
- EAP Type: ___ PEAP ___ TTLS

For wireless environments, you need the following additional information:

- Open SSID: _____
- Secure (802.1X or PSK) SSID: _____
- Network Authentication: ___ WPA ___ WPA-PSK
- Network key for WPA-PSK environments: _____
- Data Encryption: ___ AES ___ TKIP

Getting started with CASE Administrative Console

Ensure that the CASE Administrative Console application is installed. See "Installing CASE Administrative Console" on page 13. After you log in on the CASE Administrative Console web site, you can create network profiles and deployment packages.

Network profiles

Network administrators can define multiple network profiles, each with its own configuration and behavior settings. For example, the computer system of an end-user attempting to access an employee network might be configured differently than if the same user were attempting to access a guest network. In this scenario, the administrator would generate two different network profiles: one for the employee network and one for the guest network. Administrators can package these distinct profiles as one or several different CASE packages.

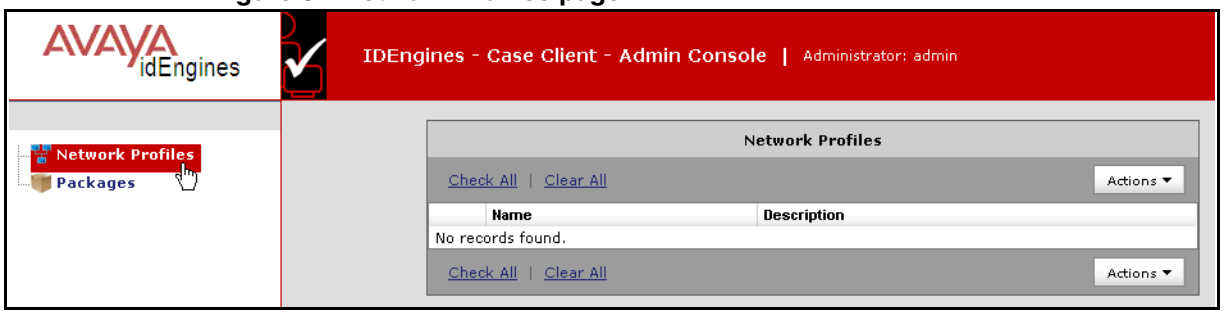
Creating a network profile

The CASE Administrative Console has a wizard-like interface that guides the administrator through the various steps to create a network profile.

To create a network profile:

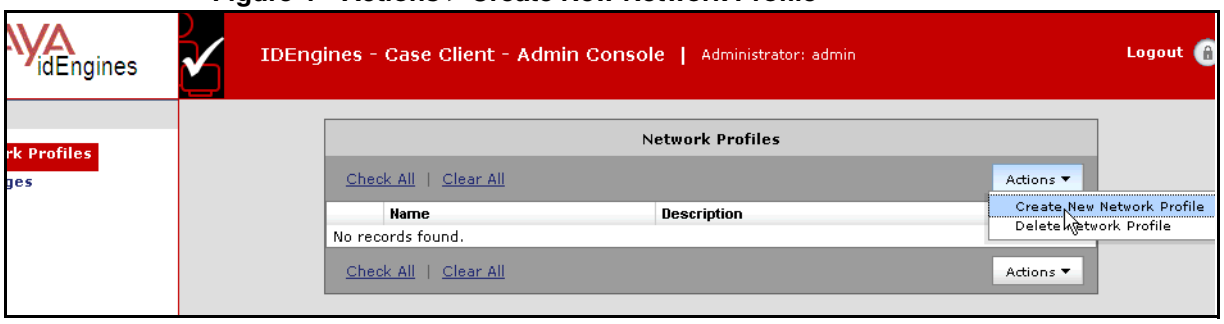
1. In the CASE Administrative Console navigation pane, click **Network Profiles**. The CASE Administrative Console displays the **Network Profiles** page.

Figure 3 Network Profiles page



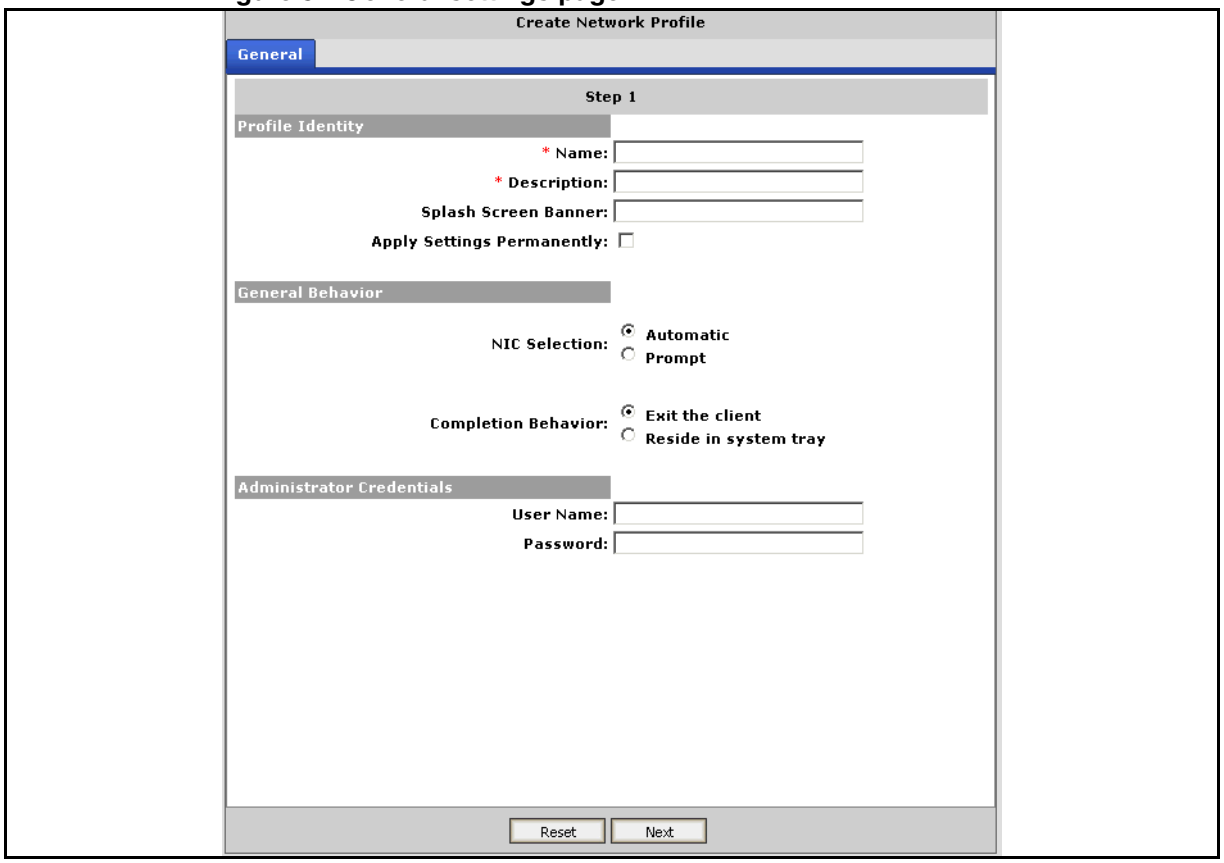
2. From the **Actions** drop-down list, click **Create New Network Profile**.

Figure 4 Actions > Create New Network Profile



The CASE Administrative Console displays the **General** settings page.

