



Avaya Identity Engines Ignition Access Portal Administration

Avaya Identity Engines Ignition Server
Release 8.0

Document Status: **Standard**
Document Number: **NN47280-604**
Document Version: **01.02**
Date: **April 2012**

© 2012 Avaya Inc.
All Rights Reserved.

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/](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

Purpose of this document

New in this release

Customer service

- Getting technical documentation** 11
- Getting product training** 11
- Getting help from a distributor or reseller** 11
- Getting technical support from the Avaya Web site** 11

Introduction

- How Access Portal works** 13
 - How a guest user logs in 14
- Access Portal administrator tasks** 15

Installing Access Portal

- Access Portal authentication components** 17
 - VMware ESXi Server requirements 17
- Network configuration for Access Portal-based authentication** 21
- Installing the Access Portal virtualization appliance** 22
- Configuring the Access Portal virtualization appliance** 28
 - Setting up the Access Portal IN port 34
 - Setting up the Access Portal firewall rules 35
 - Setting up the Access Portal's DNS forwarder 37
 - Configuring the Access Portal DHCP server settings 38
 - Configuring the appliance's Access Portal settings 39
 - Customizing user-visible pages 42
 - Creating customized user-visible pages 42
 - Uploading customized user-visible pages 42
 - Selecting the Access Portal Login page 43
 - Setting up the Success page 43
 - Selecting the Authentication error page contents 44
 - Providing access to servers or other computers from a client machine 45
- Backing up and restoring Access Portal** 45
 - Introduction to backing up and restoring Access Portal 45
 - Creating a backup 46
 - Restoring from a backup file 46
- Upgrading Access Portal** 48

Configuring the Ignition Server

Configuring the Ignition Server to work with the Access Portal 49

- Activating the Access Portal license 49
- Configuring Access Portal server details 50
- Editing Access Portal server details 51
- Introduction to device profiling 52
- Introduction to MAC authentication 53
- Setting up MAC authentication on Access Portal 54
 - Creating a MAC-Auth policy 54
 - Configuring the Access Portal Server Details to support MAC Auth 56
 - Creating a device record 57
 - Editing the device template to support MAC authentication 59
 - Enabling RADIUS MAC authentication on Access Portal 60
- Setting up the guest access policy in the Ignition server 60
- Registering authenticators that provide regular user access in the Ignition Server 62
 - Wired access for non-guest users 62
 - Wireless access for non-guest users 62

Configuring guest access on the wired switch 62

- Cabling the wired switch 62
- Configuring VLANs on the wired switch 63
- Configuring wired switch Ethernet ports 63

Configuring wireless guest access 64

- Prerequisites 64
- Configuring wireless guest access 64

Creating guest user accounts 65

Testing wireless guest access 65

Testing wired guest access 66

Configuring CASE

Configuring the CASE to work with Access Portal 67

- CASE Administrative Console overview 67
- Creating a network profile 67
- Creating a deployment package 67
- Deploying packages 67

Troubleshooting

Troubleshooting common problems 69

- Problem: Cannot access the Access Portal login page from client browser using an URL with a DNS name 69
- Problem: You are unable to authenticate a user 69
- Problem: MAC Authentication fails 69
- Problem: Cannot launch the Access Portal Administration Web UI 70

- Problem: Client is unable to communicate with Access Portal 70
- Problem: You are unable to ping IN and OUT interfaces of Access Portal. 70
- Problem: In Dashboard, you do not see “Access Portal” as the last option in the Configuration list 70
- Miscellaneous troubleshooting tips 70

Appendix A: Access Portal deployment example

Planning your deployment 73

- Determine what kinds of SSIDs exist on your wireless network 73

- Determine what kinds of VLANs exist on your wires network 73

Network requirements 73

Background 74

Configuring the Ignition (RADIUS) Server 75

Configuring the Ignition Access Portal (web server) 76

Configuring the Avaya wireless controller 80

Configuring the edge switch 81

Verification 81

Purpose of this document

The *Avaya Identity Engines Ignition Access Portal Administration* guide explains how to install and configure the Avaya Identity Engines Ignition Access Portal. This guide also explains how to configure the Ignition Server and Identity Engines Ignition Client for Accessing Secure Enterprise (CASE) to work with Access Portal. This guide is written for network administrators who need to install and configure Access Portal.

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

Avaya Identity Engines Ignition Access Portal is a virtual machine based captive portal and firewall distribution that controls the access of client devices to the network. Access Portal blocks all traffic from client devices and allows network access only after successful authentication. Access Portal allows guests with non-802.1X compatible equipment to authenticate and connect to the network in your organization.

Access Portal does not require client-side software on the connecting user's PC. Like the sign-on portals that provide guest wireless access in many hotels, Access Portal uses the user's browser to prompt for and collect the user's credentials. This allows Access Portal to provide controlled network access to client devices that are incompatible with the 802.1X protocol or not configured to use it.

Access Portal also provides Device Profiling. Device Profiling works on a Device Fingerprint which is a compact summary of software and hardware settings collected from a client device. In the Avaya Identity Engines Ignition Server environment, Device Profiling is used as an automated way to register the devices with the Identity Engines Internal Store.

How Access Portal works

Users connected to a network where Access Portal is deployed must view and interact with the Access Portal login page before access to the network is granted. Upon successful authentication, Access Portal works with the Client for Accessing Secure Enterprise (CASE) application, the Ignition Server, and your network equipment to establish an appropriate network session for the user. For example, Access Portal can host the CASE application. On successful authentication, Access Portal can download the CASE application to the user's machine and the CASE application can configure the machine to use 802.1X. Then the user can directly connect to the network by authenticating with the Ignition Server. Or if the device is not capable of doing 802.1X, Access Portal can provide inline access to the network.

How a guest user logs in

At runtime, Access Portal authentication works as follows:

1. The guest gets a temporary user name and password from the reception desk personnel. (Typically, the receptionist uses Ignition Guest Manager to create the user account.)
2. The guest connects his/her laptop or other device to the network. For example, a guest with a laptop might launch the wireless network client software (the supplicant software) on his/her laptop and connect to the guest wireless network. In this example, the guest network will identify itself with the SSID, "**Guest**". This is a wide open, guest-authentication SSID.
3. On the access point, the SSID, Guest, is associated with a restricted-reach, authentication VLAN. For example, you might define a VLAN, VLAN **200** on the Avaya 5500 switch. VLAN 200 is a local-access-only VLAN used only during the authentication process. The wired switch and wireless access point are trunked together using 802.1Q trunking.
4. The laptop's supplicant requests an IP address via DHCP.
5. The Avaya Access Portal handles the DHCP request and issues the laptop an address. The laptop is now on the authentication VLAN (in this example, that is VLAN **200**).
6. The guest user opens a browser on his/her laptop. The Access Portal forces a redirect of the browser's web traffic, causing the browser to display the login page you defined as the Access Portal login page.
7. The user enters his/her temporary user name and password, and the Access Portal authenticates the user via the Ignition Server using RADIUS:
 - a. If the CASE application is also deployed on the portal, after successful authentication, the CASE application will run on the guest's machine and configure it to use 802.1X for authenticating to the network. If CASE application is successful in doing this, the guest's laptop will be switched to a compliant VLAN and all the network access will be independent of the portal.
 - b. If the authentication succeeds but there is no CASE application on the portal, the Access Portal tunnels the guest's network session to the Internet. Note that the Access Portal remains in-line in this case; that is, all traffic to and from the client travels through the Access Portal.
 - c. If the authentication fails, the browser displays a failure notice and the laptop remains on VLAN 200, which provides no connection or limited connection to the corporate network or the Internet depending on the configured settings in the Access Portal.

Important: Access Portal does not support proxy. To allow Access Portal to capture HTTP requests from a client machine, you must either remove the proxy settings from the client browser, or choose “auto detect proxy setting for this network” setting on the browser. If a proxy is configured, Access Portal will not be able to direct HTTP requests to the Access Portal login page.

Access Portal administrator tasks

As the Avaya Identity Engines Ignition Server administrator, you can:

- Install Access Portal
- Configure Access Portal
- Perform Access Portal maintenance tasks
- Configure the Ignition Server to work with Access Portal
- Configure and test user access
- Configure the CASE application to work with Access Portal

Installing Access Portal

This chapter describes how to install Avaya Identity Engines Ignition Access Portal. You install Access Portal as a virtual appliance on a VMware ESXi 4.x or 5.0 server. After you import the Access Portal virtual appliance, the virtual appliance becomes an Access Portal. **Note:** You can deploy multiple instances of Access Portal.

This chapter also explains how to backup, restore, and upgrade Access Portal.

Access Portal authentication components

The following components are required to deploy an Access Portal-based authentication with Ignition Server:

- Ignition Server
- Access Portal (VMware ESXi 4.x or 5.0 server)
- CASE application (optional but highly recommended)
- Ignition Guest Manager account creation tool (optional)
- Existing 802.1X-capable authenticators (switches and wireless access points)
- Existing firewall

VMware ESXi Server requirements

Hardware platforms supported by VMware's ESXi servers versions 4.x and 5.0 are supported. The VM requires an x86_32 capable environment, a minimum of 2 GB of memory, 10 GB of available disk storage, two CPUs, and preferably three NICs (a minimum of two physical NIC cards). VMware lists on its site supported hardware platforms for ESXi. (<http://www.vmware.com>)

Installation on a VMware ESXi server is done using an OVF file which already incorporates the OS FreeBSD.

Reminder: Avaya provides the Ignition Access Portal as a Virtual Appliance. Do not install or uninstall any software components unless Avaya specifically provides the software and/or instructs you to do so. Also, do not modify the configuration or the properties of any software components of the VMs

(including VMware Tools) unless Avaya documentation and/or personnel specifically instructs you to do so. Avaya does not support any deviation from these guidelines.

Warning! Do not install or configure VMware Tools or any other software on the VM shipped by Avaya:

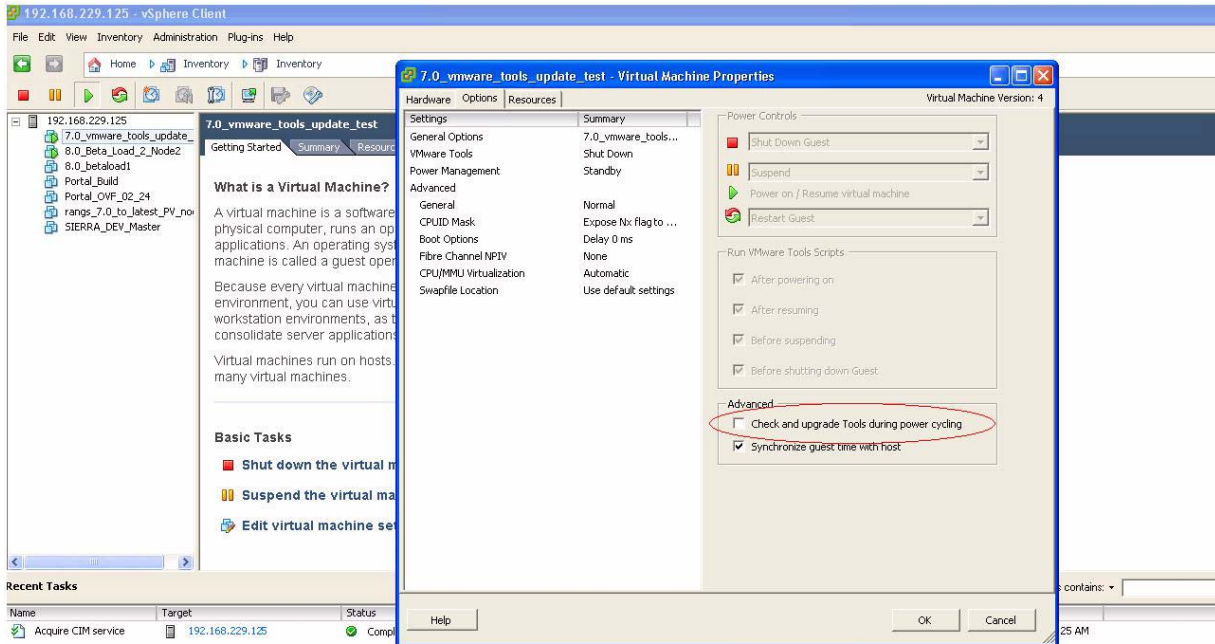
- Avaya does not support manual or automated VMware Tools installation and configuration on Avaya supplied VMs.
- Turn off automatic VMware Tools updates if you have enabled them. Refer to the instructions below to disable automatic updates and to check if you have accidentally installed VMware tools.
- Avaya determines which VMware Tools to install and configure. When required, Avaya provides these tools as part of the installation or package upgrade procedures. Avaya provides these tools because VMware Tools configures the kernel and network settings and unless Avaya tests and approves these tools, Avaya cannot guarantee the VM will work after the tool is installed and configured.
- Avaya does not support the installation of any VMware specific, RHEL specific, or any third party vendor package or RPM on its VM other than what Avaya ships as a package, image, or OVF.

Preventing automatic VMware Tools updates:

To prevent automatic VMware Tools updates:

1. Use the VI Client to log in to the ESXi Server hosting the Access Portal VM.
2. Go to **Getting Started > Edit Virtual Machine Settings > Options > VMware Tools > Advanced**, and ensure the **Check and upgrade Tools during power cycling** check box is not selected. This is the supported setting.
3. Click **OK**.

Figure 1 Preventing automatic VMware Tools updates



Checking the VMware Tools status (ESXi 4.1)

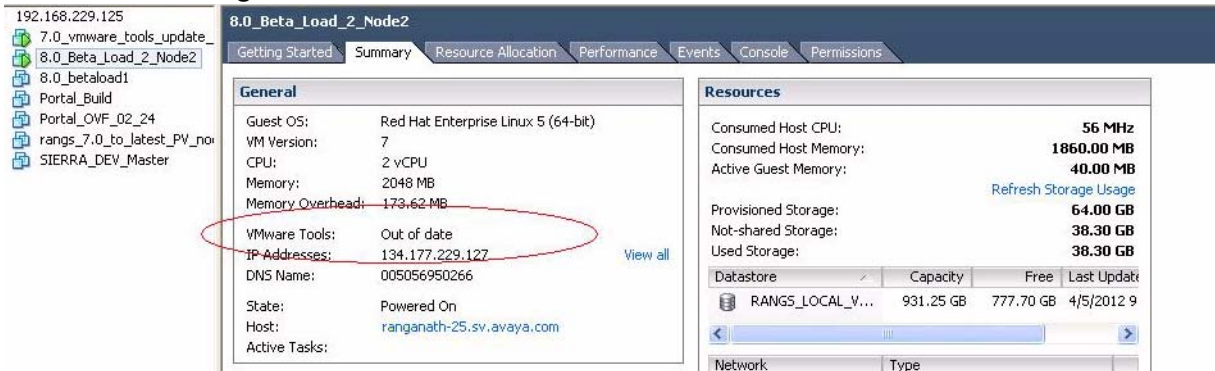
The **Summary** tab of the VM describes the VMware Tools status.

To check the VMware Tools status on an ESXi 4.1 server:

1. Use the VI Client to log in to the ESXi Server hosting the Access Portal VM.
2. Go to the **Summary** tab.

If you are using the vmware-tools supplied by Avaya and did not upgrade, the status displays as “VMware Tools: Out of date”.

Figure 2 VMware Tools: Out of date



If you upgraded the VMware Tools, the status displays as “VMware Tools: OK”.

Figure 3 VMware Tools: OK



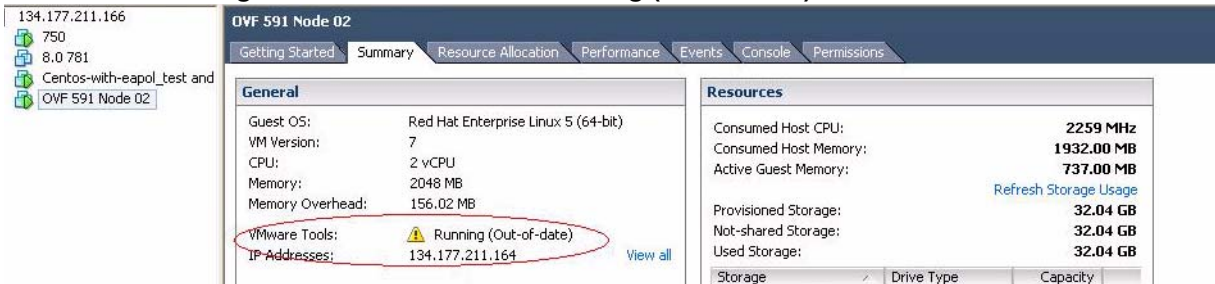
Checking the VMware Tools status (ESXi 5.x)

To check the VMware Tools status on an ESXi 5.x server:

1. Use the VI Client to log in to the ESXi Server hosting the Access Portal VM.
2. Go to the **Summary** tab.

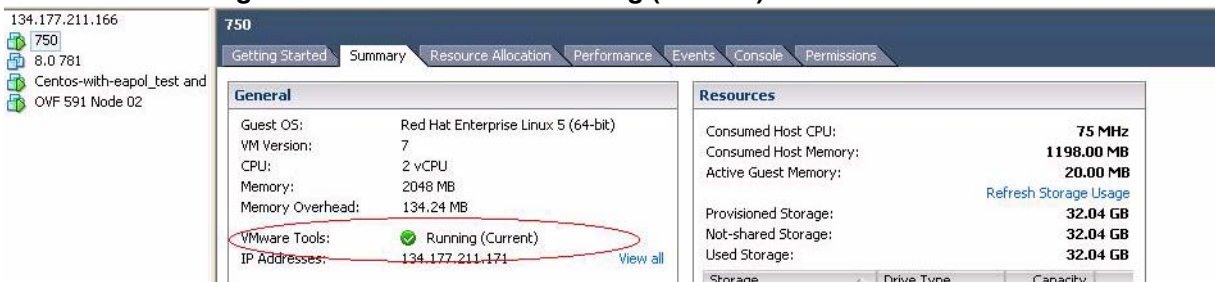
If you are using the vmware-tools supplied by Avaya and did not upgrade, the status displays as “VMware Tools: Running (Out-of-date).”

Figure 4 VMware Tools: Running (Out-of-date)



If you upgraded the VMware Tools, the status displays as “VMware Tools: Running (Current)”.

