Administering Avaya Identity Engines Ignition Access Portal

Release 9.1
NN47280-604
Issue 03.01
March 2015

Notice

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

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 websites referenced within this site or documentation 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 Avaya hardware and software. 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 website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product 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 unless expressly authorized by Avaya. 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.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

Contents

Chapter 1: Introduction

Purpose

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.

Related resources

Documentation

See the following related documents.

Title	Purpose	Document number
Avaya Identity Engines Ignition Server Getting Started	Installation and simple configuration	NN47280–300
Avaya Identity Engines Ignition Server Administration	All configuration options	NN47280–600
Avaya Identity Engines Ignition Guest Manager Configuration	Installation, configuration, and management	NN47280–501
Configuring and Managing Avaya Identity Engines Single-Sign-On	Configuration, management, and deployment	NN47280–502
Avaya Identity Engines Ignition CASE Administration	Installation, configuration, and deployment	NN47280–603
Avaya Identity Engines Ignition Analytics	Installation, configuration, and maintenance	NN47280–601
Avaya Identity Engines Ignition Server Release Notes	Reference	NN47280–400

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

  Note:

  Videos are not available for all products.

Subscribing to e-notifications

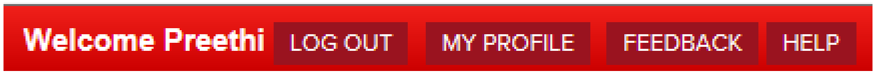
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

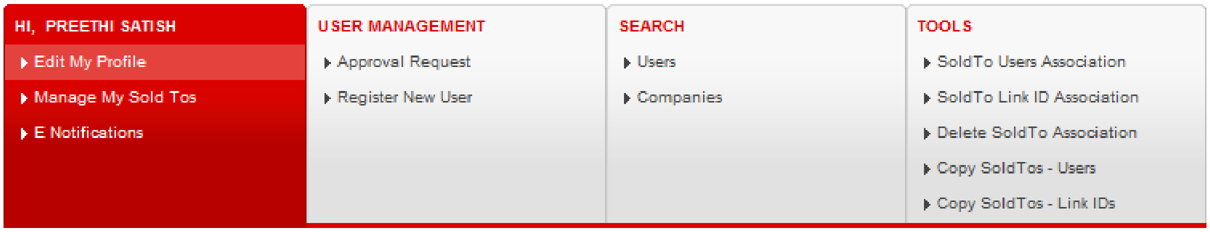
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing Switch 8800.

Procedure

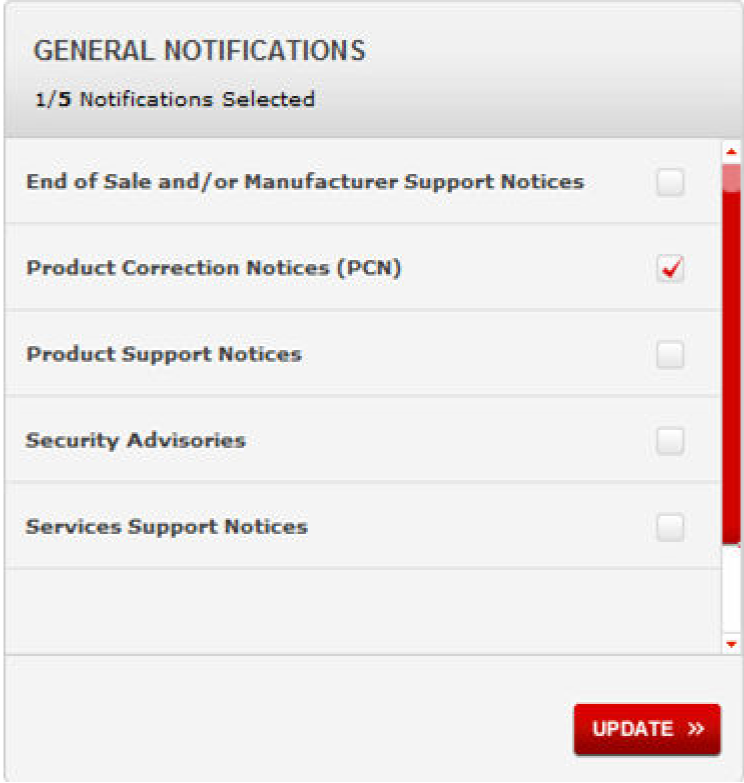
1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Click **MY PROFILE**.



4. On the site toolbar, click your name, and then click **E Notifications**.



5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.

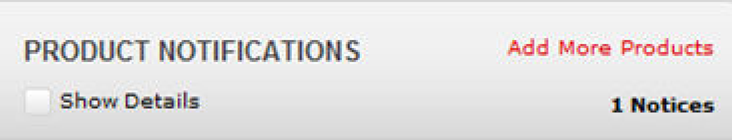


GENERAL NOTIFICATIONS

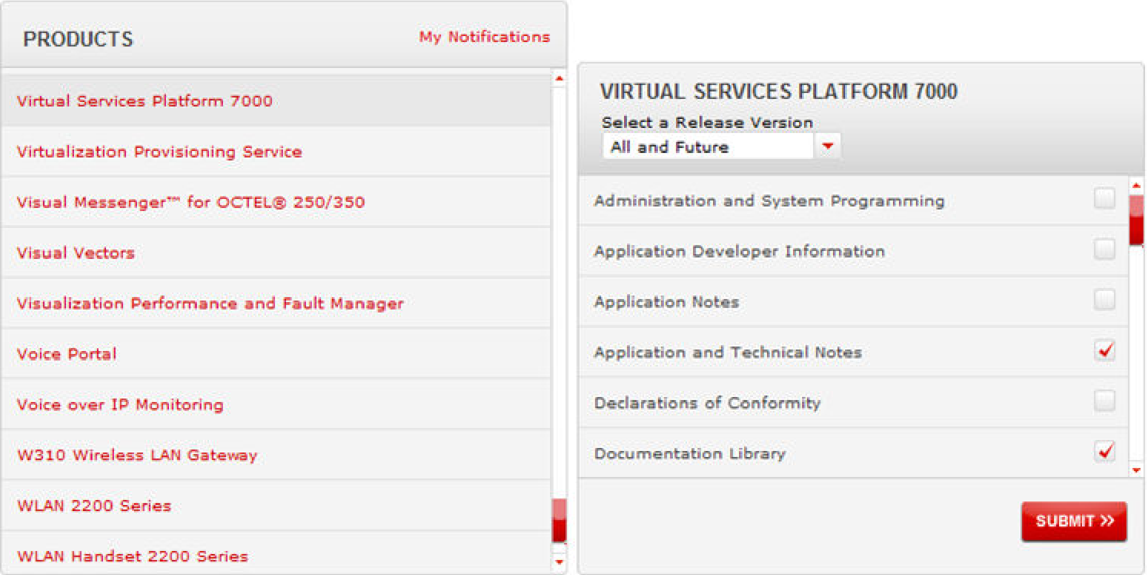
1/5 Notifications Selected

- End of Sale and/or Manufacturer Support Notices ☐
- Product Correction Notices (PCN) ☑
- Product Support Notices ☐
- Security Advisories ☐
- Services Support Notices ☐

6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.



8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.


PRODUCTS
My Notifications
Virtual Services Platform 7000
Virtualization Provisioning Service
Visual Messenger™ for OCTEL® 250/350
Visual Vectors
Visualization Performance and Fault Manager
Voice Portal
Voice over IP Monitoring
W310 Wireless LAN Gateway
WLAN 2200 Series
WLAN Handset 2200 Series
VIRTUAL SERVICES PLATFORM 7000
SUBMIT »

Select a Release Version: All and Future

- Administration and System Programming □
- Application Developer Information □
- Application Notes □
- Application and Technical Notes ☑
- Declarations of Conformity □
- Documentation Library ☑

11. Click **Submit**.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.

3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
    - Whole Words Only
    - Case-Sensitive
    - Include Bookmarks
    - Include Comments
6. Click **Search**.

    The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

The following sections detail what is new in *Avaya Identity Engines Ignition Access Portal Administration* Release 9.1.

Related Links

Features on page 11

Features

Access Portal Release 9.1 builds on top of Access Portal Release 8.0 and adds new and enhanced capabilities for management and access control of Bring Your Own Device (BYOD) technology.

Access Portal 9.1 is compatible with Avaya Identity Engines Ignition Server 9.1.

See the following sections for information about feature changes.

Related Links

Customized access on page 11

Additional enhancements on page 12

Customized access

Access Portal Release 9.1 provides increased flexibility to control and present what different users, or groups of users, experience through the Access Portal. The following sections describe the specific features that provide this flexibility.

Multiple IN and OUT interfaces

Access Portal installs with three out-of-the-box interfaces: ADMIN, IN, and OUT. Beginning with Release 9.1, you can add multiple IN and OUT interfaces. These interfaces can be physical, logical, or a combination of the two. You add additional ethernet adapters to each virtual machine as required, and then assign those adapters as an IN or OUT interfaces as required.

Multiple IN interfaces allow for more flexible deployment options; each IN interface can be associated with a different VLAN. For example, you can configure one IN interface for each physical site in your network.

Multiple OUT interfaces allow you to customize the user experience. For example, you can direct a user, or group of users, to a particular area of your network through one OUT interface, and direct different users to a different area of your network through another OUT interface.

Zones

In conjunction with multiple IN interfaces, each captive portal instance (and all associated settings) is now associated with a zone. You assign captive portal zones to one or more IN interfaces. Note that an IN interface, however, can only be associated with one zone.

Multiple success pages

In conjunction with multiple OUT interfaces, you can now customize the user experience by directing users to different pages after successful authentication.

Access Groups

In conjunction with multiple OUT interfaces, you can now create Access Portal Access Groups that determine the user experience after successful authentication. Access Groups allow you to specify the type of network access (the OUT interface through which the user gets access) and the success page that displays after successful authentication. Users get assigned to different Access Groups depending on the configuration of access policies on the Ignition Server. The outbound values configured on the Ignition Server access policies must match the Access Group names defined on the Access Portal.

Additional enhancements

VMware Tools support

The Access Portal OVA installation file now includes VMware Tools.

Device fingerprinting

Support for Bring Your Own Device (BYOD) fingerprinting is expanded to include Windows 8, Windows 12, Windows Surface RT, MAC OS Maverick (10.9), IOS 7.x, Android 4.4, Blackberry 7 OS, Kindle Fire, and Blackberry 10 OS.

You can now define an expiration time for unknown devices based on a time lapse period from initial fingerprint, or by an absolute date and time.

You can now group fingerprinted devices and associate them to one or more device groups in the Access Portal definition template.

RADIUS authentication

Enhanced session timeout options are now available.

DHCP server

Enhanced DHCP server settings are now available. In addition, you can configure different DHCP scopes for IN interfaces.

User session limits

You can now limit the number of concurrent sessions that one username can establish from multiple devices.

Static logout page

You can now upload and configure a customized static logout page for administrators and users.

Enhanced captive portal status display

If device fingerprinting is enabled, the status display for captive portals now includes device and operating system information.

Login and logout support

There is now login and logout support for the Access Portal console CLI, and logout support for the Access Portal Administration Web UI.

Chapter 3: Avaya Identity Engines Ignition Access Portal

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.

It is important to note that the Access Portal does not eliminate the need for customers to deploy an enterprise grade firewall.

Related Links

How Access Portal works on page 14

Access Portal administrator tasks on page 16

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 optionally 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 may host the Ignition Client for Accessing Secure Enterprise (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 for wired and/or wireless access. Then the user can directly connect to the network by authenticating with the

Ignition Server. If the device is not capable of using 802.1X, Access Portal can provide in-line access to the network.

Related Links

How a guest user logs in on page 15

How a guest user logs in

❗ **Important:**

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

At runtime, Access Portal authentication works as follows:

Procedure

1. The guest receives a temporary user name and password from the reception desk personnel. Typically, the receptionist uses Ignition Guest Manager to create the user account. Alternatively, the guest can create their own guest account using the self-service option of the Ignition Guest Manager, and receive the account access code through SMS or email on their mobile device.
2. The guest connects their 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 their laptop and connect to the guest wireless network. In this example, the guest network 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 ERS 4800 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 through 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, VLAN 200).
6. The guest user opens a browser on their 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 their temporary user name and password, and the Access Portal authenticates the user through the Ignition Server using RADIUS:
    a. If the CASE application is also deployed on the portal, then after successful authentication, the CASE application runs on the guest’s machine and configures it to use 802.1X for authenticating to the network. If the CASE application is successful in

doing this, the guest’s laptop is switched to a compliant VLAN and all the network access is 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.

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

Chapter 4: Installing Avaya Identity Engines Ignition 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 (5.1 and up) server. After you import the Access Portal virtual appliance, the virtual appliance becomes an Access Portal.

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

Related Links

Access Portal components on page 17
Network configuration for Access Portal-based authentication on page 18
Installing the Access Portal virtual machine on page 19
Configuring the Access Portal virtual machine on page 26
Backing up and restoring Access Portal on page 52
Upgrading Access Portal on page 54

Access Portal components

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

- Ignition Server
- Access Portal (VMware ESXi (5.1 and up) server)
- CASE application (optional)
- Ignition Guest Manager account creation tool (optional but highly recommended)
- Existing authenticators (switches and wireless access points)
- Existing Enterprise class firewall

Related Links

VMware ESXi server requirements on page 18

VMware ESXi server requirements

Hardware platforms supported by VMware's ESXi server (version 5.1 and up) are required. See HTTP://WWW.VMWARE.COM/ for a list of supported hardware platforms for ESXi.

See the *Avaya Identity Engines Release Notes* for each specific release for information about release-specific Access Portal VM minimum system requirements (memory, CPU, disk space, interfaces).

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

Warning:

Avaya provides the Ignition Access Portal as a Virtual Appliance. Do not install or configure any other software on the VM shipped by Avaya.

- Avaya does not support the installation of any VMware specific, FreeBSD specific, or any third-party vendor package or RPM on its VM, other than what Avaya ships as a package, image, or OVA.
- Do not install or uninstall any software components unless Avaya specifically provides the software and/or instructs you to do so. 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.
- Avaya determines which VMware Tools to install and configure. When required, Avaya provides these tools as part of the installation package. Avaya provides these tools because VMware Tools configures the kernel and network settings and unless Avaya tests and approves these tools, Avaya cannot guarantee that the VM will work after the tool is installed and configured.

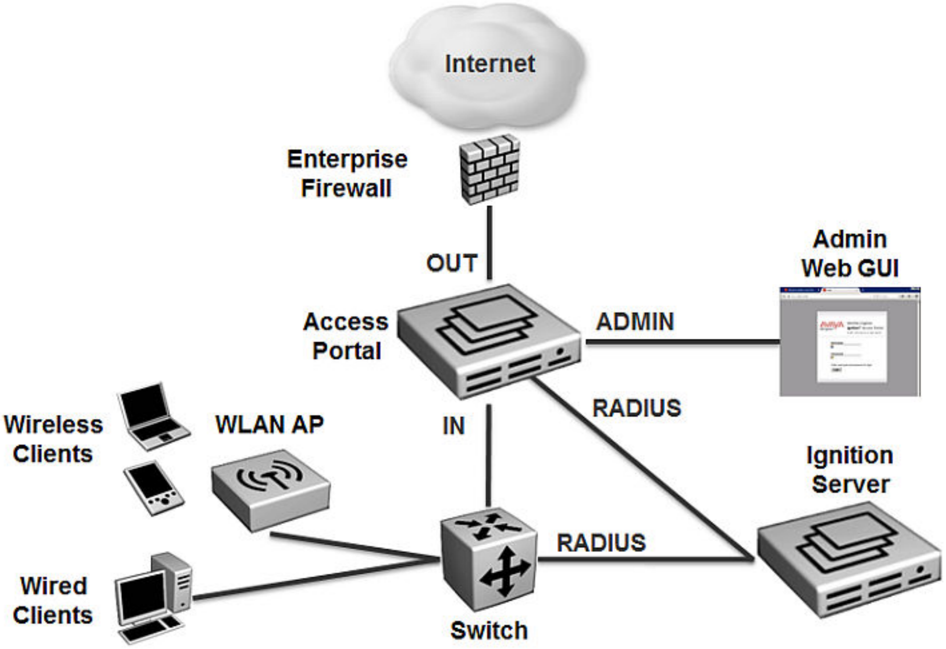
Turn off automatic VMware Tools updates if you have enabled them.

Network configuration for Access Portal-based authentication

Access Portal has three out-of-the-box network interfaces:

- **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.
- **OUT** - The OUT interface provides connectivity to the Enterprise network / Internet.

Note that you can add additional IN and OUT interfaces as required when you configure your Access Portal. The following diagram shows a network configuration with the out-of-the-box configuration.

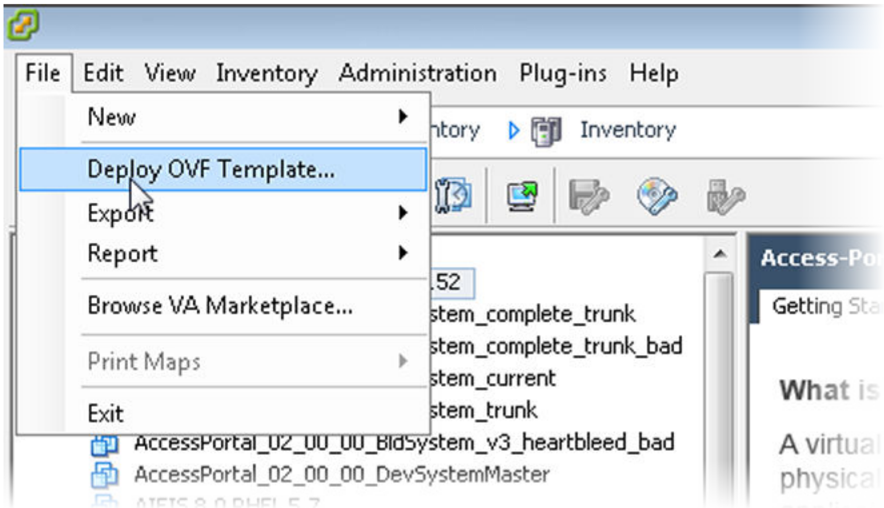


Installing the Access Portal virtual machine

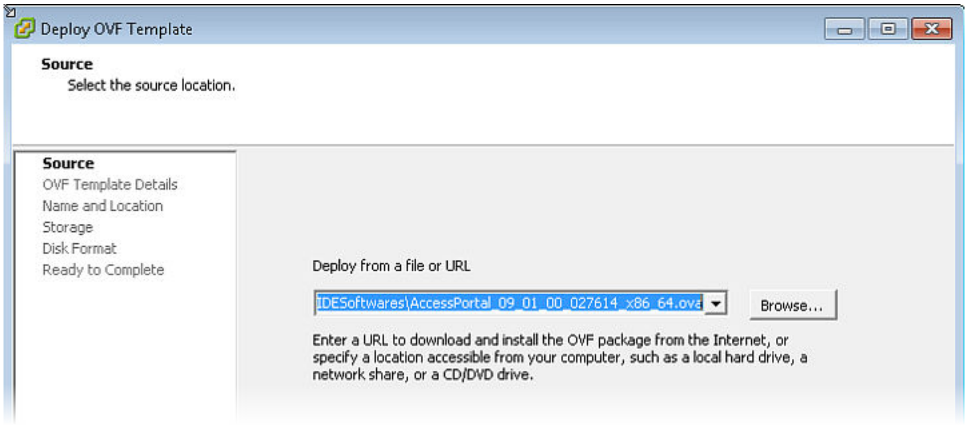
The Access Portal OVA file incorporates an OVF file. Avaya recommends that you use the VMware vSphere Client to deploy the VM into your system.

Procedure

1. Start the VMware vSphere Client and log in to the ESXi Server on which you want to install the Access Portal.
2. Click **File** > **Deploy OVF Template**.



3. The **Source** screen displays. Select the location from which you want to import the Access Portal virtual appliance.



Source

Select the source location.

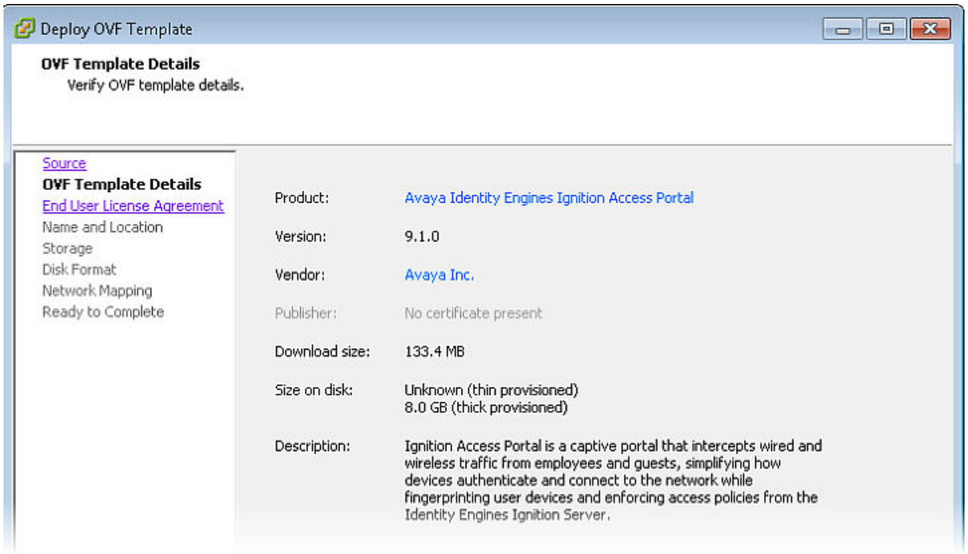
Deploy from a file or URL

IDESoftwares\AccessPortal_09_01_00_027614_x86_64.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

4. Click **Next**.

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



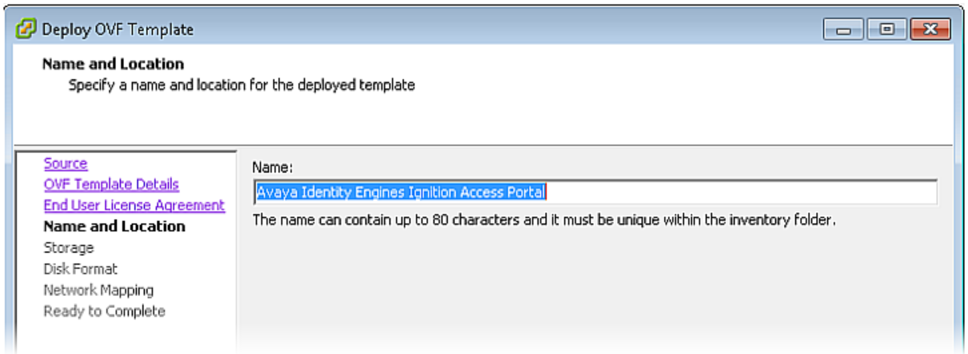
OVF Template Details

Verify OVF template details.

Product:	Avaya Identity Engines Ignition Access Portal
Version:	9.1.0
Vendor:	Avaya Inc.
Publisher:	No certificate present
Download size:	133.4 MB
Size on disk:	Unknown (thin provisioned) 8.0 GB (thick provisioned)
Description:	Ignition Access Portal is a captive portal that intercepts wired and wireless traffic from employees and guests, simplifying how devices authenticate and connect to the network while fingerprinting user devices and enforcing access policies from the Identity Engines Ignition Server.

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

6. The **Name and Location** screen displays. Either accept the default name or choose to rename the virtual machine. Click **Next**.



Name and Location

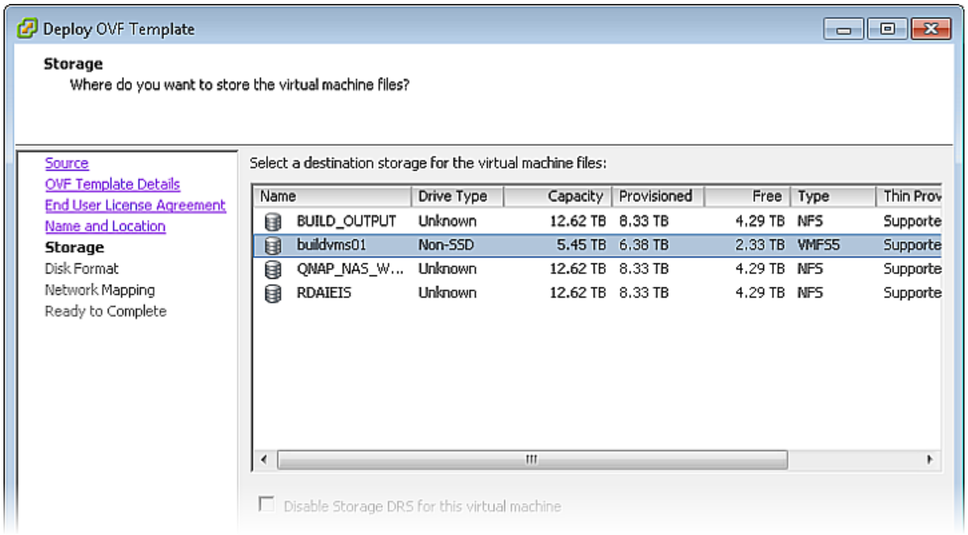
Specify a name and location for the deployed template

Name:

Avaya Identity Engines Ignition Access Portal

The name can contain up to 80 characters and it must be unique within the inventory folder.