Figure 5 General settings page

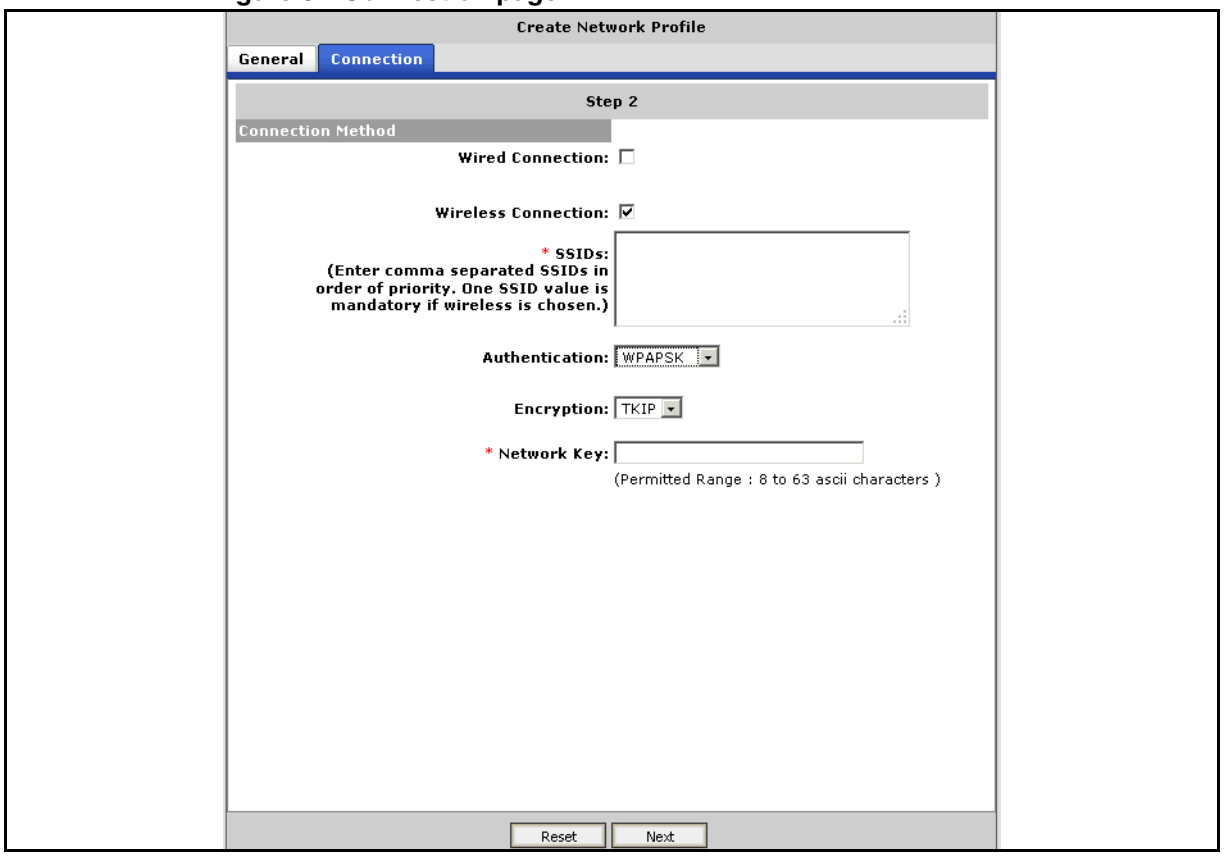


3. In the **Profile Identity** section:
   - In the **Name** field, enter a name for the network profile.
   - In the **Description** field, enter a description for the network profile.
   - In the **Splash Screen Banner** field, enter the text to display in the splash screen banner.
   - If you want the settings to be permanent, select the **Apply Settings Permanently** check box.

4. In the **General Behavior** section:
   - Use the **NIC Selection** radio buttons to select the NIC selection type. Select **Automatic** to enable automatic NIC selection or **Prompt** to prompt the user to select a NIC.
   - Use the **Completion Behavior** radio buttons to define how you want the CASE application to behave when the user joins the network. Select **Exit the client** if you want CASE to perform the network configuration and exit itself or **Reside in system tray** to have the CASE application perform the network configuration and remain alive in the system tray for additional options like revert settings.
5. In the **Administrator Credentials** section:
   - In the **User Name** field, enter an administrator name.
   - In the **Password** field, enter an administrator password.

     Note: The Administrator Credentials are only used on Windows XP SP3. On Vista and Windows 7, the administrative rights are handled by Windows User Access Control.
6. Click **Next**. The CASE Administrative Console displays the **Connection** page.

Figure 6 Connection page



7. In the **Connection Method**, section, select the **Wired Connection** check box to enable wired access or the **Wireless Connection** check box to enable wireless access. You can enable wired and wireless access on the same network profile. If you select **Wireless**, the CASE Administrative Console displays the wireless configuration fields:

   - In the **SSID field**, enter comma separated SSIDs in order of priority. One SSID value is mandatory if wireless is chosen.
   - From the **Authentication** drop-down list, select the Authentication type. The options are: Open, Shared, WPA, WPAPSK, WPA2, or WPA2PSK.
   - From the **Encryption** drop-down list, select the Encryption type. For Open and shared authentication, select **None** or **WEP**. For WPA, WPAPSK, WPA2, or WPA2PSK authentication, select **TKIP** or **AES**.
   - In the **Network Key** field, enter the network key. The CASE Administrative Console only displays the **Network Key** field if you select WPAPSK, WPA2PSK, or open or shared authentication with WEP encryption. The permitted range is 8 to 63 ascii characters.

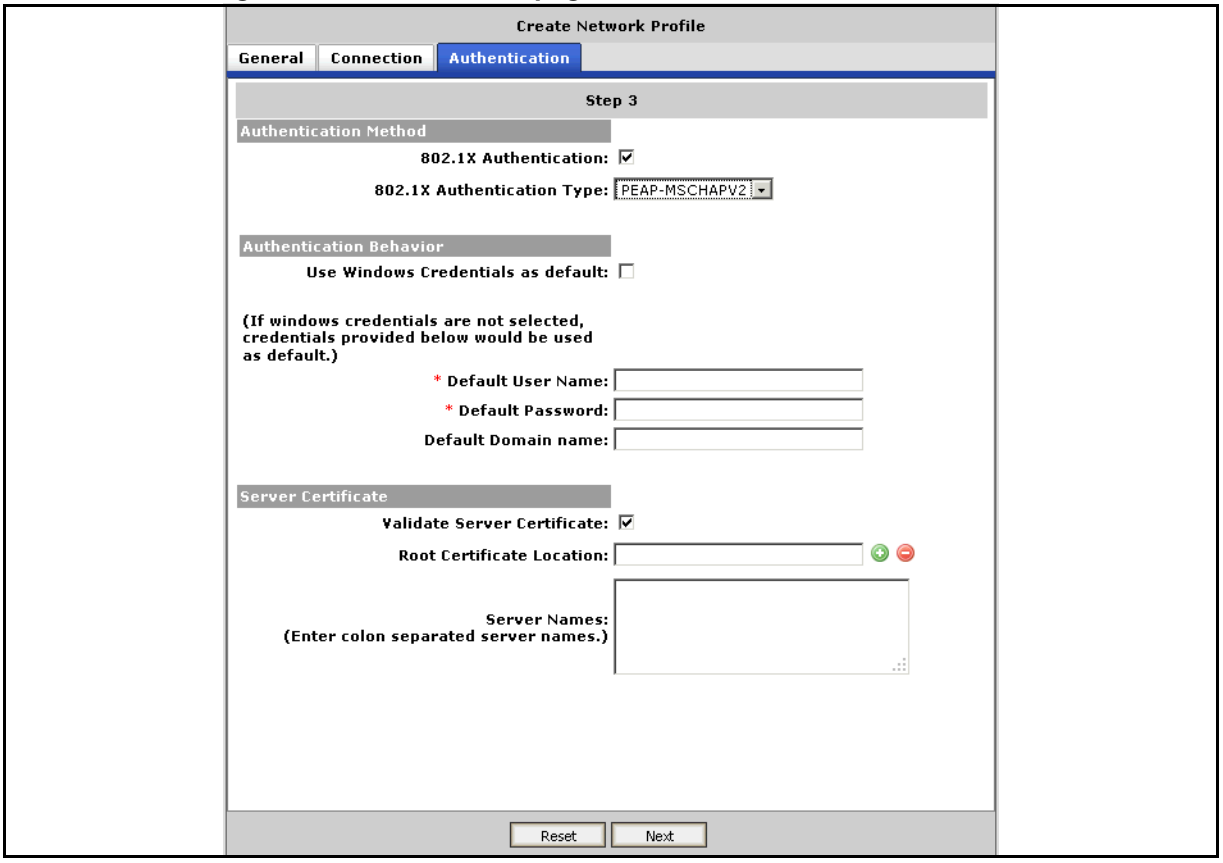
     Note: You can construct a network profile with the following Connection Method settings:

     - Wired
     - Wireless
     - Wired OR Wireless

     If you construct a network profile that is for both wired and wireless, the CASE applies the settings when the user accesses the network using either a wired or wireless interface. CASE **will not** apply the settings to both of the interfaces. If the profile requires auto NIC selection, then CASE selects the interface that can reach portal. This interface could be wired or wireless.

8. Click **Next**. The CASE Administrative Console displays the **Authentication** page.

Figure 7 Authentication page



9. In the **Authentication Method** section, select the **802.1X Authentication** check box to require the user to authenticate using 802.1X or click **Next** to skip 802.1X configuration. If you select **802.1X Authentication**, the CASE Administrative Console displays the **802.1X Authenticating** configuration fields.

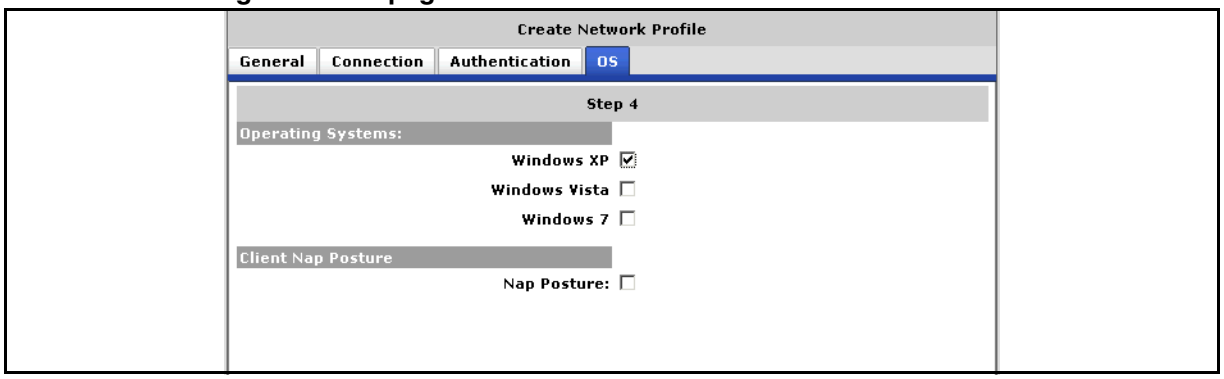
   - From the **802.1X Authentication Type** drop-down list, select the 802.1X authentication type. The options are: PEAP-MSCHAPV2, EAP-TLS, or PEAP-TLS. If you select MSCHAPV2, the CASE Administrative Console displays the **Authentication Behavior** section.
   - In the **Authentication Behavior** section, select the **Use Windows Credentials as default** check box to use Windows Credentials as default to authenticate, or use the **Default User Name**, **Default Password**, and **Default Domain name fields** to enter the user credentials.
   - In the **Server Certificate** section, select the **Validate Server Certificate** check box if you want to validate the server certificate. Click on the (**+**) sign beside the **Root Certificate Location** field, click **Browse** to navigate to your Root Certificate File and click **Submit**. In

the **Server Names** field, enter the **Server Names** separated by a colon. If you select the **Validate Server Certificate** check box, the supplicant can only authenticate to a server that provides a certificate signed by a trusted certificate authority. If you do not select the **Validate Server Certificate** check box, the supplicant can authenticate to any server.

- In the **User Certificate** section, click on the (**+**) sign beside the **User Certificate Location** field, click **Browse** to navigate to your User Certificate File and click **Submit**. Enter the certificate password in the **Password** field. The CASE Administrative Console only displays the **User Certificate** section if you select EAP-TLS or PEAP-TLS as the 802.1X Authentication Type.

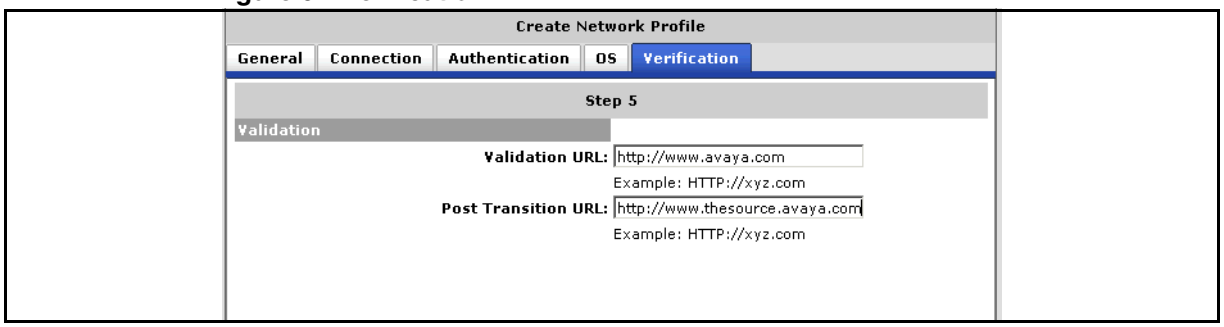
10. Click **Next**. The CASE Administrative Console displays the **OS** page.

Figure 8 OS page



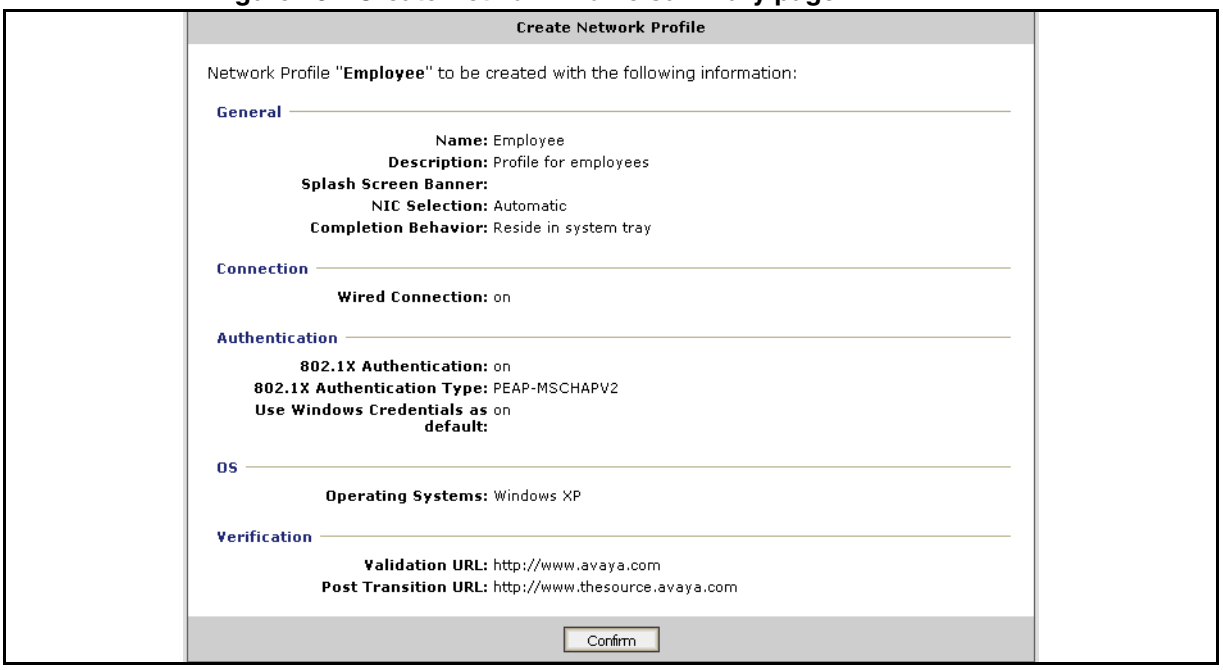
11. In the **Operating Systems** section, select the operating systems that apply to this network profile. The supported operating systems are: **Windows XP**, **Windows Vista**, and **Windows 7**.
12. In the **Client Nap Posture** section, select the **NAP Posture** check box to enable NAP for each supported OS. Clear the check box to disable NAP for each supported OS.
13. Click **Next**. The CASE Administrative Console displays the **Verification** page.