Figure 5 VMware Tools: Running (Current)

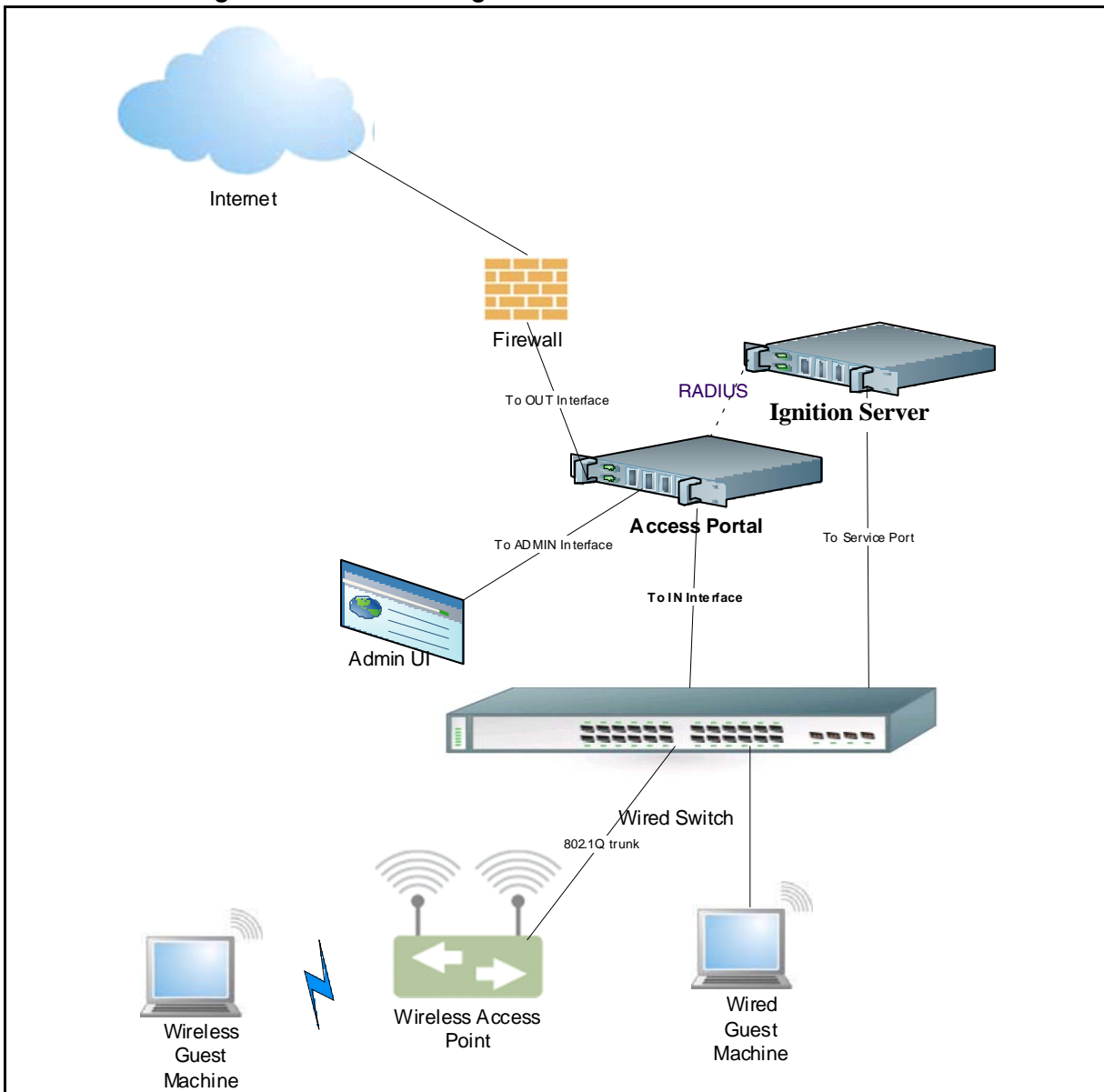


Network configuration for Access Portal-based authentication

As shown in the following figure, Access Portal has three network interfaces:

- **OUT** - The OUT interface provides connectivity to the Enterprise network / Internet.
- **ADMIN** - The ADMIN interface provides connectivity to the portal to perform administrative tasks.
- **IN** - The IN interface provides connectivity to the client network. This is the guest or unauthenticated client VLAN / network.

Figure 6 Network configuration for Access Portal-based authentication

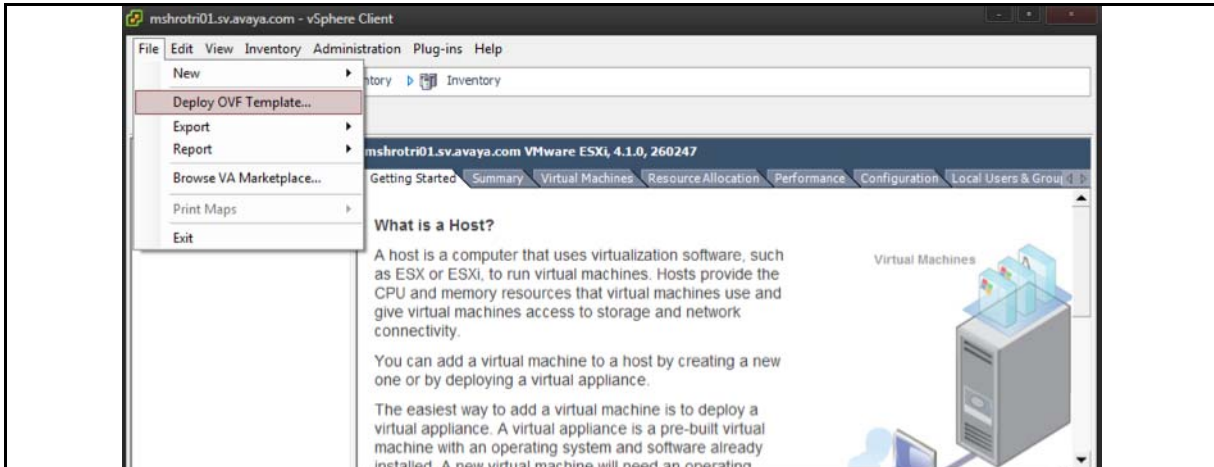


Installing the Access Portal virtualization appliance

Avaya recommends that you use the VMware vSphere Client to import the VM into your system. Start the VMware vSphere Client and log in to the ESXi Server you want to install the Access Portal on. You will need to use the Virtual Appliance Deploy OVF Template option.

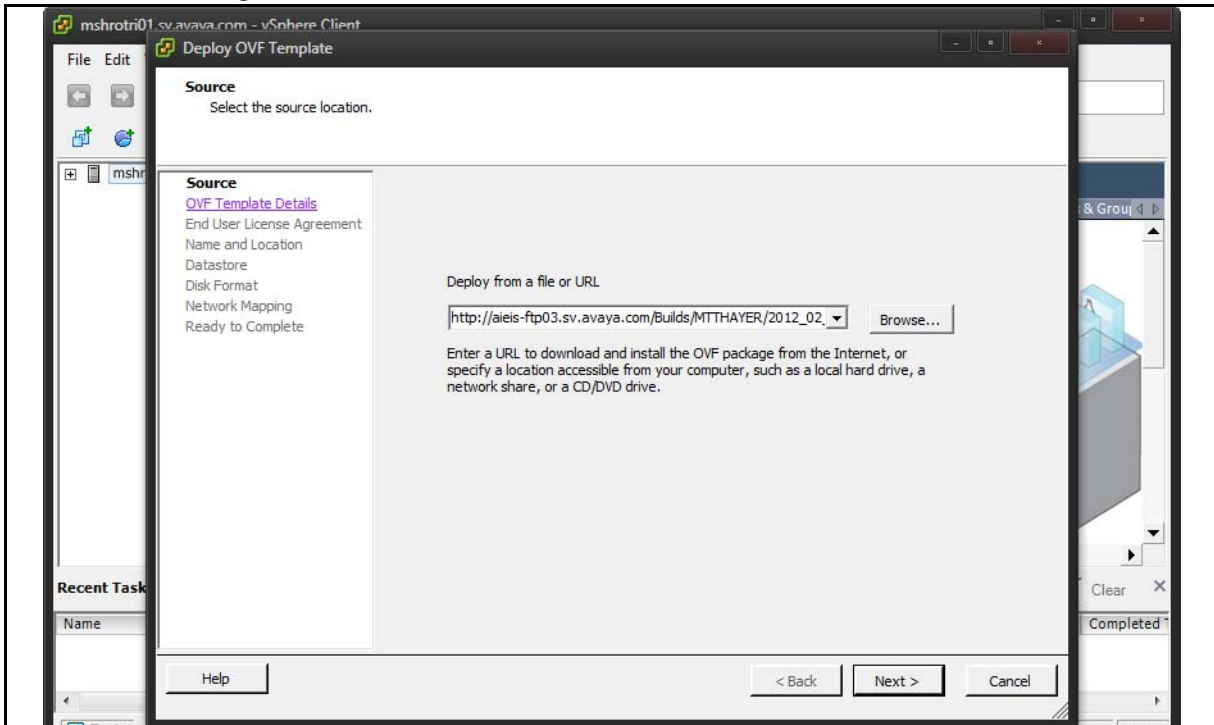
1. From the vSphere Client, select **File > Deploy OVF Template**.

Figure 7 Deploy OVF Template



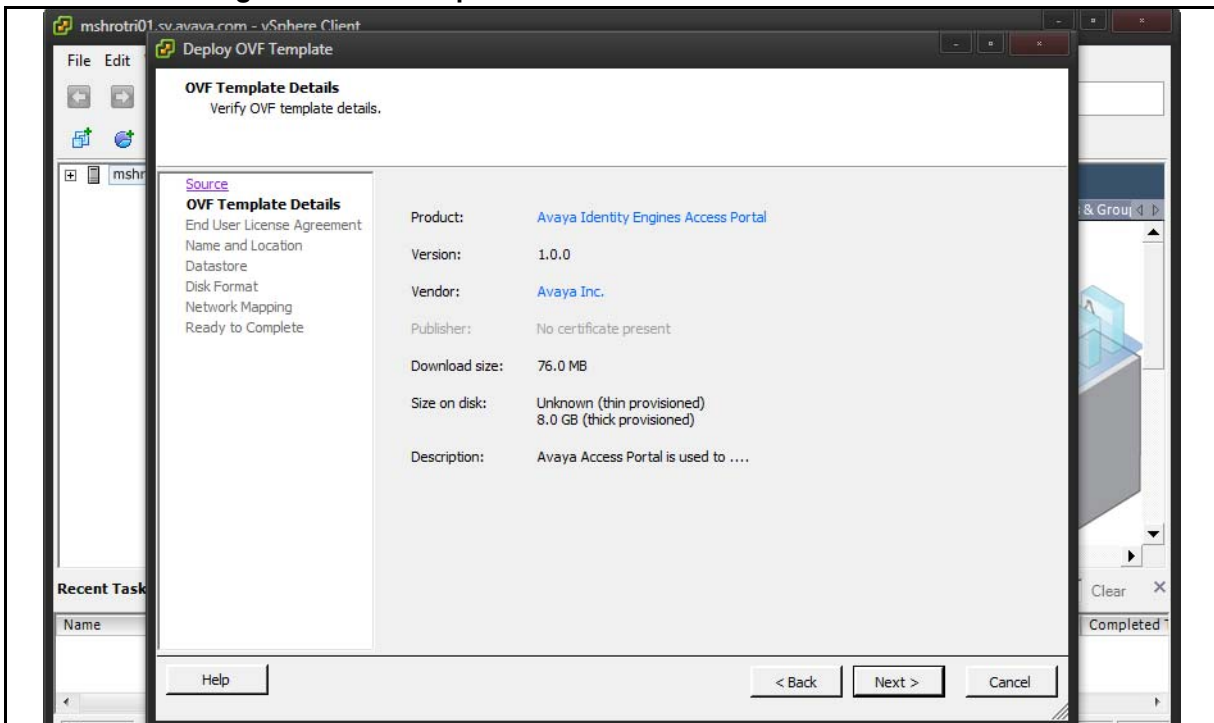
2. The Source screen appears. Select the location from which you want to import the Access Portal virtual appliance.

Figure 8 Source



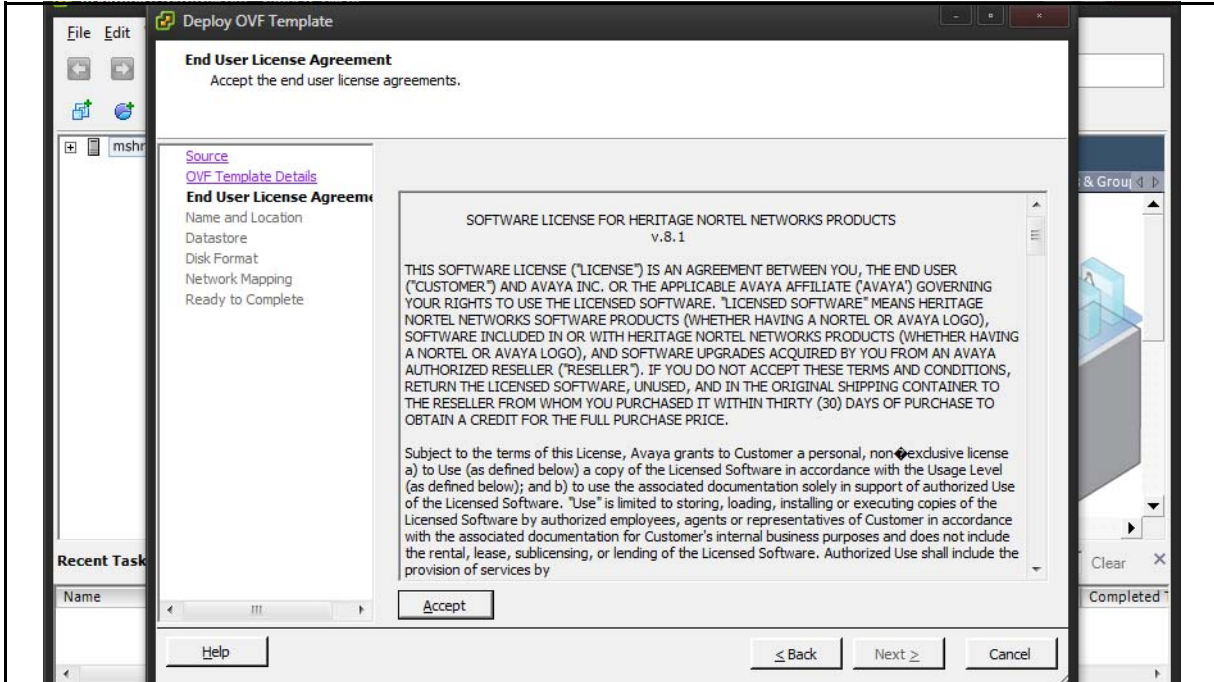
3. Click **Next**. In the OVF Template Details screen, review your settings. You can click **Back** to make changes, or click **Next** to continue.

Figure 9 OVF Template Details



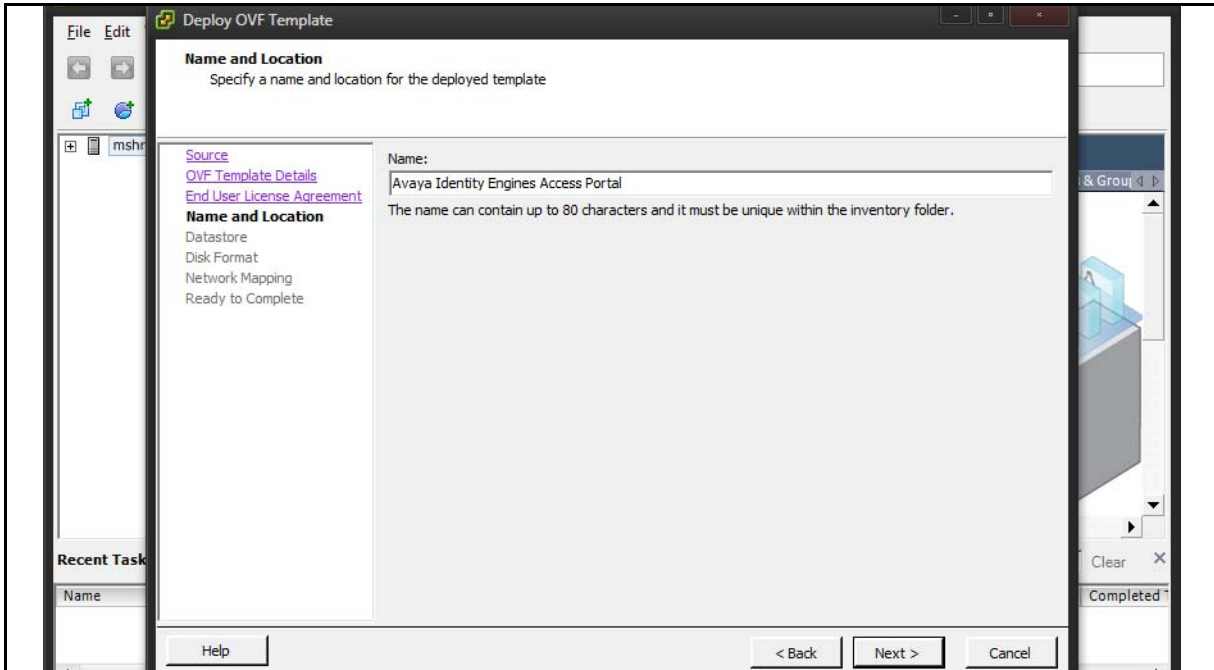
4. The **End User License Agreement** screen appears. Click **Accept** to accept the license and click **Next**.

Figure 10 End User License Agreement



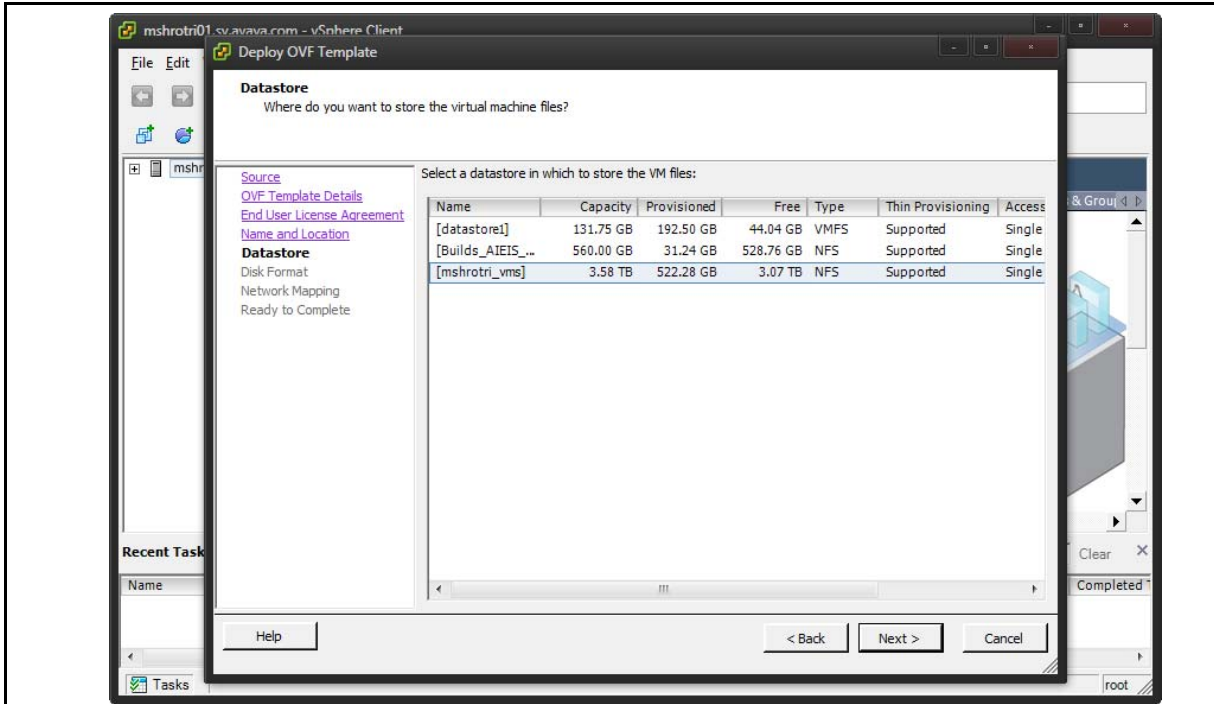
5. The **Name and Location** screen appears. You can either accept the default name or choose to rename the virtual machine. Click **Next**.