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



Storage

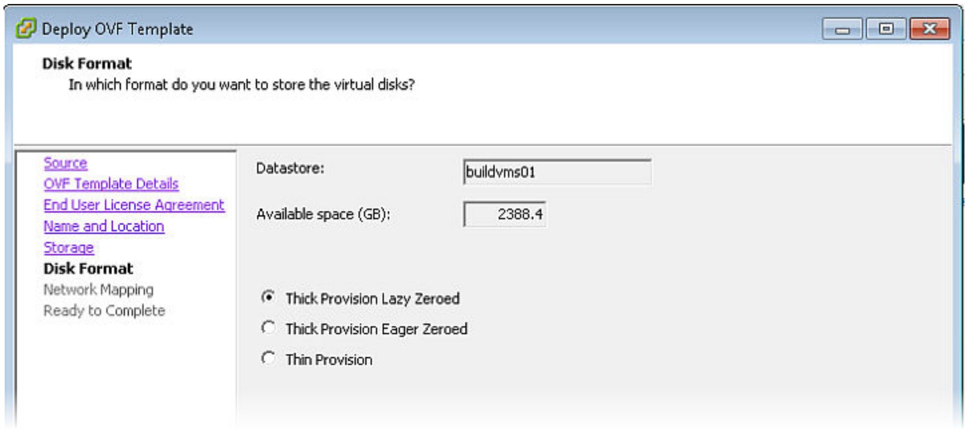
Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Prov
BUILD_OUTPUT	Unknown	12.62 TB	8.33 TB	4.29 TB	NFS	Supporte
buildvms01	Non-SSD	5.45 TB	6.38 TB	2.33 TB	VMFS5	Supporte
QNAP_NAS_W...	Unknown	12.62 TB	8.33 TB	4.29 TB	NFS	Supporte
RDAIEIS	Unknown	12.62 TB	8.33 TB	4.29 TB	NFS	Supporte

□ Disable Storage DRS for this virtual machine

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



Disk Format

In which format do you want to store the virtual disks?

Datastore: buildvms01

Available space (GB): 2388.4

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

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

Note:

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

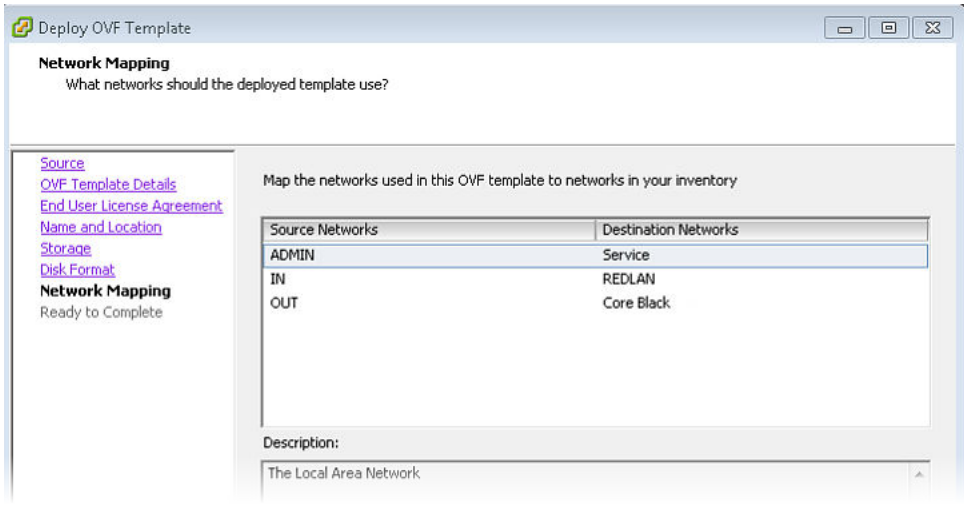
- **ADMIN**: This network is for administrative purposes. This network provides web access for administrating Access Portal and SSH access to the Access Portal console if needed. This network also provides connectivity to other servers such as the Ignition server or an external DHCP server if you are using one. Map the Access Portal ADMIN interface to the

VM network in your inventory designated for administrative purposes. In the following example, the Access Portal ADMIN interface is mapped to the Service network.

- **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 following example, the Access Portal IN interface is mapped to the REDLAN network.
- **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 following example, the Access Portal OUT interface is mapped to the Core Black network.

  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.**



Network Mapping

What networks should the deployed template use?

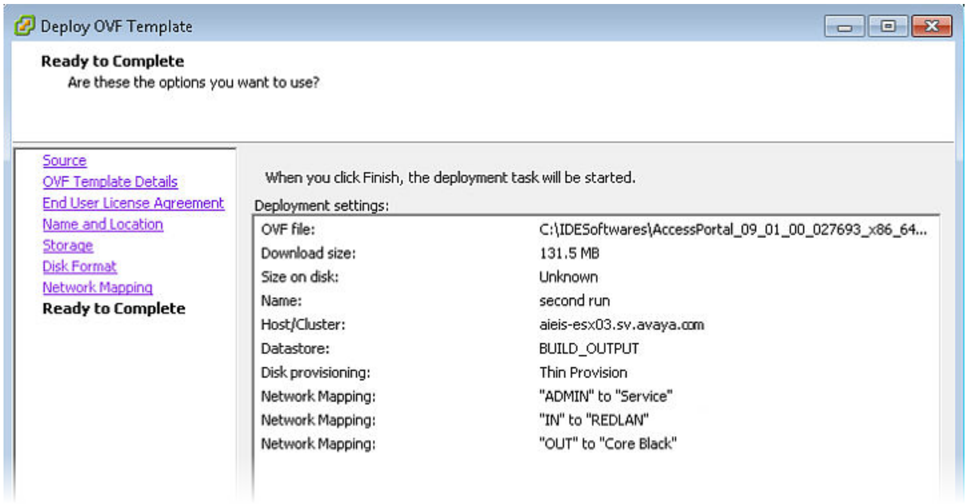
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
ADMIN	Service
IN	REDLAN
OUT	Core Black

Description:

The Local Area Network

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



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

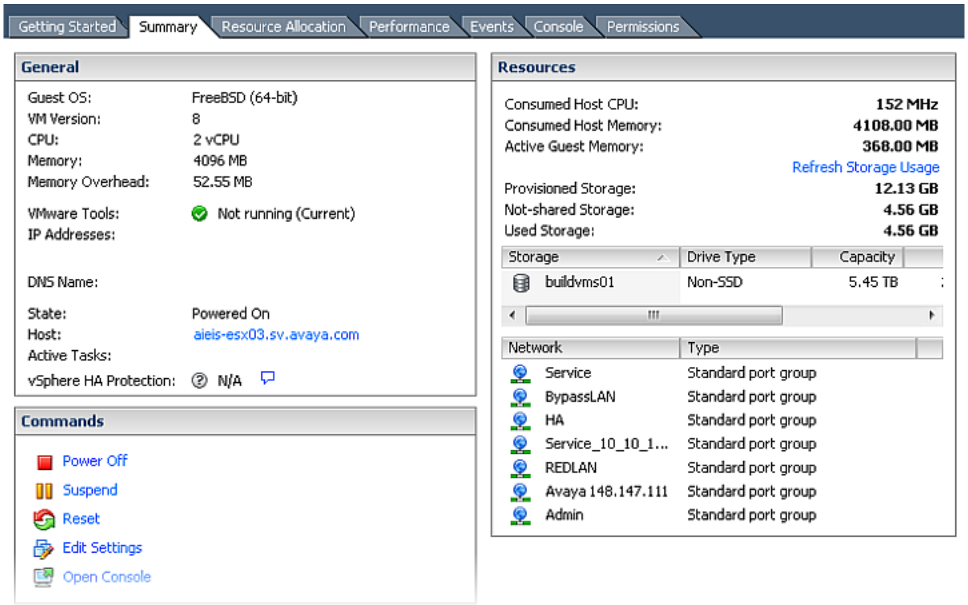
Deployment settings:

OVF file:	C:\IDESoftwares\AccessPortal_09_01_00_027693_x86_64...
Download size:	131.5 MB
Size on disk:	Unknown
Name:	second run
Host/Cluster:	aieis-esx03.sv.avaya.com
Datastore:	BUILD_OUTPUT
Disk provisioning:	Thin Provision
Network Mapping:	"ADMIN" to "Service"
Network Mapping:	"IN" to "REDLAN"
Network Mapping:	"OUT" to "Core Black"

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

Note:

VMware Tools may show as not installed. This is a known VMware issue where VMware Tools may not be detected correctly on certain hardware. However, this does not interfere with the functioning of the tools—it is a display issue only.



General

Guest OS:	FreeBSD (64-bit)
VM Version:	8
CPU:	2 vCPU
Memory:	4096 MB
Memory Overhead:	52.55 MB
VMware Tools:	✓ Not running (Current)
IP Addresses:	
DNS Name:	
State:	Powered On
Host:	aieis-esx03.sv.avaya.com
Active Tasks:	
vSphere HA Protection:	? N/A

Resources

Consumed Host CPU:	152 MHz
Consumed Host Memory:	4108.00 MB
Active Guest Memory:	368.00 MB
Provisioned Storage:	12.13 GB
Not-shared Storage:	4.56 GB
Used Storage:	4.56 GB

Storage	Drive Type	Capacity
buildvms01	Non-SSD	5.45 TB

Network	Type
Service	Standard port group
BypassLAN	Standard port group
HA	Standard port group
Service_10_10_1...	Standard port group
REDLAN	Standard port group
Avaya 148.147.111	Standard port group
Admin	Standard port group

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

Related Links

Preventing automatic VMware Tools updates on page 25

Checking the VMware Tools status (ESXi 5.1 and up) on page 25

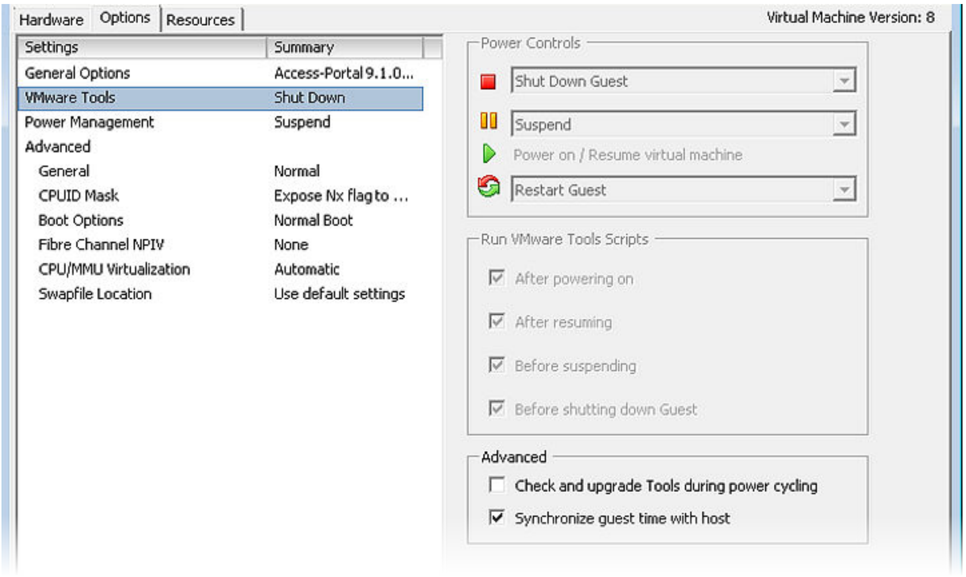
Preventing automatic VMware Tools updates

Avaya recommends that you prevent automatic VMware Tool updates and use only the tools that are delivered bundled with the installation package.

To prevent automatic VMware Tools updates:

Procedure

1. Use the vSphere client to log in to the ESXi Server.
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**.



Virtual Machine Version: 8

Settings	Summary
General Options	Access-Portal 9.1.0...
VMware Tools	Shut Down
Power Management	Suspend
Advanced	
General	Normal
CPUID Mask	Expose Nx flag to ...
Boot Options	Normal Boot
Fibre Channel NPIV	None
CPU/MMU Virtualization	Automatic
Swapfile Location	Use default settings

Power Controls

Shut Down Guest

Suspend

Power on / Resume virtual machine

Restart Guest

Run VMware Tools Scripts

☑ After powering on

☑ After resuming

☑ Before suspending

☑ Before shutting down Guest

Advanced

□ Check and upgrade Tools during power cycling

☑ Synchronize guest time with host

Checking the VMware Tools status (ESXi 5.1 and up)

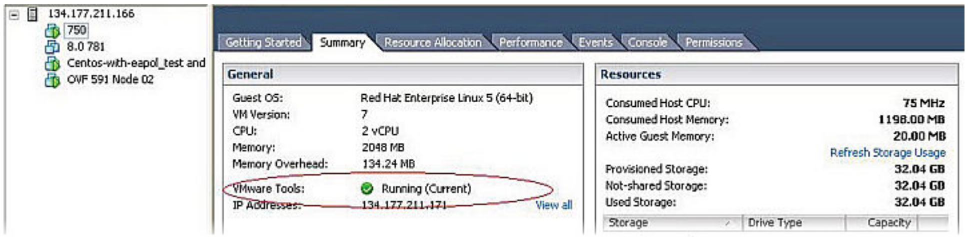
The **Summary** tab of the VM describes the VMware Tools status.

To check the VMware Tools status on an ESXi (5.1 and up) server:

Procedure

1. Use the vSphere client to log in to the ESXi Server.
2. Go to the **Summary** tab.

   After a fresh install, the VMware Tools status displays as “VMware Tools: Running (Current)”.



General

Guest OS:	Red Hat Enterprise Linux 5 (64-bit)
VM Version:	7
CPU:	2 vCPU
Memory:	2048 MB
Memory Overhead:	134.24 MB
VMware Tools:	Running (Current)
IP Addresses:	134.177.211.171

Resources

Consumed Host CPU:	75 MHz
Consumed Host Memory:	1198.00 MB
Active Guest Memory:	20.00 MB
Provisioned Storage:	32.04 GB
Not-shared Storage:	32.04 GB
Used Storage:	32.04 GB

Storage	Drive Type	Capacity

Note:

VMware Tools may show as not installed. This is a known VMware issue where VMware Tools may not be detected correctly on certain hardware. However, this does not interfere with the functioning of the tools—it is a display issue only.

Configuring the Access Portal virtual machine

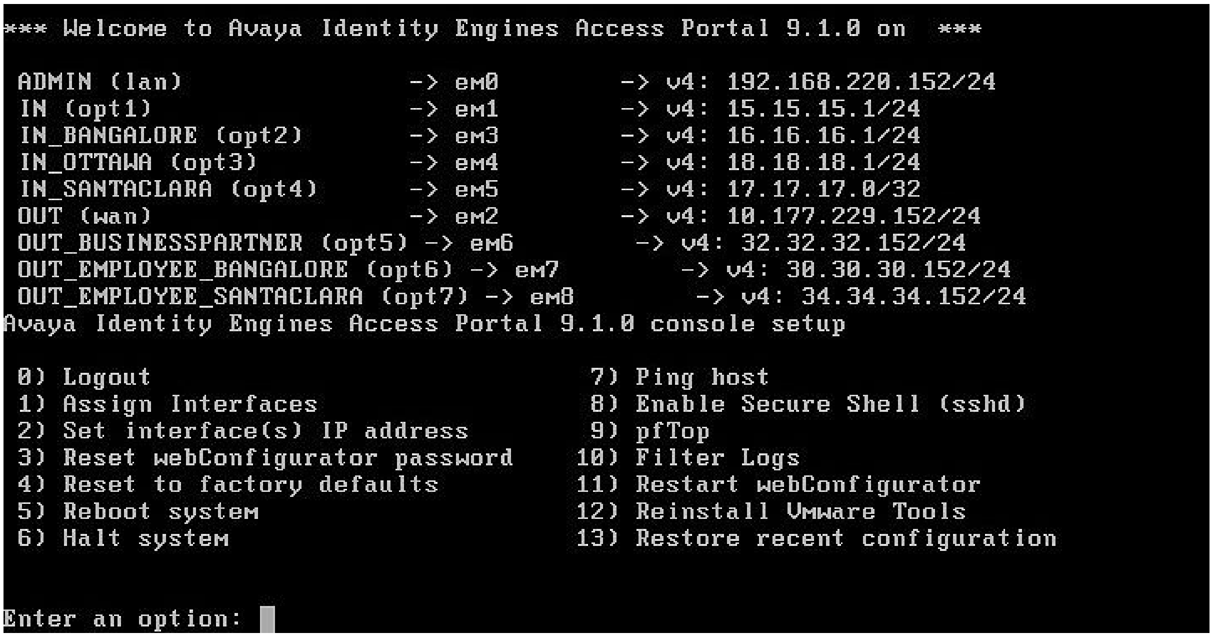
After the import completes, you need to verify and adjust some of the VM settings.

Procedure

1. Boot the Access portal.

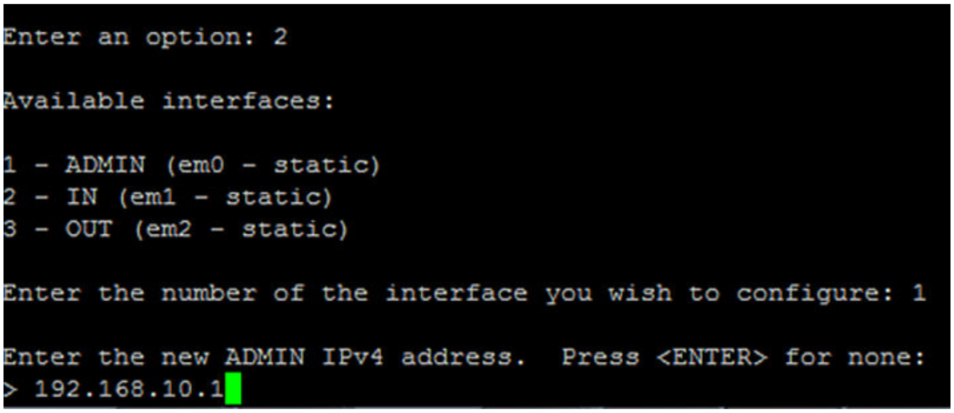
   The Access Portal console displays the interface assignments.

2. From the Access Portal console menu, enter `2`.



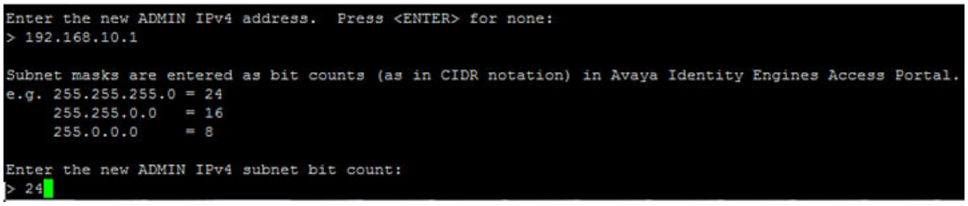
```
*** Welcome to Avaya Identity Engines Access Portal 9.1.0 on  ***

 ADMIN (lan)                -> em0        -> v4: 192.168.220.152/24
 IN (opt1)                  -> em1        -> v4: 15.15.15.1/24
 IN_BANGALORE (opt2)        -> em3        -> v4: 16.16.16.1/24
 IN_OTTAWA (opt3)           -> em4        -> v4: 18.18.18.1/24
 IN_SANTACLARA (opt4)       -> em5        -> v4: 17.17.17.0/32
 OUT (wan)                  -> em2        -> v4: 10.177.229.152/24
 OUT_BUSINESSPARTNER (opt5) -> em6        -> v4: 32.32.32.152/24
 OUT_EMPLOYEE_BANGALORE (opt6) -> em7        -> v4: 30.30.30.152/24
 OUT_EMPLOYEE_SANTACLARA (opt7) -> em8        -> v4: 34.34.34.152/24
Avaya Identity Engines Access Portal 9.1.0 console setup

 0) Logout                              7) Ping host
 1) Assign Interfaces                   8) Enable Secure Shell (sshd)
 2) Set interface(s) IP address         9) pfTop
 3) Reset webConfigurator password     10) Filter Logs
 4) Reset to factory defaults          11) Restart webConfigurator
 5) Reboot system                      12) Reinstall VMware Tools
 6) Halt system                        13) Restore recent configuration


Enter an option:
```

3. From the Access Portal console menu, enter `1` to choose the ADMIN interface, enter the `ADMIN IP address`, and press Enter.



```
Enter an option: 2

Available interfaces:

1 - ADMIN (em0 - static)
2 - IN (em1 - static)
3 - OUT (em2 - static)

Enter the number of the interface you wish to configure: 1

Enter the new ADMIN IPv4 address.  Press <ENTER> for none:
> 192.168.10.1
```

4. Enter the `subnet mask` of the ADMIN IP address and press Enter.



```
Enter the new ADMIN IPv4 address.  Press <ENTER> for none:
> 192.168.10.1

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

Enter the new ADMIN IPv4 subnet bit count:
> 24
```

   The Access Portal console displays the following prompt: `Add static route to ADMIN Interface?[y:n]?`

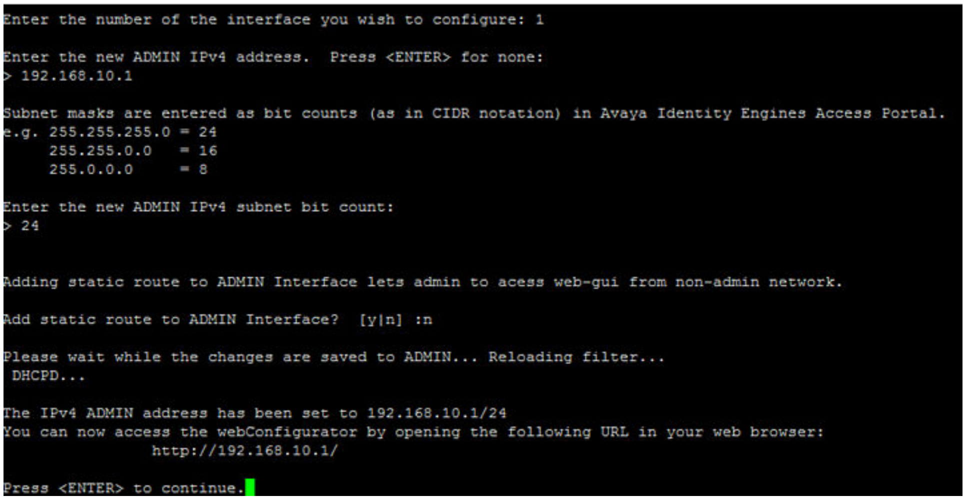
5. Do one of the following:

   - (Recommended) If you have another machine available on your ADMIN network that can be used to connect to the Access Portal Administration Web UI, skip Step 7 on page 28through Step 10 on page 28.
   - (Not recommended) If you do not have another machine available on your ADMIN network that can be used to connect to the Access Portal Administration Web UI, skip Step 6 on page 27.

6. Complete this step only if you have another machine available on your ADMIN network that can be used to connect to the Access Portal Administration Web UI.

   Enter `n` and press Enter.

   The Access Portal console displays the following message: `The IPv4 ADMIN address has been set to <ADMIN IP/mask>`.



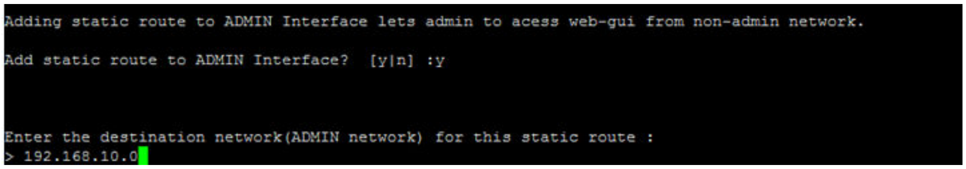
```
Enter the number of the interface you wish to configure: 1

Enter the new ADMIN IPv4 address.  Press <ENTER> for none:
> 192.168.10.1

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

Enter the new ADMIN IPv4 subnet bit count:
> 24


Adding static route to ADMIN Interface lets admin to acess web-gui from non-admin network.

Add static route to ADMIN Interface?  [y|n] :n

Please wait while the changes are saved to ADMIN... Reloading filter...
 DHCPD...

The IPv4 ADMIN address has been set to 192.168.10.1/24
You can now access the webConfigurator by opening the following URL in your web browser:
                http://192.168.10.1/

Press <ENTER> to continue.
```

Skip to Step 11 on page 29.

7. Complete steps 7 through 10 only if you do not have another machine available on your ADMIN network that can be used to connect to the Access Portal Administration Web UI.

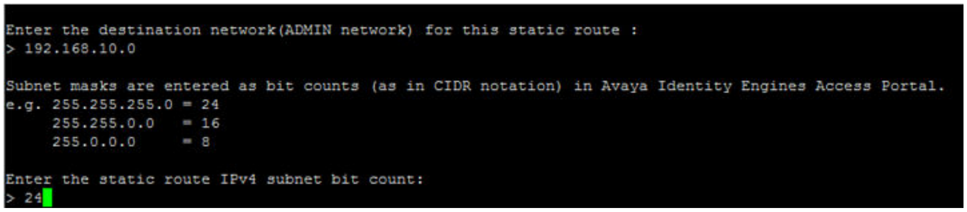
   Enter `y` and press Enter.