Figure 9 Verification



14. (Optional) In the **Validation** section:
    - In the **Validation URL** field, enter the URL the CASE application uses to verify connectivity after 802.1X configuration completes. The CASE application uses this URL in an internal process to validate network connectivity. This process begins with the verification that an IP address is received and then the verification of reachability to the configured validation URL.
    - In the **Post Transition URL** field, enter the URL that launches after 802.1X configuration completes. A web page launches after the user moves to the secure network. As an example, you can use this process for the Web-based authentication that may be required after the user moves the secure network. As an additional example, you can use this process to provide instructions to new employees as part of the on-boarding process.
15. Click **Next**. The CASE Administrative Console displays the **Create Network Profile** summary page.

Figure 10 Create Network Profile summary page



16. Review the settings and click **Confirm**. The CASE Administrative Console displays the new network profile in the Network Profiles list.

Figure 11 Successfully Created Network Profile

Editing a network profile

To edit a network profile:

1. In the CASE Administrative Console navigation pane, click **Network Profiles**. The CASE Administrative Console displays the list of network profiles.
2. Click on the name of the network profile you want to edit. The CASE Administrative Console displays the **General** page.
3. Make the required changes.
4. To make changes on another screen, click on another tab. You can edit any tab in any order. **Note**: Do not click Next to go to the next screen, as this submits the network profile.
5. After you have finished editing the network profile, click **Next** to submit the changes.

Deleting network profiles

The delete action allows you to delete one or more network profile entries at a time.

To delete network profiles:

1. In the CASE Administrative Console navigation pane, click **Network Profiles**. The CASE Administrative Console displays the list of network profiles.
2. Select the check boxes beside the network profiles you want to delete.
3. From the **Actions** drop-down list, click **Delete Network Profile**. The CASE Administrative Console displays the following message: “Are you sure you want to delete the selected Profiles?”.
4. Click **OK**.

Deployment packages

After you create the network profiles, you can create a deployment package. A deployment package can contain one or more network profiles. Any network profile can be part of zero or more deployment packages.

Creating a deployment package

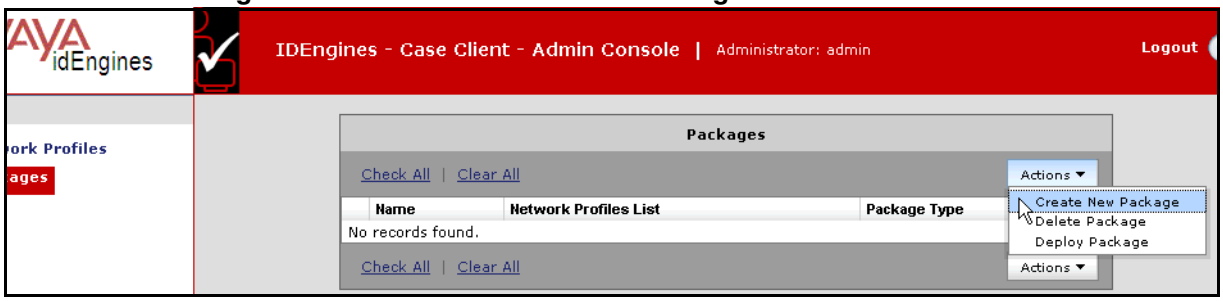
To create a deployment package:

1. In the CASE Administrative Console navigation pane, click **Packages**. The CASE Administrative Console displays the **Packages** page.

Figure 12 Packages page

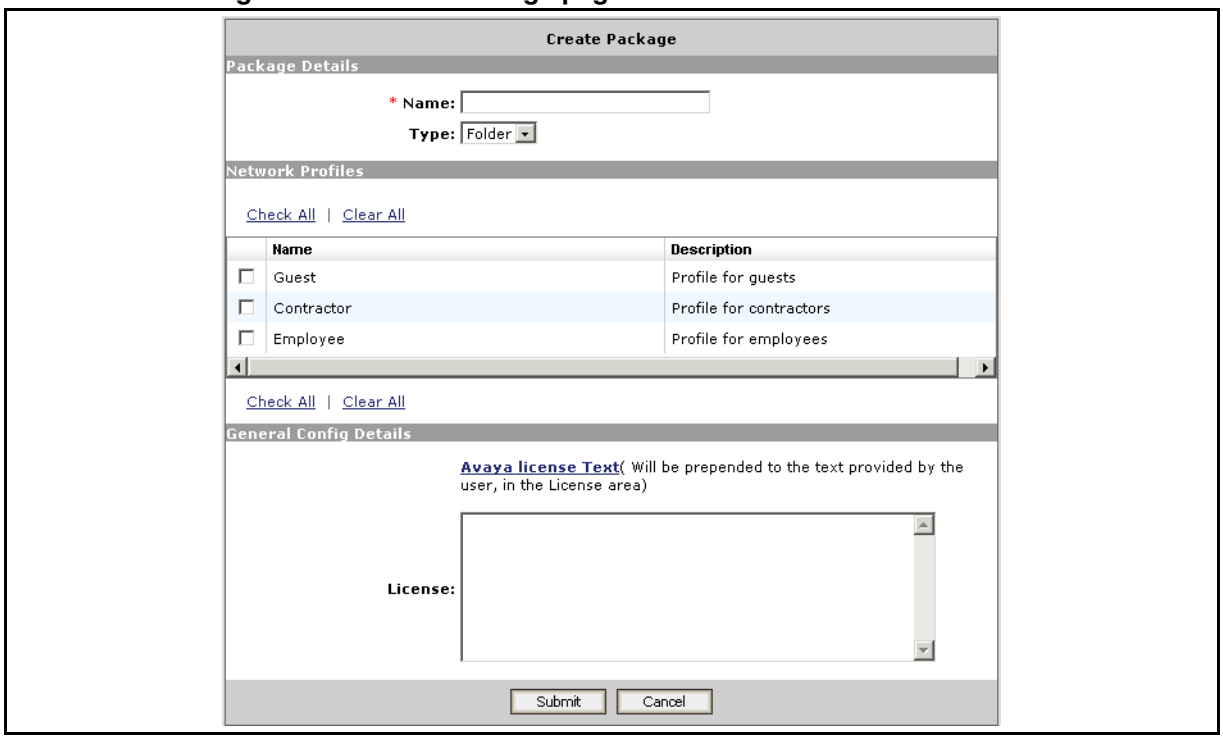
2. From the **Actions** drop-down list, click **Create New Package**.

Figure 13 Actions > Create New Package



The CASE Administrative Console displays the **Create Package** page.