Figure 11 Name and Location



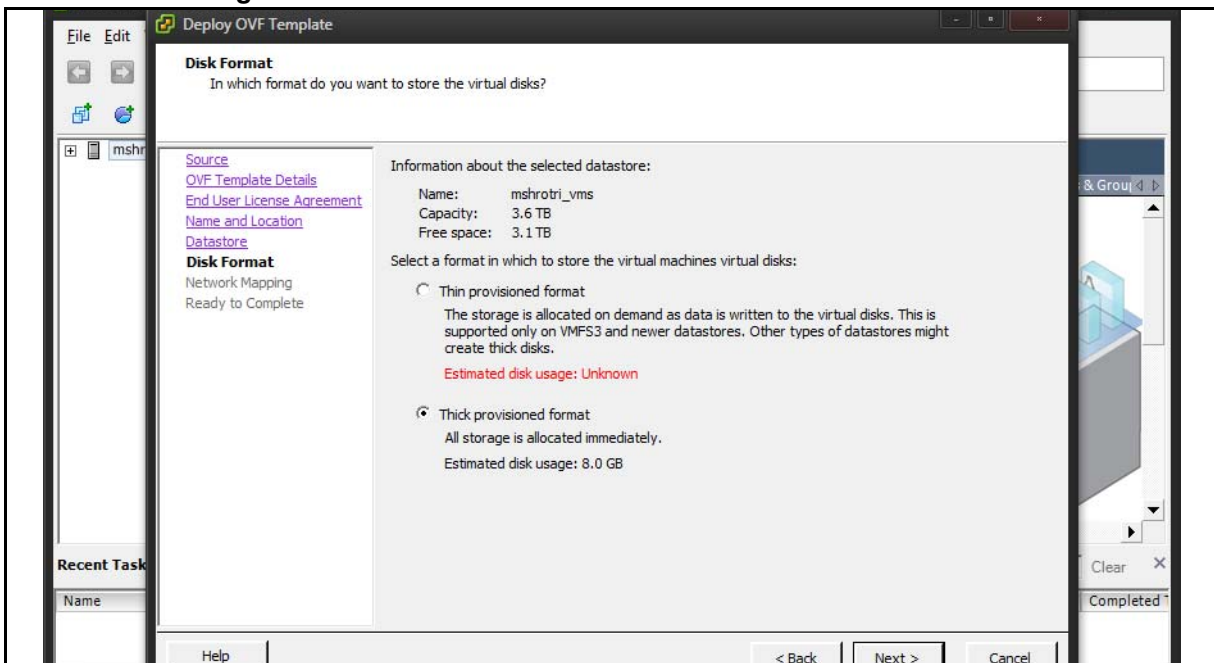
6. The **Datastore** screen appears. Select the location where you want to store the files for the virtual appliance and click **Next**.

Figure 12 Datastore



7. The **Disk Format** screen appears. Select a format in which to store the virtual machine's virtual disks and click **Next**.

Figure 13 Disk Format



-
8. The **Network Mapping** screen appears. Associate the Access Portal NICs (OUT, ADMIN, and IN) to the correct VM Network based on your site configuration.

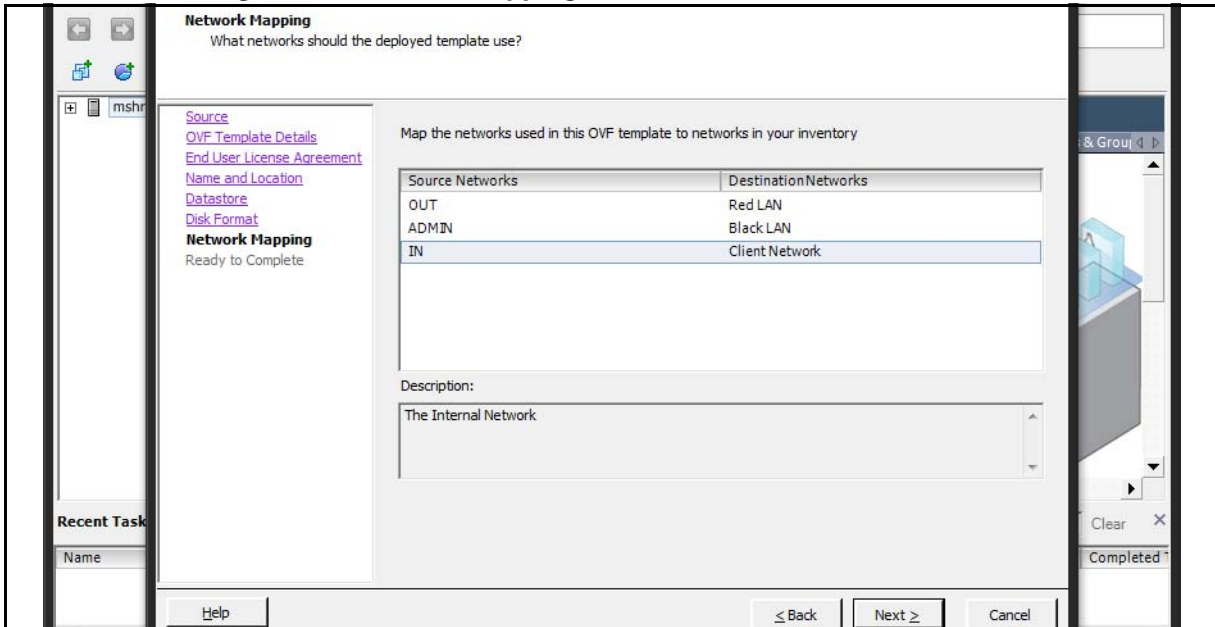
Note: Access Portal auto-configures itself to map OUT to em0, ADMIN to em1, and IN to em2, irrespective of how the OUT, ADMIN, and IN interfaces are mapped to VM Networks on the ESXi server. The Access Portal association of OUT to em0, ADMIN to em1, and IN to em2 is binding in Access Portal and will always be there. Changing the OUT, ADMIN, and IN mapping to ESXi server network mapping while deploying portal OVF does not affect the mapping done in Access Portal.

- × **OUT:** This network provides access to the Internet. Map the Access Portal OUT interface to the VM network in your inventory that provides access to the Internet. In the example below, the Access Portal OUT interface is mapped to the RedLAN.
- × **ADMIN:** This network is for administrative purposes. This network provides web access for administrating Access Portal and SSH access to the Access Portal console if needed. This network also provides connectivity to other servers like the Ignition server, or an external DHCP server if you are using one. Map the Access Portal ADMIN interface to the VM network in your inventory designated for administrative purposes. In the example below, the Access Portal ADMIN interface is mapped to the BLackLAN.
- × **IN:** This is the network where client machines are present whose access to OUT network needs to be controlled by the portal. Map the Access Portal IN interface to the VM network in your inventory that provides connectivity to the client network. In the example below, the Access Portal ADMIN interface is mapped to the ClientNetwork.

Note: If your ESXi server only has 2 physical NICs, you can map the Access Portal logical OUT and ADMIN interfaces to the same physical NIC. However, you must map the Access Portal IN interface to its own separate NIC.

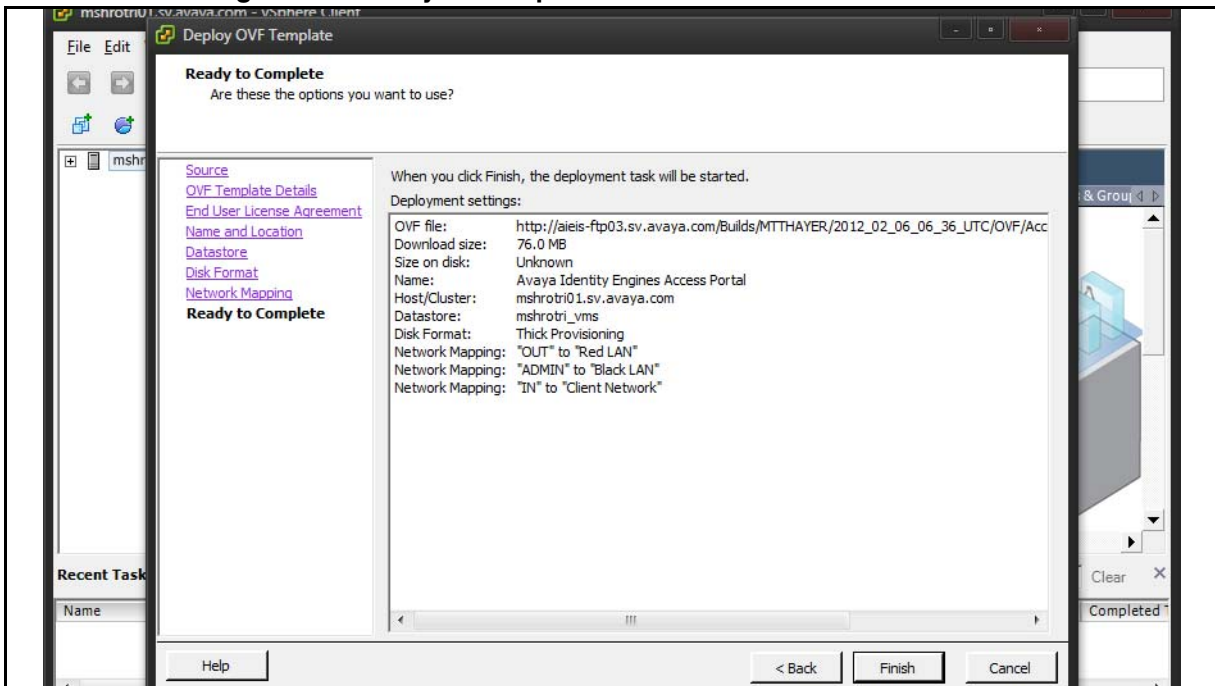
- × Click **Next**.

Figure 14 Network Mapping



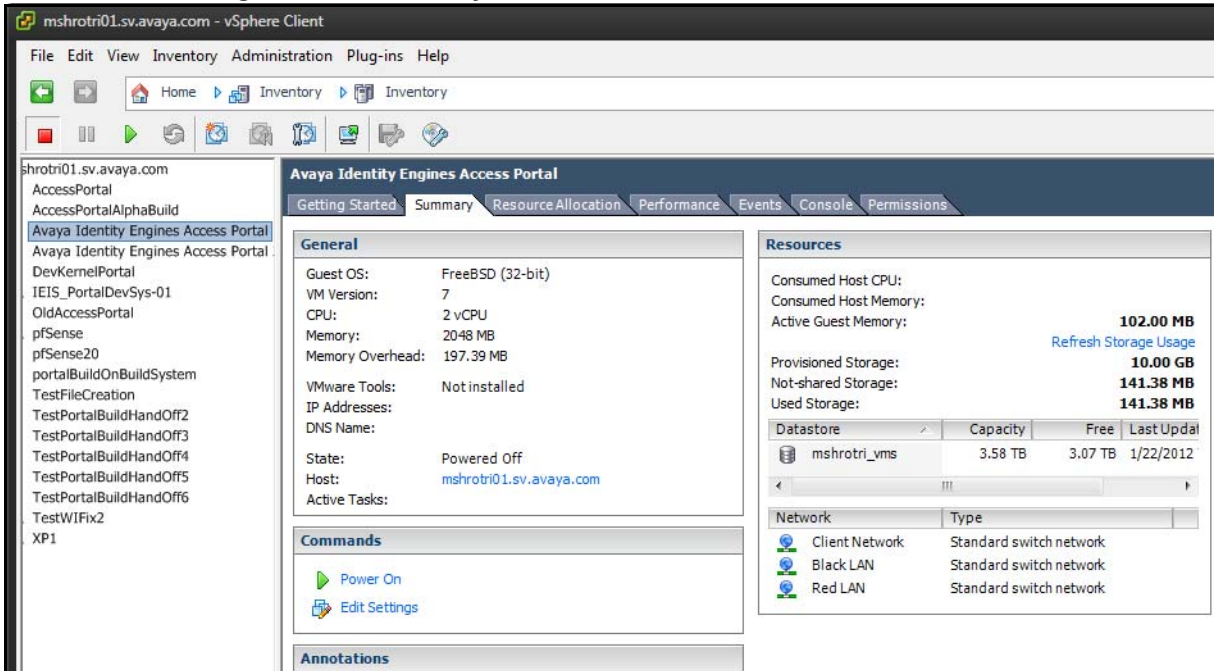
9. On the **Ready to Complete** screen, review your settings. Use the **Back** button to make any changes or click **Finish** to start the import.

Figure 15 Ready to Complete



The Import now starts. When the import completes, a **Summary** window displays.

Figure 16 Summary



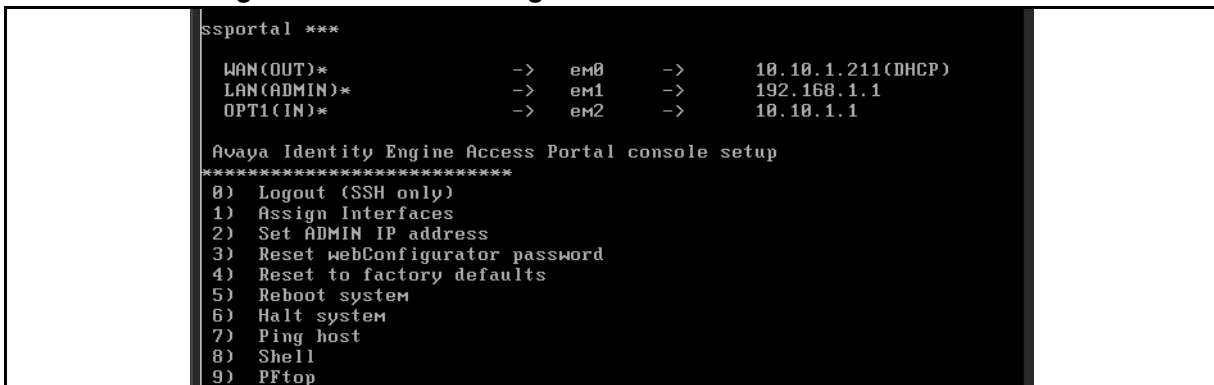
You are now ready to boot the Access Portal for the first time.

Configuring the Access Portal virtualization appliance

After the import completes you need to verify and adjust some of the VM settings.

1. Boot the Access portal. The Access Portal console displays the interface assignments.

Figure 17 Interface assignments



2. From the Access Portal console menu, enter **2** and enter the ADMIN IP address. Press **Enter**.

Figure 18 Entering the ADMIN IP address

```
LAN(ADMIN)*          -> em1    -> 192.168.1.1
OPT1(IN)*            -> em2    -> 10.10.1.1

Avaya Identity Engine Access Portal console setup
*****
0) Logout (SSH only)
1) Assign Interfaces
2) Set ADMIN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) Pftop
10) Filter Logs
11) Restart webConfigurator
12) Avaya Identity Engine Access Portal Developer Shell
13) Upgrade from console
14) Disable Secure Shell (sshd)

Enter an option: 2

Enter the new ADMIN IP address: 192.168.10.2
```

3. Enter the subnet mask of the ADMIN IP address and press **Enter**.

Figure 19 Entering the subnet mask of the ADMIN IP address

```
14) Disable Secure Shell (sshd)

Enter an option: 2

Enter the new ADMIN IP address: 192.168.10.2

Subnet masks are entered as bit counts (as in CIDR notation) in Avaya Identity Engine Access Portal.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new ADMIN subnet bit count: 24

Do you want to enable the DHCP server on ADMIN [y;n]? n

The ADMIN IP address has been set to 192.168.10.2/24.
You can now access the webGUI by opening the following URL
in your web browser:

http://192.168.10.2/

Press ENTER to continue.
```

4. The Access Portal console displays the following prompt: “Do you want to enable the DHCP server on ADMIN [y:n]?” Enter **n** and press **Enter**. The Access Portal console displays the following message: “The ADMIN IP address has been set to <ADMIN IP/mask>. You can now access the webGUI by opening the following URL in your web browser: http://<ADMIN IP>”
5. Using another machine in your network, access the Access Portal Administration Web UI at http://<ADMIN IP>. The default credentials are username: **admin** and Password: **admin**.

Note: You might have to remove any proxy settings on the browser to access this UI.

Workaround: If it is not possible to have a machine on the Admin network to connect to the Access Portal Administration Web UI, then you can use the shell to add a static route to the network where the admin machine resides.

Important: Using the shell to add the static route is only a workaround and is not an Avaya recommendation. **Avaya does not support Access Portal configuration through the shell.** You must perform all management actions through the Access Portal Administration Web UI. The only supported way to add a static route is after installation from the Access Portal Administration Web UI: Go to System > Static routes.

6. A wizard launches the first time you access the Access Portal Administration Web UI. On the General Information Wizard page, do the following:

Figure 20 General Information page

On this screen you will set the General pfSense parameters.

General Information	
Hostname:	<input type="text" value="accessportal"/> EXAMPLE: myserver
Domain:	<input type="text" value="local"/> EXAMPLE: mydomain.com
Primary DNS Server:	<input type="text"/>
Secondary DNS Server:	<input type="text"/>

Next

- In the **Hostname** field, enter host name of the Access Portal.
 - In the **Domain** field, enter the network domain that the Access Portal will serve.
 - In the **Primary DNS Server** field, enter the IP address of the primary DNS server.
 - In the **Secondary DNS Server** field, enter the IP address of the secondary DNS server.
 - Click **Next**. The Time Server Information page appears
7. On the Time Server Information page, do the following:
 - * In the **Time server hostname** field, enter the fully qualified name of your NTP server. This must be the same NTP server that your Ignition Server appliance uses.
 - * From the **Timezone** drop-down list, select your time zone.
 - * Click **Next**. The Wide Area Network information page appears.

Figure 21 Time Server Information page

Please enter the time, date and time zone.

Time Server Information	
Time server hostname:	<input type="text" value="time.nist.gov"/> Enter the name of the time server.
Timezone:	<input type="text" value="America/Los_Angeles"/>

8. On the Wide Area Network information page, do the following:
 - × From the **SelectedType** drop-down list, click **Static**.
Tip: Most deployments require you to assign a static IP to the WAN interface of the Access Portal.
 - × The **MAC Address** field is usually left blank. To modify (“spoof”) the MAC address of the WAN interface, enter a MAC address in the following format xx:xx:xx:xx:xx:xx. This may be required with some cable connections.
 - × If you chose Static as the selected type for the WAN interface, in the **IP Address** field, assign an IP address to the port. Set the subnet mask in the adjacent drop-down list. Choose the subnet mask, expressed as a bit count.
 - × If you chose Static as the selected type for the WAN interface, in the **Gateway** field, enter the IP address of the default gateway for the firewall.
 - × If you chose DHCP as the selected type for the WAN interface, in the **DHCP Hostname** field, enter the DHCP Hostname. The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs require this for client identification.
 - × Click **Next**. The Local Area Network information page appears.

Figure 22 Wide Area Network information page

On this screen we will configure the Wide Area Network information.

Configure OUT Interface	
SelectedType:	Static
General configuration	
MAC Address:	<input type="text"/> <small>This field can be used to modify ("spoof") the MAC address of the OUT interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank</small>
MTU:	<input type="text"/> <small>If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.</small>
Static IP Configuration	
IP Address:	<input type="text"/> / 1
Gateway:	<input type="text"/>
DHCP client configuration	
DHCP Hostname:	<input type="text"/> <small>The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).</small>

Next

9. (Optional) On the Local Area Network information page, do the following:
- × In the **LAN IP Address** field, enter the new LAN IP address.
 - × From the **Subnet Mask** drop-down list, select the subnet mask, expressed as a bit count.
 - × Click **Next**. The Admin Password page appears.