8. Enter the destination network (ADMIN network) for this static route.



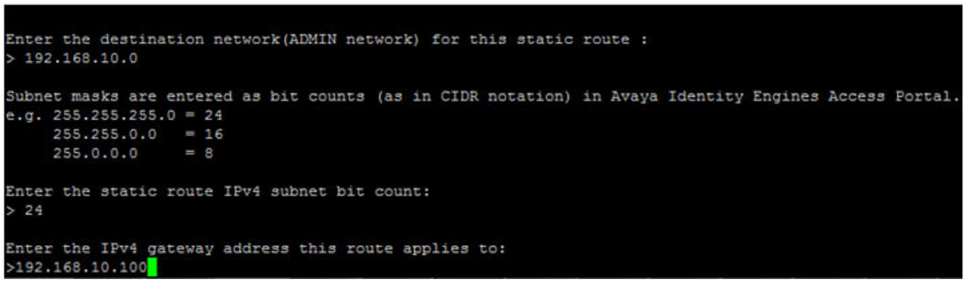
```
Adding static route to ADMIN Interface lets admin to acess web-gui from non-admin network.

Add static route to ADMIN Interface?  [y|n] :y



Enter the destination network(ADMIN network) for this static route :
> 192.168.10.0
```

9. Enter the static route IPv4 subnet bit count.



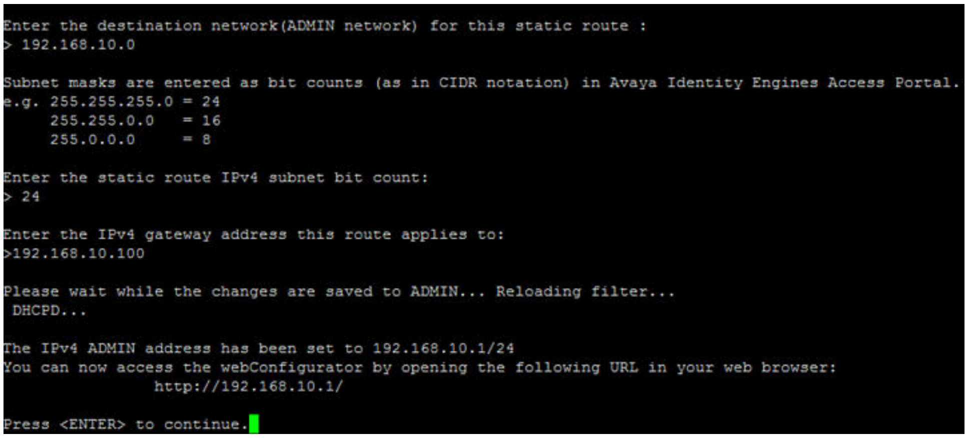
```
Enter the destination network(ADMIN network) for this static route :
> 192.168.10.0

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

Enter the static route IPv4 subnet bit count:
> 24
```

10. Enter the IPv4 gateway address this route applies to and press Enter.



```
Enter the destination network(ADMIN network) for this static route :
> 192.168.10.0

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

Enter the static route IPv4 subnet bit count:
> 24

Enter the IPv4 gateway address this route applies to:
>192.168.10.100
```

The Access Portal console displays the following message: `The IPv4 ADMIN address has been set to <ADMIN IP/mask>`.

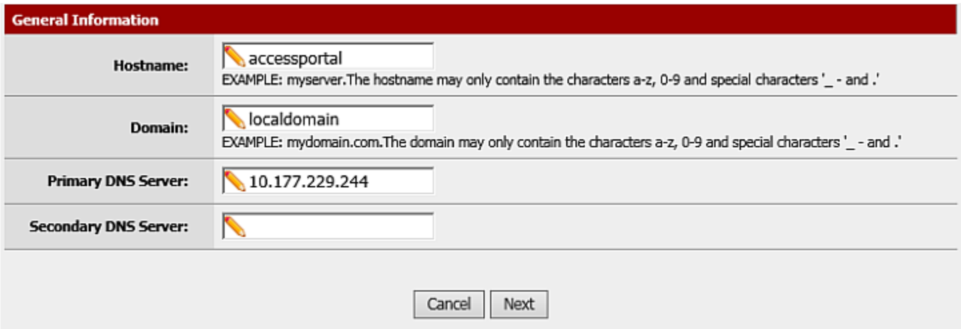


```
Enter the destination network(ADMIN network) for this static route :
> 192.168.10.0

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

Enter the static route IPv4 subnet bit count:
> 24

Enter the IPv4 gateway address this route applies to:
>192.168.10.100

Please wait while the changes are saved to ADMIN... Reloading filter...
 DHCPD...

The IPv4 ADMIN address has been set to 192.168.10.1/24
You can now access the webConfigurator by opening the following URL in your web browser:
                http://192.168.10.1/

Press <ENTER> to continue.
```

11. Access the Access Portal Administration Web UI by opening the following URL in your web browser: `http://<ADMIN IP>`.

    The default credentials are username: `admin` and Password: `admin`.

    A wizard launches the first time you access the Access Portal Administration Web UI, and displays the General Information page.

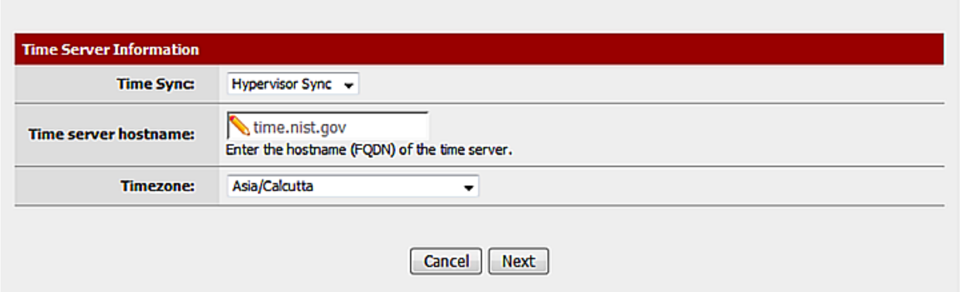


General Information

Hostname:	accessportal EXAMPLE: myserver.The hostname may only contain the characters a-z, 0-9 and special characters '_ - and .'
Domain:	localdomain EXAMPLE: mydomain.com.The domain may only contain the characters a-z, 0-9 and special characters '_ - and .'
Primary DNS Server:	10.177.229.244
Secondary DNS Server:	

12. On the General Information page, do the following:
    - In the **Hostname** field, enter host name of the Access Portal.
    - In the **Domain** field, enter the network domain that the Access Portal serves.
    - 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 displays.

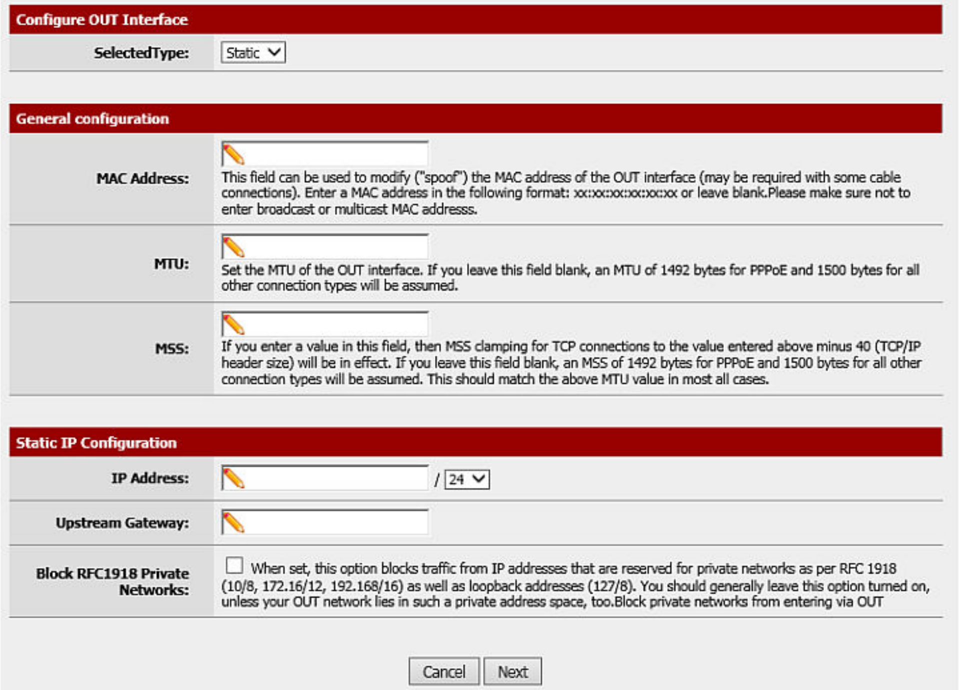


Time Server Information

Time Sync:	Hypervisor Sync
Time server hostname:	time.nist.gov Enter the hostname (FQDN) of the time server.
Timezone:	Asia/Calcutta

13. On the Time Server Information page, do the following:
    - In the **Time Sync** field, do one of the following:
        - leave the default value of **Hypervisor Sync**. Note that Access Portal sets the clock forward for Hypervisor Sync—but not back. If the hypervisor time lags behind the virtual machine time, you must reboot the virtual machine to synchronize the time. If the hypervisor time is ahead of the virtual machine time, no reboot is necessary.
        - to synchronize with a time server, click **NTP Sync** from the drop-down list.
    - If you chose NTP Synch, 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 OUT interface information page displays.



Configure OUT Interface

SelectedType:	Static

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.Please make sure not to enter broadcast or multicast MAC address.
MTU:	Set the MTU of the OUT interface. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
MSS:	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 MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address:	/ 24
Upstream Gateway:	
Block RFC1918 Private Networks:	□ When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your OUT network lies in such a private address space, too.Block private networks from entering via OUT

14. On the OUT interface information page, do the following:

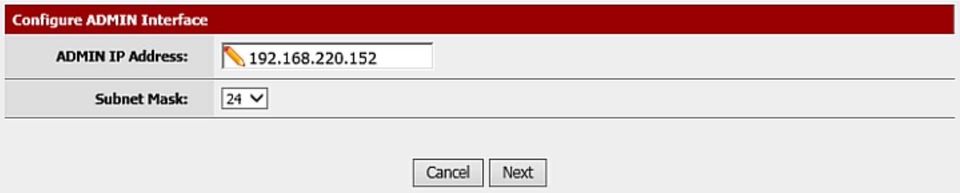
    - Leave the **Selected Type** value as **Static**.

      Note that the OUT interface now requires a Static IP address, unlike previous versions, because of the multiple OUT interface capabilities.

      Also note that at least one OUT interface must have access to DNS in order to be able to capture clients.

    - The **MAC Address** field is usually left blank. To modify ("spoof") the MAC address of the OUT interface, enter a MAC address in the following format xx:xx:xx:xx:xx:xx. This may be required with some cable connections.
    - In the **IP Address** field, assign an IP address to the port. Configure the subnet mask in the adjacent drop-down list. Choose the subnet mask, expressed as a bit count.
    - In the **Gateway** field, enter the IP address of the default gateway for the firewall.
    - Click **Next**.

    The ADMIN interface information page displays.



Configure ADMIN Interface

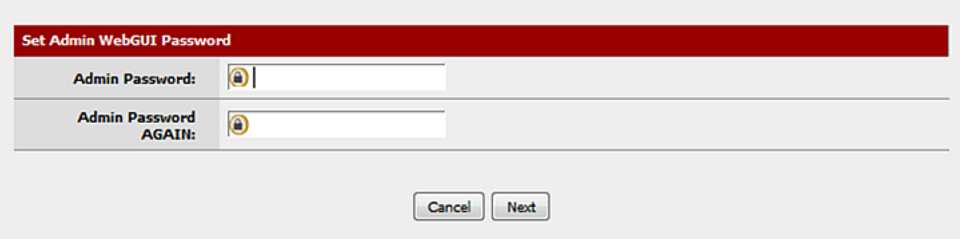
ADMIN IP Address: 192.168.220.152

Subnet Mask: 24

15. On the ADMIN interface information page, do the following:

    - In the **ADMIN IP Address** field, enter the new IP address.
    - From the **Subnet Mask** drop-down list, select the subnet mask, expressed as a bit count.
    - Click **Next**.

    The Admin Password page displays. This password is used to access the Web GUI and SSH services, if enabled.



Set Admin WebGUI Password

Admin Password:

Admin Password AGAIN:

16. (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**.

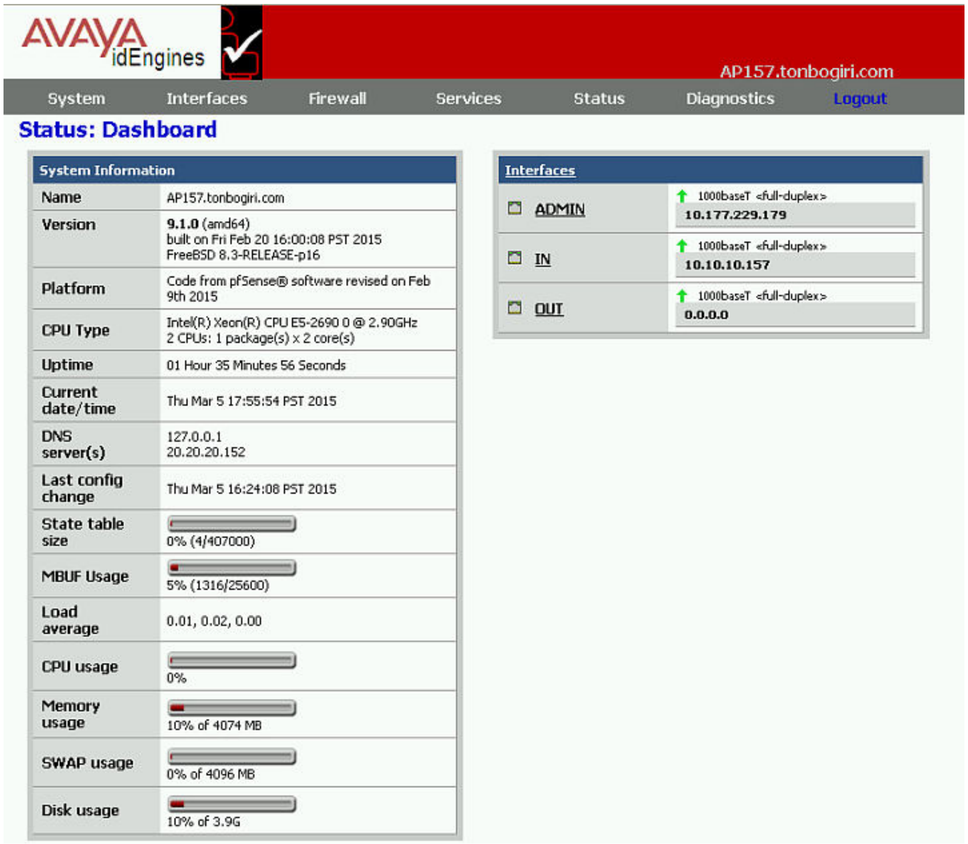
17. Click **Reload** to load the new settings.

If you changed the password, Access Portal prompts you to log in again.

After you click the Avaya icon, or wait for the page to refresh, the System Overview page displays.

You can now access the following Access Portal Administration Web UI main menu headings for further configuration:

- System
- Interfaces
- Firewall
- Services
- Status
- Diagnostics



Status: Dashboard

System Information	
Name	AP157.tonbogiri.com
Version	**9.1.0** (amd64) built on Fri Feb 20 16:00:08 PST 2015 FreeBSD 8.3-RELEASE-p16
Platform	Code from pfSense® software revised on Feb 9th 2015
CPU Type	Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz 2 CPUs: 1 package(s) x 2 core(s)
Uptime	01 Hour 35 Minutes 56 Seconds
Current date/time	Thu Mar 5 17:55:54 PST 2015
DNS server(s)	127.0.0.1 20.20.20.152
Last config change	Thu Mar 5 16:24:08 PST 2015
State table size	0% (4/407000)
MBUF Usage	5% (1316/25600)
Load average	0.01, 0.02, 0.00
CPU usage	0%
Memory usage	10% of 4074 MB
SWAP usage	0% of 4096 MB
Disk usage	10% of 3.9G

Interfaces	
ADMIN	1000baseT <full-duplex> 10.177.229.179
IN	1000baseT <full-duplex> 10.10.10.157
OUT	1000baseT <full-duplex> 0.0.0.0

Related Links

Setting up the Access Portal IN port on page 33

Adding multiple IN and OUT interfaces on page 34

Setting up the Access Portal DNS forwarder on page 38

Configuring the Access Portal DHCP settings on page 39

Configuring the Captive Portal settings on page 41

Customizing user-visible pages on page 45

Configuring Access Groups on page 49
Providing access to servers or other computers from a client machine on page 51

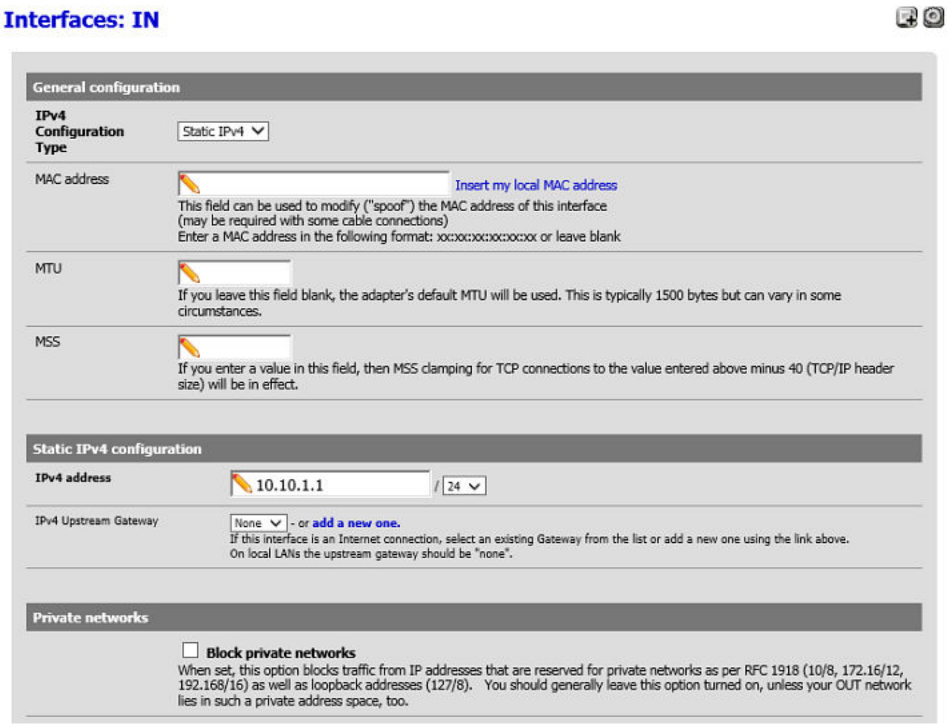
Setting up the Access Portal IN port

The IN port of the Access Portal is the entry point by which guests enter your authentication VLAN. You configure 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 configuration details, see Configuring VLANs on the wired switch on page 71.

To configure the IN port, use the following procedure.

Procedure

1. On the main Access Portal Administration Web UI page, click **Interfaces** > **IN**.
2. In the **IPv4 address** field, enter the IP address of the IN interface.
3. From the adjacent drop-down list, click the subnet mask of the IN interface.
4. Click **Save**.



Interfaces: IN

General configuration

IPv4 Configuration Type	Static IPv4
MAC address	Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this 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 leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	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.

Static IPv4 configuration

IPv4 address	10.10.1.1 / 24
IPv4 Upstream Gateway	None - or **add a new one.** If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the link above. On local LANs the upstream gateway should be "none".

Private networks

☐ **Block private networks**
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your OUT network lies in such a private address space, too.

Adding multiple IN and OUT interfaces

Beginning with Release 9.1, Access Portal allows you to add multiple IN and OUT interfaces. In addition to the three network adapters required for the three out-of-the-box ADMIN, IN, and OUT interfaces, you can add additional adapters to your virtual machine, and then assign them as additional IN or OUT interfaces. The Access Portal can have only one ADMIN interface. Use the following procedure to add additional adapters, assign them as IN or OUT interfaces, and then enable the new interfaces.

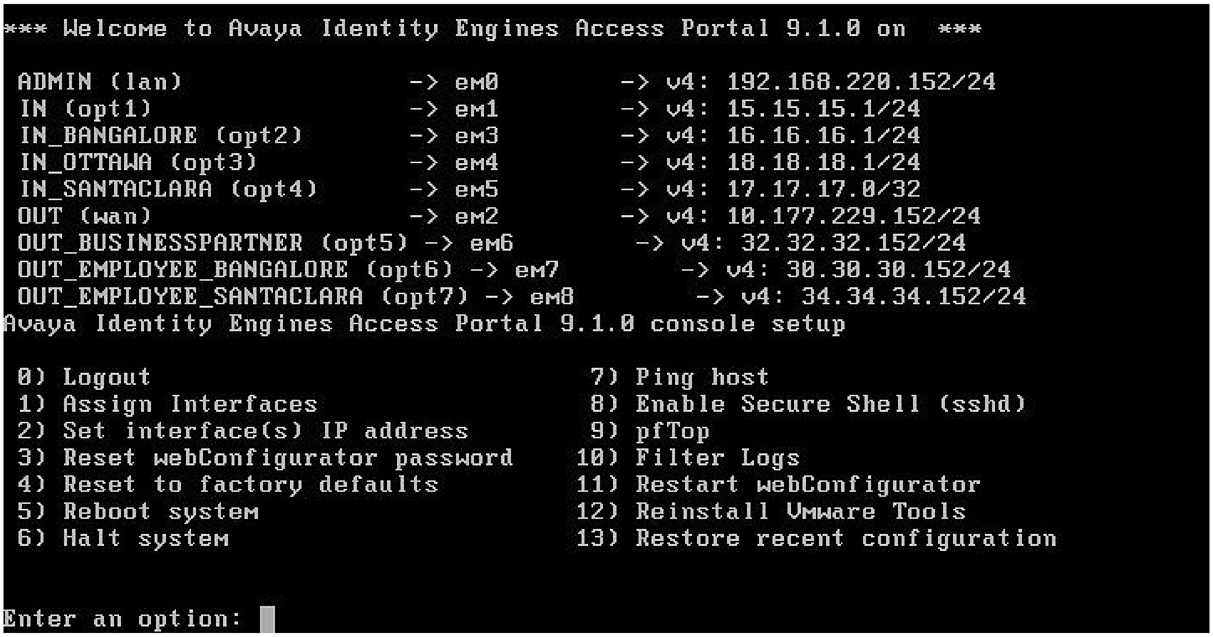
Important:

It is important to ensure that you make the correct assignments between Ethernet adapters and interfaces, and between Ethernet adapters and port groups. Additionally, ensure that the network port assigned has a one-to-one mapping with the interface.

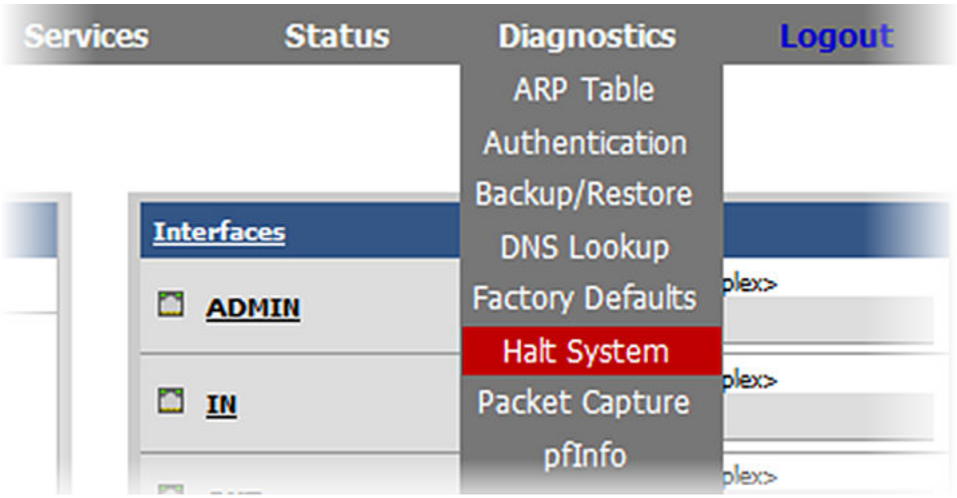
Although it is possible to assign interfaces using the Access Portal console CLI, it is not recommended. Use the Access Portal Administration Web UI to assign adapters to interfaces.

Procedure

1. Do one of the following to halt the system:
   - Open the Access Portal console CLI, and enter `6`.
   - On the main Access Portal Administration Web UI page, click **Diagnostics** > **Halt System**.

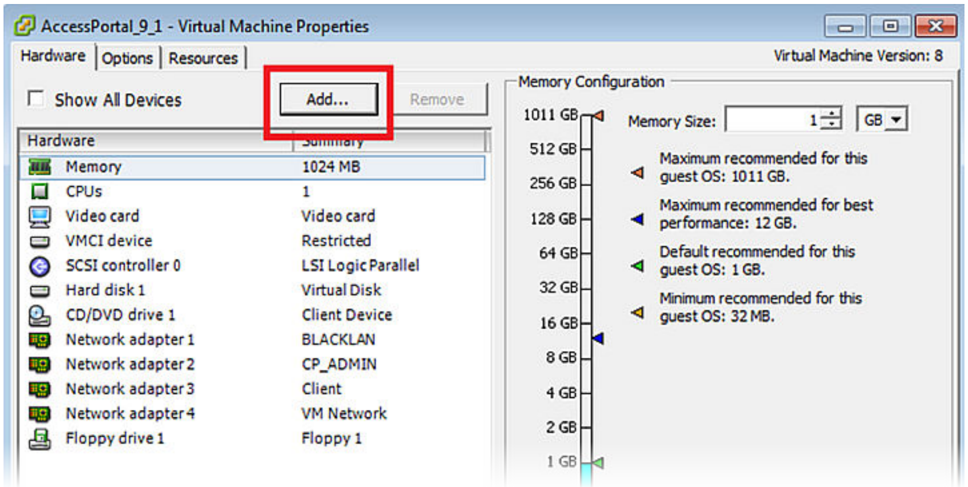


```
*** Welcome to Avaya Identity Engines Access Portal 9.1.0 on  ***

 ADMIN (lan)                -> em0        -> v4: 192.168.220.152/24
 IN (opt1)                  -> em1        -> v4: 15.15.15.1/24
 IN_BANGALORE (opt2)        -> em3        -> v4: 16.16.16.1/24
 IN_OTTAWA (opt3)           -> em4        -> v4: 18.18.18.1/24
 IN_SANTACLARA (opt4)       -> em5        -> v4: 17.17.17.0/32
 OUT (wan)                  -> em2        -> v4: 10.177.229.152/24
 OUT_BUSINESSPARTNER (opt5) -> em6         -> v4: 32.32.32.152/24
 OUT_EMPLOYEE_BANGALORE (opt6) -> em7         -> v4: 30.30.30.152/24
 OUT_EMPLOYEE_SANTACLARA (opt7) -> em8         -> v4: 34.34.34.152/24
Avaya Identity Engines Access Portal 9.1.0 console setup

 0) Logout                              7) Ping host
 1) Assign Interfaces                   8) Enable Secure Shell (sshd)
 2) Set interface(s) IP address         9) pfTop
 3) Reset webConfigurator password     10) Filter Logs
 4) Reset to factory defaults          11) Restart webConfigurator
 5) Reboot system                      12) Reinstall VMware Tools
 6) Halt system                        13) Restore recent configuration


Enter an option:
```



2. In the VMware vSphere Client, right-click the virtual machine name and click **Edit Settings**.

   The Virtual Machine Properties page displays.