Figure 14 Create Package page



3. In the **Package Details** section:

- In the **Name** field, enter a name for the package.
- From the **Type** drop-down list, select the package file type. The options are: **Folder**, **Zip**, or **Tar**. Choose **Folder** if you want to deploy the package to Access Portal.

4. In the **Network Profiles section**, select the check boxes beside network profiles you want to include in the package.
5. In the **General Config Details** section, in the **License** field, enter License text for the CASE application to display to the user before the CASE application starts.
6. Click **Submit**. The CASE Administrative Console displays the new deployment package in the Packages list.

Deleting deployment packages

The delete action allows you to delete one or more deployment package entries at a time.

To delete deployment packages:

1. In the CASE Administrative Console navigation pane, click **Packages**. The CASE Administrative Console displays the list of packages.
2. Select the check boxes beside the packages you want to delete.
3. From the **Actions** drop-down list, click **Delete Package**. The CASE Administrative Console displays the following message: “Are you sure you want to delete the selected Packages?”.
4. Click **OK**.

Deploying packages

You can only deploy a package directly to Access Portal if the package type is **Folder**.

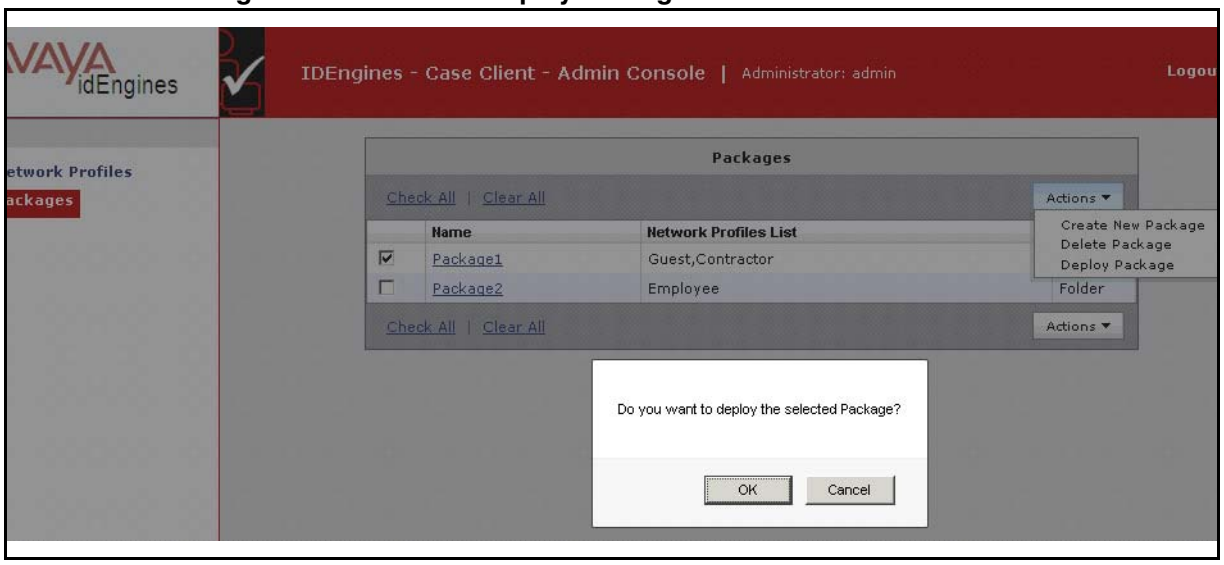
To deploy a package:

1. In the CASE Administrative Console navigation pane, click **Packages**.
2. Select the check boxes beside the packages you want to deploy.

Figure 15 Select packages to deploy

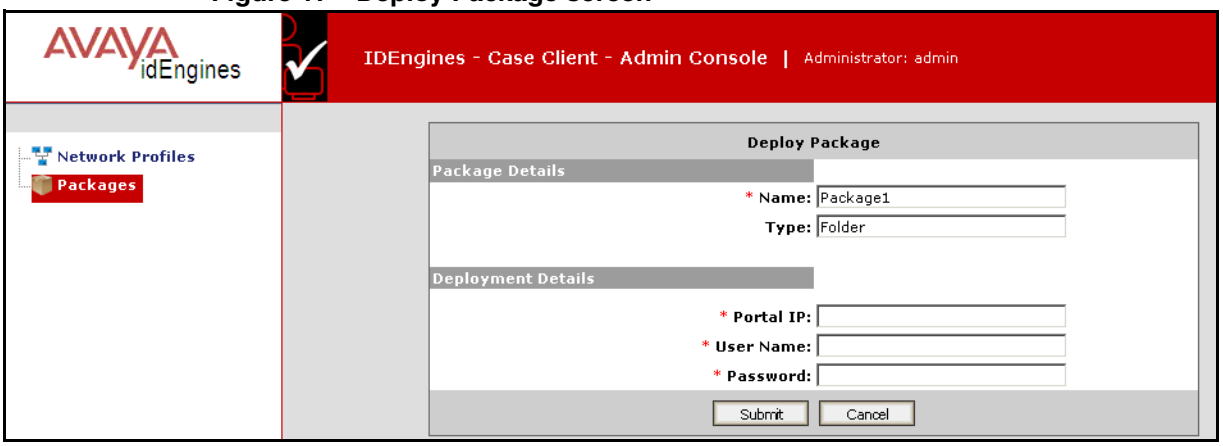
3. From the **Actions** drop-down list, click **Deploy Package**. The CASE Administrative Console displays the following message: “Do you want to deploy the selected Package?”.

Figure 16 Actions > Deploy Package



4. Click **OK**. The CASE Administrative Console displays the Deploy Package screen.

Figure 17 Deploy Package screen



5. In the **Package Details** section, confirm that the package **Name** and **Type** are correct. **Note**: The **Type** field must be **Folder** if you want to deploy the package to Access Portal.
6. In the **Deployment Details** section:
   - In the **Portal IP** field, enter the IP address of the Access Portal.
   - In the **User Name** field, enter a user name.
   - In the **Password** field, enter a user password.
7. Click **Submit**.

Lab testing

Network users access CASE through their browser using an open SSID or a guest VLAN. The CASE application automatically fixes the system's configuration, reconnects to the secure network, and guides the user through the authentication process. After authentication, the CASE application verifies network connectivity and connects the user to the network.

If you have a wired environment, follow the steps in "Wired usage" on page 33. If you have a wireless environment, follow the steps in "Wireless usage" on page 34.

Wired usage

This procedure assumes you have deployed the CASE package on Ignition Access Portal. To demonstrate CASE in a wired scenario, use your laptop and follow these steps:

1. Ensure that 802.1X is disabled on the laptop's supplicant.
2. Use an Ethernet cable to connect the laptop to an end-user port on the switch.
3. Wait for the guest VLAN to be assigned. Verify that the laptop receives an IP address on the guest VLAN.

4. Open the browser and query the wizard-specific URL on the web server. A web login page displays.
5. Click the **Click here to apply CASE Security Profile** link, and follow the CASE flow.
6. Under certain conditions, you may be prompted to select your network connection. If so, select the appropriate wired interface and click **OK**.
   a. CASE begins analyzing your laptop, applying its configuration, and reconnecting to the network.
   b. In 802.1X environments, the Windows supplicant may prompt you to authenticate.
   c. Next, CASE waits to receive an IP address.
7. The final taskbar notification **OR** a message dialog appears, confirming that you are connected to the secure network.
   a. After CASE applies the settings, CASE minimizes into the System Tray.
   b. To revert your system to its original state, right click on the CASE icon in System Tray and click on the **Revert** menu item.