Figure 23 Local Area Network information page

On this screen we will configure the Local Area Network information.

Configure ADMIN Interface	
ADMIN IP Address:	<input type="text" value="134.177.229.206"/> <small>Type dhcp if this interface uses DHCP to obtain its IP address.</small>
Subnet Mask:	24

Next

10. (Optional) On the Admin Password page, do the following:
- × In the **Admin Password** field, enter the new password.
 - × In the **Admin Password AGAIN** field, enter the new password again.
 - × Click **Next**. The Reload page appears.

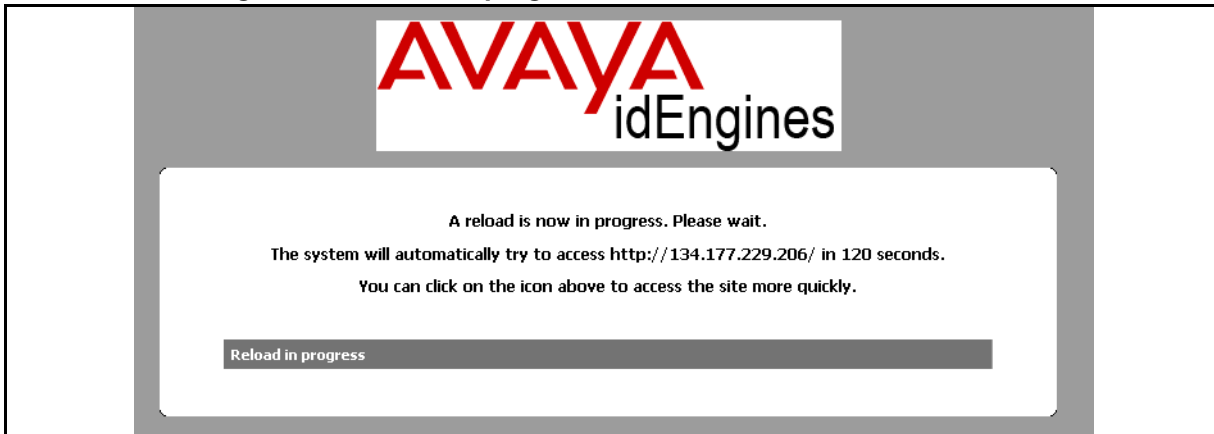
Figure 24 Admin Password page

On this screen we will set the Admin password which is used to access the WebGUI and also SSH services if you wish to enable.

Set Admin WebGUI Password	
Admin Password:	<input type="password"/>
Admin Password AGAIN:	<input type="password"/>





11. Click **Reload** to load the new settings. If you changed the password, Access Portal prompts you to log in again. The following message displays “A reload is now in progress. Please wait. The system will automatically try to access <http://xxx.xxx.xxx.xxx> in 120 seconds. You can click on the icon above to access the site more quickly.”

Figure 25 Reload in progress



After you click the Avaya icon, or wait for the page to refresh, the System Overview page appears. You can now access the following Access Portal Administration Web UI main menu headings for further configuration: System, Interfaces, Firewall, Services, Status, and Diagnostics.

Figure 26 System Overview page

System information	
Name	accessportal.local
Version	1.2.3-RELEASE built on Mon Feb 27 02:57:01 UTC 2012
Platform	pfSense
Uptime	7 days, 21:23
State table size	62/10000 Show states
MBUF Usage	772 /1665
CPU usage	 0%
Memory usage	 4%
SWAP usage	 0%
Disk usage	 3%

Setting up the Access Portal IN port

Set up the IN port. The IN port of the Access Portal is the entry point by which guests enter your authentication VLAN. You set up the guest-accessible switches in your organization so that, when a client attempts to connect to the network and fails (the 802.1X authentication attempt fails) the switch places his or her session on a restricted-reach VLAN that includes the Access Portal IN port. For VLAN set-up details, see [“Configuring VLANs on the wired switch” on page 63](#).

To set up the IN port, follow the steps below:

1. On the main Access Portal Administration Web UI page, click **Interfaces > IN** and do the following:
 - × In the **Description** field, enter a name for the interface.
 - × In the **IP address** field, enter the IP address of the IN interface.
 - × From the adjacent drop-down list, click the subnet mask of the IN interface.
 - × Click **Save**.

Figure 27 Assigning an IP address to the IN interface

The screenshot displays the configuration page for the 'Optional 1 (IN)' interface. At the top, there are navigation tabs: System, Interfaces, Firewall, Services, Status, and Diagnostics. The 'Interfaces: Optional 1 (IN)' section is selected. Below this, there are three main configuration sections: 'Optional Interface Configuration', 'General configuration', and 'IP configuration'. In the 'Optional Interface Configuration' section, the 'Enable Optional 1 interface' checkbox is checked, and the 'Description' field is set to 'IN'. The 'General configuration' section includes a 'Type' dropdown set to 'Static', a 'MAC address' field with a 'Copy my MAC address' link, and an 'MTU' field. The 'IP configuration' section shows the 'IP address' set to '10.10.10.2 / 24' and an empty 'Gateway' field.

Setting up the Access Portal firewall rules

The Access Portal firewall rules determine what traffic can travel to and from guest devices and what networks guests are allowed to reach.

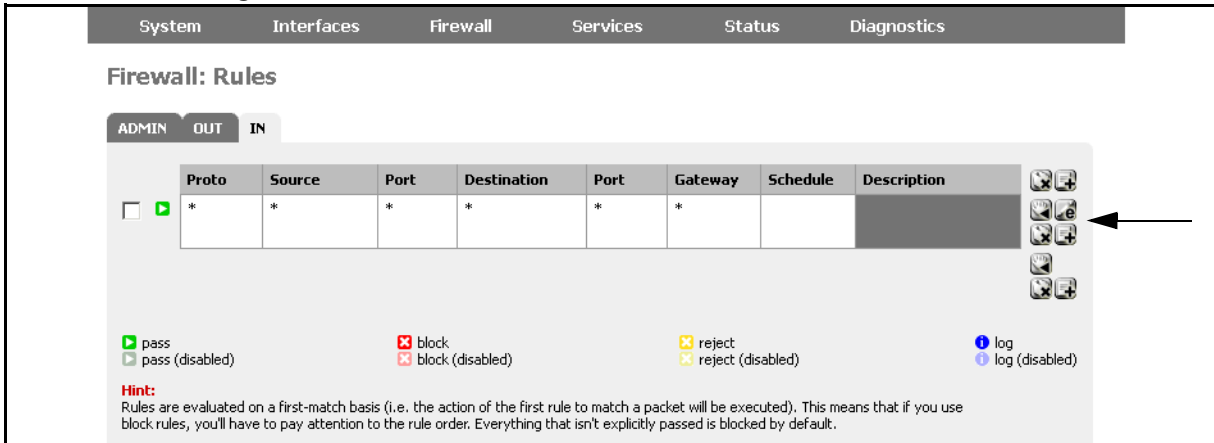
When you install Access Portal, there is a default firewall rule populated that allows all traffic to pass. Only change the default firewall rule if you want to restrict the type of traffic allowed. For example, you could change the firewall rule to only allow TCP/UDP traffic.

Note: Although the firewall is open on a default Access Portal installation, you cannot ping the IN interface. You can only ping the Admin interface. For more information, see [“Problem: You are unable to ping IN and OUT interfaces of Access Portal.”](#) on page 70.

To set up the Access Portal firewall rules:

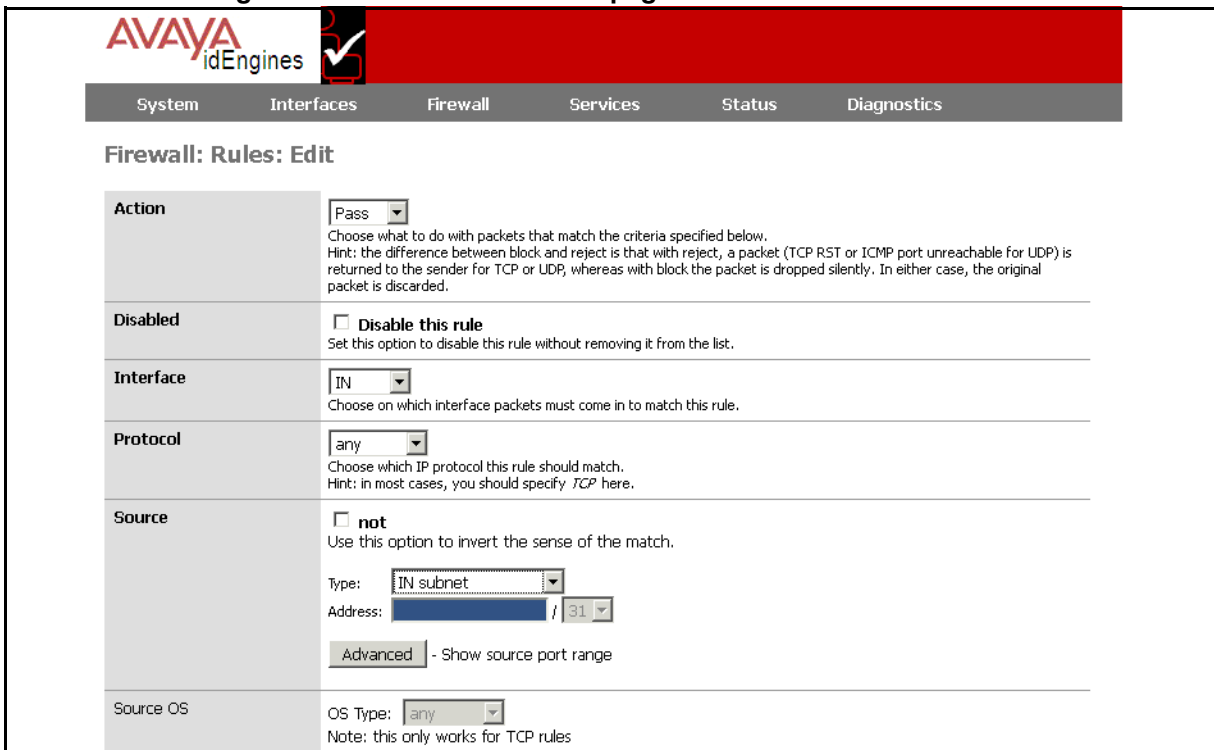
1. On the main Access Portal Administration Web UI page, click **Firewall > Rules**.
2. On the Firewall: Rules page, click the **IN** tab to select the IN port, and on the right of the table, table click the “**e**” button to edit the current rule. If no rule exists, click the “**+**” to create one.

Figure 28 Firewall > Rules > IN



3. On the **Firewall: Rules: Edit** page, clear the **Disable this rule** check box and ensure that the rule **Action** is set as **Pass**.
4. In the **Protocol** field, select the type of traffic to permit. Typically, this is TCP/UDP. The protocol choices are: TCP, UDP, TCP/UDP, ICMP, ESP, AH, GRE, IGMP, any, carp, and pfsync.
5. The **Source** field defines a filter that determines what traffic the IN port will accept. From the **Type** drop-down list, click **IN Subnet**.

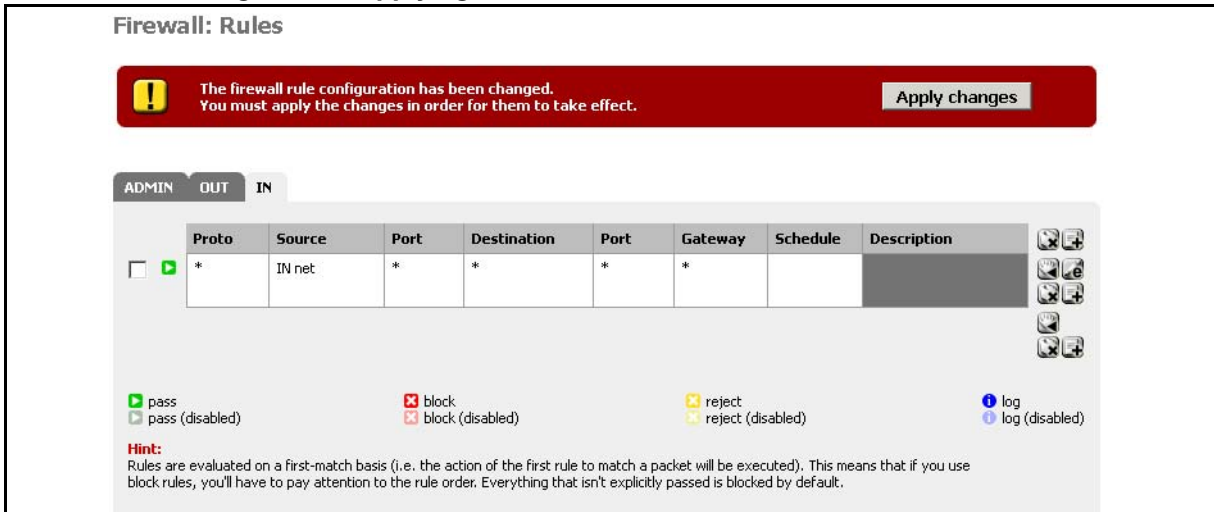
Figure 29 Firewall: rules: Edit page



6. Click **Save**. The Firewall: Rules page appears.

7. On the **Firewall: Rules** page, click **Apply changes**.

Figure 30 Applying the firewall rules



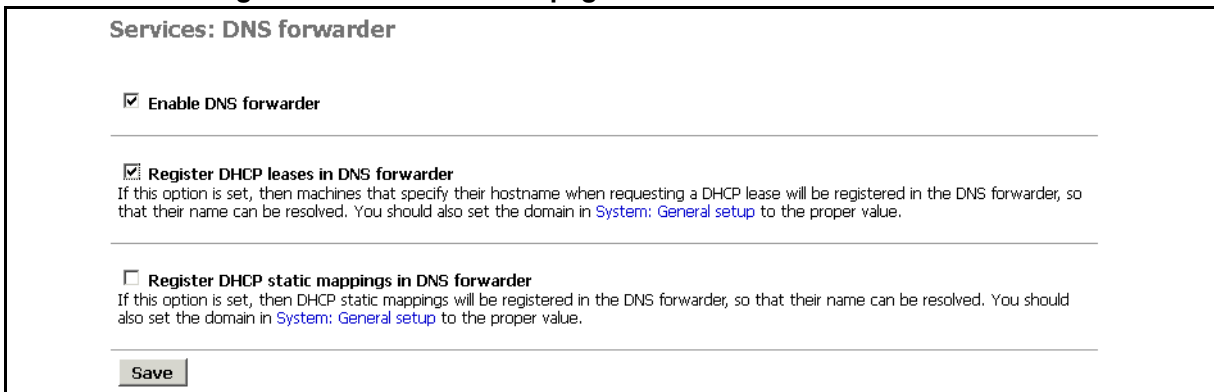
8. To apply the new or modified firewall rules to all captive portal sessions, existing in-line user sessions as well as new sessions, you must go to **Services > Captive Portal** and click **Save**.
Warning! Clicking Save causes all existing clients to disconnect.

Setting up the Access Portal's DNS forwarder

To set up the Access Portal's DNS forwarder:

1. On the main Access Portal Administration Web UI page, click **Services > DNS forwarder**. The DNS forwarder page appears.

Figure 31 DNS forwarder page



2. Select the **Enable DNS forwarder** check box.
3. Select the **Register DHCP leases in DNS forwarder** check box.
4. Click **Save**.

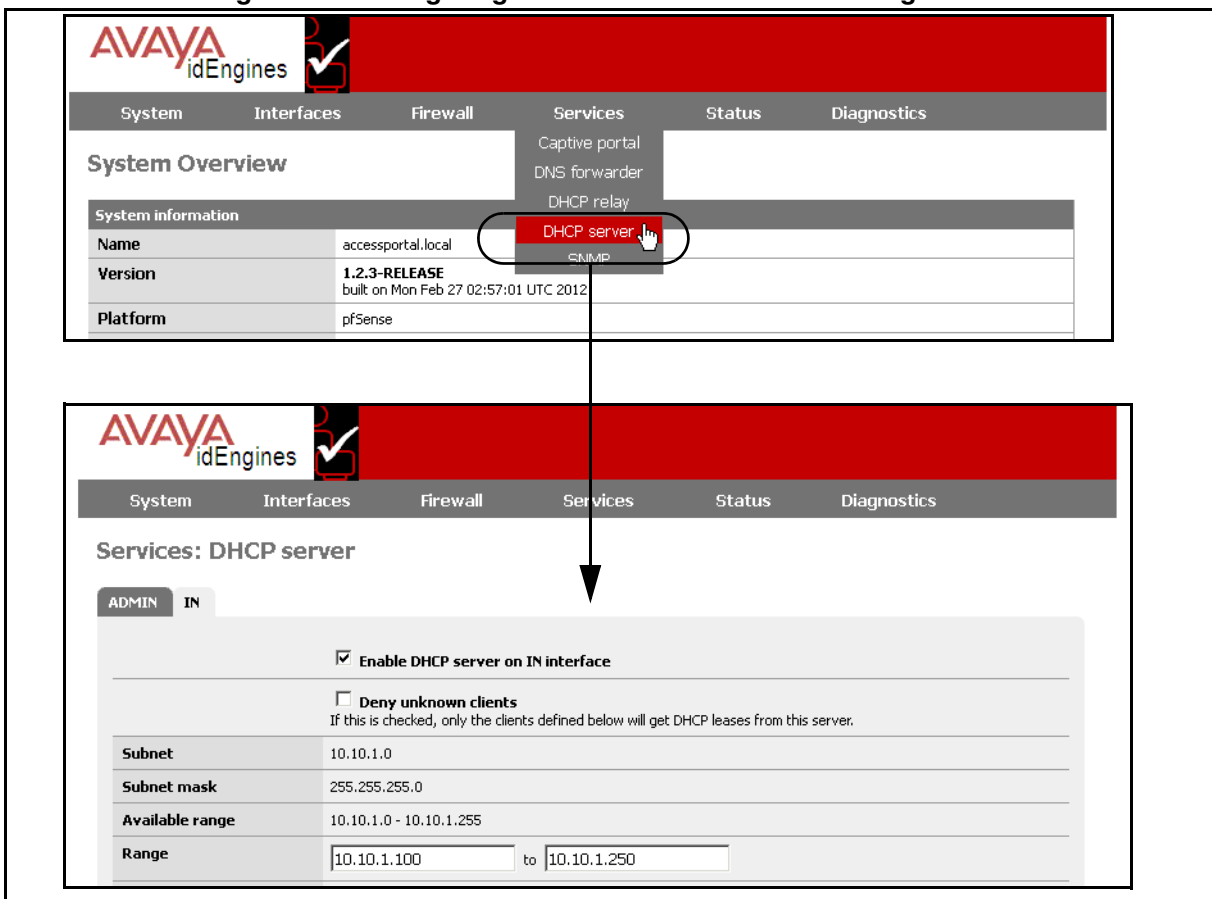
Configuring the Access Portal DHCP server settings

The Access Portal DHCP server settings allow the Ignition Portal to provide an IP address to each guest user device upon connection to the network. By default, the DHCP server is enabled on the IN interface. You can also configure Access Portal to use an external DHCP server.

To configure Access Portal to act as a DHCP server for the client network (default setting):

1. On the main Access Portal Administration Web UI page, click **Services > DHCP Server**.
2. On the Services: DHCP server page, click the **IN** tab.
3. Ensure that the **Enable DHCP Server on IN interface** check box is selected.
4. In the **Range** fields, set the range of IP addresses that the DHCP server will assign to guest devices.
5. Click **Save**.