☐ Show All Devices

Hardware	Summary
Memory	1024 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
CD/DVD drive 1	Client Device
Network adapter 1	BLACKLAN
Network adapter 2	CP_ADMIN
Network adapter 3	Client
Network adapter 4	VM Network
Floppy drive 1	Floppy 1

Memory Size: 1 GB

Maximum recommended for this guest OS: 1011 GB.

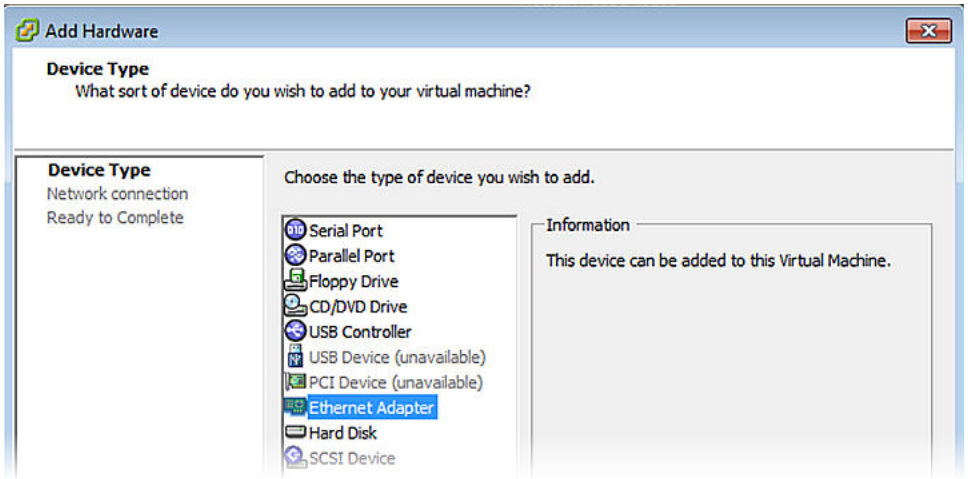
Maximum recommended for best performance: 12 GB.

Default recommended for this guest OS: 1 GB.

Minimum recommended for this guest OS: 32 MB.

3. On the Virtual Machine Properties page, click **Add**.

   The Add Hardware page displays.



Add Hardware

Device Type

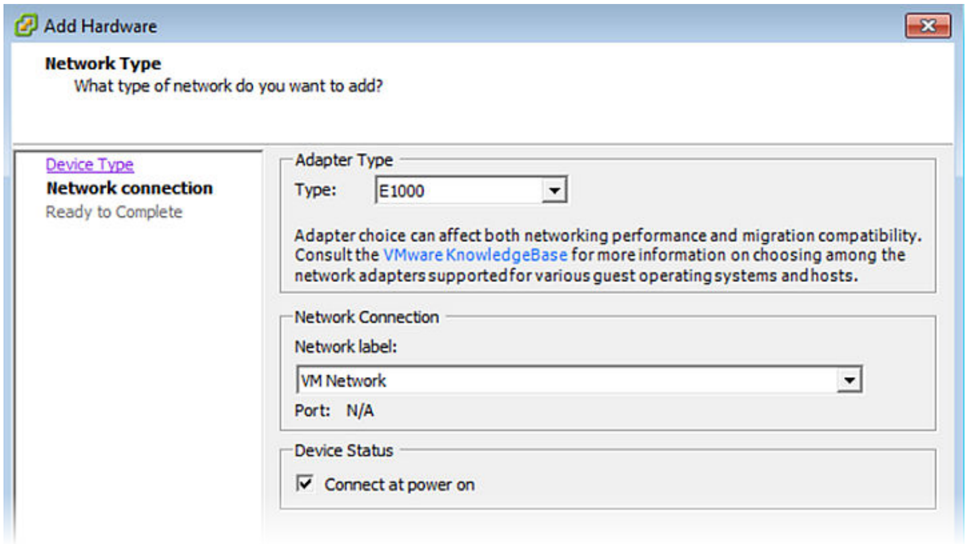
What sort of device do you wish to add to your virtual machine?

Choose the type of device you wish to add.

Information

This device can be added to this Virtual Machine.

4. In the **Device Type** area, click **Ethernet Adapter**, and click **Next**.
5. Leave the **Adapter Type** as the default value of E1000, select the appropriate network in the **Network Label** field, select the **Connect at power on checkbox**, and click **Next**.



Add Hardware

Network Type

What type of network do you want to add?

Adapter Type

Type: E1000

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

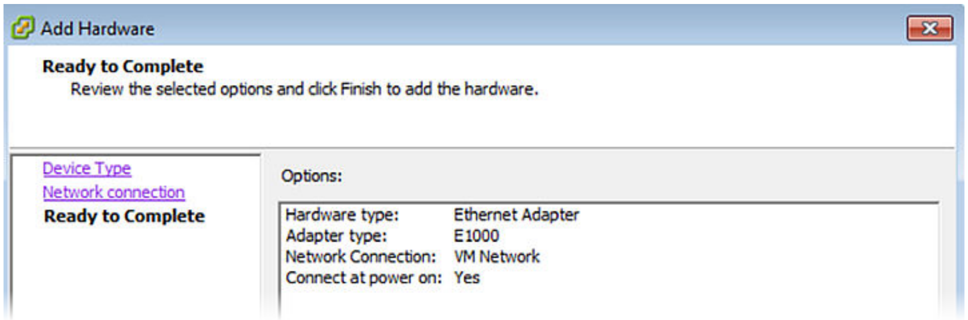
Network Connection

Network label: VM Network

Port: N/A

Device Status

☑ Connect at power on



Add Hardware

Ready to Complete

Review the selected options and click Finish to add the hardware.

Options:

Hardware type:	Ethernet Adapter
Adapter type:	E1000
Network Connection:	VM Network
Connect at power on:	Yes

6. Verify the settings and click **Finish**.
7. Repeat Step 4 on page 35 through Step 7 on page 36 for each adapter you want to add.

8. After all adapters have been added, power on the virtual machine and wait for it to boot completely.

   You must now assign the newly added adapters as interfaces to your Access Portal.

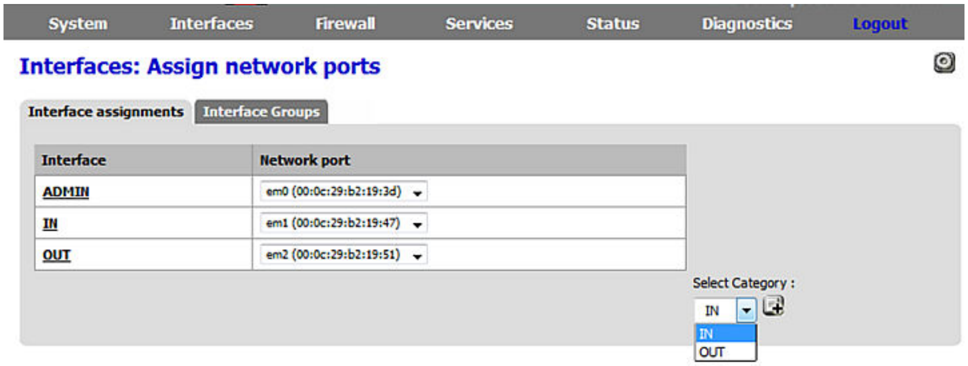
   Although it is possible to assign interfaces using the Access Portal console CLI, it is not recommended. Use the Access Portal Administration Web UI to assign adapters to interfaces.

9. On the main Access Portal Administration Web UI page, click **Interfaces** > **(assign)**.

   The Interfaces: Assign network ports page displays.

10. Do one of the following:

    - To assign a newly added network adapter as an IN interface, click **IN** in the **Select Category** drop-down list, and then click the Add icon to the right of the drop-down list.
    - To assign a newly added network adapter as an OUT interface, click **OUT** in the **Select Category** drop-down list, and then click the Add icon to the right of the drop-down list.



Interfaces: Assign network ports

Interface	Network port
ADMIN	em0 (00:0c:29:b2:19:3d)
IN	em1 (00:0c:29:b2:19:47)
OUT	em2 (00:0c:29:b2:19:51)

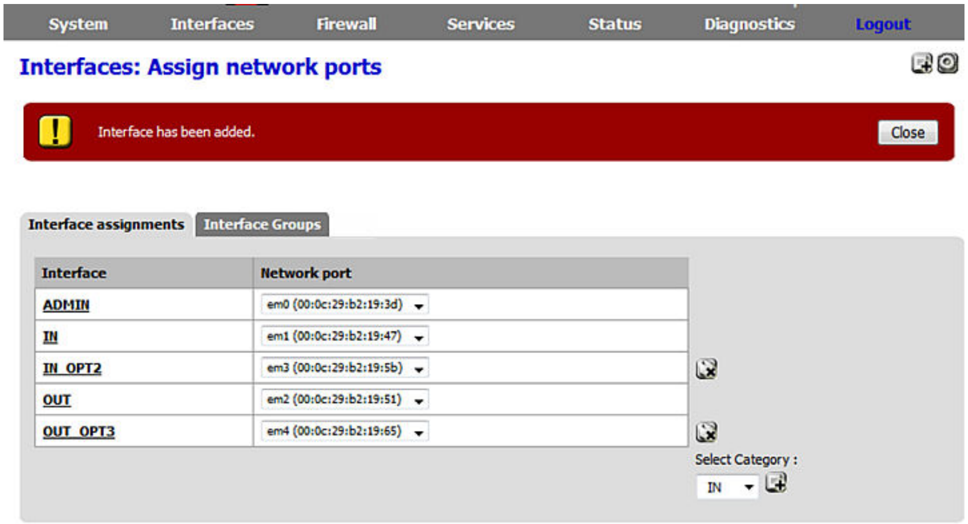
Select Category : IN

The page refreshes and displays the newly added interface in the **Interface Assignments** list.

11. Click the **Network Port** drop-down list for the new interface, and select the Ethernet adapter that you want to assign to this interface.

    Important:

    The three basic ADMIN, IN, and OUT interfaces are by default assigned to the “em0”, “em1”, and “em2” network ports. Do not change the default network port assignments for these three interfaces.



Interfaces: Assign network ports

Interface has been added.

Interface	Network port
ADMIN	em0 (00:0c:29:b2:19:3d)
IN	em1 (00:0c:29:b2:19:47)
IN_OPT2	em3 (00:0c:29:b2:19:5b)
OUT	em2 (00:0c:29:b2:19:51)
OUT_OPT3	em4 (00:0c:29:b2:19:65)

12. Click **Save**.

    The newly added interface is saved and is ready to be enabled.

13. To enable the newly added interface, on the main Access Portal Administration Web UI page, click **Interfaces**, and then click the name of the interface.

    The Interfaces: <interface name> page displays.

14. Do the following:

    - Ensure that the **Enable Interface** check box is selected.
    - In the **Description** field, enter a name for the interface.

      Important:

      The name for additional IN or OUT interfaces should start with the prefix “IN” or “OUT” respectively. For example, you could name additional IN interfaces “IN_Employee”, or “INGuest”, or conversely, you could name additional OUT interfaces “OUT_Employee”, or “OUTGuest”, and so on. This ensures that all interfaces are presented in a coherent manner for future administration and monitoring.
    - In the **IPv4 Address** field, enter the IP address of the interface.
    - From the adjacent drop-down list, select the subnet mask of the interface.
    - Click **Save**.

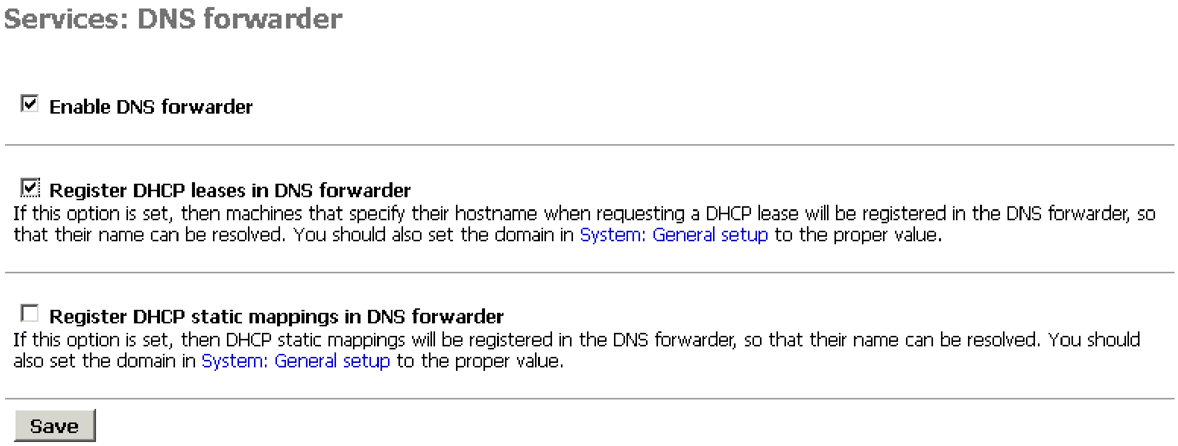
Setting up the Access Portal DNS forwarder

Use the following procedure to configure the Access Portal DNS forwarder.

Procedure

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

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



Services: DNS forwarder

☑ Enable DNS forwarder

☑ Register DHCP leases in DNS forwarder
If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

□ Register DHCP static mappings in DNS forwarder
If this option is set, then DHCP static mappings will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

Configuring the Access Portal DHCP settings

The Access Portal DHCP server settings allow the Ignition Server 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.

Follow this procedure to configure Access Portal to act as a DHCP server for the client network (default setting).

Procedure

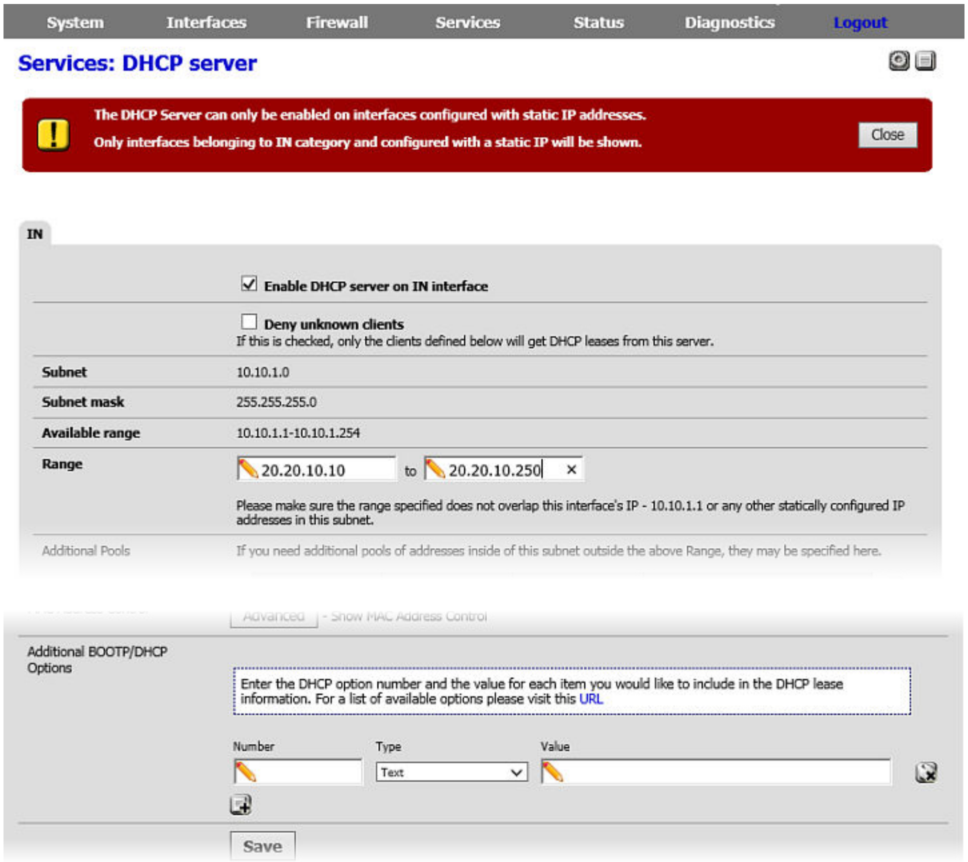
1. On the main Access Portal Administration Web UI page, click **Services** > **DHCP Server**.
2. On the Services: DHCP server page, click the appropriate IN interface tab.
3. Select the **Enable DHCP Server on IN interface** check box.
4. In the **Range** fields, enter the range of IP addresses that the DHCP server will assign to guest devices.
5. Optionally scroll down to the **Additional BOOTP/DHCP Options** section, click **Advanced**, and click the Add icon to send additional DHCP options to the client. Click **Save**.

   This can include other DHCP options such as proxy settings. See Appendix A: Access Portal deployment example on page 84 for an example deployment that includes pushing the proxy setting to the clients to make the clients work with Access Portal and a proxy server.
6. Configure remaining settings as required.

Note that the behavior of the Default lease time is as follows:

- If the default lease time is configured as 300 seconds or more, then this value is used as the default lease time and the renew time the clients use is half of that value.
- If default lease time is configured as anything less than 300 seconds, Access Portal considers the default lease time as 300 seconds and this value is used as the renew time by the clients.

7. Click **Save**.



Services: DHCP server

The DHCP Server can only be enabled on interfaces configured with static IP addresses.
Only interfaces belonging to IN category and configured with a static IP will be shown.

☑ Enable DHCP server on IN interface

□ Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this server.

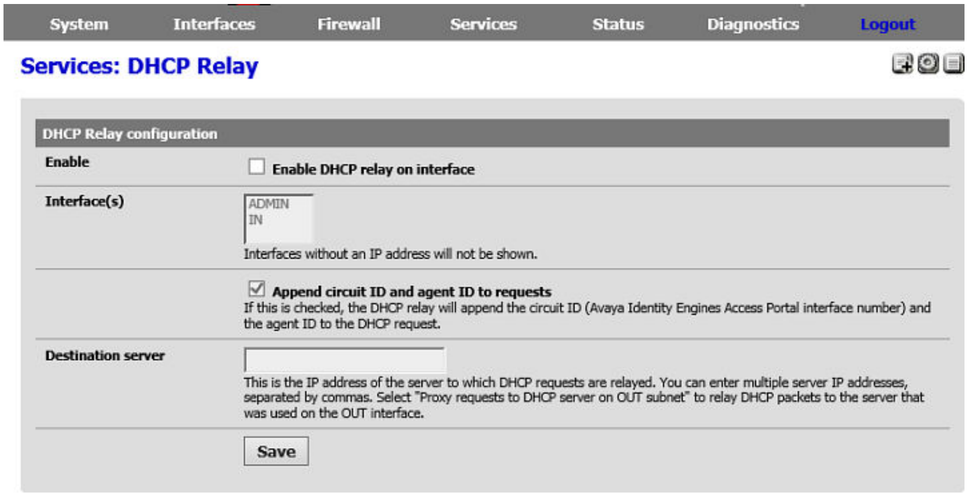
Subnet	10.10.1.0
Subnet mask	255.255.255.0
Available range	10.10.1.1-10.10.1.254
Range	20.20.10.10 to 20.20.10.250 Please make sure the range specified does not overlap this interface's IP - 10.10.1.1 or any other statically configured IP addresses in this subnet.
Additional Pools	If you need additional pools of addresses inside of this subnet outside the above Range, they may be specified here.
	Advanced - Show MAC Address Control
Additional BOOTP/DHCP Options	Enter the DHCP option number and the value for each item you would like to include in the DHCP lease information. For a list of available options please visit this URL

Number	Type	Value
	Text	

To configure Access Portal to use an external DHCP server:

a. On the main Access Portal Administration Web UI page, click **Services** > **DHCP Relay**.

The Services: DHCP Relay page displays.



Services: DHCP Relay

DHCP Relay configuration

Enable	□ Enable DHCP relay on interface
Interface(s)	ADMIN IN Interfaces without an IP address will not be shown.
	☑ Append circuit ID and agent ID to requests If this is checked, the DHCP relay will append the circuit ID (Avaya Identity Engines Access Portal interface number) and the agent ID to the DHCP request.
Destination server	This is the IP address of the server to which DHCP requests are relayed. You can enter multiple server IP addresses, separated by commas. Select "Proxy requests to DHCP server on OUT subnet" to relay DHCP packets to the server that was used on the OUT interface.
	Save

b. Select the **Enable DHCP relay on interface** check box.

c. In the **Interfaces** field, click the **IN** interface.

d. In the **Destination server** section, enter the IP address of the server to which the DHCP packet is relayed.

e. Click **Save**.

Configuring the Captive Portal settings

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

Beginning with Release 9.1, in addition to the ability to add multiple IN interfaces, you can define zones for captive portal. Zones are captive portal settings that apply to one or more IN interfaces.

Note that session time out settings do not apply to the Access Portal CLI Console. Administrators must log out manually from the Console.

Important:

Ensure that you enable the DHCP server on your captive portal interface. Ensure that the default/maximum DHCP lease time is greater than the time-out entered on this page. The DNS forwarder must be enabled for DNS lookups by unauthenticated clients to work.

Warning:

This procedure contains steps that disconnect all clients!

It is therefore advised to perform this procedure only during a maintenance window.

Procedure

1. On the main Access Portal Administration Web UI page, click **Services** > **Captive Portal**.

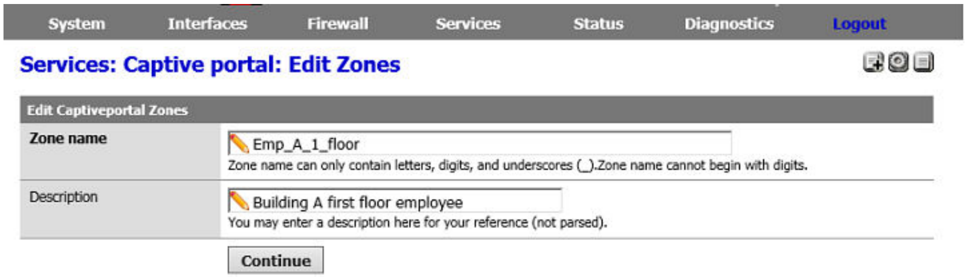
   The Captiveportal: Zones page displays.

2. Click the Add icon on the right side of the page.

   The Services: Captive portal: Edit Zones page displays.

3. Enter a name for the zone into the **Zone name** field.

4. Optionally enter a description into the **Description** field.



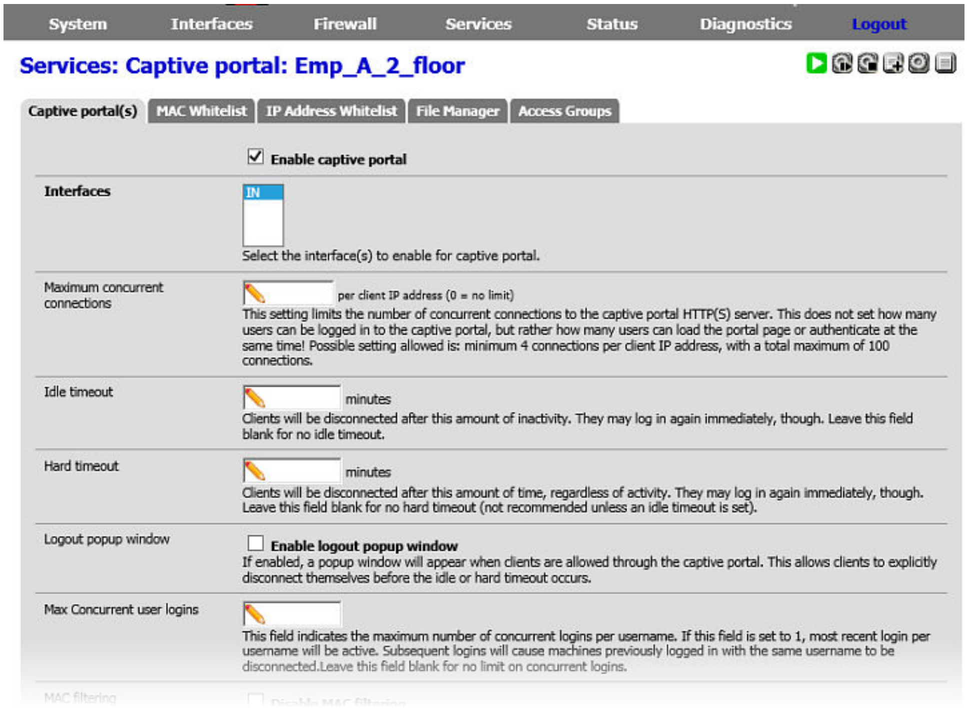
Services: Captive portal: Edit Zones

Edit Captiveportal Zones

Zone name	Emp_A_1_floor Zone name can only contain letters, digits, and underscores (_).Zone name cannot begin with digits.
Description	Building A first floor employee You may enter a description here for your reference (not parsed).