Wireless usage

This procedure assumes you have an open (unsecured) SSID and that the CASE deployment package is on a web server visible from that open SSID. To demonstrate CASE in a wireless scenario, use your laptop and follow these steps:

1. Ensure that the laptop does not have a profile for the secure SSID.
2. Connect the laptop to the open SSID.
3. Verify that the laptop receives an IP address on the open SSID.
4. Open the browser and query the wizard-specific URL on the web server. A web login page displays.
5. Click the **Click here to apply CASE Security Profile** link, and follow the CASE flow.
6. Under certain conditions, you may be prompted to select your network connection. If so, select the appropriate wired interface and click **OK**.
   a. CASE will begin analyzing your laptop, applying its configuration, and reconnecting to the network.
   b. In 802.1X environments, the Windows supplicant may prompt you to authenticate.
   c. Next, CASE waits to receive an IP address.

7. The final taskbar notification **OR** a message dialog appears, confirming that you are connected to the secure network.
   a. After CASE applies the settings, CASE minimizes into the System Tray.
   b. To revert your system to its original state, right click on the CASE icon in System Tray and click on the **Revert** menu item.

CASE example

This chapter shows you how to deploy an Avaya Identity Engines Ignition Client for Accessing Secure Enterprise (CASE) package that helps users connect to a network in which users must connect via an Avaya wireless controller. This chapter describes the intentions for deploying the network, the hardware involved, the required configurations, and the end-user experience.

Overview of the CASE example

You can deploy CASE in conjunction with an Avaya wireless controller and Avaya Ignition Access Portal to provide a seamless, automated experience for end-users accessing secure wireless networks. The Avaya Access Portal web-hijack mechanism and customized web-login pages provide a fluid mechanism to deliver the CASE package to the end-user. The end-user experience begins when the user accesses an open SSID. The Avaya Access Portal limits the end-user's network traffic and, as soon as the user attempts to load any web page (generates any HTTP traffic), Avaya Access Portal provides the end-user with a modified web-login page. On the modified web-login page, the web-login fields are hidden. The modified web-login page provides the user with a link to a CASE package, which automatically configures the end-user for access to an 802.1X-based or pre-shared key-based SSID and transitions the user to the secure network.

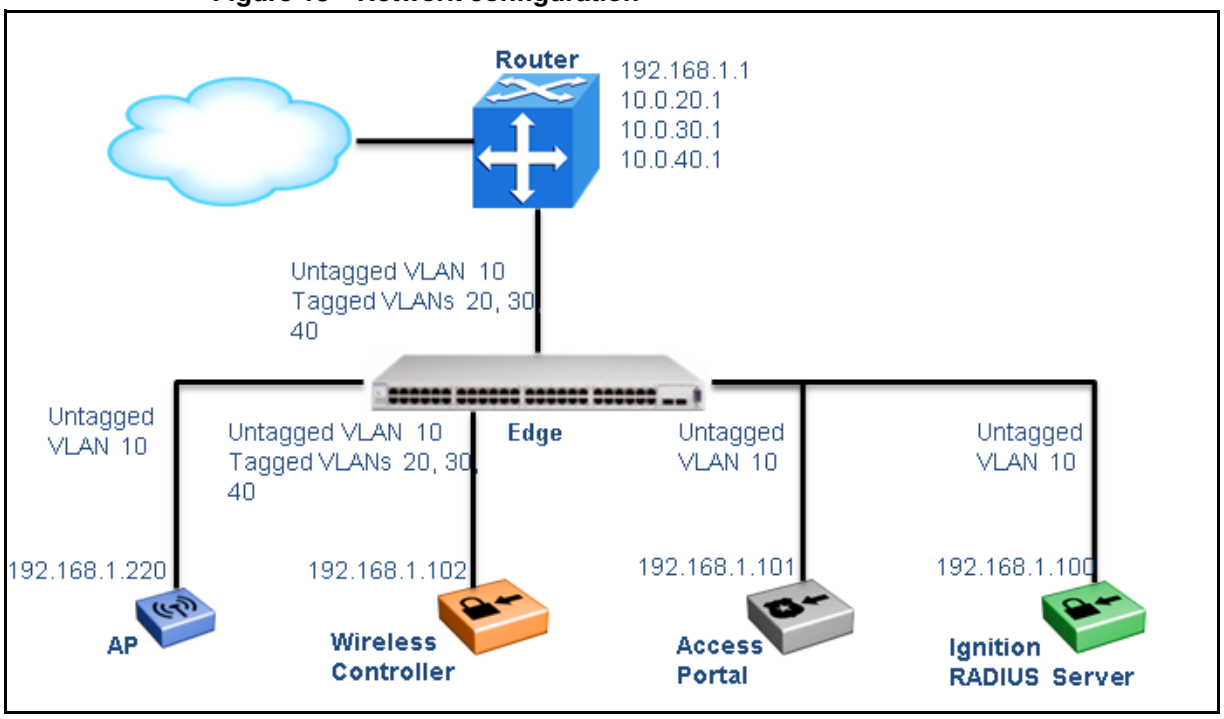
Background

In this example, see “Network configuration” on page 38, the network is divided into three logical networks: an open network, a secure guest network, and a contractor network.

The hardware in the environment includes the following:

- Router (Avaya ERS 8600)
- Avaya ERS 5500 switch
- Avaya Wireless Controller 8100
- Avaya Access Point
- Identity Engines Ignition (RADIUS) server
- Ignition Access Portal (web server)

Figure 18 Network configuration



The first logical network is an **open network**. This network acts as the entry-point for unconfigured end-users. It is available only from wireless connections, using the wireless SSID “open@enterprise.com”, an open, broadcast SSID. It is an Internet-only network and requires web-based login. It does not enforce any application-specific settings, such as firewall. However, the web-hijack mechanism on this SSID encourages end-users accessing this network to use one of the secure networks. This network is on the 10.0.20/24 network.

The second logical network is the **secure guest network**. It is available only from wireless connections and uses the wireless SSID “guest@enterprise.com”, a broadcast SSID. It uses WPA-PSK (pre-shared keys) with TKIP. Authentication uses the web-login capabilities of the Access Portal. Using existing VLANs, it provides Internet-only access. This network is on the 10.0.30/24 network.

The third logical network is the **contractor network**. It is available from wireless connections using the SSID, “contractor@enterprise.com”, an 802.1X, non-broadcast SSID. It uses WPA and TKIP. Authentication uses PEAP/MSCHAPv2. Using existing VLANs, it provides internal and external access. This network is on the 10.0.40/24 network.

Configuring the Ignition (RADIUS) server

The RADIUS server is an Identity Engines Ignition Server installation with Ignition RADIUS installed. The RADIUS server authenticates users joining the contractor network. It resides at 192.168.1.101 and has a RADIUS authentication port of 1812. It is configured to allow PEAP/MSCHAPv2 and TTLS authentications. Several user accounts were created and stored locally. The entire 192.168.1/24 network is defined as a NAS client with the shared secret “test.”

Configuring the Ignition Access Portal (web server)

The web server is an Ignition Access Portal installation. The portal hosts the CASE deployment package. It resides at 192.168.1.100. The portal captures the HTTP traffic and redirects the user to login page on port 8000 and 8001.

To support the web-based login, we need to create a user account on the Access Portal. Under the Local User Manager tab, add a user with the name “user1” and the password “user1”.

Configuring the Avaya wireless controller

Interfaces

When an end-user accesses one of the SSIDs, their traffic needs to be sent out through an interface on the controller. We need to create an interface for each of the SSIDs. In doing so, we will use multiple VLANs, but only the first physical port.

Table 1 Interface configuration

	Interface 1	Interface 2	Interface 3
Interface Name	10.0.20/24	10.0.30/24	10.0.40/24
VLAN Identifier	20	30	40
VLAN Name	open	guest	contractor
Port Number	1	1	1

RADIUS authentication services

We need to define the RADIUS server that the wireless controller will use for authentication. To do so, we will create a new RADIUS server. Use the following CLI commands:

Wireless-Controller-8100(config-security)#radius profile test type auth
Wireless-Controller-8100(config-security)#radius server 192.168.1.100 test
Wireless-Controller-8100(config-security)#radius server 192.168.1.100 test secret

Configure the RADIUS server according to the following table.