Figure 32 Configuring the Access Portal DHCP settings



To configure Access Portal to use an external DHCP server:

1. On the main Access Portal Administration Web UI page, click **Services > DHCP Relay**.
2. On the Services: DHCP Relay page, click the **IN** tab.

Figure 33 Enabling DHCP relay

The screenshot shows the 'Services: DHCP Relay' configuration page. At the top, there are navigation tabs: System, Interfaces, Firewall, Services, Status, and Diagnostics. Below these, the 'Services: DHCP Relay' title is displayed. There are two tabs: 'ADMIN' and 'IN', with 'IN' being the active tab. The main configuration area contains the following elements:

- A checked checkbox labeled 'Enable DHCP relay on IN interface'.
- An unchecked checkbox labeled 'Append circuit ID and agent ID to requests' with a note: 'If this is checked, the DHCP relay will append the circuit ID (Avaya Identity Engine Access Portal interface number) and the agent ID to the DHCP request.'
- A 'Destination server' section containing:
 - An unchecked checkbox labeled 'Proxy requests to DHCP server on OUT subnet'.
 - A text input field for the destination server IP address.
 - A note: 'This is the IP address of the server to which the DHCP packet is relayed. Select "Proxy requests to DHCP server on OUT subnet" to relay DHCP packets to the server that was used on the OUT interface.'
- A 'Save' button at the bottom.

3. Select the **Enable DHCP relay on IN interface** check box.
4. In the Destination server section perform one of the following actions:
 - × If you want to relay DHCP packets to the server that was used on the WAN interface, select the **Proxy requests to DHCP server on WAN subnet** check box.
 - × If you do not want to relay DHCP packets to the server that was used on the WAN interface, enter the IP address of the server to which the DHCP packet is relayed.
5. Click **Save**.

Configuring the appliance's Access Portal settings

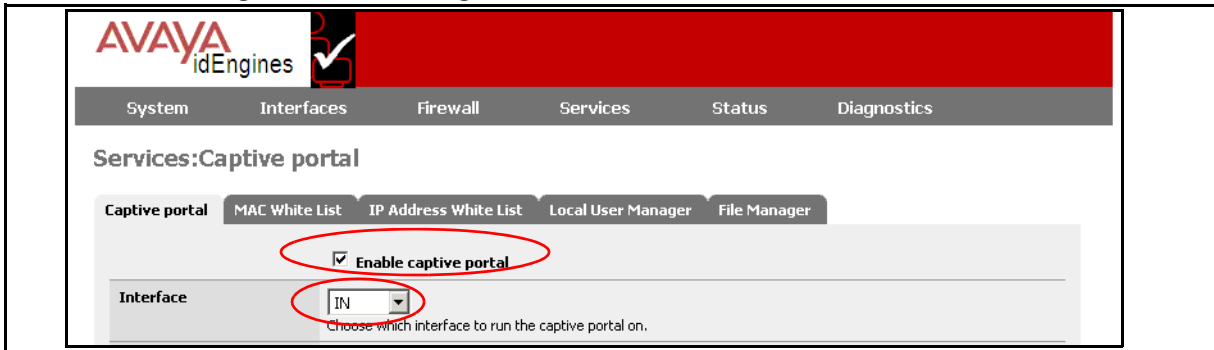
The Captive Portal settings determine how Access Portal authenticates guests and how it enforces their session timeouts.

1. On the main Access Portal Administration Web UI page, click **Services > Captive Portal** and click the **Captive Portal** tab. The Services: Captive portal page appears.

Warning: Changing any settings on this page will disconnect all clients!

2. On the Services: Captive portal page, do the following:
 - × Ensure that the **Enable captive portal** check box is selected.
 - × Ensure that the **Interface** field is set to **IN**.

Figure 34 Ensuring Access Portal is enabled and active on the IN interface



3. In the **Idle timeout** field, enter the maximum amount of time, in minutes, the client can sit idle before being disconnected.
4. In the **Hard timeout** field, enter the maximum length of the session, regardless of activity, in minutes.

Figure 35 Setting timeouts

Interface	IN Choose which interface to run the captive portal on.
Maximum concurrent connections	<input type="text"/> per client IP address (0 = no limit) This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Default is 4 connections per client IP address, with a total maximum of 16 connections.
Idle timeout	<input type="text"/> minutes Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout	60 minutes Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

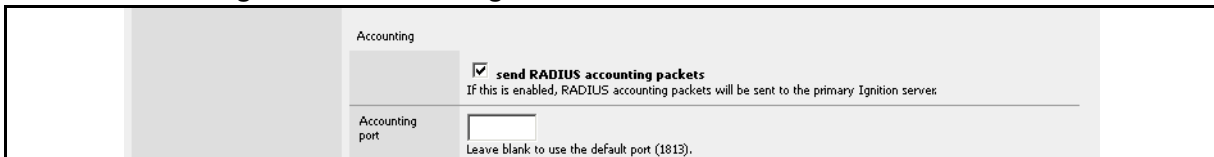
5. Scroll down to the **Authentication** section and do the following:
 - Select the **RADIUS authentication** radio button.
 - In the **First Ignition Server** section, in the **IP address** field, enter the IP address of the Ignition Server which users of the Access Portal have to authenticate against.
 - In the **Shared secret** field, enter the Ignition Server appliance Shared secret.

Figure 36 Setting Access Portal Authentication

Authentication	<input type="radio"/> No authentication <input type="radio"/> Local user manager <input checked="" type="radio"/> RADIUS authentication
First Ignition Server	IP address: 192.168.1.10 Enter the IP address of the Ignition Server which users of the captive portal have to authenticate against.
Port	<input type="text"/> Leave this field blank to use the default port (1812).
Shared secret	<input type="password"/> Leave this field blank to not use a RADIUS shared secret (not recommended).

- × In the **Accounting** section, ensure that the **Send RADIUS accounting packets** check box is selected.
- × **Note:** Access Portal only sends the following standard RADIUS attributes:
 - Calling and Called station IDs
 - Framed IP address
 - NAS port
 - NAS port type and
 - Certain RADIUS VSAs for device profiling functionality
- × **Note:** Access Portal does not process any outbound attributes that the Ignition Server sends.

Figure 37 Accounting section



Accounting

send RADIUS accounting packets
If this is enabled, RADIUS accounting packets will be sent to the primary Ignition server.

Accounting port
Leave blank to use the default port (1813).

- × Set up reauthentication to enforce the timeout of guest network sessions. (The session expiry periods are set in your Ignition Server authorization policy.) To set up reauthentication, in the **Reauthentication** section, ensure that the **Reauthenticate connected users every 60 seconds** check box is selected.
- × In the **Accounting updates** section, select the **Stop/start accounting** radio button.

Figure 38 Reauthentication and Accounting updates sections



Reauthentication

Reauthenticate connected users every 60 seconds
If reauthentication is enabled, Access-Requests will be sent to the Ignition server for each user that is logged in every minute. If an Access-Reject is received for a user, that user is disconnected from the captive portal immediately.

Accounting updates

no accounting updates

stop/start accounting

interim update

Note: There is an alternative to the reauthenticate-every-minute approach. You may instead set the timeout directly using an Ignition provisioning policy. To use that approach, leave the Reauthenticate every minute checkbox unchecked and create a provisioning policy that sends a RADIUS session timeout attribute value upon authentication of a guest. For instructions, see the chapter “Session Provisioning” in the *Ignition Server Administration Guide*.

6. Click **Save**.
Warning: Changing any settings on this page will disconnect all clients! Don't forget to enable the DHCP server on your captive portal

interface! Make sure that the default/maximum DHCP lease time is higher than the timeout entered on this page. Also, the DNS forwarder needs to be enabled for DNS lookups by unauthenticated clients to work.

Customizing user-visible pages

You can customize three user-visible pages: the login page, the success page, and the authentication error page. First, you create and upload the user-visible HTML pages, and then you select which login, success, and error pages Access Portal will display to users.

Creating customized user-visible pages

Use a text editor or HTML editor, to create customized user-visible pages.

Note: Your login page must include the PORTAL_ACTION login form shown in the example code in the **Portal page contents** section under **Services > Captive Portal**.

Figure 39 PORTAL_ACTION login form

****system default login page**** ▼

Upload an HTML file for the portal page here (leave blank to keep the current one). Make sure the file includes a form (POST to "\$PORTAL_ACTION\$") with a submit button (name="accept") and a hidden field with name="redirurl" and value="\$PORTAL_REDIRURL\$". Include the "auth_user" and "auth_pass" input fields if authentication is enabled, otherwise it will always fail. Example code for the form:

```
<form method="post" action="$PORTAL_ACTION$">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
  <input name="accept" type="submit" value="Continue">
</form>
```

Ensure that you save your customized pages in HTML format.

Uploading customized user-visible pages

After you save your customized pages in HTML format, you can upload the files into Access Portal. To load your customized HTML pages into Access Portal:

1. On the main Access Portal Administration Web UI page, click **Services > Captive Portal**, and click the **File Manager** tab. The window displays a table listing all the files that were previously uploaded.
2. Click the plus sign (+) to the right of the bottom row in the table.
3. Click the **Browse** button, navigate to the desired file, and click **Open**
4. Click **Upload** to load the file.
5. Repeat Step 2 and Step 4 for each file you want to upload.

If your customized HTML pages require supporting image files and Cascading Style Sheets (CSS) files, you can upload them using the above procedure.

Note: Any files that you upload here will be made available in the root directory of the captive portal HTTP(S) server. You can reference them directly from your portal page HTML code using relative paths. Example: You uploaded an image with the name “test.jpg” using the file manager. Then you can include it in your portal page like this:

```

```

You can also upload .php files for execution. You can pass the filename to your custom page from the initial page by using text similar to:

```
<a href="/aup.php?redirurl=$PORTAL_REDURL$" > Acceptable usage policy</a>
```

The total size limit for all files is 256 KB. If your file size is larger than 256KB, use the **Upload Big Files** interface on the File Manager page to upload the large files.

Note: The files you upload using the **Upload Big Files** interface, will not be backed up. Use the interface above the **Upload Big Files** interface to upload files under 256KB.

Selecting the Access Portal Login page

To select the Access Portal login page:

1. On the main Access Portal Administration Web UI page, click **Services > Captive Portal**.
2. Scroll down to the **Portal page contents** section.
3. From the drop-down list, select the HTML file you want to use for your login page.
4. Click **Save**. portal page appears.

Warning: Changing any settings on this page will disconnect all clients!

Setting up the Success page

To set up the Success page:

1. On the main Access Portal Administration Web UI page, click **Services > Captive Portal**.
2. Scroll down to the **Success Page** section.

Figure 40 Success page

3. Perform one of the following actions to specify which URL to direct the client to after the client authenticates:
 - × If, after clients authenticate, you want to direct them to the URL they initially tried to access, select the **Originally Accessed Page** radio button.
 - × If, after clients authenticate, you want to direct them to an URL on this portal, select the **A URL on this portal** radio button, and specify the URL in the field below.
4. From the drop-down list, perform one of the following actions:
 - × To use your customized Success page, select the HTML file you want to use. The guest user will see this page upon successful authentication.
 - × To redirect clients, after they have authenticated, to an URL other than the one they initially tried to access, click **On Other Servers: Specify URL below**, and specify the URL in the field below.
5. Click **Save**.

Warning: Changing any settings on this page will disconnect all clients!

Note: If a CASE package is deployed on Access Portal, the CASE application will provide its own success page.

Selecting the Authentication error page contents

To select the Authentication error page contents:

1. On the main Access Portal Administration Web UI page, click **Services > Captive Portal**.
2. Scroll down to the **Authentication error page contents** section.
3. From the drop-down list, select the HTML file you want to use for your authentication failure page. The guest user will see this page if his or her authentication attempt fails.
4. Click **Save**.

Warning: Changing any settings on this page will disconnect all clients!

Providing access to servers or other computers from a client machine

Normally, when Access Portal deploys, a client machine on the IN network issues an HTTP request, Access Portal captures this request and displays the Access Portal login page, if that client machine is not already authenticated through the portal.

However, in certain situations, you may want to let clients access some servers even before they authenticate. For example, you might want to allow access to Guest Manager from client machines before authenticating with Access portal. The guests can first access Guest Manager's self provisioning portal to register themselves and get a temporary username and password. Guests can then log in to Access Portal with those credentials.

To allow this kind of access before Access Portal authentication, add the IP address of your server (Guest Manager in this use case) to IP White List.

To add an IP address to the IP White List:

- Go to **Services > Captive Portal** and click the **IP white List** tab.

Warning: Changing any settings on this page will disconnect all clients!

Backing up and restoring Access Portal

This section explains how to back up and restore Access Portal.

Introduction to backing up and restoring Access Portal

You can save your Access Portal configuration to a backup file and later restore the configuration by loading the saved file. Having a backup file ensures you can recover from accidental data loss or administrator error. You can also use backup files to set up a replacement Access Portal or to upgrade to a newer version of Access Portal.

Access Portal allows you to backup and restore the entire configuration or parts of the configuration. The backup and restore areas include:

- Aliases
- Firewall Rules
- NAT
- Captive Portal
- Interfaces
- DHCP Server
- Syslog

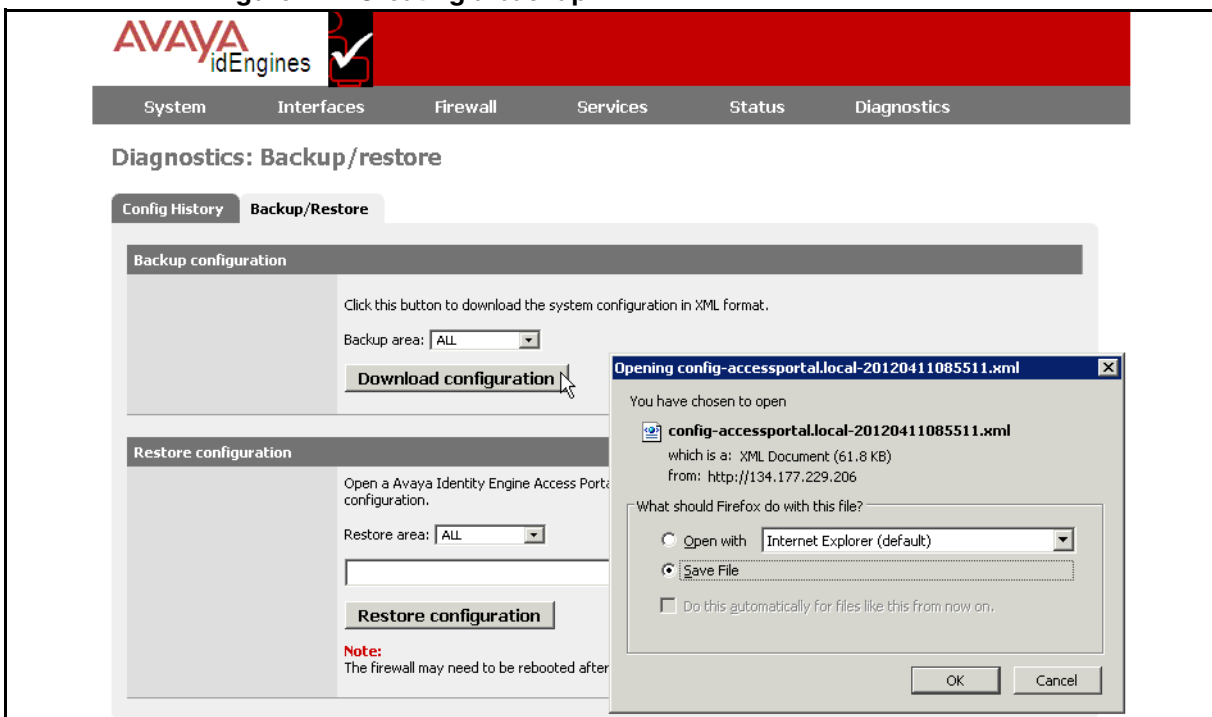
- System
- or ALL

Creating a backup

To create a backup of the data on your Access Portal:

1. On the main Access Portal Administration Web UI page, click **Diagnostics > Backup/Restore**.
2. Under the Backup configuration section, in the **Backup area** drop-down list, choose the configuration areas you want to back up. Choose **ALL** to back up the entire configuration.
3. Click **Download configuration**. The browser prompts you to open or save the file.

Figure 41 Creating a backup



4. Select the **Save File** radio button and click **OK**.
5. Browse to the desired location on your computer, and click **Save**.

Restoring from a backup file

When you perform a restore on Access Portal, the restoration process overwrites the configuration on the Access Portal. Access Portal allows you to restore the entire configuration or parts of the configuration.

Admin interface IP address WARNING:

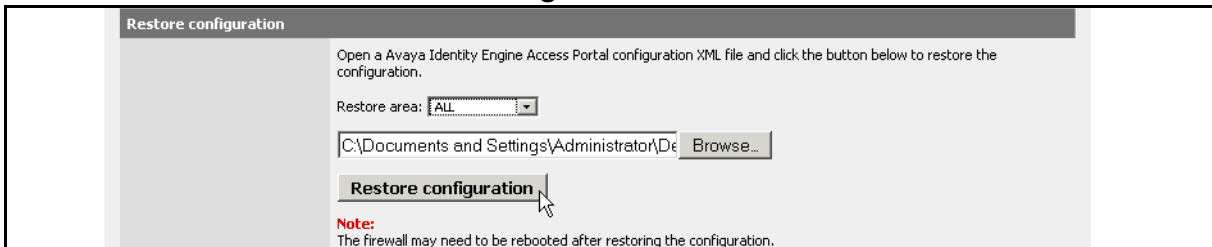
When restoring from a backup file, if you choose **All** to restore the entire configuration or if you choose **interfaces** to restore the interfaces configuration, your Admin port IP address and other network settings are set to the settings from the backup file. Make sure that you know which IP address the ADMIN interface is going to use. If the IP address is different from the current ADMIN IP, the Access Portal Administration Web UI will no longer be able to function. You will have to point your browser to the new ADMIN IP address.

Admin password WARNING:

If your backed up configuration contains an admin password that is different from the current password, after restoring, you may have to login again with the new password.

To restore your Access Portal from a backup file:

1. On the main Access Portal Administration Web UI page, click **Diagnostics > Backup/Restore**.
2. Under the Restore configuration section, in the **Restore area** drop-down list, choose the configuration areas you want to restore. Choose **ALL** to restore the entire configuration.
3. Click **Browse** to specify the path and filename for the backup file from which you are restoring the data, and select the file.
4. Click **Restore Configuration**.



Note: Access Portal may need to reboot the firewall after restoring the configuration.

5. Admin port IP address: If you chose **All** to restore the entire configuration or if you chose **interfaces** to restore the interfaces configuration in [Step 2](#), then the backup file contains an IP address assignment for the Admin Port. The restoration process applies this IP address to the Admin Port of the virtual appliance that you are restoring. If the Admin IP changes when restoring from a backed up configuration, you must reconnect to the Administration Web UI on the new ADMIN IP interface. If the admin password in the backed up configuration is different from the default admin/admin, you must use the new password to connect to the Administration Web UI after restoration.

Upgrading Access Portal

Access Portal does not support an in-line upgrade. The only way to upgrade is to deploy a new OVF and restore the new OVF with the configuration backed up from the earlier version of the Portal OVF.