5. Click **Continue**.

   The **Services: Captive portal** page displays, listing all available **IN** interfaces in the **Interfaces** field.



Services: Captive portal: Emp_A_2_floor

	☑ Enable captive portal
Interfaces	IN Select the interface(s) to enable for captive portal.
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! Possible setting allowed is: minimum 4 connections per client IP address, with a total maximum of 100 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.
Max Concurrent user logins	This field indicates the maximum number of concurrent logins per username. If this field is set to 1, most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.Leave this field blank for no limit on concurrent logins.
MAC filtering	□ Disable MAC filtering

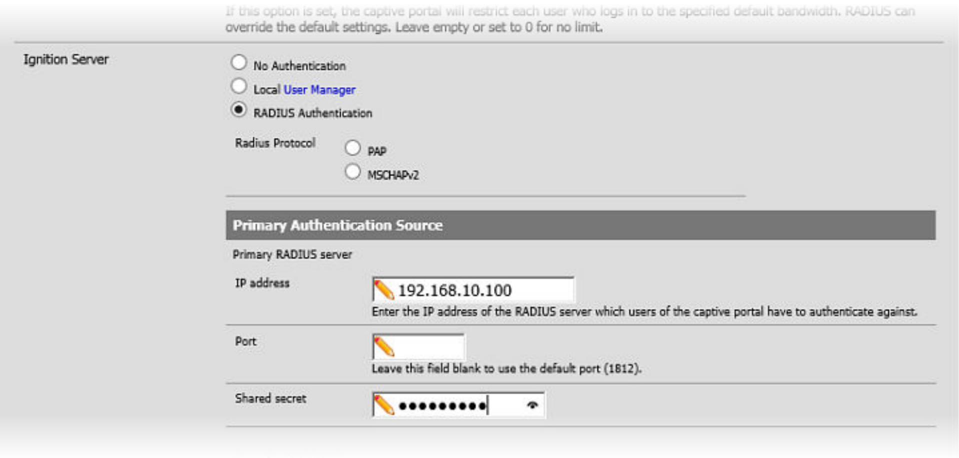
6. On the **Services: Captive portal** page, do the following:
   - Select the **Enable captive portal** check box.
   - Select the IN interfaces that you want to enable for this zone in the **Interface** field.

Note:

You can choose more than one IN interface. However, an interface an only be enabled for one zone; you cannot enable this interface in another zone.

- In the **Maximum Concurrent connections** field, enter a value to limit the number of users that can concurrently load the portal page or authenticate.
- In the **Idle timeout** field, enter the maximum amount of time, in minutes, that the client can sit idle before being disconnected.
- In the **Hard timeout** field, enter the maximum length of the session regardless of activity, in minutes.
- Select the **Enable logout popup window** check box to allow users to manually log out before Idle or Hard timeouts.
- In the **Max Concurrent user logins** field, enter a value for the maximum number of devices a user can log onto concurrently.

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



If this option is set, the captive portal will restrict each user who logs in to the specified default bandwidth. RADIUS can override the default settings. Leave empty or set to 0 for no limit.

Ignition Server

○ No Authentication
○ Local User Manager
● RADIUS Authentication

Radius Protocol ○ PAP ○ MSCHAPv2

Primary Authentication Source

Primary RADIUS server

IP address: 192.168.10.100

Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.

Port:

Leave this field blank to use the default port (1812).

Shared secret: ••••••••••

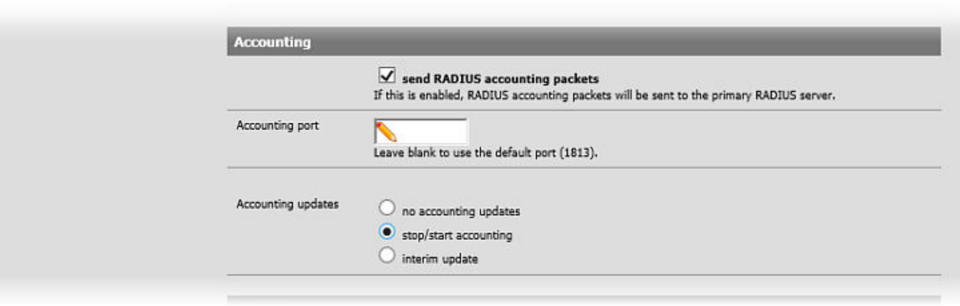
8. In the **Accounting** section, ensure that the **Send RADIUS accounting packets** check box is selected.

    Access Portal sends only the following standard RADIUS attributes:

    - Calling-Station-Id: This attribute contains the MAC address of the authenticating client device.
    - Framed-IP-Address: This attribute contains the IP address of the authenticating client device.
    - NAS-IP-Address: This attribute contains the IP address of the ADMIN interface. Note that, in previous releases, this contained the IP address of the OUT interface.

- NAS-Port: This attribute contains a fixed value of 1.
- NAS-Port-Type: This attribute contains a fixed value of 15.
- NAS-Identifier: By default, this attribute contains the name of the Access Portal. You can, however, configure the value under **Services** > **Captive Portal** > **<Zone>**, within the **RADIUS options** section of the **Captive Portal(s)** tab.
- Service-Type: This attribute contains a fixed value of 1.
- Avaya RADIUS VSAs for device profiling, the name of the IN interface that the client enters through, and the name of the captive portal zone that the client belongs to.

9. In the **Accounting updates** section, select **Stop/start accounting**.



Accounting

☑ send RADIUS accounting packets

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

Accounting port

Leave blank to use the default port (1813).

Accounting updates

○ no accounting updates

● stop/start accounting

○ interim update

10. Configure RADIUS reauthentication to enforce the timeout of guest network sessions. (The session expiry periods are configured in your Ignition Server authorization policy.) In the **RADIUS options Session-Timeout** section, do one of the following:

    - Select **No Timeout**.
    - Select **Soft Timeout**.

    For a soft timeout, the portal attempts to reauthenticate the client after the timeout period using the cached credentials. If the authentication succeeds, there is no disruption to the client; the client is unaware of the authentication happening in the background. However, if the authentication fails, the client gets disconnected and the user must log in again.

    Be aware that a soft timeout and subsequent reauthentication implies the same user session. This may have implications for any policies that you may configure on the Ignition Server. For example, inbound attributes sent by Access Portal are only sent upon initial login—not during reauthentication for a soft timeout. Therefore, if a policy contains inbound attributes, and the inbound attributes change during the course of the user session, the user may experience a failed reauthentication after a soft timeout. A hard timeout would be a better option for this type of policy. Conversely, device fingerprinting attributes do not change during the course of a user session, so policies that contain device attributes work with the soft timeout option.

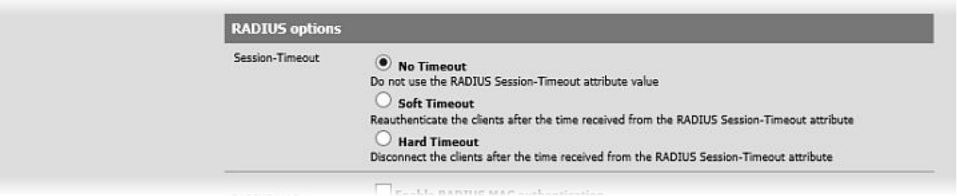
    Note that this option is similar to the “Reauthenticate Connected Users Every Minute” functionality in previous releases, but is more flexible. The reauthentication frequency is configurable by defining the RADIUS outbound session time out value. Additionally, this reauthentication strategy does not have to apply to all users, instead choosing the users based on the policies defined on the Ignition Server.

- Select **Hard Timeout**.

  For a hard timeout, after the timeout period, the portal disconnects the client and the user must log in again.

  It is important to be aware of the differences and interaction between the Captive Portal Hard Timeout option you defined in Step 6 on page 42, and this RADIUS Session Hard Timeout option. Consider the following:

  - This RADIUS Session Hard Timeout setting only applies if you enabled RADIUS Authentication in Step 7 on page 43, while the Captive Portal Hard Timeout setting is unrelated to RADIUS Authentication.
  - This RADIUS Session Hard Timeout setting is applicable only for those users for whom this value is received. This value may be different for different users or not present for some users. Conversely, the Captive Portal Hard Timeout setting applies to all users.
  - If a timeout value is specified for both Hard Timeout options, the lower value takes precedence.



RADIUS options

Session-Timeout

● **No Timeout**
Do not use the RADIUS Session-Timeout attribute value

○ **Soft Timeout**
Reauthenticate the clients after the time received from the RADIUS Session-Timeout attribute

○ **Hard Timeout**
Disconnect the clients after the time received from the RADIUS Session-Timeout attribute

11. Click **Save**.

Customizing user-visible pages

You can customize four user-visible pages: the login page, the success page, the static logout page, and the authentication error page. First, you create and upload the user-visible HTML pages, and then you select which login, success, static logout, and error pages that Access Portal displays to users.

Warning:

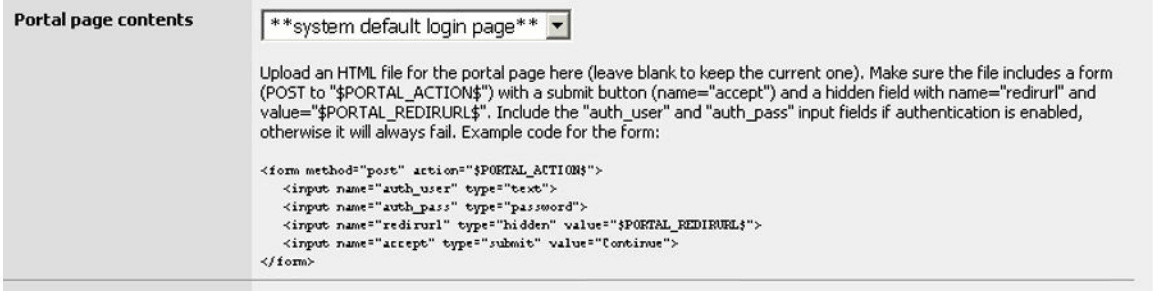
Any procedure for selecting user-visible pages contains steps that disconnect all clients!

It is therefore advised to perform those procedures only during a maintenance window.

Creating customized user-visible pages

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

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**.



Portal page contents

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. Use the following procedure to load your customized HTML pages, as well as any supporting image and Cascading Style Sheet (CSS) files.

Any files that you upload here are 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:

<img src="test.jpg" width=... height=...>

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=$PORTAL_REDIRURL$"> Acceptable usage policy</a>

For this procedure, the total size limit for all files is 1 MB. If your file size is larger than 1 MB, use the Upload Big Files interface on the File Manager page to upload the large files. Note that the files you upload using the Upload Big Files interface are not backed up.

Procedure

1. On the main Access Portal Administration Web UI page, click **Services** > **Captive Portal**.

   The Captive Portal: Zones page displays.

2. Click the Edit icon to the right of the desired captive portal.

   The Services: Captive portal page displays with the Captive Portal(s) tab selected.

3. Click the **File Manager** tab.

   The window displays a table listing all the files that were previously uploaded.

4. Click the plus sign (**+**) to the right of the bottom row in the table.
5. Click **Browse**, navigate to the desired file, and click **Open**.
6. Click **Upload** to load the file.

7. Repeat Step 4 on page 46 through Step 6 on page 46 for each file you want to upload.

Selecting the Access Portal login page

Follow this procedure to select the Access Portal login page.

⚠ **Warning:**

This procedure contains steps that disconnect all clients!

It is therefore advised to perform this procedure only during a maintenance window.

Procedure

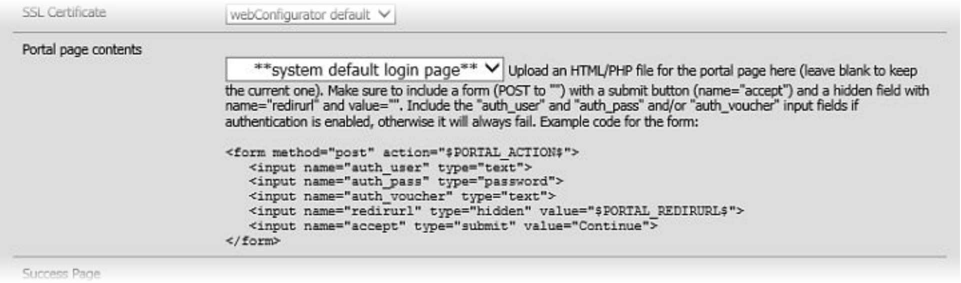
1. On the main Access Portal Administration Web UI page, click **Services** > **Captive Portal**.

   The Captive Portal: Zones page displays.

2. Click the Edit icon to the right of the desired captive portal.

   The Services: Captive portal page displays with the Captive Portal(s) tab selected.

3. Scroll down to the **Portal page contents** section.



SSL Certificate: webConfigurator default

Portal page contents: **system default login page** Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "") with a submit button (name="accept") and a hidden field with name="redirurl" and value="". Include the "auth_user" and "auth_pass" and/or "auth_voucher" 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="auth_voucher" type="text">
   <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
   <input name="accept" type="submit" value="Continue">
</form>
```

Success Page

4. From the drop-down list, select the HTML file you want to use for your login page.
5. Click **Save**.

   The portal page displays.

Selecting the Success page

Follow this procedure to configure the **Success** page.

Note:

If a CASE package is deployed on Access Portal, the CASE application provides its own success page.

⚠ **Warning:**

This procedure contains steps that disconnect all clients!

It is therefore advised to perform this procedure only during a maintenance window.

Procedure

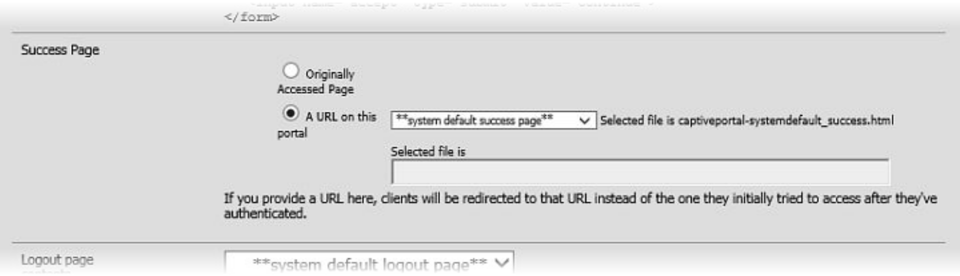
1. On the main Access Portal Administration Web UI page, click **Services** > **Captive Portal**.

The Captive Portal: Zones page displays.

2. Click the Edit icon to the right of the desired captive portal.

   The Services: Captive portal page displays with the Captive Portal(s) tab selected.

3. Scroll down to the **Success Page** section.



</form>

Success Page

○ Originally Accessed Page

● A URL on this portal   **system default success page**   Selected file is captiveportal-systemdefault_success.html

Selected file is

If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.

Logout page   **system default logout page**

4. 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 **Originally Accessed Page**.
   - If, after clients authenticate, you want to direct them to an URL on this portal, select **A URL on this portal** , and specify the URL in the **Selected file is** field.

5. 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 sees this page upon successful authentication.
   - If, after clients authenticate, you want to direct them to a URL on this portal, select the appropriate file name from the drop-down list that corresponds to the Success page you want to show. The guest user sees this page upon successful authentication.
   - If, after clients authenticate, you want to direct them to a URL on another server, click **On Other Servers: Specify URL below**, and specify the full URL in the field below.

6. Click **Save**.

Selecting the Authentication error page

Follow this procedure to select the Authentication error page contents.

⚠ **Warning:**

This procedure contains steps that disconnect all clients!

It is therefore advised to perform this procedure only during a maintenance window.

Procedure

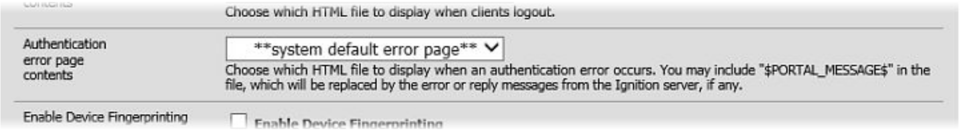
1. On the main Access Portal Administration Web UI page, click **Services** > **Captive Portal**.

   The Captive Portal: Zones page displays.

2. Click the Edit icon to the right of the desired captive portal.

The Services: Captive portal page displays with the Captive Portal(s) tab selected.

3. Scroll down to the **Authentication error page contents** section.



Choose which HTML file to display when clients logout.

Authentication error page contents: **system default error page** ▾

Choose which HTML file to display when an authentication error occurs. You may include "$PORTAL_MESSAGE$" in the file, which will be replaced by the error or reply messages from the Ignition server, if any.

Enable Device Fingerprinting: □ Enable Device Fingerprinting

4. From the drop-down list, select the HTML file you want to use for your authentication failure page.

   The guest user sees this page if an authentication attempt fails.

5. Click **Save.**

Selecting the static Logout page

Users can access this page to log out by entering the following address in a web browser:

```
http(s)://<ip:port>/<static logout filename>
```

Follow this procedure to select the static Logout page.

Warning:

This procedure contains steps that disconnect all clients!

It is therefore advised to perform this procedure only during a maintenance window.

Procedure

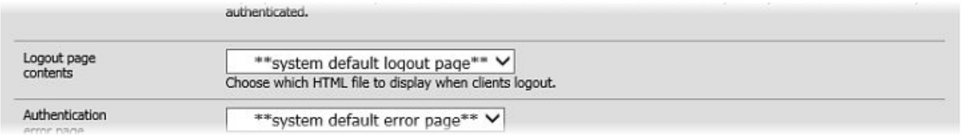
1. On the main Access Portal Administration Web UI page, click **Services** > **Captive Portal**.

   The Captive Portal: Zones page displays.

2. Click the Edit icon to the right of the desired captive portal.

   The Services: Captive portal page displays with the Captive Portal(s) tab selected.

3. Scroll down to the **Logout page contents** section.



authenticated.

Logout page contents: **system default logout page** ▾

Choose which HTML file to display when clients logout.

Authentication: **system default error page** ▾

4. From the drop-down list, select the HTML file you want to use for your static Logout page.

5. Click **Save**.

Configuring Access Groups

Access Groups control which success page is shown to users after successful authentication, and determine the OUT interface through which network access is granted. When Access Portal makes a RADIUS request to the Ignition Server for authentication for a user, Ignition Server performs a policy evaluation and sends out the Access Group to which the user belongs as an outbound value in the RADIUS ACCEPT response. Access Portal uses this value to determine the Access Group for the user and then grants network access and displays a success page accordingly.

Zones can have multiple Access Groups. Follow this procedure to configure one or more Access Groups for each zone.

Procedure

1. On the main Access Portal Administration Web UI page, click **Services** > **Captive Portal**.

   The Captive Portal: Zones page displays.

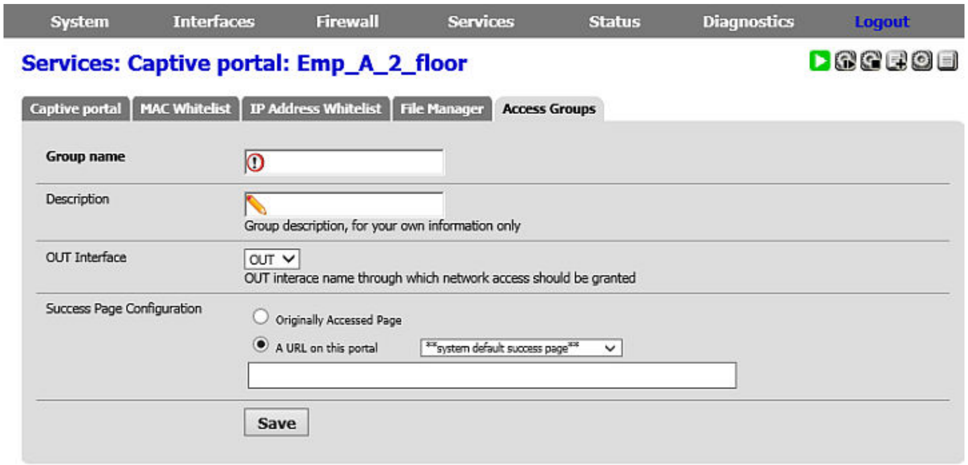
2. Click the Edit icon to the right of the desired captive portal.

   The Services: Captive portal page displays with the Captive Portal(s) tab selected.

3. Click the **Access Groups** tab.

4. Click the Add icon.

   The Services: Captive Portal page displays.



Services: Captive portal: Emp_A_2_floor

Group name

Description
Group description, for your own information only

OUT Interface: OUT
OUT interace name through which network access should be granted

Success Page Configuration
○ Originally Accessed Page
● A URL on this portal **system default success page**

5. Enter the group name in the **Group** name field.

   The Access Group name must exactly match the Outbound Attribute value for the Access Group Name attribute configured in the access policy on the Ignition Server. If there is a name mismatch, the settings configured under Captive portal are not applied.

6. Optionally enter a description for the group in the **Description** field.

7. Select the desired OUT interface from the **OUT Interface** drop-down list.

8. 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 **Originally Accessed Page**.

- If, after clients authenticate, you want to direct them to a URL on this portal, select the appropriate file name from the drop-down list that corresponds to the Success page you want to show. The guest user sees this page upon successful authentication.
- If, after clients authenticate, you want to direct them to a URL on another server, click **On Other Servers: Specify URL below**, and specify the full URL in the field below.

9. Click **Save**.

Providing access to servers or other computers from a client machine

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

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 user name 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 the IP White List.

Alternatively, you can add MAC addresses to the MAC White List to direct users to a specific device before authenticating with Access Portal.

⚠ **Warning:**

This procedure contains steps that disconnect all clients!

It is therefore advised to perform this procedure only during a maintenance window.

Procedure

1. On the main Access Portal Administration Web UI page, click **Services** > **Captive Portal**.

   The Captive Portal: Zones page displays.

2. Click the Edit icon to the right of the desired captive portal.

   The Services: Captive portal page displays with the Captive Portal(s) tab selected.

3. Do one of the following:
   - To add an IP address to the white list, click the **IP Address Whitelist** tab.
   - To add a MAC address to the white list, click the **MAC Whitelist** tab.

4. Click the Add icon on the right side of the page.

5. Do one of the following:
   - On the Services: Captive Portal: Edit IP Address Whitelist page, in the **IP Address** field, enter the IP address that you want to direct users to.
   - On the Services: Captive Portal: Edit MAC Whitelist page, in the **MAC Address** field, enter the MAC address for the device that you want to direct users to. Alternatively, click **Copy my MAC address** to populate the field with the MAC address for the current device.
6. Optionally enter a description into the **Description** field.
7. To limit the amount of bandwidth allowed for upload for this address, enter a value in Kbit/s in the **Bandwidth Up** field.
8. To limit the amount of bandwidth allowed for download for this address, enter a value in Kbit/s in the **Bandwidth Down** field.
9. Click **Save**.

Backing up and restoring Access Portal

It is recommended to back up the configuration after making changes to the Access Portal. There is no upgrade ability to the Access Portal. For updates and new versions of the Access Portal, Avaya will provide a new Virtual Appliance to be deployed on the VMware ESXi server and you must restore a configuration back from your existing Access Portal in order to bring it online up and running to replace a previous version of the Access Portal. Therefore, it is recommended to back up the Access Portal configuration upon making configuration changes.

Related Links

Introduction to backing up and restoring Access Portal on page 52
Creating a backup on page 52
Restoring from a backup file on page 53

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.

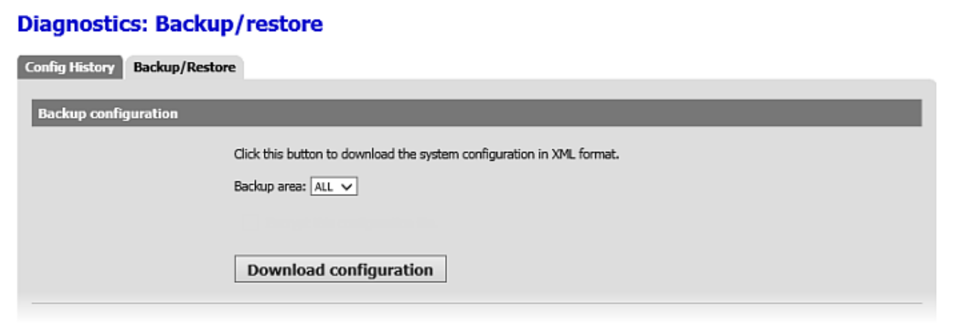
Creating a backup

Follow this procedure to create a backup of the data on your Access Portal.

Procedure

1. On the main Access Portal Administration Web UI page, click **Diagnostics** > **Backup/ Restore**.
2. Click **Download configuration**.

   The browser prompts you to open or save the file.



Diagnostics: Backup/restore

Click this button to download the system configuration in XML format.

Backup area: ALL

3. Select **Save File** and click **OK**.
4. 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.

ADMIN interface IP address warning

⚠ **Warning:**

When restoring from a backup file, 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 address, the Access Portal Administration Web UI will no longer be able to function. You must point your browser to the new ADMIN IP address.

ADMIN password warning

⚠ **Warning:**

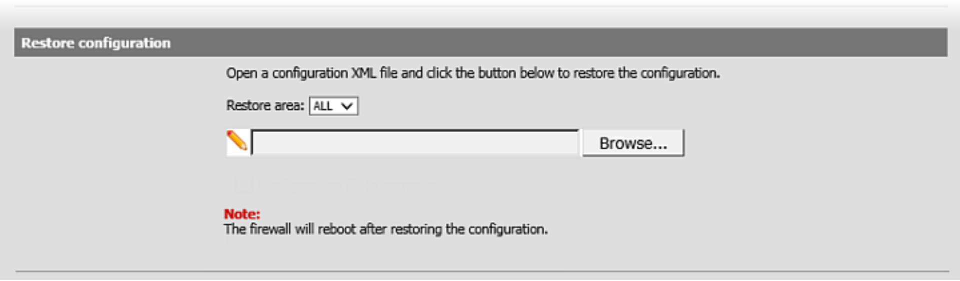
If your backed up configuration contains an ADMIN password that is different from the current password, after restoring, you may have to log in again with the new password.

Follow this procedure to restore your Access Portal from a backup file.

1. On the main Access Portal Administration Web UI page, click **Diagnostics** > **Backup/ Restore**.

2. Click **Browse** to specify the path and filename for the backup file from which you are restoring the data, and select the file.
3. Click **Restore Configuration**.

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



Open a configuration XML file and click the button below to restore the configuration.

Restore area: ALL

Note:
The firewall will reboot after restoring the configuration.

Upgrading Access Portal

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

Important considerations:

Be aware of the following when upgrading Access Portal from a previous version:

- When upgrading from a previous release that supported the legacy “Reauthenticate Connected Users Every 60 Seconds” captive portal option, if that option was selected, the restore disables that functionality and sets the RADIUS Session-Timeout option to “No Timeout”. You must reconfigure the Session-Timeout option as described in Configuring the Appliance Access Portal Settings on page 41.
- When upgrading from a previous release that did not support the ability to time synchronize with the hypervisor, the default time synchronization method after upgrade is synchronization with an NTP server. You must change the setting as described in Configuring the Access Portal Virtualization Appliance on page 26 if desired.
- When upgrading from a release that did not support multiple captive portals associated with zones, a default zone is created in the newer version, and the captive portal is automatically associated with that default zone.
- Avaya Identity Engines Ignition CASE Release 8.0 is not compatible with Access Portal Release 9.1. Therefore, the CASE files are not automatically included in an upgraded Access Portal deployment, and you must manually upload CASE files. See “Deploying Packages” in *Administering Avaya Identity Engines Ignition CASE, NN47280-603*.
- An upgrade from Release 8.0 results in a default firewall rule, associated with the IN interface, that was part of the installation for Release 8.0. If you plan to have multiple OUT interfaces and use Access Portal Access Groups, you must delete this default firewall rule. Release 9.1 does not require this rule, and you must manually delete the rule for the correct operation of multiple

OUT interfaces and Access Portal Access Groups. Note that, if you only plan to have one OUT interface, the rule can remain in place. However, it is recommended to remove the rule immediately after upgrade to avoid future issues if your access needs require additional OUT interfaces in the future.

To upgrade Access Portal to the latest version:

About this task

Procedure

1. Create a backup of the existing configuration. See Creating a backup on page 52.
2. Make a note of the admin IP address and netmask. You will assign this to the new OVA.
3. Shut down this instance of Access Portal either through the Access Portal Administration Web UI (**Diagnostics** > **Halt System**) or through the console option 6.
4. Install a fresh OVA. See Installing the Access Portal virtual machine on page 19.
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 53.
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>.

Chapter 5: Configuring the Avaya Identity Engines Ignition Server

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

Related Links

Configuring the Ignition Server to work with the Access Portal on page 56
Configuring guest access on the wired switch on page 71
Configuring wireless guest access on page 73
Creating guest user accounts on page 74
Testing wireless guest access on page 74
Testing wired guest access on page 74

Configuring the Ignition Server to work with the Access Portal

Now that you have finished configuring your Access Portal, you must configure 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.

Related Links

Activating the Access Portal license on page 57
Configuring Access Portal server details on page 57
Editing Access Portal server details on page 59
Introduction to device profiling on page 59
Introduction to MAC authentication on page 60
Configuring MAC authentication on Access Portal on page 61
Configuring a guest access policy on page 67
Registering authenticators that provide regular user access in the Ignition Server on page 70

Activating the Access Portal license

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

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:

Procedure

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**.

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.

⚠ **Warning:**

Any mismatch in RADIUS configuration between the Ignition Server and Access Portal (for example, server IP address, shared secret, password, and so on) can result in fatal or internal errors to the clients. Always perform a test user authentication after configuring RADIUS settings in Ignition Server and Access Portal.

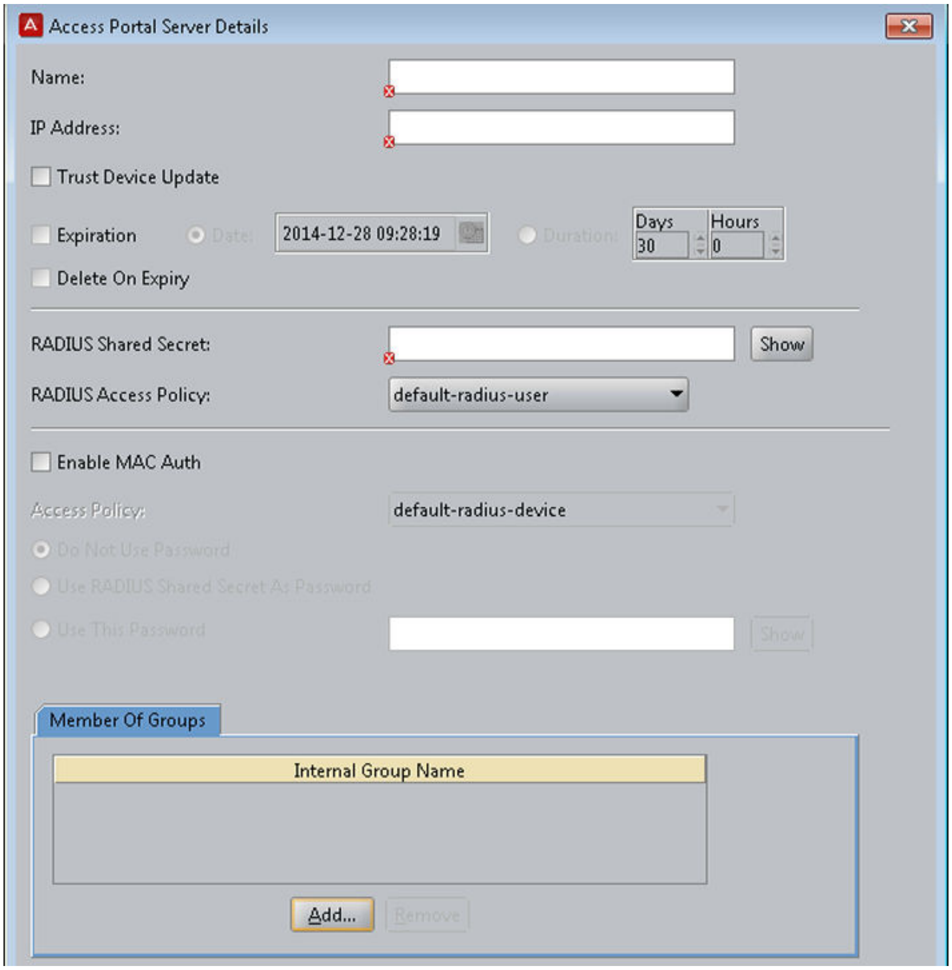
See the following sections for information related to this procedure:

- Configuring the Captive Portal settings on page 41
- Introduction to MAC authentication on page 60
- Configuring MAC authentication on Access Portal on page 61

Procedure

1. In the Dashboard **Configuration** tree, expand the **Access Portal** folder and click **Access Portal Servers**.
2. Click **New**.

   The **Access Portal Server Details** page displays.



Access Portal Server Details

Name:

IP Address:

□ Trust Device Update

□ Expiration ● Date: 2014-12-28 09:28:19 ○ Duration: Days 30 Hours 0

□ Delete On Expiry

RADIUS Shared Secret:

RADIUS Access Policy: default-radius-user

□ Enable MAC Auth

Access Policy: default-radius-device

● Do Not Use Password

○ Use RADIUS Shared Secret As Password

○ Use This Password

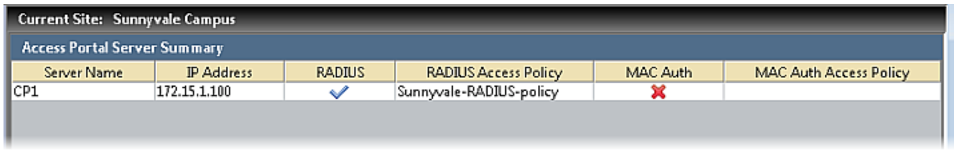
3. In the **Access Portal Server Details** window, specify the following:

   - **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 the Ignition Server to create a device record in the local store with the device fingerprint of the authenticating user. Note that, 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**: Select this check box if you want to specify an expiry date or lapse period for the devices learned through Access Portal.
     - To specify an expiration date, click **Date** and 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.
     - To specify a lapse period, click **Duration** and use the arrow keys to specify the number of days and hours from the time the device was learned until the time it expires.

- **Delete On Expiry**: Select this check box if you want the Ignition Server to delete learned devices after the expiry date. Note that it may take up to 24 hours after the expiry date for the devices to be purged from the local store.
- **RADIUS Shared Secret**: Enter the Shared Secret that you configured for RADIUS server.
- **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-radiususer).
- **Enable MAC Auth**: Select this check box to provide authentication based on the MAC address of the device that is trying to connect.
- **Member of Groups**: Select one or more internal groups to which unregistered devices can be auto-associated. Click **Add**, select the internal group or groups, and click **OK**.

4. Click **OK**.

   The **Access Portal Server Summary** page displays.



Current Site: Sunnyvale Campus

Access Portal Server Summary

Server Name	IP Address	RADIUS	RADIUS Access Policy	MAC Auth	MAC Auth Access Policy
CP1	172.15.1.100	✓	Sunnyvale-RADIUS-policy	✗	

Editing Access Portal server details

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

Procedure

1. In the Dashboard **Configuration** tree, expand the **Access Portal** folder and click **Access Portal Servers**.
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; it learns the necessary device attributes such as device type, sub type, operating system, and version, and then 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 e-mail access for mobile devices.

Configuring device profiling

Follow this procedure to configure device profiling.

Procedure

1. From Dashboard, configure Access Portal as an authenticator as a trusted source to learn the devices. See Configuring the Access Portal Server Details to support MAC Auth on page 64. When specifying Access Portal Server details, select the **Trust Device Update** checkbox.
2. On the main Access Portal Administration Web UI page, click **Services** > **Captive Portal**.
3. Select the **Enable Device Fingerprinting** check box.

   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.

   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 65. 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 updates the other device record attributes such as device type, sub type, and OS.

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 using 802.1X, you can configure 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 create “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.

Important:

Do not confuse MAC authentication with Windows machine authentication and asset correlation, which uses Windows machine authentication. See *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

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 through 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, 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, place all MAC- authenticated devices on a limited-access VLAN, as explained in the sections that follow.

Configuring MAC authentication on Access Portal

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

- Creating a MAC-Auth policy on page 62
- Configuring Access Portal server details on page 57
- Creating a device record on page 65
- Editing the device template to support MAC authentication on page 66
- Enabling RADIUS MAC authentication on Access Portal on page 67

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.

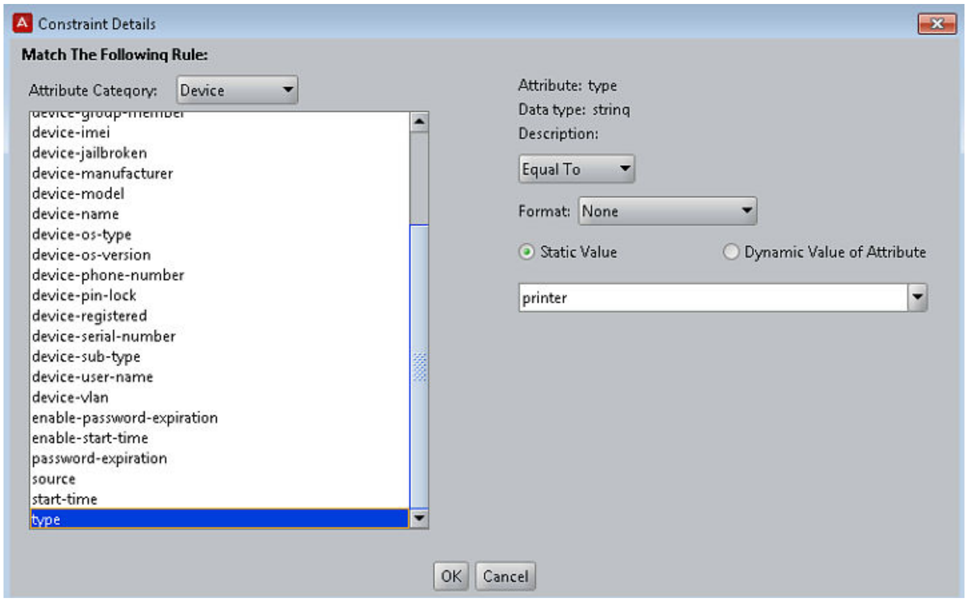
Procedure

1. In the Dashboard **Configuration** tree, expand the **Access Policies** folder, and click **MAC Auth**.
2. Click **New**.

   You can edit an existing policy by clicking its name in the Configuration tree and clicking **Edit** on the right side of the window.
3. Enter a name for the policy and click **OK**.
4. Click the policy name in the tree and click **Edit** .
5. In the **Edit Authorization Policy** window, configure a MAC-Auth policy just as you would a RADIUS user authorization policy. For more information, see *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

   Typically, your MAC-Auth rules evaluates attributes of the connecting device. To configure 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 require.)



Constraint Details

Match The Following Rule:

Attribute Category: Device

device-group-member
device-imei
device-jailbroken
device-manufacturer
device-model
device-name
device-os-type
device-os-version
device-phone-number
device-pin-lock
device-registered
device-serial-number
device-sub-type
device-user-name
device-vlan
enable-password-expiration
enable-start-time
password-expiration
source
start-time
type

Attribute: type
Data type: string
Description:

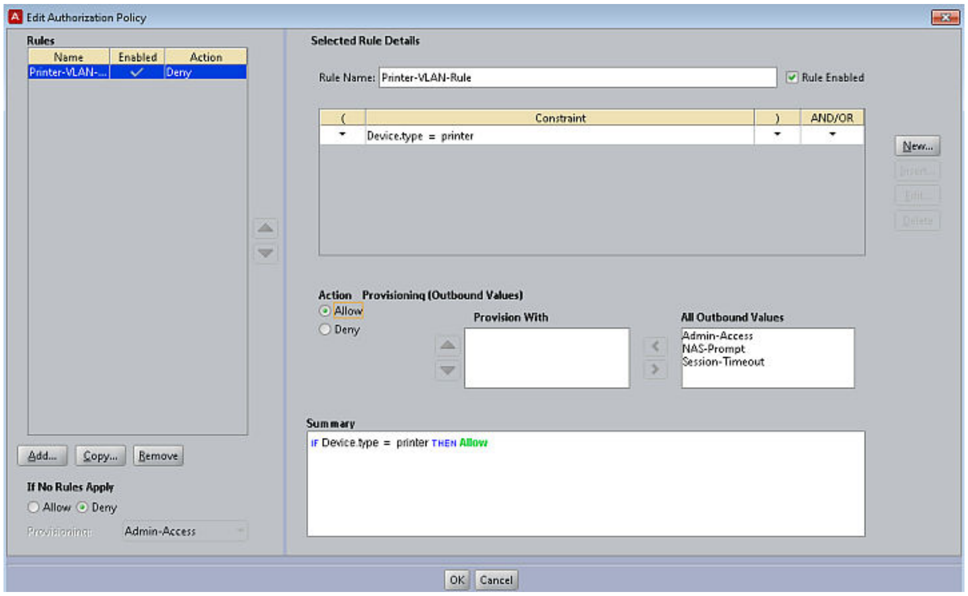
Equal To

Format: None

● Static Value ○ Dynamic Value of Attribute

printer

- In the **Constraint Details** window, go to the **Attribute Category** dropdown list and click **Device**. In the list below this, choose **type**. In the drop-down list on the right, click **Equal To**. Select **Static Value** . 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 Provisioning** select **Allow**. Click **OK**.



Edit Authorization Policy

Rules

Name	Enabled	Action
Printer-VLAN-...	✓	Deny

Selected Rule Details

Rule Name: Printer-VLAN-Rule ☑ Rule Enabled

(	Constraint	)	AND/OR
	Device.type = printer		

Action ● Allow ○ Deny

Provisioning (Outbound Values)

Provision With

All Outbound Values
Admin-Access
NAS-Prompt
Session-Timeout

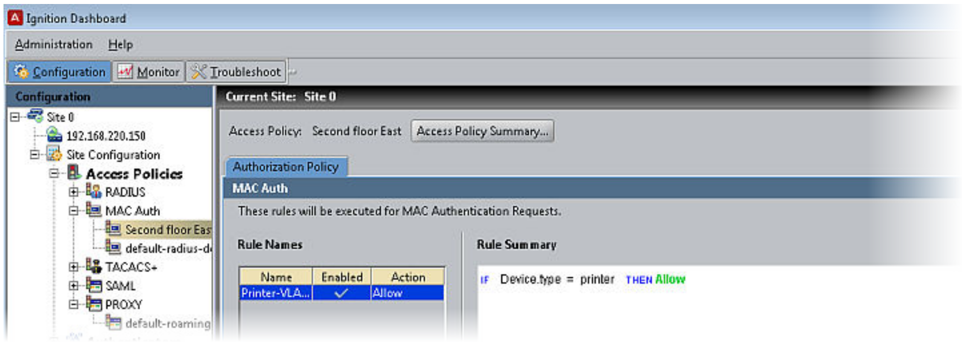
Summary

IF Device.type = printer THEN Allow

If No Rules Apply ○ Allow ● Deny

Provisioning: Admin-Access

Your policy is saved.



Current Site: Site 0

Access Policy: Second floor East

These rules will be executed for MAC Authentication Requests.

Name	Enabled	Action
Printer-VLA...	✓	Allow

IF Device.type = printer THEN Allow

If your situation requires that your rules evaluate more detailed information, you can store and evaluate additional device information as described in *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

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.

Follow this procedure to configure the Access Portal Server Details to support MAC authentication.

Procedure

1. In the Dashboard **Configuration** tree, expand the **Access Portal** folder and click **Access Portal Servers**.
2. 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**.
3. 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 configured in Creating a MAC-Auth policy on page 62.
   - 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.
4. Click **OK**.

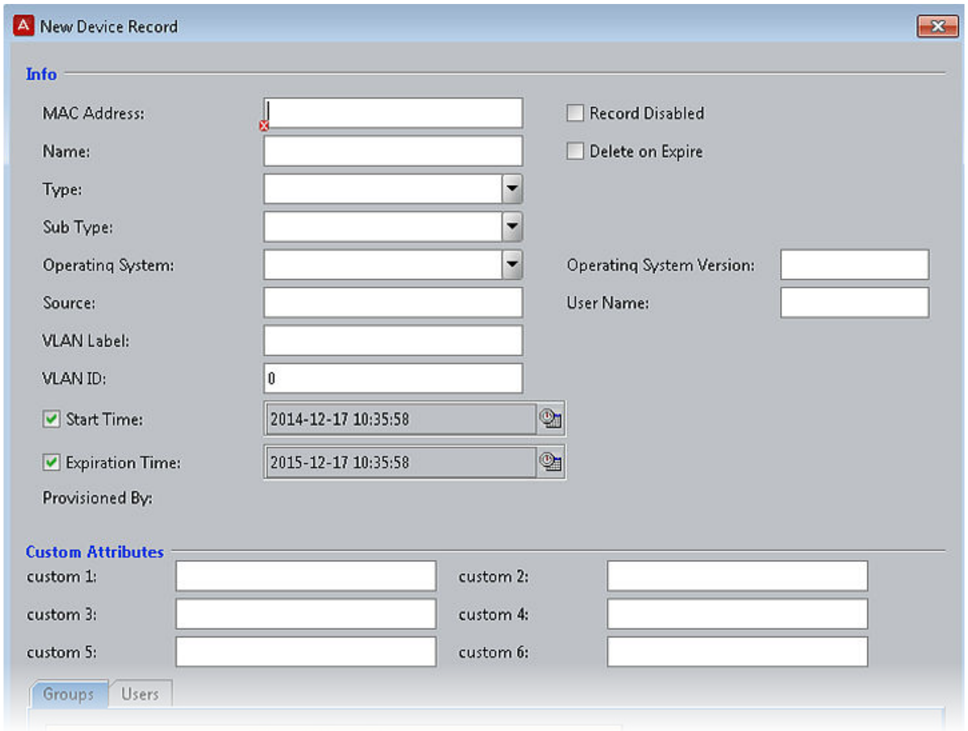
Creating a device record

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. For more information, see *Avaya Identity Engines Ignition Server Administration*, NN47280-600.)

To create a device record in Ignition:

Procedure

1. In the Dashboard **Configuration** tree, click your site, expand the **Site Configuration** > **Directories** > **Internal Store** folders, and click **Internal Devices**. Click **New**.



New Device Record

Info

MAC Address:

Name:

Type:

Sub Type:

Operating System:

Source:

VLAN Label:

VLAN ID: 0

☑ Start Time: 2014-12-17 10:35:58

☑ Expiration Time: 2015-12-17 10:35:58

Provisioned By:

□ Record Disabled

□ Delete on Expire

Operating System Version:

User Name:

Custom Attributes

custom 1:

custom 2:

custom 3:

custom 4:

custom 5:

custom 6:

2. In the **MAC Address** field, specify the MAC address of the device. Enter the address as a string of six octets. You can write the twelve characters without separators, or you can 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 agroup 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, and so on.
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 *Avaya Identity Engines Ignition Server Administration*, NN47280-600). 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 Step 5.)
15. The **Custom Attributes** fields allow you to record additional information about the device. For more information, see *Avaya Identity Engines Ignition Server Administration*, NN47280-600.
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 “genericdefault”. 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.

Follow this procedure to change the MAC Address source field to “Inbound-User-Name”.

Procedure

1. In the Dashboard **Configuration** tree, expand the **Site Configuration** > **Provisioning** folders, 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 displays.
4. Click **Edit**. The **Edit Device Template Details** window displays.
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.

Follow this procedure to enable RADIUS MAC authentication on Access Portal.

Procedure

1. On the main Access Portal Administration Web UI page, click **Sevices** > **Captive Portal**.
2. Scroll down to the **Authentication** section.
3. 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.
4. Click **Save**.

Configuring a guest access policy

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 *Avaya Identity Engines Ignition Guest Manager Configuration*, NN47280-501 for instructions.

Use this procedure to create a basic guest access policy.

Procedure

1. In the Dashboard **Configuration** tree, click the name of your site.
2. Expand **Site Configuration**, expand **Access Policies** and click **RADIUS**.
3. Click **New**.
4. Enter a name for the new access policy and click **OK**.

5. In the left navigation pane, highlight the name of the new access policy, click the **Authentication Policy** tab and click **Edit**.
6. Configure your tunnel settings. Ensure that you select **PAP** under **None**. Click **OK**.
7. Configure your identity routing policy to enable the Ignition Server to find guest user accounts in the Ignition Server embedded user store. Click the **Identity Routing** tab and click **Edit**.
    - If you already have an identity routing policy that you wish to use, click **Enable Default Directory Set**, and select the **Directory Set** from the drop-down list. Click **OK** to save the policy. Proceed to Step 8.
    - To create a new identity routing policy, do the following:
        - Click **New**.
        - Configure the Ignition Server to use the embedded user store (or any other target directory). In the **Directory Set** section, select **default set** (or any other target set that you wish to use). In the **Match Realm** section, select **Realm Not Specified**. 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**.
8. In the **Access Policy** window, click the **Authorization Policy** tab.
9. In the **RADIUS Authorization Policy** section of the window, click **Edit**.
10. In the **Rules** section, click **Add**.
11. In the **New Rule** window, type a name for the rule and click **OK**.
12. With your rule selected, go to the buttons to the right of the **Constraint** list and click **New**.
13. In the **Attribute Category** drop-down list, select the attribute category **Inbound**.

    In response, the list shows all the attributes for **Inbound**.
14. In the list, select one of the following Access Portal Inbound Attributes:

    RADIUS VSA Attributes

    - Inbound-Avaya-Access-Portal-Captive-Portal-Zone-Name
    - Inbound-Avaya-Access-Portal-IN-Interface-Name

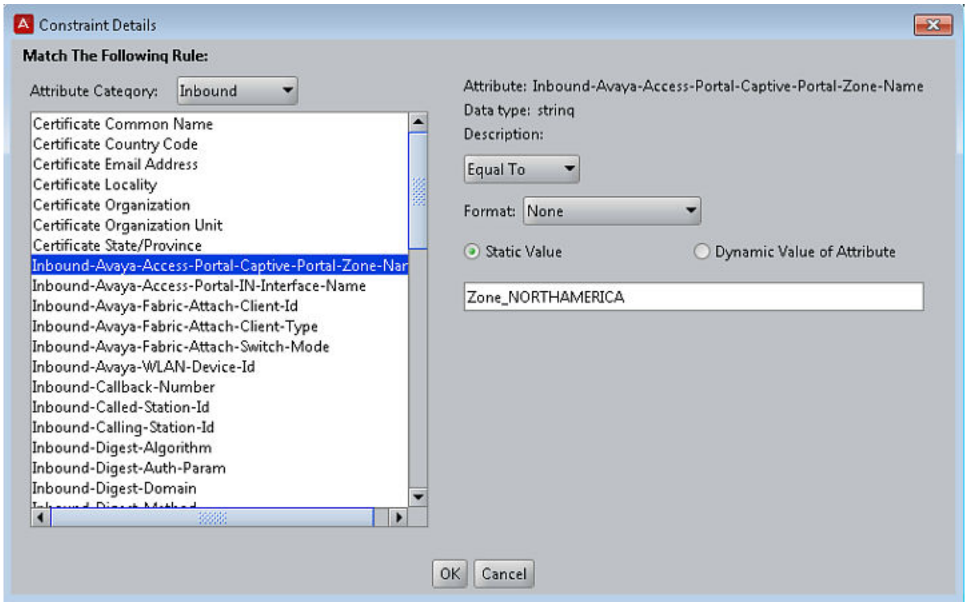
    RADIUS Standard Attributes

    - Calling-Station-Id - This attribute contains the MAC address of the authenticating client device.
    - Framed-IP-Address - This attribute contains the IP address of the authenticating client device.
    - NAS-Identifier - By default, this attribute contains the name of the Access Portal. You can, however, configure the value under Services > Captive Portal > <Zone>, within the RADIUS options section of the Captive Portal(s) tab.

- NAS-Port - This attribute contains a fixed value of 1.
- NAS-Port-Type - This attribute contains a fixed value of 15.

15. Select the appropriate value options and enter the value for the selected attribute.

    In this example, the Inbound attribute “Inbound-Avaya-Access-Portal-Captive-Portal-Zone-Name” is used with a value of “Zone_NORTHAMERICA”. Zone_NORTHAMERICA has two IN interfaces associated with it. This rule therefore applies to all users who enter through either of the two IN interfaces associated with Zone_NORTHAMERICA.



Match The Following Rule:

Attribute Category: Inbound

Certificate Common Name
Certificate Country Code
Certificate Email Address
Certificate Locality
Certificate Organization
Certificate Organization Unit
Certificate State/Province
Inbound-Avaya-Access-Portal-Captive-Portal-Zone-Nar
Inbound-Avaya-Access-Portal-IN-Interface-Name
Inbound-Avaya-Fabric-Attach-Client-Id
Inbound-Avaya-Fabric-Attach-Client-Type
Inbound-Avaya-Fabric-Attach-Switch-Mode
Inbound-Avaya-WLAN-Device-Id
Inbound-Callback-Number
Inbound-Called-Station-Id
Inbound-Calling-Station-Id
Inbound-Digest-Algorithm
Inbound-Digest-Auth-Param
Inbound-Digest-Domain

Attribute: Inbound-Avaya-Access-Portal-Captive-Portal-Zone-Name
Data type: string
Description:

Equal To

Format: None

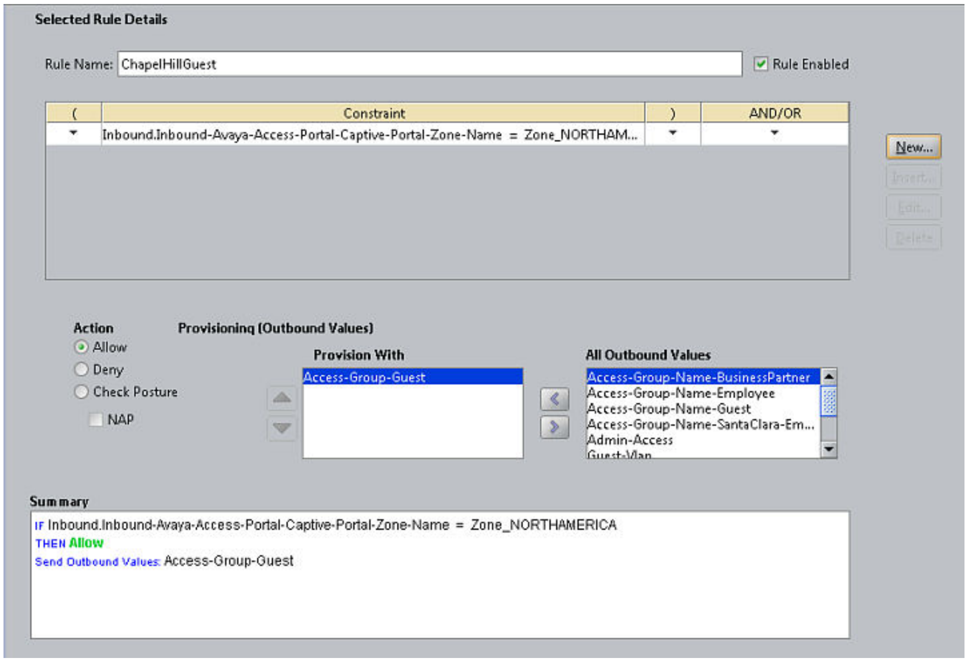
● Static Value ○ Dynamic Value of Attribute

Zone_NORTHAMERICA

16. Click **OK** to close the Constraint Details window and return to the Edit Authorization Policy window.
17. In the **Action** section of the Edit Authorization Policy window, click **Allow**.

    A list of available Outbound Values displays. Any Access Portal Access Groups that have been created are listed as available Outbound Values.
18. Select one of the following Access Portal Outbound Values using the arrows to move the desired values into the **Provision With** field:
    - <Access Group Name>
    - Session-Timeout
19. Click **OK**.

    In this example, “Access-Group-Guest” is the selected Outbound Value. That is, all users who enter through either of the two IN interfaces associated with Zone_NORTHAMERICA will be granted access through the OUT interface, and see the success page associated with the Access Portal Access Group named “Access-Group-Guest”.



Selected Rule Details

Rule Name: ChapelHillGuest ☑ Rule Enabled

(	Constraint	)	AND/OR
	Inbound.Inbound-Avaya-Access-Portal-Captive-Portal-Zone-Name = Zone_NORTHAM...		

Action

● Allow
○ Deny
○ Check Posture
□ NAP

Provisioning (Outbound Values)

Provision With: Access-Group-Guest

All Outbound Values:
Access-Group-Name-BusinessPartner
Access-Group-Name-Employee
Access-Group-Name-Guest
Access-Group-Name-SantaClara-Em...
Admin-Access
Guest-Vlan

Summary

IF Inbound.Inbound-Avaya-Access-Portal-Captive-Portal-Zone-Name = Zone_NORTHAMERICA
THEN Allow
Send Outbound Values: Access-Group-Guest

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 configure for guest user access in Configuring guest access on the wired switch on page 71.

Configure your wired switches as authenticators in the Ignition Server, configuring each to require 802.1X authentication. If authentication fails, the user is mapped to the authentication VLAN network that you 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 can include the AP that you configure for guest user access in Configuring wireless guest access on page 73, note that you do 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 *Avaya Identity Engines Ignition Server Administration*, NN47280-600).

Now that you have created your guest and non-guest access policies, your Ignition Server configuration is complete. For further instructions, consult *Avaya Identity Engines Ignition Server Administration*, NN47280-600 and *Avaya Identity Engines Ignition Guest Manager Configuration*, NN47280-501.

Configuring guest access on the wired switch

Related Links

Cabling the wired switch on page 71
Configuring VLANs on the wired switch on page 71
Configuring wired switch Ethernet ports on page 72

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.

Procedure

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 port0/1 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.

Follow this procedure to configure your VLANs.

Procedure

1. Configure 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. Configure your authenticated-access VLAN. This example uses a VLAN called Vlan1 for this, and we have configured Vlan1 to connect to the Internet through 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 configuration on each guest-accessible wired switch.

Procedure

1. Configure each guest-accessible Ethernet port on the wired switch to require 802.1X authentication. Regular users will authenticate through 802.1X, and guests with non-802.1X compatible hardware will authenticate through 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. The 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
   520-48T-PWR(config-if)#eapol quiet-interval 15
   5520-48T-PWR(config-if)#eapol transmit-interval 15
   ```