Table 2 RADIUS configuration

	Server Settings
Server Address	192.168.1.100
Shared Secret	test
Port Number	1812
Profiles	test

SSIDs

Next, we need to configure our SSIDs. We will create three SSIDs to support our desired environment. Add the following three SSIDs:

SSID1

open@enterprise.com

```
WC8180(config-wireless)#network-profile 1
WC8180(config-network-profile)#profile-name Open
WC8180(config-network-profile)#ssid open@enterprise.com
WC8180(config-network-profile)#mobility-vlan open
```

SSID2

guest@enterprise.com

```
WC8180(config-wireless)#network-profile 2
WC8180(config-network-profile)#profile-name Secure-Guest
WC8180(config-network-profile)#ssid guest@enterprise.com
WC8180(config-network-profile)#security-mode wpa-personal
WC8180(config-network-profile)#wpa2 versions-supported wpa2-and-wpa
WC8180(config-network-profile)#wpa2 key test1234
WC8180(config-network-profile)#mobility-vlan guest
```

SSID3

contractor@enterprise.com

```
WC8180(config-wireless)#network-profile 3
WC8180(config-network-profile)#profile-name Contractor
WC8180(config-network-profile)#ssid contractor@enterprise.com
WC8180(config-network-profile)#security-mode wpa-enterprise
WC8180(config-network-profile)#radius authentication-profile test
WC8180(config-network-profile)#wpa2 versions-supported wpa2-and-wpa
WC8180(config-network-profile)#wpa2 cipher-suite ccmp-and-tkip
WC8180(config-network-profile)#mobility-vlan contractor
```

Table 3 SSID configuration

	SSID 1	SSID 2	SSID 3
Name	Open	Secure Guest	Contractor
WLAN SSID	open@enterprise.com	guest@enterprise.com	contractor@enterprise.com
Broadcast SSID	Yes	Yes	No
Interface Name	10.0.20/24	10.0.30/24	10.0.40/24
Layer 2 Security	N/A	WPA+WPA2	WPA+WPA2
RADIUS Server	N/A	N/A	192.168.1.100
WPA2 Policy	N/A	N/A	AES, TKIP
Auth Key Mgmt	N/A	PSK	802.1X
PSK Format	N/A	ASCII	N/A

In this example, SSID 3 is set up for 802.1X. Because 802.1X is wireless encryption and authentication in one, once the end-user is on the 802.1X network, the connection is both encrypted and authenticated.

SSID 2, however, is set up for PSK. PSK is wireless encryption only, so once the end-user is on the PSK network, the connection is merely encrypted. If the network is to enforce authentication, it must be done using an additional mechanism. In this example, the Secure Guest network uses PSK for encryption and then uses the web-login capabilities of the Access Portal for authentication.

Creating CASE packages

After you have performed the steps above, the network is functional and secure, but, as with any secure network, users may have a difficult time connecting to it for the first time. In the section below, we make the network usable and supportable by creating a CASE Profile that guides users through their initial connection to the secure network.

To begin

Log in to the CASE Administrative Console.

In the CASE Administrative Console navigation pane, click **Network Profiles**. The CASE Administrative Console displays the Network Profiles page. If you want to simplify the view in the Administrative Console, you may want to take a moment now to delete any existing profiles you no longer need. Select the check box in front of the name of each network profile you want to delete and from the Actions drop-down list, click **Delete Network Profile**.

For this example, we will define two secure network profiles: “guest” and “contractor”.

Creating a secure guest network profile (guest@enterprise.com)

To create a secure guest network profile:

1. In the CASE Administrative Console navigation pane, click **Network Profiles**.
2. From the **Actions** drop-down list, click **Create New Network Profile**.
3. In the **Name** field, enter “guest”.
4. In the **Description** field, enter “Secure Guest Network”.
5. In the **Splash Screen Banner** field, enter “Security Settings for Guests”.
6. Leave the **Apply Settings Permanently** check box clear.
7. Leave the **NIC Selection** at the default setting of **Automatic**. With Automatic NIC selection, Access Portal automatically selects the network interface on which the security settings will be applied.
8. In the **Completion Behavior** section, select the **Reside in system tray** radio button.
9. Click **Next** to move to the Connection settings.
10. In the **Connection Method section**, clear the **Wired Connection** check box and select the **Wireless Connection** check box.
11. Under the **Wireless Connection** section, in the **SSIDs** text field, enter “guest@enterprise”.
12. From the **Authentication** drop-down list, select **WPAPSK**.
13. From the **Encryption** drop-down list, select **TKIP**.
14. In the **Network Key** field, enter “secureguest”.
15. Click **Next** to move to the Authentication settings.
16. In this case there are no required 802.1X settings. Click **Next** to move to Operating Systems selection.
17. In the **Operating Systems** section, select the check boxes for all of the operating systems and click **Next**.
18. (Optional) In the **Validation** section:
    - In the **Validation URL** field, enter the URL the CASE application uses to verify connectivity after 802.1X configuration completes.
    - In the **Post Transition URL** field, enter the URL that launches after 802.1X configuration completes.
    - Click **Next**.
19. Review the settings on the **Create Network Profile** summary page and click **Confirm** to save the network profile.

Creating a contractor network profile (contractor@enterprise.com)

1. In the CASE Administrative Console navigation pane, click **Network Profiles**.
2. From the **Actions** drop-down list, click **Create New Network Profile**.
3. In the **Name** field, enter “contractor”.
4. In the **Description** field, enter “Contractor Network”.
5. In the **Splash Screen Banner** field, enter “Security Settings for Contractors”.
6. Leave the **Apply Settings Permanently** check box clear.
7. Leave the **NIC Selection** at the default setting of **Automatic**. With Automatic NIC selection, Access Portal automatically selects the network interface on which the security settings will be applied.
8. In the **Completion Behavior** section, select the **Reside in system tray** radio button.
9. Click **Next** to move to the Connection settings.
10. In the **Connection Method section**, clear the **Wired Connection** check box and select the **Wireless Connection** check box.
11. Under the **Wireless Connection** section, in the **SSIDs** text field, enter “contractor@enterprise”.
12. From the **Authentication** drop-down list, select **WPA2**.
13. From the **Encryption** drop-down list, select **TKIP**.
14. Click **Next** to move to the Authentication settings.
15. In the **Authentication Method** section, select the **802.1X Authentication** check box and from the **802.1X Authentication Type** drop-down list, select **PEAP-MSCHAPv2**. Leave the other fields on this page at default.
16. Click **Next** to move to Operating Systems selection.
17. In the **Operating Systems** section, select the check boxes for all of the operating systems and click **Next**.
18. (Optional) In the **Validation** section:
    - In the **Validation URL** field, enter the URL the CASE application uses to verify connectivity after 802.1X configuration completes.
    - In the **Post Transition URL** field, enter the URL that launches after 802.1X configuration completes.
    - Click **Next**.
19. Review the settings on the **Create Network Profile** summary page and click **Confirm** to save the network profile.

Creating the CASE deployment package

1. In the CASE Administrative Console navigation pane, click **Packages**.
2. From the **Actions** drop-down list, click **Create New Package**.
3. In the **Name** field, enter “secure_enterprise”.
4. Leave the **Type** field as **Folder**.
5. Select the check boxes beside the newly created network profiles: **guest** and **contractor**.
6. (Optional) In the **License** text field, enter text to append to the Avaya licensing agreement.
7. Click **Submit** to save the package.