To upgrade Access Portal to the latest version:

1. Create a backup of the existing configuration. See [“Creating a backup” on page 46](#).
2. Make a note of the admin IP address and netmask. You will assign this to the new OVF.
3. Shut down this instance of Access Portal either through the Access Portal Administration Web UI (**Diagnostics > Halt System**) or through the console option 4.
4. Install a fresh OVF. See [“Installing the Access Portal virtualization appliance” on page 22](#).
5. Use the console to assign the admin IP address that you noted in [Step 2](#).
6. Point to the URL `http://<admin ip>>` and use username: **admin** and Password: **admin** to log in.
7. Restore the backed up configuration. See [“Restoring from a backup file” on page 46](#).
8. After the restore, you must use the password that was in effect when you took the backup of the configuration to log in to the Access Portal Administration Web UI at `http://<<admin ip>>`.

Configuring the Ignition Server

This chapter explains how to configure the Ignition Server to work with the Access Portal and how to configure and test user access.

Configuring the Ignition Server to work with the Access Portal

Now that you have finished configuring your Access Portal, you must set up the Ignition Server to work with the Access Portal.

Make sure your Ignition Server is running and accessible on the network. Run Dashboard and configure as shown in the steps below. Note that this is a basic configuration that assumes you will store the guest user accounts locally, on the Ignition Server appliance.

Activating the Access Portal license

Access Portal is a licensed feature. You must activate the Access Portal license to enable this feature.

Note: The Access Portal license must match the level of the Ignition Server base license: LARGE, SMALL, or LITE. You can deploy multiple Access Portals under the same single license.

To activate the Access Portal license:

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Click the **Licenses** tab.
3. Click **Install**.
4. Find the Access Portal license you received from support and open it in your e-mail tool or text editor. Highlight and copy the text of your license. Copy the whole license including “BEGIN IGNITION LICENSE CERTIFICATE” and “END IGNITION LICENSE CERTIFICATE”.
5. Return to the License Installation window of Dashboard and click **Paste** to paste the license text there. Click **OK**.

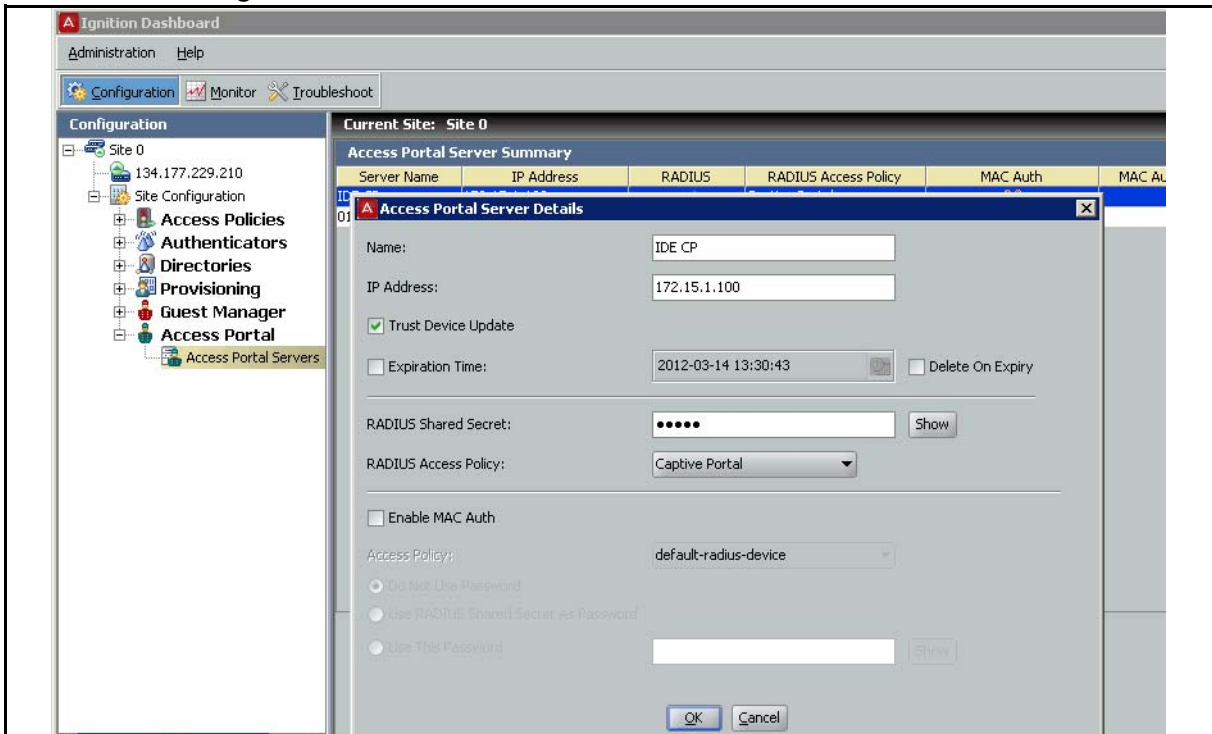
After you activate the license, an Access Portal node appears under Site Configuration.

Configuring Access Portal server details

After you activate the Access Portal license, you can configure the Access Portal server details. This procedure registers the Access Portal as an authenticator in the Ignition server.

1. In the Dashboard **Configuration** tree, expand the **Access Portal** node, and click on **Access Portal Servers**.
2. Click **New**. The Access Portal Server Details window appears.

Figure 42 Access Portal Server Details window



3. In the **Access Portal Server Details** window, specify the following:
 - × **Name:** Enter a name for the Access Portal.
 - × **IP Address:** Enter the IP address of the Access Portal. Ensure that you enter the IP address of the ADMIN interface. Also make sure that Access Portal's ADMIN interface is reachable from the Ignition Server.
 - × **Trust Device Update:** Select this check box if you want to use this Access Portal Server for device learning or automatic registration of devices. **Note:** If you select this check box, you must go to the Access Portal Administration Web UI, click **Services > Captive Portal**, and select the **Enable Device Fingerprinting** check box.
 - × **Expiration Time:** Select this check box if you want to specify an expiry date for the devices learned through Access Portal. Click the clock-

and-calendar icon and use the arrow keys to set the date and time it expires. Click outside the clock and calendar dialog to close it.

- × **Delete On Expiry:** Select this check box if you want the Ignition Server to delete learned devices after the expiry date.
- × **RADIUS Shared Secret:** Enter the **Shared Secret** that you configured for RADIUS server in [“Configuring the appliance’s Access Portal settings” on page 39](#).
- × **RADIUS Access Policy:** The RADIUS access is enabled by default. Select the Ignition Server access policy that regulates RADIUS access requests relayed by Access Portal. If you do not select an access policy, Access Portal uses the default access policy (default-radius-user).
- × **Enable MAC Auth:** Select this check box to provide authentication based on the MAC address of the device that is trying to connect. See [“Introduction to MAC authentication” on page 53](#) and [“Setting up MAC authentication on Access Portal” on page 54](#) for information on setting up MAC authentication on Access Portal.

4. Click **OK**. The Access Portal Server Summary page appears.

Figure 43 Access Portal Server Summary



Editing Access Portal server details

You can edit the details of the Access Portal server from the Access Portal Server Summary page.

1. In the Dashboard **Configuration** tree, expand the **Access Portal** node, and click on **Access Portal Servers**. A list of Access Portals appears.
2. From the list of Access Portals, click on the Access Portal you want to edit.
3. Click **Edit**, and make the required changes.
4. Click **OK**.

Introduction to device profiling

With Bring Your Own Device (BYOD) to work becoming a common scenario in the Enterprise, Enterprise IT needs to support all the unmanaged and untrusted “smart” devices trying to access the enterprise network. The Avaya Identity Engines Ignition Server (AIEIS) Device Profiling feature addresses this need.

Device Profiling works on a Device Fingerprint which is a compact summary of software and hardware settings collected from a client device. In the AIEIS environment, Device Profiling is used as an automated way to register the devices with the Identity Engines Internal Store.

A user trying to gain network access using a personal or unmanaged device is transitioned to an Access Portal where the portal profiles the device i.e. learns the necessary device attributes like device type, sub type, operating system, and version and updates the Ignition Server with the device information.

Device profiling allows administrators to write policies based not only on the user that is attempting to connect, but also on the type of device that is being used to connect to the network. The administrator can define policies based on the device attributes, for example, setting bandwidth limitation based on the type of device, allowing laptops to have unlimited access while iPads would not, and setting application-specific QoS, such as allowing only Internet and email access for mobile devices.

To set up device profiling:

1. From Dashboard, configure Access Portal as an authenticator as a trusted source to learn the devices. See [“Configuring Access Portal server details” on page 50](#). When specifying Access Portal Server details, select the **Trust Device Update** checkbox.
2. From the Access Portal Administration Web UI, click **Services > Captive Portal** and select the **Enable Device Fingerprinting** check box.

Note: Either enable Trust Device Update on the Ignition Server and Device Fingerprinting on Access Portal, or disable both, as a mismatch can result in unintended updates to the device records.

Note: Device Profiling can work with MAC Authentication. If you want device profiling to work with MAC Authentication, you must first add the device to the internal store, see [“Creating a device record” on page 57](#). You can add the device by just specifying the MAC address, and not specifying any other device attributes. When the user tries to login through Access Portal using that device, Identity Engines will update the other device record attributes such as device type, sub type, OS etc.

Introduction to MAC authentication

MAC authentication, or MAC address checking, verifies that the MAC address submitted by a connecting client device matches an entry on your list of known MAC addresses. Based on your policies, Ignition Server allows the device to connect to your network (and optionally assigns it to a VLAN) or rejects the device. The list of known MAC addresses is stored in the Ignition Server internal data store (you cannot use an LDAP or AD store for this).

MAC authentication is typically employed on 802.1X-authenticated networks as an 802.1X bypass mechanism for devices that are incapable of performing 802.1X authentication. For example, if your environment contains printers that cannot authenticate via 802.1X, you can set Ignition Server to allow those devices to connect without performing an 802.1X authentication and to place them on an appropriate, limited-access VLAN.

To enforce MAC authentication, create device records that specify your set of allowed MAC addresses, and “MAC Auth” rules in Ignition Server that determine which devices are allowed to connect, as well as where and how they are allowed to connect. Typically, these rules also force the device onto the appropriate VLAN.

Note: Do not confuse MAC authentication with Windows machine authentication and asset correlation, which uses Windows machine authentication. See “Introduction to Windows Machine Authentication” in the *Ignition Server Administration Guide* for details.



Warning: Allowing MAC Authentication Can Reduce Network Security

Using MAC authentication incorrectly can reduce the overall security of your network. When you activate MAC authentication on an authenticator along with one or more 802.1X authentication methods, the default behavior of most switches means that, even though you have specified 802.1X authentication, the typical switch attempts MAC authentication if the 802.1X user authentication fails. As a result, an ill-intentioned user can exploit the weakness of the less secure MAC authentication to bypass the 802.1X authentication.

In some cases, MAC authentication can be less secure than 802.1X user authentication if it is configured to use only the client device’s MAC address as the credential (instead of using a shared secret as a password). In such a case, if an ill-intentioned user acquires the MAC address of one of your allowed devices, he can pass that MAC address in his access request and gain access to the resources that your policy lists as available via MAC Auth in the applicable access policy.

Avaya recommends you take the following precautions: **First**, for switches that support per-port configuration of MAC authentication, you should enable MAC authentication on only those ports that require it, such as ports to which printers and other non-802.1X-compliant devices connect. **Second**, you should place all MAC- authenticated devices on a limited-access VLAN, as explained in the sections that follow.

Setting up MAC authentication on Access Portal

This section shows you how to set up MAC authentication on Access Portal. The required steps are:

- [“Creating a MAC-Auth policy” on page 54](#)
- [“Configuring the Access Portal Server Details to support MAC Auth” on page 56](#)
- [“Creating a device record” on page 57](#)
- [“Editing the device template to support MAC authentication” on page 59](#)
- [“Enabling RADIUS MAC authentication on Access Portal” on page 60](#)

Creating a MAC-Auth policy

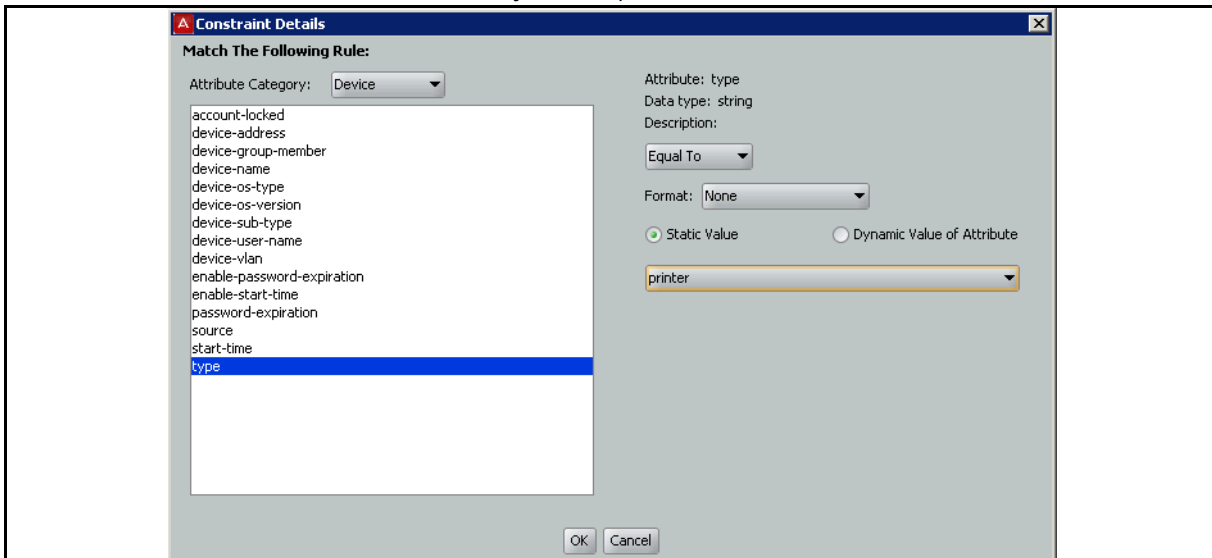
This procedure shows you how to write a device authorization policy for client devices such as laptops and printers. We refer to these policies as “MAC-Auth policies.” The MAC-Auth policy identifies each device by means of its MAC address and authorizes it appropriately.

Important! Do not include any outbound attributes for the Access Portal MAC-Auth policy. Access Portal cannot process any outbound values that the Ignition server sends.

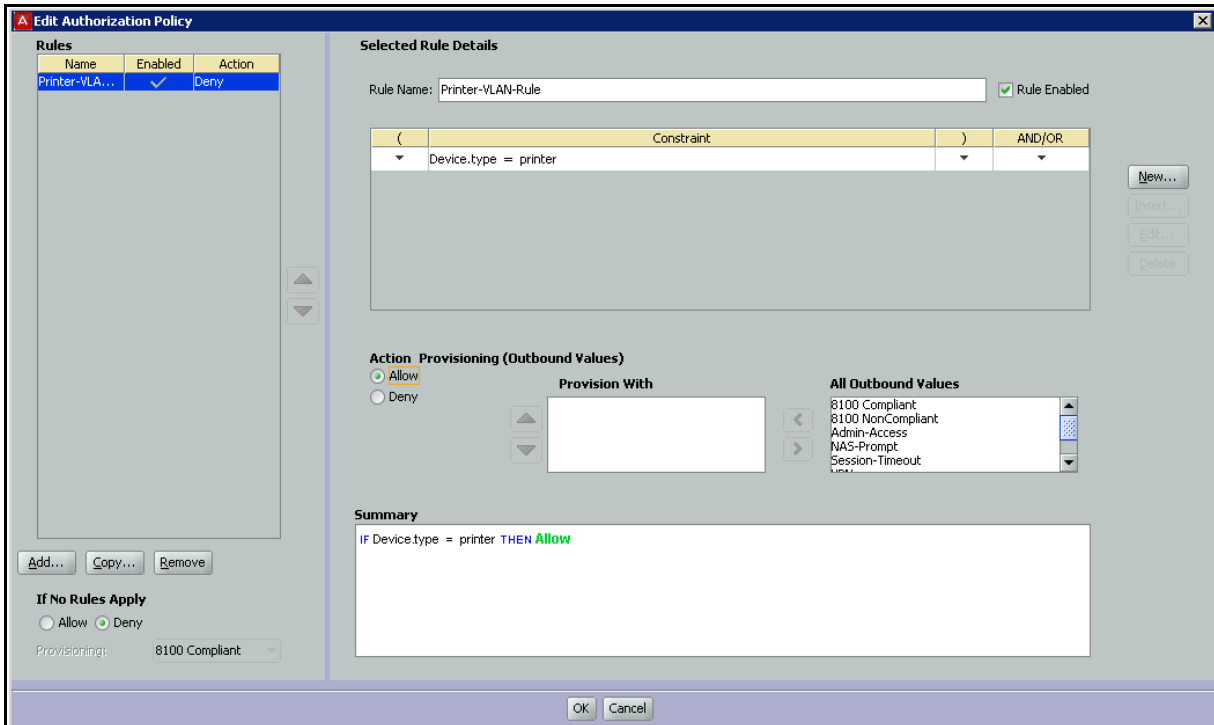
1. In the Configuration tree, expand **Access Policies**.
2. Expand **MAC Auth**.
3. Click **New**. (**Note:** You can edit an existing policy by clicking its name in the **Configuration** tree and clicking the **Edit** button on the right side of the window.)
4. Enter a name for the policy and click **OK**.
5. Click the policy name in the tree and click **Edit** on the right side of the window.
6. In the Edit Authorization Policy window, set up a MAC-Auth policy just as you would a RADIUS user authorization policy. For information on using that window, see “Creating a RADIUS User Authorization Policy” *Ignition Server Administration Guide* for details.

Typically, your MAC-Auth rules will evaluate attributes of the connecting device. To set up a MAC Auth rule:

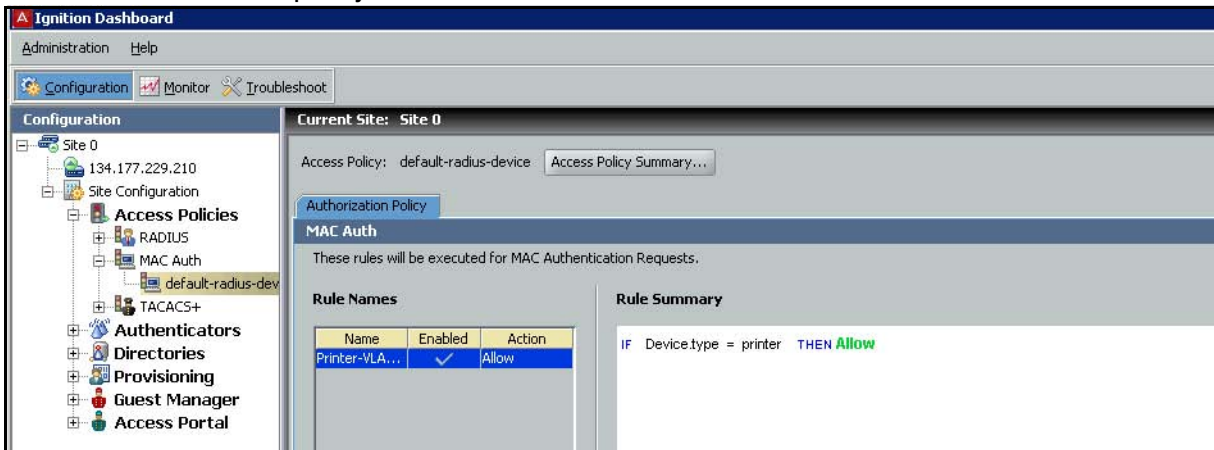
- × In the Edit Authorization Policy window, click the **Add** button below the **Rules** list.
- × In the New Rule dialog, give the rule a name and click **OK**. For example, you might call the rule, “Printer-VLAN-Rule”,
- × In the Edit Authorization Policy window, in the Selected Rule details section, click **New** to add a constraint. (You can add as many constraints as you like.)