2. If guests will connect over wireless, configure the wired switch's Ethernet port that connects to the wireless access point. Configure this port for 802.1Q trunking to the access point. Configure the trunk to carry both the restrictedreach 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. Configure the wired switch's Ethernet port that connects to the Access Portal appliance's IN port. This port should be configured to carry only the restrictedreach 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 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 following sections provide generic instructions.

Before you begin

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

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

Procedure

1. Configure the AP's **Primary DNS Server Address** to the IP address of the Access Portal IN port.
2. Configure the AP's **Default Router Address** to the IP address of the Access Portal IN port.
3. Configure 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 71. This is your guest authentication VLAN / SSID.
   - Configure Layer 2 security to **None** on the VLAN.
   - Configure 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.
   - Configure 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 71.

   This is the VLAN / SSID your guests use after successfully authenticating.
   - Typically you leave beaconing turned off for this SSID.

Creating guest user accounts

Create your guest user accounts using either:

- Ignition Guest Manager, as explained in *Avaya Identity Engines Ignition Guest Manager Configuration*, NN47280-501.
- Ignition Dashboard, as explained in *Avaya Identity Engines Ignition Server Administration*, NN47280-600. To allow your front desk personnel to continue creating guest user accounts, configure 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 the "**auto detect proxy setting for this network**" setting on the browser. If a proxy is configured, Access Portal is not able to direct HTTP requests to the Access Portal login page.

Follow this procedure to test the wireless guest access.

Procedure

1. Using a laptop with wireless capability, connect to the "guest" SSID that you created in this procedure: Configuring wireless guest access on page 73.
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 forces the browser to display a login page. Enter your Ignition-generated guest user name and password. After authentication, the browser is 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 the "**auto detect proxy setting for this network**" setting on the browser. If a proxy is configured, Access Portal is not able to direct HTTP requests to the Access Portal login page.

Follow this procedure to test wired guest access.

Procedure

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 71. 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 user name and password, causing authentication to fail.
2. Wait one minute.

   The DHCP negotiation for a wired connection can take up to one minute.

   If you do not want to wait, and if you are using a Windows- based PC, then at the DOS prompt, enter: >**`ipconfig /release`** and then enter >**`ipconfig /renew`**.
3. Open a web browser on the PC.
4. If correctly configured, the Access Portal forces the browser to display a login page. Enter your Ignition-generated guest user name and password. After authentication, the browser is able to access the Internet.

   Some enterprises can require you to configure the proxy on the browser to access the Internet. If so, configure the proxy after authentication.

   ! **Important:**

   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.

Chapter 6: Configuring CASE

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

Note:

Avaya Identity Engines Ignition CASE Release 8.0 is not compatible with Access Portal Release 9.1. Therefore, the CASE files are not automatically included in an upgraded Access Portal deployment, and you must manually upload CASE files. See “Deploying Packages” in *Administering Avaya Identity Engines Ignition CASE, NN47280-603*.

Related Links

Configuring the CASE to work with Access Portal on page 76

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.

Related Links

CASE Administrative Console overview on page 76
Creating a network profile on page 77
Creating a deployment package on page 77
Deploying packages on page 77

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*, NN47280-603.

Creating a deployment package

To create a deployment package, see the “Creating a deployment package” procedure in *Avaya Identity Engines Ignition CASE Administration*, NN47280-603.

Deploying packages

To deploy a package, see the “Deploying packages” procedure in *Avaya Identity Engines Ignition CASE Administration*, NN47280-603.

Chapter 7: Troubleshooting

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

Related Links

Troubleshooting common problems on page 78

Troubleshooting common problems

Access Portal provides the following options for viewing the overall health of your system and performing common diagnostic and troubleshooting tasks:

To view the overall health of your system, on the main Access Portal Administration Web UI page click **Status**:

- Dashboard
- DHCP leases
- Filter Reload
- Gateways
- Interfaces
- Services
- System logs

To view diagnostic information or perform common troubleshooting tasks, on the main Access Portal Administration Web UI page click **Diagnostics**:

- ARP table
- Authentication
- Backup/Restore
- DNS Lookup
- Factory Defaults
- Halt System
- Packet Capture
- pfInfo

- pfTop
- Ping
- Reboot
- Routes
- Sockets
- Test Port
- Traceroute

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

Related Links

Problem: Cannot access Access Portal on page 79
Problem: Unable to authenticate user on page 79
Problem: MAC authentication failure on page 80
Problem: Cannot launch Access Portal Administration Web UI on page 80
Problem: Client unable to communicate with Access Portal on page 81
Problem: Unable to ping IN and OUT interfaces on page 81
Problem: In Dashboard, “Access Portal” not listed as option in Configuration list on page 81
Problem: VM not synchronizing with Hypervisor on page 82
Problem: Access Group members cannot access network on page 82
Problem: Users experience fatal errors on page 82
Miscellaneous troubleshooting tips on page 83

Problem: Cannot access Access Portal

Possible cause

- 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 the DNS name. The issue is with DNS name resolution.

Solution

- Ensure that the DNS servers specified in the Access Portal Administration Web UI are correct and the DNS forwarder is configured.
- Ensure that the connectivity is working.

Problem: Unable to authenticate user

Possible cause

- RADIUS server address mismatch.

- Shared secret mismatch.
- Stale data.

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 can feed stale data to Access Portal.

Problem: MAC authentication failure

Possible cause

- Incomplete configuration on Access Portal and Ignition Server.
- Shared secret mismatch.

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 Access Portal Administration Web UI

Possible cause

- Browser proxy configuration issue.
- The machine you are using to connect to the Access Portal Administration Web UI is not on the ADMIN network.
- The ADMIN interface subnet has been changed.

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.
- If ADMIN interface IP address is changed such that it falls in a different subnet than before, it may render the default route associated with that interface invalid. In this case, in order to

access the Access Portal Administration Web UI from a machine not on the ADMIN subnet, either reboot the machine or add a static route.

Problem: Client unable to communicate with Access Portal

Possible cause

- Browser proxy configuration issue.
- 802.1x authentication configuration issue
- IP selection configuration issue.
- Client default gateway configuration issue.

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 configured as static. Access Portal is designed to be used in conjunction with a DHCP server.
- Make sure the client's default gateway is pointing towards the IN interface IP address of the Access Portal and they are able to talk to each other.

Problem: Unable to ping IN and OUT interfaces

Possible cause

- Ping requests originating from incorrect source.

Solution

- If ADMIN interface responds to ping requests, but not IN and OUT interfaces, perform ping requests from IN and OUT interfaces to other hosts on the network, rather than pinging from other hosts to these interfaces.

Problem: In Dashboard, “Access Portal” not listed as option in Configuration list

Possible cause

- License not correctly installed.

Solution

- Install new FEATURE_PORTAL license.

Problem: VM not synchronizing with Hypervisor

Possible cause

- The hypervisor time may be lagging behind the virtual machine time. Access Portal does not set the clock backward for time synching with a Hypervisor—it only sets the clock forward.

Solution

- Reboot the virtual machine.

Problem: Access Group members cannot access network

Possible cause

- If an Access Group member successfully authenticates but cannot access the network as expected, the Access Group may be associated with an obsolete OUT interface. This can happen if an OUT interface is deleted when the VM is powered down. In this case, the Access Group is now associated with the obsolete OUT interface. Additionally, if any gateways are associated with the deleted OUT interface, those gateways must be manually removed from the system.

Solution

- Check to make sure that the OUT interface associated with the Access Group has not been deleted. If it has, manually configure the Access Group to associate the correct OUT interface. Additionally, check to make sure that the gateway associated with the deleted OUT interface is not in the system. If it is, manually delete the gateway.

Problem: Users experience fatal errors

Possible cause

- Any mismatch in RADIUS configuration between the Ignition Server and Access Portal (for example, server IP address, shared secret, password, and so on) can result in fatal or internal errors to the clients.

Solution

- Check for any configuration errors that involve a mismatch in RADIUS settings between Ignition Server and Access Portal. Correct any errors and perform a test user authentication to confirm the correct configuration.

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 (that is, clear the "Trusted Device Update" check box). 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 still attempts 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** > **Routing** > **Routes** and add a route to the network where the RADIUS server is present.

Appendix A: Avaya Identity Engines Ignition Access Portal deployment example

This section assumes that you are familiar with setting up and maintaining networks and network security.

It also assumes that you have:

- deployed the Avaya Identity Engines Ignition Server OVA and configured the virtual machine. For more information, see *Avaya Identity Engines Ignition Server Getting Started Configuration, NN47280-300*.
- installed and configured the Dashboard desktop application. For more information, see *Avaya Identity Engines Ignition Server Getting Started Configuration, NN47280-300*.
- installed all applicable licenses. For more information, see *Avaya Identity Engines Ignition Server Getting Started Configuration, NN47280-300*.
- deployed the Avaya Identity Engines Access Portal OVA and configured the virtual machine. For more information, see Configuring the Access Portal virtual machine on page 26 in this document.
- added six additional Ethernet adapters to the virtual machine, in preparation for assigning and enabling the multiple interfaces as described in this deployment. For more information, see Adding Mulitiple IN and OUT interfaces on page 34 in this document.

Related Links

Background on page 84
Configuring Ignition Server on page 87
Configuring Access Portal on page 90
Example with proxy server for clients on page 93

Background

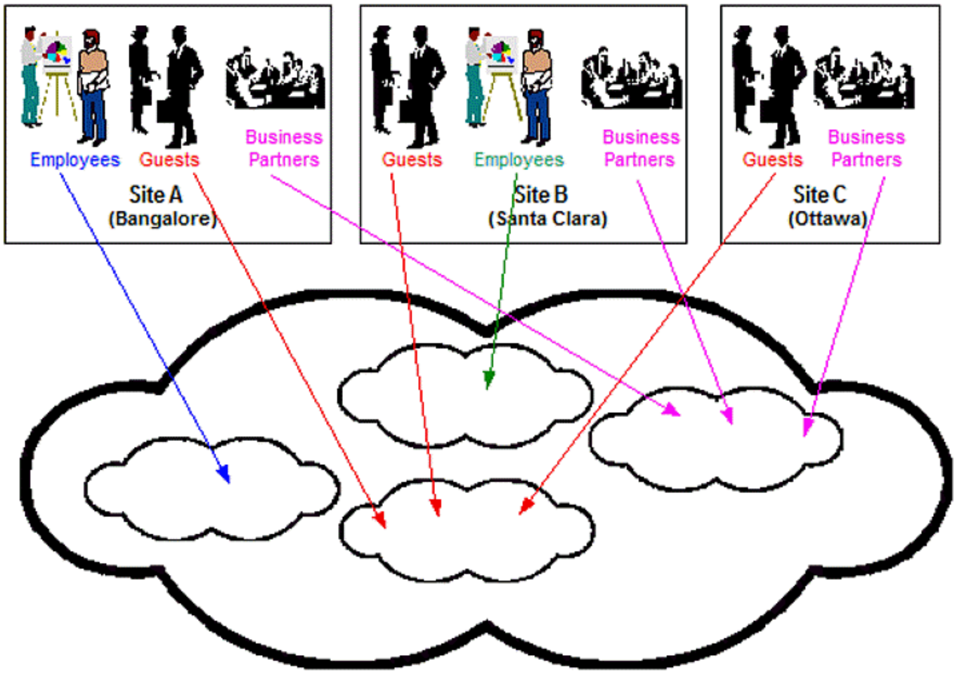
The example deployment in this section services a customer with geographically dispersed sites and different access requirements for those sites, as follows:

- Site A is located in Bangalore, India, and has employees, business partners, and guests

- Site B is located in Santa Clara, USA, and has employees, business partners, and guests
- Site C is located in Ottawa, Canada, and has business partners and guests, but no employees

All of the different employees, business partners, and guests at all of the sites have remote devices and require access to company network resources as follows:

- Guests at Sites A, B, and C can access but should be restricted to one portion of the company network.
- Employees at Site A can access but should be restricted to one portion of the company network.
- Employees at Site B can access but should be restricted to one portion of the company network.
- Business partners at Sites A, B, and C can access but should be restricted to one portion of the company network.



To accommodate the access requirements for the various sites and types of users, this deployment is configured with:

- two captive portals, associated with different zones
  - one zone services Site A (Zone_BANGALORE)
  - one zone services Sites B and C (Zone_NORTHAMERICA)
- one default out-of-the-box ADMIN interface for centralized administration (there is always only one ADMIN interface)

- four IN interfaces, including:
    - the default out-of-the-box IN interface (IN) (not used in this example)
    - one additional IN interface, configured for managing access for all users in Site A (IN_BANGALORE)
    - one additional IN interface, configured for managing access for all users in Site B (IN_SANTACLARA)
    - one additional IN interface, configured for managing access for all users in Site C (IN_OTTAWA)
- four OUT interfaces, including:
    - the default out-of-the-box OUT interface, configured for guests of Sites A, B, and C (OUT)
    - one additional OUT interface, configured for employees of Site A (OUT_EMPLOYEE_BANGALORE)
    - one additional OUT interface, configured for employees of Site B (OUT_EMPLOYEE_SANTACLARA)
    - one additional OUT interface, configured for business partners of Sites A, B, and C (OUT_BUSINESSPARTNER)
- Access Portal Access Groups as follows:
    - Under Zone_BANGALORE:

      Access-Group-Employees (mapped to interface OUT_EMPLOYEE_BANGALORE)

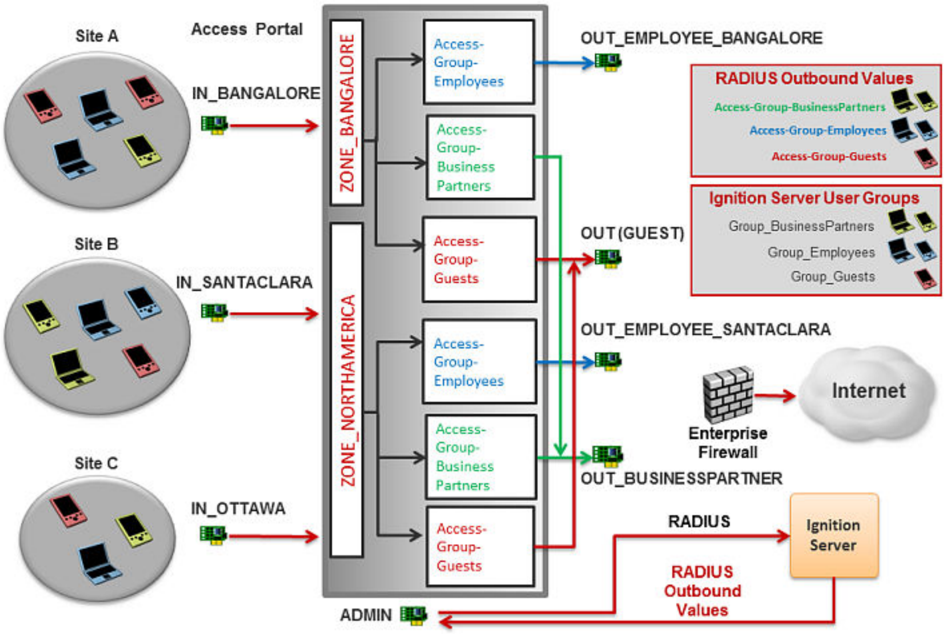
      Access-Group-Guests (mapped to interface OUT)

      Access-Group-BusinessPartners (mapped to interface OUT_BUSINESSPARTNER)
    - Under Zone_NORTHAMERICA:

      Access-Group-Employees (mapped to interface OUT_EMPLOYEE_SANTACLARA)

      Access-Group-Guests (mapped to interface OUT)

      Access-Group-BusinessPartners (mapped to interface OUT_BUSINESSPARTNER)



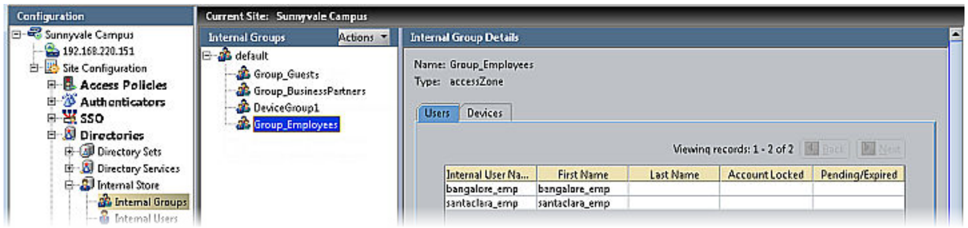
Configuring Ignition Server

For detailed instructions about the tasks in this section, see *Administering Avaya Identity Engines Ignition Server, NN47280–600*.