Deploying the CASE package

1. In the CASE Administrative Console navigation pane, click **Packages**.
2. Select the check box beside the newly created package: **secure_enterprise.**
3. From the **Actions** drop-down list, click **Deploy Package**. The CASE Administrative Console displays the following message “Do you want to deploy the selected Package?”.
4. Click **OK**. The CASE Administrative Console displays the Deploy Package screen.
5. In the **Deployment Details** section:
   - In the **Portal IP** field, enter the IP address of the Access Portal.
   - In the **User Name** field, enter the Access Portal Administrator name.
   - In the **Password** field, enter the Access Portal Administrator password.
6. Click **Submit**.

Web-login page

We now point the standard web-login page on the Avaya Ignition Access Portal to the CASESuccess.html page provided as a part of the CASE Deployment package. This page contains the link(s) to the CASE Profiles based on number of network profiles selected while creating a deployment package. You can modify this html page to suite your needs to display the logo and other instructions.

Important! It is strongly advised to not remove any Avaya Specific code under the Script TAG.

End-user experience

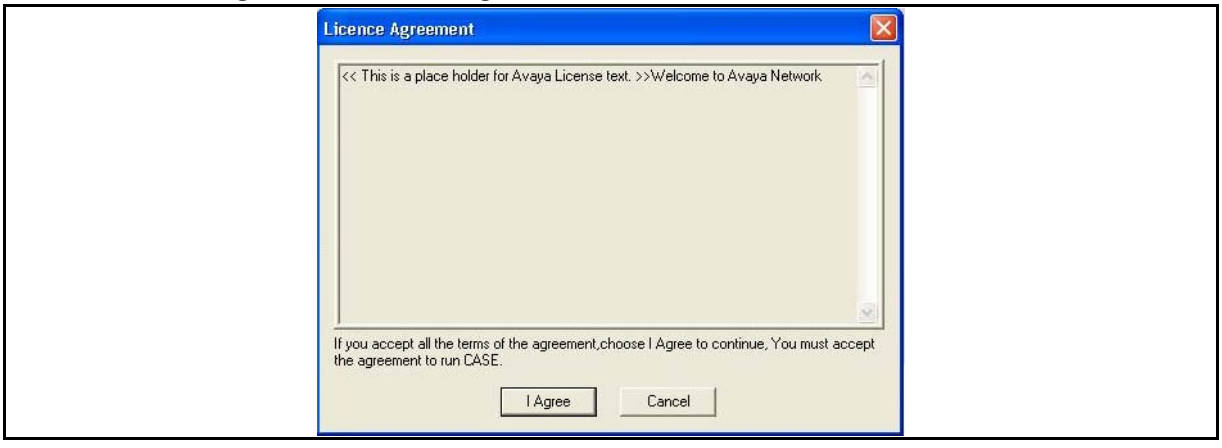
As the end-user enters the Enterprise premises, they will recognize the broadcast, open SSID “open@enterprise.com” of our open network. The end-user uses their wireless management software to attach to this SSID. After attaching to the open SSID, the network capabilities of the end-user are limited until the end-user opens a browser. When the end-user opens a browser, the Ignition Access Portal presents the customized web-login page used in this example.

Figure 19 Customized web-login page

From this initial page, the end-user has the option to enable security or continue with the web-based logon on this insecure SSID. When the end-user selects either **Enable Guest Security** or **Enable Contractor Security**, they begin the CASE experience.

Depending on the browser support for ActiveX or Java Applet, the CASE launches. The CASE begins the process by presenting the Licence Agreement dialog loaded with licensing terms.

Figure 20 Licence agreement



After the end user accepts the licensing terms, the CASE application starts analyzing the current settings. The CASE application then downloads the Network Profile hosted on the Portal and starts applying the settings for the Network Interface.

Figure 21 CASE applies the settings

Depending on the configuration of the user's computer, CASE displays various status messages on the screen. After CASE updates the network interface with the secure settings, the user is prompted for user credentials to authenticate if the user is joining the contractor network.

For the authentication to succeed, the user must have a valid user record in the Ignition appliance. Once configured, the system is migrated to the secure network. The user is automatically transferred to the secure network in about 60 seconds.

Summary

The CASE application and the web-hijacking capabilities of Ignition Access Portal, provide end-users with an intuitive and hassle-free migration to secure networks. The CASE application and Ignition Access Portal allow Administrators to deploy network security without burdening support staff and frustrating end-users.

Troubleshooting

This chapter lists solutions for common errors that can occur when configuring Avaya Identity Engines Ignition Client for Accessing Secure Enterprise (CASE) Administrative Console or running the CASE application.

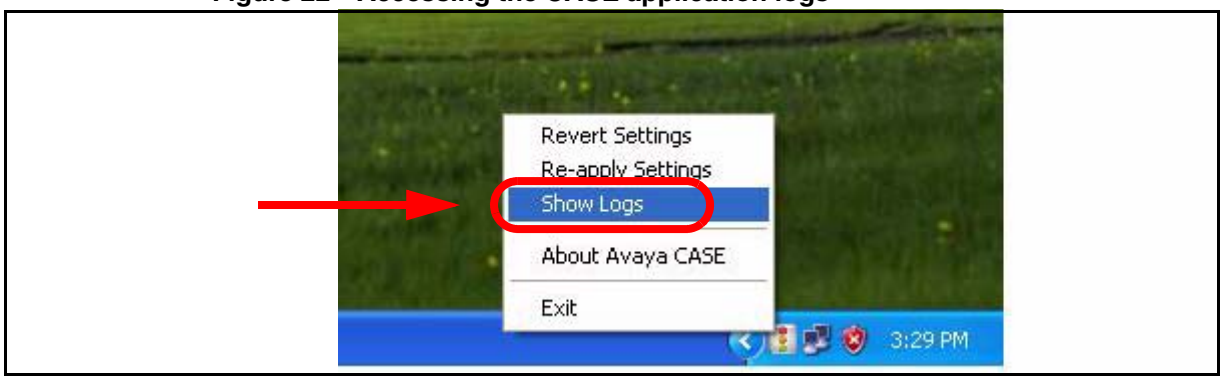
Troubleshooting common problems

The following sections offer solutions and workarounds for commonly reported issues:

Logging

- The **CASE Administrative Console log file** contains entries regarding potential issues and exceptions. The CASE Administrative Console log file is located at: <TOMCAT_INSTALL_DIR>/webapps/AdminConsole/logs/AdminConsole.log
- You can use the **CASE application logs** to troubleshoot errors that can occur when executing the CASE application. The CASE application does not delete the CASE application log file after reverting the settings. New logs are appended to the end of the CASE application log file including when the CASE application is executed multiple times.
  - To access the CASE application logs, from the system tray menu, click **Show Logs**.

Figure 22 Accessing the CASE application logs



Problem: Browser reports certificate errors when attempting to connect to the CASE Administrative Console

Solution: Refer to "Setting up Tomcat to require HTTPS connections" on page 15.

Problem: OS not supported

Solution: Make sure that correct supported OS network profile was downloaded.

Problem: Invalid administrator credentials

Solution: Make sure that correct credentials are given in the Network profiles when deploying on non-admin clients.

Problem: Failed to deploy EAP-PEAP/TLS or EAP-TLS

Solution: Choose the “show logs” option from the CASE system tray menu and look for the key word “Error”. For example, “Error: ImportPerCert: Error in PFXImportCertStore. Probably password incorrect.” means the password for installing client certificate is not correct.

Problem: Failed to deploy network profiles with error “configured supplicant failed”

Solution: Choose the “show logs” option from the CASE system tray menu and look for the key word “Error”. For example, “Error: selected Interface does not match with connection settings.” means the client chose the incorrect network profile such as trying to apply a wireless network profile on a wire network connection.