- × In the Constraint Details window, go to the **Attribute Category** drop-down list and click **Device**. In the list below this, choose **type**. In the drop-down list on the right, click **Equal To**. Select the **Static Value** check box. In the drop-down list below this, click **printer**. Click **OK**.
- × In the Edit Authorization Policy window, with your “Printer-VLAN-Rule” still selected, under **Action** select the **Allow** radio button. Click **OK**.



Your policy has been saved.



If your situation requires that your rules evaluate more detailed information, you can store and evaluate additional device information as shown in “Device Virtual Attributes” in the *Ignition Server Administration Guide*.

Configuring the Access Portal Server Details to support MAC Auth

Configure the Access Portal Server Details to support MAC authentication. These settings tell Ignition Server that Access Portal relays MAC authentication requests from devices to the Ignition Server RADIUS service.

To configure the Access Portal Server Details to support MAC authentication.

1. In the Dashboard **Configuration** tree, expand the **Access Portal** node, and click on **Access Portal Servers**. Create or edit the Access Portal Server Details:
 - × To create a new Access Portal entry, click **New**.
 - × To edit an existing Access Portal entry, from the list of Access Portals, click on the Access Portal you want to edit and click **Edit**.
2. Use the **Access Portal Server Details** window to make these settings:
 - × Select the **Enable MAC Auth** check box.
 - × In the Access Policy drop-down list, click the name of the MAC Auth policy you set up in [“Creating a MAC-Auth policy” on page 54](#).
 - × Specify how the authenticator password should be checked.
Caution: Do not select the **Do not use password** check box. Access Portal requires a password. To use the authenticator’s shared secret as the password, select the **Use authenticator’s shared secret as password** check box. To specify a password, select the **Use this password** check box, and type the password in the text field.
3. Click **OK**.

Creating a device record

Create a device record for each device allowed to connect to the network. Each device record is a record of a known MAC address. These records are stored in the Ignition Server internal data store; you cannot retrieve device information from an external store. (If you need to create many device definitions, you may prefer to create them in bulk as shown in “Importing Device Records” in the *Ignition Server Administration Guide*.)

To create a device record in Ignition:

1. In Dashboard's Configuration hierarchy tree, click your site, expand Site Configuration, expand **Directories**, expand **Internal Store**, and click **Internal Devices**. Click **New**.

Figure 44 Creating a device record

The screenshot shows the 'New Device Record' form. The 'Info' section includes the following fields and options:

- MAC Address: [Text input field]
- Name: [Text input field]
- Type: [Dropdown menu]
- Sub Type: [Dropdown menu]
- Operating System: [Dropdown menu]
- Source: [Text input field]
- VLAN Label: [Text input field]
- VLAN ID: [Text input field, value: 0]
- Start Time: [Date/Time picker, value: 2012-03-29 07:25:28]
- Expiration Time: [Date/Time picker, value: 2013-03-29 07:25:28]
- Record Disabled: [Check box]
- Delete on Expire: [Check box]
- User Name: [Text input field]

The 'Custom Attributes' section includes six text input fields labeled custom 1 through custom 6. At the bottom, there are 'Groups' and 'Users' tabs, and a dropdown menu for 'Internal Group Name'.

2. In the **MAC Address** field, specify the MAC address of the device. Enter the address as a string of six octets. You may write the twelve characters without separators, or you may separate the octets with period, colon, or hyphen characters. Do not mix separator characters.
3. If you want to disallow this device from connecting to the network, select the **Record Disabled** check box.
4. In the **Name** field, type a name for the device. This name identifies the device in logs and when you associate it with a group or user.
5. If you want Ignition Server to delete this record automatically after its expiration date, select the **Delete on Expire** check box. Ignition Server checks hourly for device records in the internal store that have been expired for at least one week. Upon finding such an expired record, Ignition Server checks its **Enable Auto Deletion** setting, and, if the record is set for automatic deletion, deletes it. Deletions take place as time permits. For large sets of records, deletions are spread over a period of hours. Each deletion is logged in the Ignition Server logs.
6. In the **Type** drop-down list, designate what sort of device this is, such as a laptop, printer, or handheld device. You can choose one of the preset values or type your own value.
7. In the **Sub Type** drop-down list, define the details of the device from one of the preset values. For example, if you chose **mobile** as your device **Type**, you can define the **Sub Type** as iphone, blackberry, or android phone etc.

8. In the **Operating System** drop-down list, select the operating system of the device. You can choose one of the preset values.
9. In the **Operating System Version** field, enter the version of the operating system.
10. In the **User Name** field, enter the name of the user of this device.
11. The **Source** field is typically used only for bulk-imported device records (see “Importing Device Records” in the *Ignition Server Administration Guide*). The **Source** indicates the origin of this record. Usually this is the name of the file from which the device record was imported.
12. If you want to have Ignition Server automatically assign this device to a VLAN, enter the VLAN name in the **VLAN Label** field and enter the integer VLAN number in the **VLAN ID** field. If you do not want to assign it to a VLAN, leave these fields blank.
13. Select the **Start Time** check box if you want to specify when the account is to be activated. Click the clock-and-calendar icon and use the arrow keys to set the date and time to enable the account. Click outside the clock and calendar dialog to close it.
14. Select the **Expiration Time** check box if you want to specify an expiry date for the device record. Click the clock-and-calendar icon and use the arrow keys to set the date and time it expires. Click outside the clock and calendar dialog to close it. When an account expires, Ignition Server may delete it, depending on the **Delete on Expire** setting. (See above.)
15. The **Custom Attributes** fields allow you to record additional information about the device. See “Adding Virtual Attributes for Devices” in the *Ignition Server Administration Guide*.
16. Click **Save** to store the device record.

Editing the device template to support MAC authentication

Ensure that the default device template you are using points to “generic-default”. Or, if you are using the “generic-avaya” device template, ensure that your MAC Address Source is not set to “Inbound-Calling-Station-Id”. If your MAC Address Source is set to “Inbound-Calling-Station-Id”, change the MAC Address Source to “Inbound-User-Name” to ensure that MAC address recognition will work.

To change the MAC Address source field to “Inbound-User-Name”:

1. In the Dashboard **Configuration** tree, expand the **Site Configuration** node, expand the **Provisioning** node, and click **Vendors/VSAs**.
2. In the **Vendors** panel, double-click **Avaya** and then click **Device Templates** to display the list of templates.

3. In the list on the right, select **generic-Avaya** and click **Edit**. The Edit Device Template window appears.
4. Click **Edit**. The Edit Device Template Details window appears.
5. From the **MAC Address Source field**, select **Inbound-User-Name**.
6. Click **OK** and then click **Done**.

Enabling RADIUS MAC authentication on Access Portal

After you set up MAC authentication on Access Portal using Dashboard, you must enable RADIUS MAC authentication on Access Portal using the Access Portal Administration Web UI page.

To enable RADIUS MAC authentication on Access Portal:

1. On the main Access Portal Administration Web UI page, click **Services > Captive Portal** and scroll down to the **Authentication** section.
2. In the **RADIUS MAC authentication** section:
 - × Select the **Enable RADIUS MAC authentication** check box.
 - × In the **Shared secret** field, enter the Ignition Server shared secret.
3. Click **Save**

Setting up the guest access policy in the Ignition server

Your guest access policy determines how, when, and where guests can connect to your network, and what sections of your network they can use. If you will use Ignition Guest Manager to create guest user accounts, consult the *Ignition Guest Manager Configuration Guide*, and read the chapter, “Setting Guest Access Policies” for instructions.

To create a basic guest access policy, perform the following tasks in Dashboard:

1. Set up your guest user access policy in the Access Policy panel. In the **Configuration hierarchy** tree, expand the **Access Policy** node, expand **RADIUS**, and click **New** (or, if you wish to edit an existing policy, click its name in the tree).
2. Set your tunnel policies. In the **Access Policy** window, click the **Authentication Policy** tab, and click **Edit**. In the **Authentication Protocols window**, make your tunnel settings. Ensure that you select **PAP** under **None**.
3. Set your identity routing policy to enable the Ignition Server to find guest user accounts in the Ignition Server embedded user store. To edit this policy, in the **Access Policy** window, click the **Identity Routing** tab and click **Edit**.

-
- × If you already have an identity routing policy that you wish to use, add the Directory Set, “**default set**” to your policy, and click **OK** to save the policy. Proceed to Step 4.
 - × If you wish to create a new identity routing policy, do the following:
 - In the Identity Routing Policy window, click **New**.
 - In the Realm-Directory Set Map window set the Ignition Server to use the embedded user store (or any other target directory): in the Match Realm section, select **Realm Not Specified**; in the Directory Set section, select **default set** (or any other target set that you wish to use); and in the Match Authenticator Container section, select **Disable Authenticator Container Matching**. Click **OK**.
 - In the Identity Routing Policy window, select the **Enable Default Directory Set** check box and select **default set** as the Directory Set. Click **OK**.
4. Set up your authorization rules. During user log-in, the Ignition Server checks the user’s credentials (e.g., password) to authenticate him or her, and if authentication succeeds, the Ignition Server evaluates the authorization rules before it grants access.

The example steps below create an authentication-only rule so that authentication alone is sufficient to gain access. (If you wish to add rules that enforce your company’s network access policy, see the chapter, “User Authorization Policy” in the *Ignition Server Administration Guide*.)

To create a basic authorization policy, perform the following tasks:

- × In the **Access Policy** window, click the **Authorization Policy** tab.
- × In the RADIUS Authorization Policy section of the window, click **Edit**.
- × In the Rules section, click **Add**.
- × In the New Rule window, type the name “allow-all” and click **OK**.
- × With your rule selected, go to the buttons to the right of the Constraint list and click **New**.
- × In the Attribute Category drop-down list, select the attribute category, **System**. In response, the list shows all the attributes for System. In the list, select the attribute **True**.
- × Click **OK** to close the Constraint Details window and return to the Edit Authorization Policy window.
- × In the Action part of the Edit Authorization Policy window, click **Allow**, and click **OK**.

Registering authenticators that provide regular user access in the Ignition Server

A typical Access Portal deployment runs on the same equipment as the Ignition deployment that authenticates your regular users (for example, your employees). Make sure that your regular user access is configured in Ignition as well.

Wired access for non-guest users

Make sure that regular user access is configured on the wired switch. This is typically the same switch that you will configure for guest user access in [“Configuring guest access on the wired switch” on page 62](#).

Configure your wired switches as authenticators in the Ignition Server, setting each to require 802.1X authentication. If authentication fails, the user will be mapped to the authentication VLAN network that you will create later in this procedure.

Wireless access for non-guest users

Make sure that regular user access is configured on your wireless access points (APs). While this set may include the AP that you will configure for guest user access in [“Configuring wireless guest access” on page 64](#), note that you will not configure the guest SSID for regular users. The SSID that you configure for guest access is a wide-open SSID. For all other SSIDs, configure 802.1X authentication as usual on the Ignition Server appliance. (See the *Ignition Server Administration Guide*.)

Now that you have created your guest and non-guest access policies, your Ignition Server configuration is complete. For further instructions, consult the *Ignition Server Administration Guide* and the *Ignition Guest Manager Configuration Guide*.

Configuring guest access on the wired switch

Cabling the wired switch

On the wired switch that will support guest user connections, make the following cable connections. These steps provide examples based on an Avaya Ethernet Routing Switch 5520.

1. Connect the Ignition server appliance to the network. For example, connect the Ignition server appliance's Service Port A to port 1/7 of the Avaya Ethernet Routing Switch 5520.
2. Connect the switch to the IN port of the Access Portal appliance. For example, connect switch port 1/11 to the IN port of the Access Portal.
3. Connect the Access Portal to the firewall that will provide an Internet connection for guest users. For example, you might connect the Access Portal WAN port to the WAN1 port of a Fortinet firewall.

4. To provide wireless guest access, connect the wired switch to your guest-accessible wireless access point (AP). For example, connect switch port 0/1 to the AP's IN port. This will be an 802.1Q trunk connection.

Configuring VLANs on the wired switch

At a minimum, you need two VLANs to support Access Portal-based authentication:

- A **restricted-reach VLAN** that connects only the guest-accessible wired switches, the guest-accessible wireless access points, and the IN port on the Access Portal. (Note: You set the IP address of the Access Portal IN port in this section: [“Setting up the Access Portal IN port” on page 34.](#))
- One or more **authenticated-access VLANs** that provide the level of access you wish to grant users after they successfully authenticate to Ignition.

To set up your VLANs:

1. Set up your restricted-reach VLAN. In this example, we have created a VLAN called Vlan200 for this. Its VLAN ID is 200. On the example Avaya Ethernet Routing Switch 5520, the Vlan200 settings are:

```
vlan create 200 name Restricted type port
```

2. Set up your authenticated-access VLAN. This example uses a VLAN called Vlan1 for this, and we have set up Vlan1 to connect to the Internet via the firewall. Its VLAN ID is 1. On the example Avaya Ethernet Routing Switch 5520, the settings of Vlan1 are:

```
ip address 172.16.100.9 255.255.255.0
```

Configuring wired switch Ethernet ports

Perform the following set-up on each guest-accessible wired switch:

1. Set up each guest-accessible Ethernet port on the wired switch to require 802.1X authentication. Regular users will authenticate via 802.1X, and guests with non-802.1X compatible hardware will authenticate via the Access Portal. Ports set up for 802.1X supplicant traffic must be assigned to the restricted-reach (guest) VLAN. In this example, we use port 1/12 on an Avaya Ethernet Routing Switch 5520, and the VLAN is VLAN 200. Example Avaya Ethernet Routing Switch 5520 settings are:

```
5520-48T-PWR(config)#interface fastEthernet 1/12
5520-48T-PWR(config-if)#eapol guest-vlan enable
5520-48T-PWR(config-if)#eapol guest-vlan 200
```

```
5520-48T-PWR(config-if)#eapol quiet-interval 15
5520-48T-PWR(config-if)#eapol transmit-interval 15
```

2. If guests will connect over wireless, set up the wired switch's Ethernet port that connects to the wireless access point. Configure this port for 802.1Q trunking to the access point. Set the trunk to carry both the restricted-reach VLAN and authenticated-access VLAN. On the example Avaya Ethernet Routing Switch 5520, the settings are:

```
5520-48T-PWR(config)#vlan ports 1 tagging enable
5520-48T-PWR(config)#vlan ports 1 tagging tagall
5520-48T-PWR(config)#vlan members add 1 1
5520-48T-PWR(config)#vlan members add 200 1
```

3. Set up the wired switch's Ethernet port that connects to the Access Portal appliance's IN port. This port should be set up to carry only the restricted-reach VLAN. In this example, we have designated VLAN 200 for this purpose. Example settings for an Avaya Ethernet Routing Switch 5520 are:

```
5520-48T-PWR(config)#vlan members add 200 11
5520-48T-PWR(config)#vlan ports 1 pvid 200
```

Configuring wireless guest access

To provide wireless guest access, you will create a wide-open SSID on a wireless access point (AP). This SSID does not require authentication and places the user on a restricted-reach VLAN. No initial 802.1X session is attempted.

The guest user's supplicant associates with the SSID in open mode (no authentication). The supplicant is automatically mapped to the restricted-reach VLAN (the SSID is statically mapped on the AP). This VLAN is the authentication VLAN network, which forces authentication through the Access Portal. In this architecture, the Access Portal is defined as the authenticator in the Ignition server appliance.

The sections below provide generic instructions.

Prerequisites

Make sure the wired switch is configured and connected to the wireless access point (AP).

Configuring wireless guest access

Log into the management screen for your wireless access point and make the following settings.

1. Set the AP's **Primary DNS Server Address** to the IP address of the Access Portal IN port.

-
2. Set the AP's **Default Router Address** to the IP address of the Access Portal IN port.
 3. Set the AP's DHCP **Server Address**. For most APs, use the IP address of the Access Portal **IN port** as your **DHCP Server Address**.
 4. Create VLAN and SSID definitions on the AP for the restricted-reach VLAN you configured in [“Configuring VLANs on the wired switch” on page 63](#). This is your guest authentication VLAN / SSID.
 - × Set layer-2 security to **None** on the VLAN.
 - × Set layer-3 security to **None** on the VLAN.
 - × Give the guest authentication SSID a name that your guest users will easily recognize. In this example, we use the name “Guest” for this SSID.
 - × Set the guest authentication SSID to beacon.
 5. Create VLAN and SSID definitions on the AP for the authenticated-access VLAN you configured in this section [“Configuring VLANs on the wired switch” on page 63](#). This is the VLAN / SSID your guests use after successfully authenticating.
 - × Typically you will leave beaconing turned off for this SSID.

Creating guest user accounts

Create your guest user accounts using either:

- × Ignition Guest Manager, as explained in the *Ignition Guest Manager Configuration Guide*.
- × Ignition Dashboard, as explained in the *Ignition Server Administration Guide*. To allow your front desk personnel to continue creating guest user accounts, set up each front desk clerk as a provisioner in Guest Manager.

Testing wireless guest access

Important: Access Portal does not support proxy. To allow Access Portal to capture HTTP requests from a client machine, you must either remove the proxy settings from the client browser, or choose “auto detect proxy setting for this network” setting on the browser. If a proxy is configured, Access Portal will not be able to direct HTTP requests to the Access Portal login page.

To test the wireless guest access:

1. Using a laptop with wireless capability, connect to the “guest” SSID that you created in this procedure: [“Configuring wireless guest access” on page 64](#).
2. Open a web browser on the laptop.

-
3. Browse to any site. For example, type “http://www.yahoo.com”.
 4. If correctly configured, the Access Portal will force the browser to display a login page. Enter your Ignition-generated guest username and password. After authentication, the browser will be able to access the Internet.

Testing wired guest access

Important: Access Portal does not support proxy. To allow Access Portal to capture HTTP requests from a client machine, you must either remove the proxy settings from the client browser, or choose “auto detect proxy setting for this network” setting on the browser. If a proxy is configured, Access Portal will not be able to direct HTTP requests to the Access Portal login page.

To test wired guest access:

1. Connect your PC's Ethernet cable to a port connected to the switch you configured in [“Configuring guest access on the wired switch”](#) on page 62. Make sure that either:
 - × the PC has no 802.1X supplicant software installed, or
 - × if the PC has an 802.1X supplicant, then make sure you provide an incorrect username and password, causing authentication to fail.
2. Wait one minute. The DHCP negotiation for a wired connection can take up to one minute. **Note:** If you do not want to wait, and if you are using a Windows- based PC, you can do this: At the DOS prompt, issue: **>ipconfig /release** and then issue **>ipconfig /renew**.
3. Open a web browser on the PC.
4. If correctly configured, the Access Portal will force the browser to display a login page. Enter your Ignition-generated guest username and password. After authentication, the browser will be able to access the Internet. **Note:** Some enterprises may require you to configure the proxy on the browser to access the Internet. If so, configure the proxy after authentication. **Reminder:** When you start a new session, you must remove the proxy to get redirected to the portal login page.

Network access should be available from the client machine. Other internal sites on the intranet should be accessible.

Configuring CASE

This chapter explains how to configure Avaya Identity Engines Ignition Client for Accessing Secure Enterprise (CASE) to work with Access Portal.

Configuring the CASE to work with Access Portal

After you deploy Access Portal, you must configure CASE to work with Access Portal. Use the CASE Administrative Console to create a CASE package for your network and to deploy the CASE package to the Access Portal.

CASE Administrative Console overview

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 deployment packages that contain one or more network profiles and deploys these packages directly to Access Portal.

Creating a network profile

To create a network profile, see the “Creating a network profile” procedure in the *Avaya Identity Engines Ignition CASE Administration* guide.

Creating a deployment package

To create a deployment package, see the “Creating a deployment package” procedure in the *Avaya Identity Engines Ignition CASE Administration* guide.

Deploying packages

To deploy a package, see the “Deploying packages” procedure in the *Avaya Identity Engines Ignition CASE Administration* guide.

Troubleshooting

This chapter lists solutions for common errors that can occur when configuring Access Portal.

Troubleshooting common problems

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

Problem: Cannot access the Access Portal login page from client browser using an URL with a DNS name

Details: You can get to the portal login page from the client machine's browser, by specifying any URL with an IP address, but not when specifying a URL containing DNS name.

Possible cause: The issue is with DNS name resolution.

Solution:

- Make sure that the DNS servers specified in the Access Portal Administration Web UI are correct and the DNS forwarder is set up.
- Make sure that the connectivity is working.

Problem: You are unable to authenticate a user

Solution:

- Under **Services > Captive Portal:** Verify that your Identity Engines RADIUS server address is correct and the shared secret is identical.
- Under **Status > Captive Portal:** Remove older sessions and unwanted session(s).
- When connecting from a client, make sure that you close any older browser windows to clear out older sessions. Browser cookies may feed stale data to Access Portal.

Problem: MAC Authentication fails

Solution:

- Verify that MAC Authentication is enabled on both the Access Portal Administration Web UI and the Ignition Server.

- Make sure that the shared secret is identical.
- Make sure that your MAC Address Source is not set to “Inbound-Calling-Station-Id”. If it is, change your MAC Address Source to “Inbound-User-Name” or MAC address recognition will not work.

Problem: Cannot launch the Access Portal Administration Web UI

Solution:

- Remove any proxy settings on the browser.
- If the machine you are using to connect to the Access Portal Administration Web UI is **not** on the Admin network, you can add a static route to the network where the machine resides. See the “Workaround” in [Step 5 on page 29](#).

Problem: Client is unable to communicate with Access Portal

Solution:

- Make sure that the proxy configuration on your Web GUI for the Access Portal Server as well as the client machine are turned off.
- Make sure that 802.1x is turned off
- Make sure that the IP selection is not set to static. Access Portal is designed to be used in conjunction with a DHCP server.
- Make sure the client’s default gateway is pointing towards IN interface IP address of the Access Portal and they are able to talk to each other.

Problem: You are unable to ping IN and OUT interfaces of Access Portal.

Cause: The Access Portal IN and OUT interfaces do not respond to ping requests, only the ADMIN interface responds to PING requests.

Solution: To check for connectivity on IN and OUT networks, originate ping requests from the IN and OUT interfaces pinging other hosts on the network, rather than pinging from other hosts to these interfaces.

Problem: In Dashboard, you do not see “Access Portal” as the last option in the Configuration list

Solution: You need to install the new FEATURE_PORTAL license.

Miscellaneous troubleshooting tips

- To disable device profiling, turn off device profiling on the Access Portal Administration Web UI **as well as** in the Ignition Server’s Access Portal configuration (i.e. clear the “Trusted Device Update” checkbox). If you turn off device profiling only on the Access Portal, that only prevents Access Portal from sending attribute information to the Ignition server. The Ignition Server will still attempt to learn devices.

- If you want to specify a RADIUS server that is not accessible through the default gateway configured in the WAN interface, go to System > Static Route and add a route to the network where the RADIUS server is present.
- You can view the overall health of your Captive Portal under **Status > System**.
- Under the **Status** heading, you can also view the following:
 - × DHCP
 - × Interfaces
 - × Services
 - × System logs
- Under the **Diagnostics** heading, you can view:
 - × DHCP leases
 - × ARP Table data
 - × Routing table diagnostics
- Under the **Diagnostics** heading, you can perform the following actions:
 - × Reset state tables
 - × Halt system
 - × Ping Test
 - × Traceroute

Appendix A: Access Portal deployment example

This section covers basic Access Portal configuration, deployment, and verification tasks. This section assumes you are familiar with setting up and maintaining networks and network security.

Planning your deployment

The following is a summary of the process to set up and run Access Portal.

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 is one SSID, you can define this SSID as the Access Portal network for guest users.

Determine what kinds of VLANs exist on your wires network

Is there a single, secure VLAN for everyone, or are there multiple VLANs? If there are multiple VLANs, you can define the VLANs as different networks for different users. In this case, if 802.1x is enabled, you can deploy the guest VLAN as an Access Portal VLAN in case 802.1x authentication fails.

Network requirements

To deploy Access Portal, 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 one or multiple SSIDs
- A configured Ignition Server supporting providing RADIUS authentication.
- For testing, you will also need a laptop (running Windows XP SP3 or later) with wired and wireless NICs.

Once the network is configured, Avaya recommends that you go through the process manually to verify that the configuration is correct. Before you start using Access Portal, use your wired/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. Connect to an edge switch. Verify that the laptop receives an IP address from DHCP.

Background

In this example, see [“Network configuration” on page 74](#), the network is divided into two logical networks: a wireless guest network, and a wired guest 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

Figure 45 Network configuration

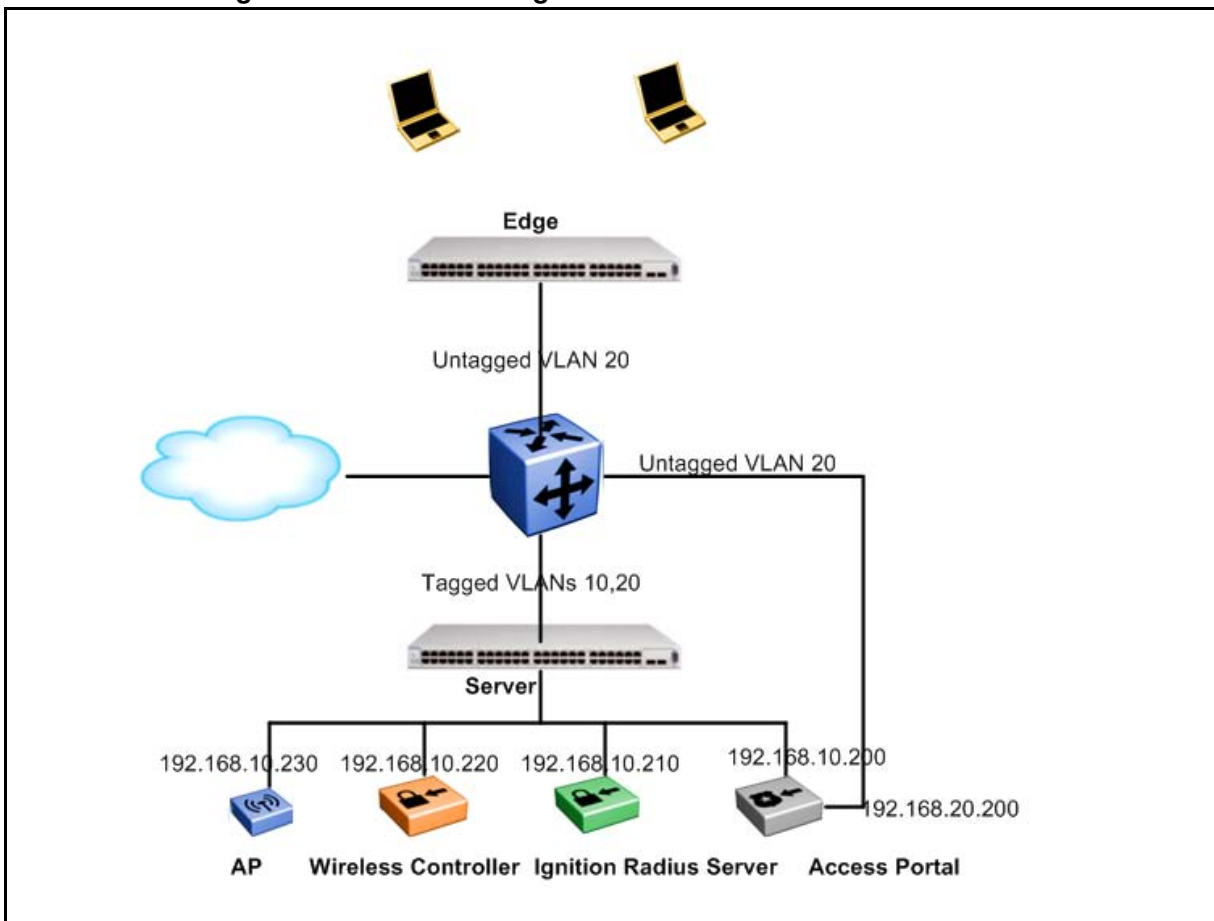


Table 1 Network configuration

	Interface Admin	IN Interface (Access Portal clients)	OUT Interface
Access Portal	192.168.10.200/24	192.168.20.200/24	134.177.213.200/24
Ignition RADIUS Server	192.168.10.210/24		
Wireless Con troller	192.168.10.220/24		
Access Point	192.168.10.230/24		

The first logical network is an **open network**. This network acts as the entry-point for unconfigured end-users. It is available from both wireless connections and wired 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 the 192.168.20.0/24 network.

Configuring the Ignition (RADIUS) Server

The RADIUS server is an Identity Engines Ignition Server installation with Ignition RADIUS installed. The RADIUS server authenticates access portal users after users join the open network. It resides at 192.168.10.210 and has a RADIUS authentication port of 1812. It is configured to allow PAP authentication. Several user accounts were created and stored locally.

Under the Access Portal section, add 192.168.10.200 as the Access Portal Server with “test” as the shared secret.

Configuring the Ignition Access Portal (web server)

The following steps explain how to configure the Ignition Access Portal:

1. Configure the Admin interface.

Figure 46 Configuring the Admin interface

```
Enter an option: 2

Enter the new ADMIN IP address: 192.168.10.200

Subnet masks are entered as bit counts (as in CIDR notation) in Avaya Identity Engine Access Portal.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new ADMIN subnet bit count: 24

Do you want to enable the DHCP server on ADMIN [y;n]? n

The ADMIN IP address has been set to 192.168.10.200/24.
You can now access the webGUI by opening the following URL
in your web browser:

http://192.168.10.200/

Press ENTER to continue.
```

After configuring the admin interface, use a client machine in same 192.168.10.0/24 network to access the Access Portal Administration Web UI at <http://192.168.10.200>. Use the Access Portal Administration Web UI to perform the following steps.

2. Configure the DNS server and the OUT interface.

Figure 47 Configuring the DNS server

AVAYA
idEngines

On this screen you will set the General pfSense parameters.

General Information	
Hostname:	<input type="text" value="accessportal"/> EXAMPLE: myserver
Domain:	<input type="text" value="enterprice.com"/> EXAMPLE: mydomain.com
Primary DNS Server:	<input type="text" value="x.x.x.x"/>
Secondary DNS Server:	<input type="text"/>

Next

Figure 48 Configuring the OUT interface

AVAYA
idEngines

On this screen we will configure the Wide Area Network information.

Configure OUT Interface

SelectedType:

General configuration

MAC Address:
This field can be used to modify ("spoof") the MAC address of the OUT interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU:
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

Static IP Configuration

IP Address: /

Gateway:

DHCP client configuration


DHCP Hostname:
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

Make sure that your DNS is reachable from the OUT Interface.

Click **Next** to accept all the default values, and then click **Reload**. Access Portal redirects you to the Access Portal main page after 120 seconds or you can click on the Avaya icon to reach the Access Portal main page immediately.

3. Configure the IN interface. Click **Interfaces > IN**, configure the IN interface and click **Save**.

Figure 49 Configuring the IN interface

System	Interfaces	Firewall	Services	Status	Diagnostics
Interfaces: Optional 1 (IN)					
					
Optional Interface Configuration					
<input checked="" type="checkbox"/> Enable Optional 1 interface					
Description	<input type="text" value="IN"/> <small>Enter a description (name) for the interface here.</small>				
General configuration					
Type	<input type="text" value="Static"/>				
MAC address	<input type="text"/> <small>This field can be used to modify ("spoof") the MAC address of the OUT interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank</small>				
MTU	<input type="text"/> <small>If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.</small>				
IP configuration					
Bridge with	<input type="text" value="none"/>				
IP address	<input type="text" value="192.168.20.200"/> / <input type="text" value="24"/>				
Gateway	<input type="text"/>				

4. Configure DHCP. If you chose Access Portal as a DHCP Server for the Access Portal Client network, click **Services > DHCP Server > IN**, and then select the **Enable DHCP server on IN interface** check box.

Figure 50 Configuring DHCP

The screenshot shows the configuration page for the DHCP server on the IN interface. The page is titled "Services: DHCP server" and has tabs for "ADMIN" and "IN". The "IN" tab is selected. The configuration is as follows:

<input checked="" type="checkbox"/> Enable DHCP server on IN interface	
<input type="checkbox"/> Deny unknown clients If this is checked, only the clients defined below will get DHCP leases from this server.	
Subnet	192.168.20.0
Subnet mask	255.255.255.0
Available range	192.168.20.0 - 192.168.20.255
Range	192.168.20.20 to 192.168.20.80
WINS servers	
DNS servers	
	NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS forwarder is enabled, otherwise the servers configured on the General page.
Gateway	
	The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network.
Default lease time	86400 seconds This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum lease time	seconds This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP:	
	Leave blank to disable. Enter the REAL address of the other machine. Machines must be using CARP.

If you want to configure external DHCP, select the **Enable DHCP relay** check box on the IN interface and enter your DHCP Server IP address. In addition, configure 192.168.20.200 as the default gateway and DNS for this subnet.

5. Enable Captive Portal on the IN interface. Click **Services > Captive Portal** and do the following:

- × Select the **Enable captive portal** check box.
- × From the **Interface** drop-down menu, select **IN**.

. If you want to authenticate all Access Portal clients against the Ignition RADIUS Server, scroll down to the **Authentication** section and do the following:

- × Select the **RADIUS authentication** radio button.
- × In the **First Ignition Server section**, in the **IP address** field, enter 192.168.10.210.
- × In the **Shared Secret** field, enter "test".

Figure 51 Enabling Captive Portal on the IN interface

Services: Captive portal

Captive portal | MAC White List | IP Address White List | Local User Manager | File Manager

Enable captive portal

Interface: IN
Choose which interface to run the captive portal on.

Maximum concurrent connections: [] per client IP address (0 = no limit)
This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Default is 4 connections per client IP address, with a total maximum of 16 connections.

Idle timeout: [] minutes
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Hard timeout: [] minutes
Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

Logout popup window: Enable logout popup window
If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

Concurrent user logins: Disable concurrent logins
If this option is set, only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.

MAC filtering: Disable MAC filtering
If this option is set, no attempts will be made to ensure that the MAC address of clients stays the same while they're logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between Avaya Identity Engine Access Portal and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

Authentication: No authentication
 Local user manager
 RADIUS authentication

First Ignition Server

IP address: 192.168.10.210
Enter the IP address of the Ignition Server which users of the captive portal have to authenticate against.

Port: []
Leave this field blank to use the default port (1812).

Shared secret: []

Configuring the Avaya wireless controller

When an end-user accesses the SSID, the end-user traffic needs to be sent out through an interface on the controller. We need to create an interface for this SSID. In doing so, we will use VLAN 20.

- Configure guest VLAN 20 on WC8100 and map it to “open” mobility VLAN
- Configure open SSID mapped to this VLAN

SSID

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
```

Configuring the edge switch

To configure the edge switch, you must:

- Configure guest VLAN 20
- Assign all the port to this VLAN

```
5520-48T-PWR(config)#vlan create 20 name guest type port
5520-48T-PWR(config)#vlan members add 20 1-48
5520-48T-PWR(config)#vlan ports 1-48 pvid 20
```

Verification

To verify your configuration:

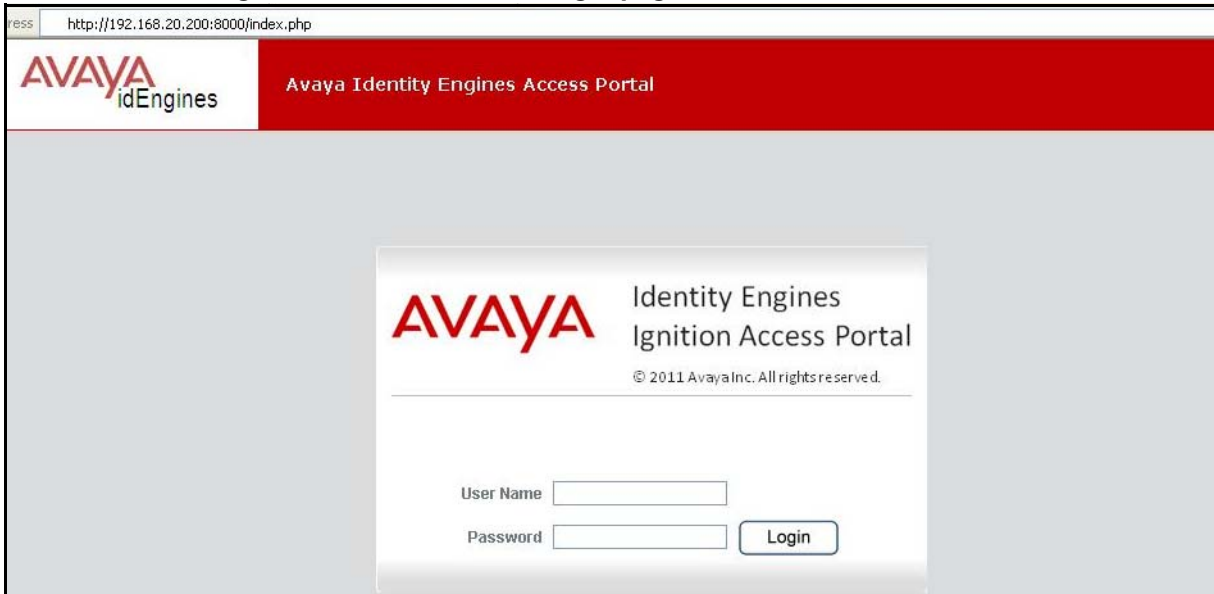
1. Connect your laptop to a wireless or wired connection and check the IP address settings. The gateway and DNS IP address must be 192.168.20.200.

Table 2 Ethernet adapter External

Connection-specific DNS Suffix	enterprise.com
Description	Realtek RTL8139 Family PCI Fast Ethernet NIC
Physical Address	00-40-F4-35-05-C8
DHCP Enabled	Yes
IP Address	192.168.20.80
Subnet Mask	255.255.255.0
Default Gateway	.192.168.20.200
DNS Servers	192.168.20.200

2. Open a web browser and try to access any web page. Access Portal redirects to the Access Portal Login page.

Figure 52 Access Portal Login page



3. On the Access Portal Login page, enter the **User Name** and **Password** that you created on the Ignition RADIUS Server and click **Login**. Access Portal displays a success page.

Figure 53 Access Portal success page