Procedure

1. **Configure Internal Groups:** In the Ignition Server Dashboard Configuration tree, expand **Site Configuration**, expand **Directories**, expand **Internal Store**, and click **Internal Groups**. Under the Default Internal Group, create the following Internal Groups:

   - “Group_Employees”, and add users as required
   - “Group_Guests”, and add users as required
   - “Group_BusinessPartners”, and add users as required
   - “DeviceGroup1”, and add devices as required



Name: Group_Employees
Type: accessZone

Viewing records: 1 - 2 of 2

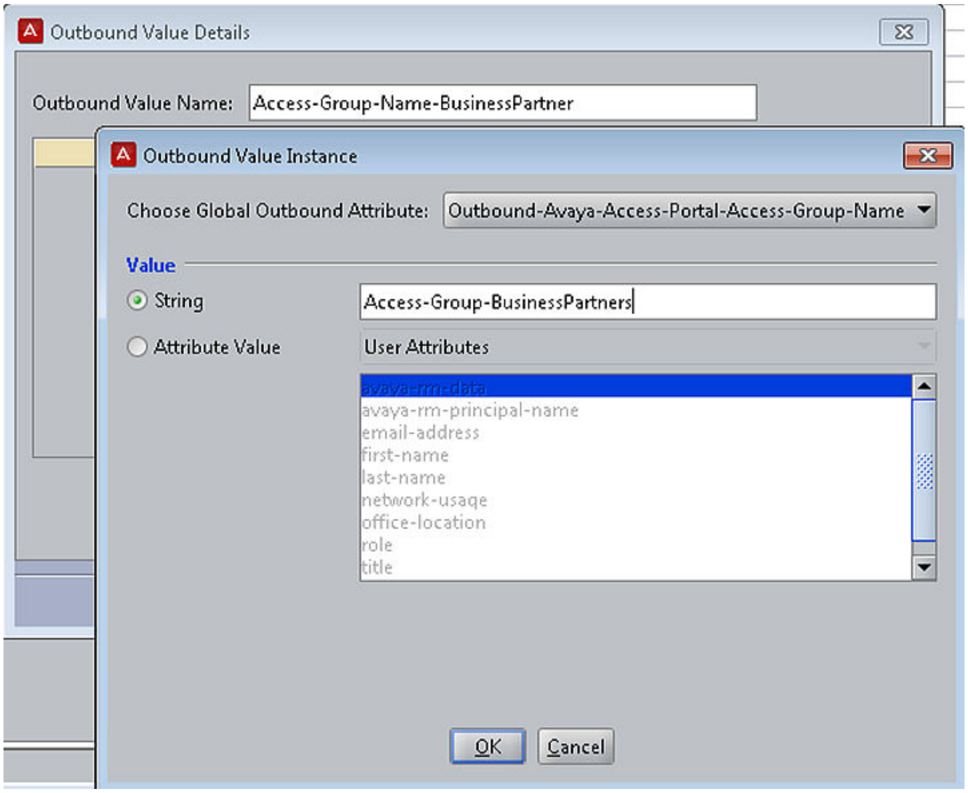
Internal User Na...	First Name	Last Name	Account Locked	Pending/Expired
bangalore_emp	bangalore_emp			
santaclara_emp	santaclara_emp			

2. **Configure RADIUS Outbound Values:** In the Ignition Server Dashboard Configuration tree, expand **Site Configuration**, expand **Provisioning**, expand **RADIUS**, and click

Outbound Values. Click **New**, enter a name, and click **New** to configure the Outbound Value instance. Create the following Outbound Values:

- "Access-Group-Name-Employee" with the Global Outbound Attribute "Outbound-Avaya-Access-Portal-Access-Group-Name" and a Value of String "Access-Group-Employees"
- "Access-Group-Name-Guest" with the Global Outbound Attribute "Outbound-Avaya-Access-Portal-Access-Group-Name" and a Value of String "Access-Group-Guests"
- "Access-Group-Name-BusinessPartner" with the Global Outbound Attribute "Outbound-Avaya-Access-Portal-Access-Group-Name" and a Value of String "Access-Group-BusinessPartners"

Note that the string values defined for these attributes will be used to create Access Portal Access Groups later in this section.



Outbound Value Details

Outbound Value Name: Access-Group-Name-BusinessPartner

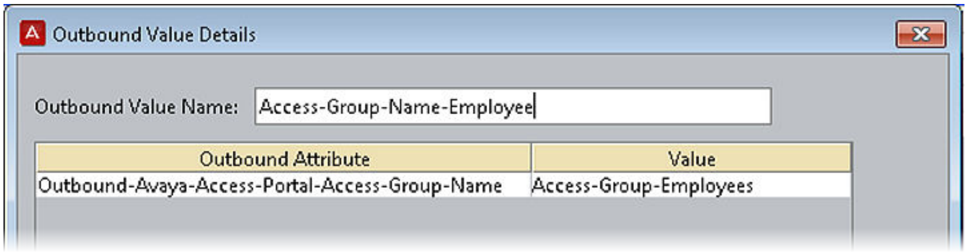
Outbound Value Instance

Choose Global Outbound Attribute: Outbound-Avaya-Access-Portal-Access-Group-Name

Value

● String: Access-Group-BusinessPartners

○ Attribute Value: User Attributes

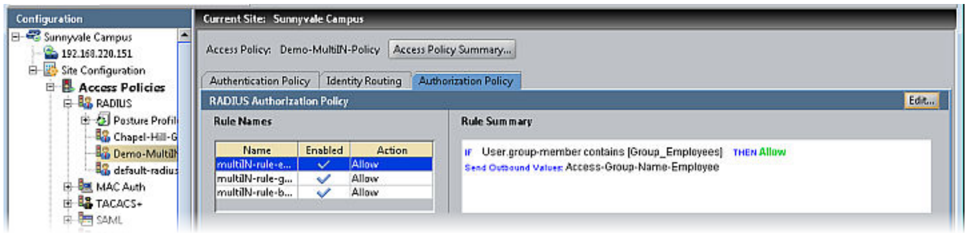


Outbound Value Details

Outbound Value Name: Access-Group-Name-Employee

Outbound Attribute	Value
Outbound-Avaya-Access-Portal-Access-Group-Name	Access-Group-Employees

3. **Configure RADIUS Access Policies:** In the Ignition Server Dashboard Configuration tree, expand **Site Configuration**, expand **Access Policies**, and click **RADIUS**. Create an Access Policy named “demo-MultiIN-policy” and associate it with the following rules:
    - If the user belongs to Group_Employee, send Outbound Value “Access-Group-Name-Employee”
    - If the user belongs to Group_Guest, send Outbound Value “Access-Group-Name-Guest”
    - If the user belongs to Group_BusinessPartner, send Outbound Value “Access-Group-Name-BusinessPartner”



Access Policy: Demo-MultiIN-Policy

RADIUS Authorization Policy

Rule Names

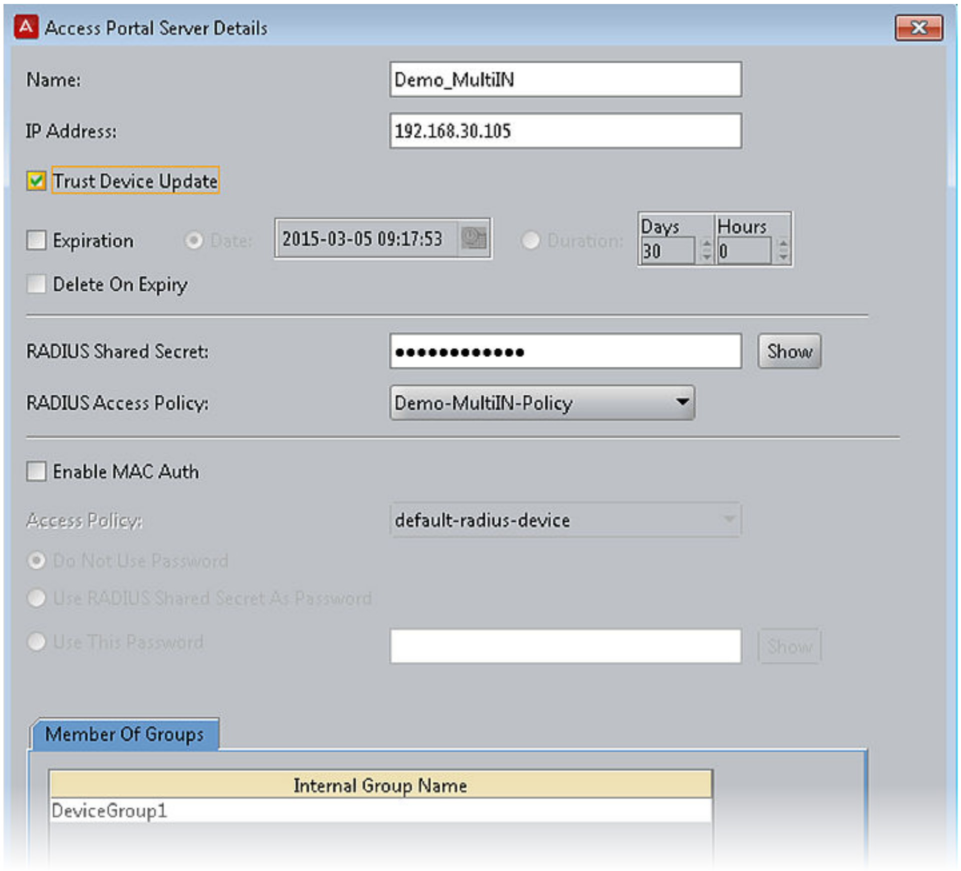
Name	Enabled	Action
multiIN-rule-e...	✓	Allow
multiIN-rule-g...	✓	Allow
multiIN-rule-b...	✓	Allow

Rule Summary

IF User.group-member contains [Group_Employees] THEN Allow
Send Outbound Values: Access-Group-Name-Employee

4. **Configure the Access Portal server details:** In the Ignition Server Dashboard Configuration tree, expand **Access Portal**, click **Access Portal Servers**, and click **New**. Enter a name for the server, the ADMIN interface IP address, and RADIIUS shared secret. Enable device fingerprinting, , associate the server with access policy demo-MultiIN-policy, and choose DeviceGroup1 for auto-association.

    For more information, see Configuring the Access Portal Server Details on page 57 in this document.



Access Portal Server Details

Name: Demo_MultiIN

IP Address: 192.168.30.105

☑ Trust Device Update

□ Expiration ● Date: 2015-03-05 09:17:53 ○ Duration: Days 30 Hours 0

□ Delete On Expiry

RADIUS Shared Secret: ●●●●●●●●●●●●● Show

RADIUS Access Policy: Demo-MultiIN-Policy

□ Enable MAC Auth

Access Policy: default-radius-device

● Do Not Use Password

○ Use RADIUS Shared Secret As Password

○ Use This Password Show

Member Of Groups

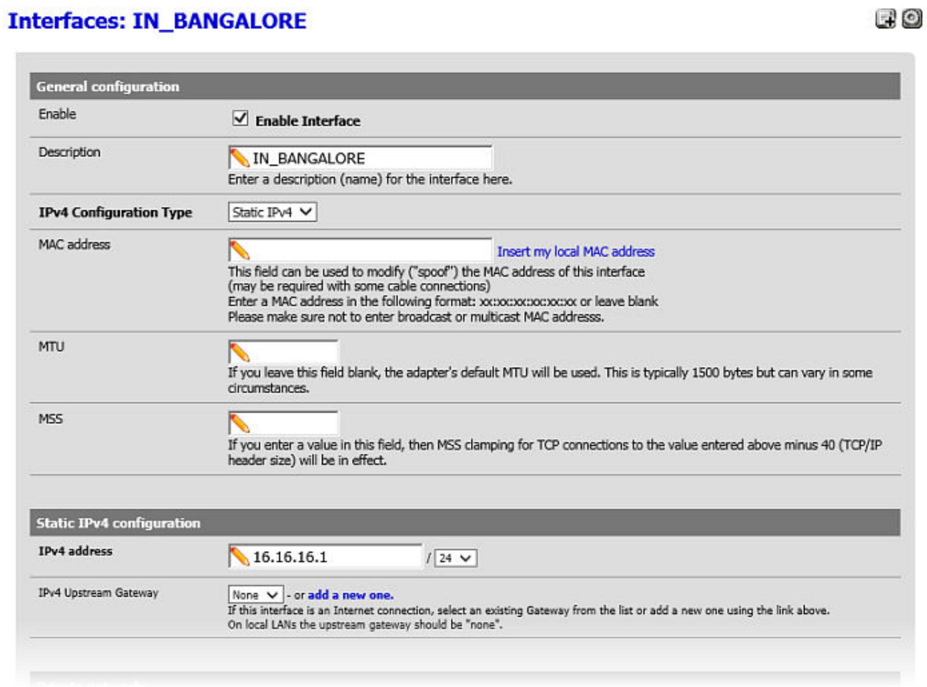
Internal Group Name
DeviceGroup1

Configuring Access Portal

Procedure

1. **Assign and enable additional IN and OUT interfaces:** On the main Access Portal Administration Web UI page, click **Interfaces** > **(assign)**. For each Ethernet adapter you previously added, select IN or OUT from the drop-down list, click the Add icon, and choose the appropriate network port. Click the name of the interface and enable the interface, enter the appropriate name, and enter the IP address and subnet mask.

   For more information, see Adding multiple IN and OUT interfaces on page 34 in this document.



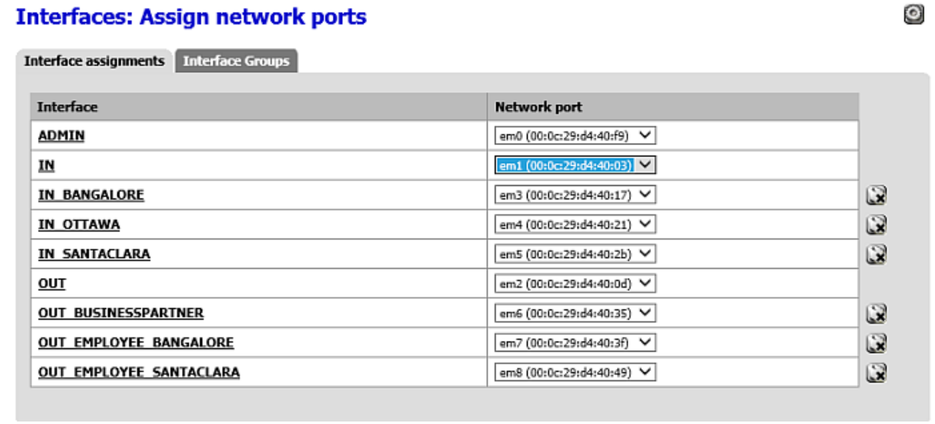
Interfaces: IN_BANGALORE

General configuration

Enable	☑ **Enable Interface**
Description	IN_BANGALORE Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
MAC address	Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this 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 Please make sure not to enter broadcast or multicast MAC addresss.
MTU	If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	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.

Static IPv4 configuration

IPv4 address	16.16.16.1 / 24
IPv4 Upstream Gateway	None - or **add a new one.** If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the link above. On local LANs the upstream gateway should be "none".

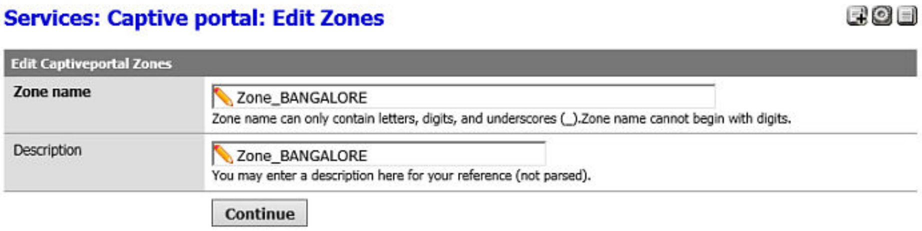


Interfaces: Assign network ports

Interface	Network port
ADMIN	em0 (00:0c:29:d4:40:f9)
IN	em1 (00:0c:29:d4:40:03)
IN_BANGALORE	em3 (00:0c:29:d4:40:17)
IN_OTTAWA	em4 (00:0c:29:d4:40:21)
IN_SANTACLARA	em5 (00:0c:29:d4:40:2b)
OUT	em2 (00:0c:29:d4:40:0d)
OUT_BUSINESSPARTNER	em6 (00:0c:29:d4:40:35)
OUT_EMPLOYEE_BANGALORE	em7 (00:0c:29:d4:40:3f)
OUT_EMPLOYEE_SANTACLARA	em8 (00:0c:29:d4:40:49)

2. **Configure Zones:** On the main Access Portal Administration Web UI page, click **Services** > **Captive Portal**. Configure one captive portal for Zone_BANGALORE and associate it with the IN_BANGALORE interface. Configure another captive portal for Zone_NORTHAMERICA and associate it with the IN_OTTAWA and the IN_SANTACLARA interfaces.

   For more information, see Configuring the Appliance Access Portal Settings on page 41 in this document.

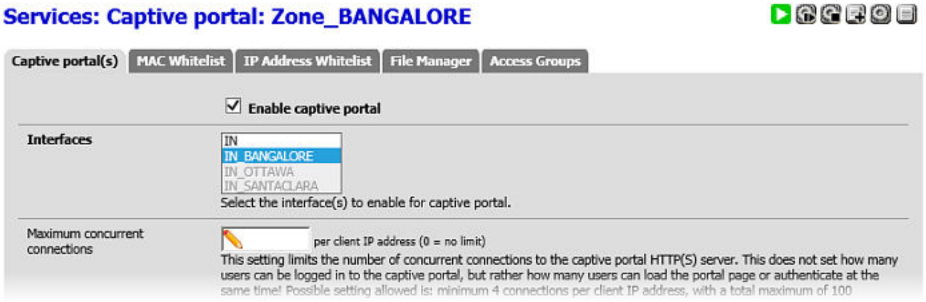


Services: Captive portal: Edit Zones

Edit Captiveportal Zones

Zone name	Zone_BANGALORE Zone name can only contain letters, digits, and underscores (_).Zone name cannot begin with digits.
Description	Zone_BANGALORE You may enter a description here for your reference (not parsed).

Continue



Services: Captive portal: Zone_BANGALORE

Captive portal(s) | MAC Whitelist | IP Address Whitelist | File Manager | Access Groups

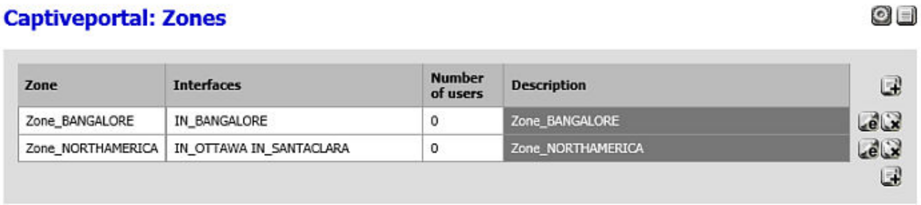
☑ Enable captive portal

Interfaces: IN, IN_BANGALORE, IN_OTTAWA, IN_SANTACLARA

Select the interface(s) to enable for captive portal.

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! Possible setting allowed is: minimum 4 connections per client IP address, with a total maximum of 100



Captiveportal: Zones

Zone	Interfaces	Number of users	Description
Zone_BANGALORE	IN_BANGALORE	0	Zone_BANGALORE
Zone_NORTHAMERICA	IN_OTTAWA IN_SANTACLARA	0	Zone_NORTHAMERICA

3. **Configure Access Portal Access Groups:** On the main Access Portal Administration Web UI page, click **Services** > **Captive Portal**. Click the Edit icon for Zone_Bangalore and click the **Access Groups** tab. Click the Add icon to create an Access Group. Create six Access Groups as follows:

   For Zone_BANGALORE:

Group name	Description	OUT Interface	Success Page setting
Access-Group-Employees	OUT_EMPLOYEE_BANGALORE interface	OUT_EMPLOYEE_BANGALORE	originally accessed page
Access-Group-Guests	Default OUT interface	OUT	system default success page
Access-Group-BusinessPartners	OUT_BUSINESSPARTNER interface	OUT_BUSINESSPARTNER	http://<URL of choice>

   For Zone_NORTHAMERICA:

Group name	Description	OUT Interface	Success Page setting
Access-Group-Employees	OUT_EMPLOYEE_SANTACLARA interface	OUT_EMPLOYEE_SANTACLARA	originally accessed page
Access-Group-Guests	Default OUT interface	OUT	system default success page

Table continues…

Group name	Description	OUT Interface	Success Page setting
Access-Group-BusinessPartners	OUT_BUSINESSPARTNER interface	OUT_BUSINESSPARTNER	http://www.<URL of choice>

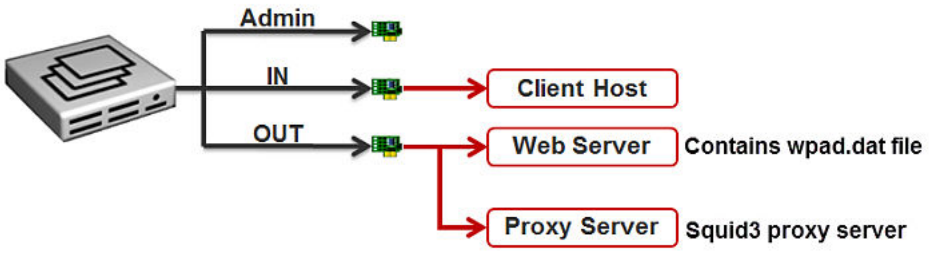
For more information, see Configuring Access Groups on page 49 in this document.

Example with proxy server for clients

The following section contains an example of how to automatically push the proxy setup from the Access Portal to guest devices.

This example uses IIS as a web server and Squid as a proxy server. The configuration for other web servers and proxy servers will differ.

In this example, the client is redirected to the Web and proxy server on the OUT interface. The proxy server and web server must be on the OUT interface since all the traffic from client will always goes through the OUT interface.



Related Links

Configuring the example deployment on page 93

Configuring the example deployment

Procedure

Create the .dat file:

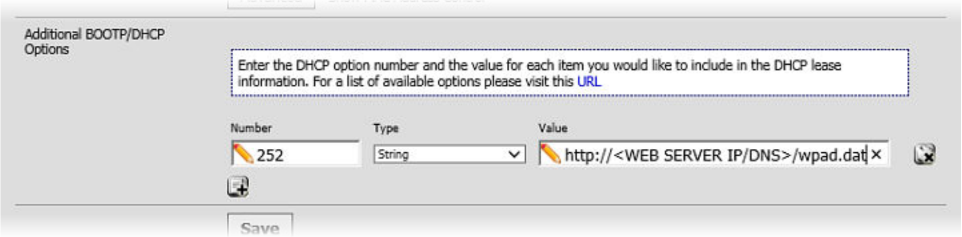
1. Create a .dat file, in this example named “wpad.dat”, with the following contents:

```
function FindProxyForURL(url, host) {
 return "PROXY <PROXY SERVER IP>:<PORT NUMBER>;
}
```

Configure the Access Portal DHCP settings:

2. On the main Access Portal Administration Web UI page, click **Services** > **DHCP Server**.
3. On the Services: DHCP server page, click the appropriate IN interface tab.
4. Select the **Enable DHCP Server on IN interface** check box.

5. In the **Range** fields, enter the range of IP addresses that the DHCP server will assign to guest devices.
6. Scroll down to the **Additional BOOTP/DHCP Options** section, click **Advanced**, and click the Add icon.
7. Enter `252` in the **Number** field, choose **String** from the **Type** drop-down list, enter `http://<WEB SERVER IP/DNS>/wpad.dat` in the **Value** field, and click **Save**.



Additional BOOTP/DHCP Options

Enter the DHCP option number and the value for each item you would like to include in the DHCP lease information. For a list of available options please visit this URL

Number	Type	Value
252	String	http://<WEB SERVER IP/DNS>/wpad.dat

Configure the proxy server:

In this example, the proxy server is a squid3 Linux proxy server

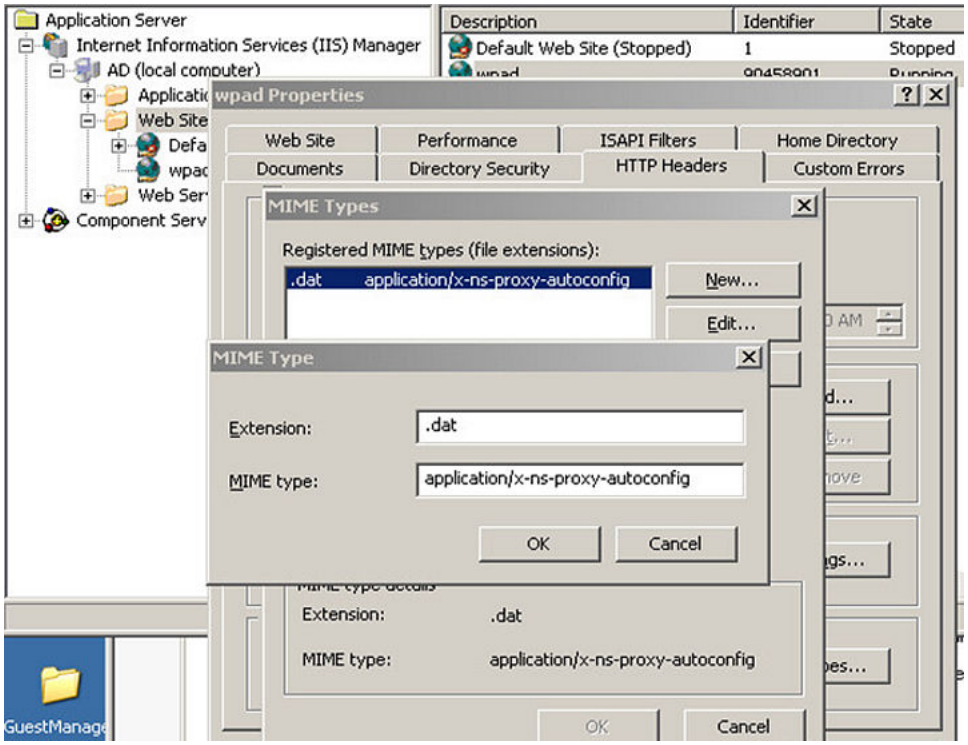
8. Do the following to configure the squid3 Linux proxy server:
   - Enter `apt-get install squid3`
   - Edit `/etc/squid3/squid.conf`:
     - Find “http_port” and change the port number if necessary (by default squid3 listens on 3128 port)
     - Find “http_access” change from `deny all` to `allow all`
   - Enter `Service squid3 restart` or `/sbin/squid3 -s -n -v -f /etc/squid3/squid.conf`
   - If necessary enter to view the logs enter `tail -f /var/log/squid3/access.logs`

Configure the web server:

This example uses IIS as a web server.

9. Open **Manage your server** and click **manage application server** > **IIS manager** > **<local computer>** > **Web sites**.
10. Right-click **Create new web site**, right-click on the newly created web site, and open **Properties**.

11. Click **HTTP headers** > **Edit mime types** and configure as follows:



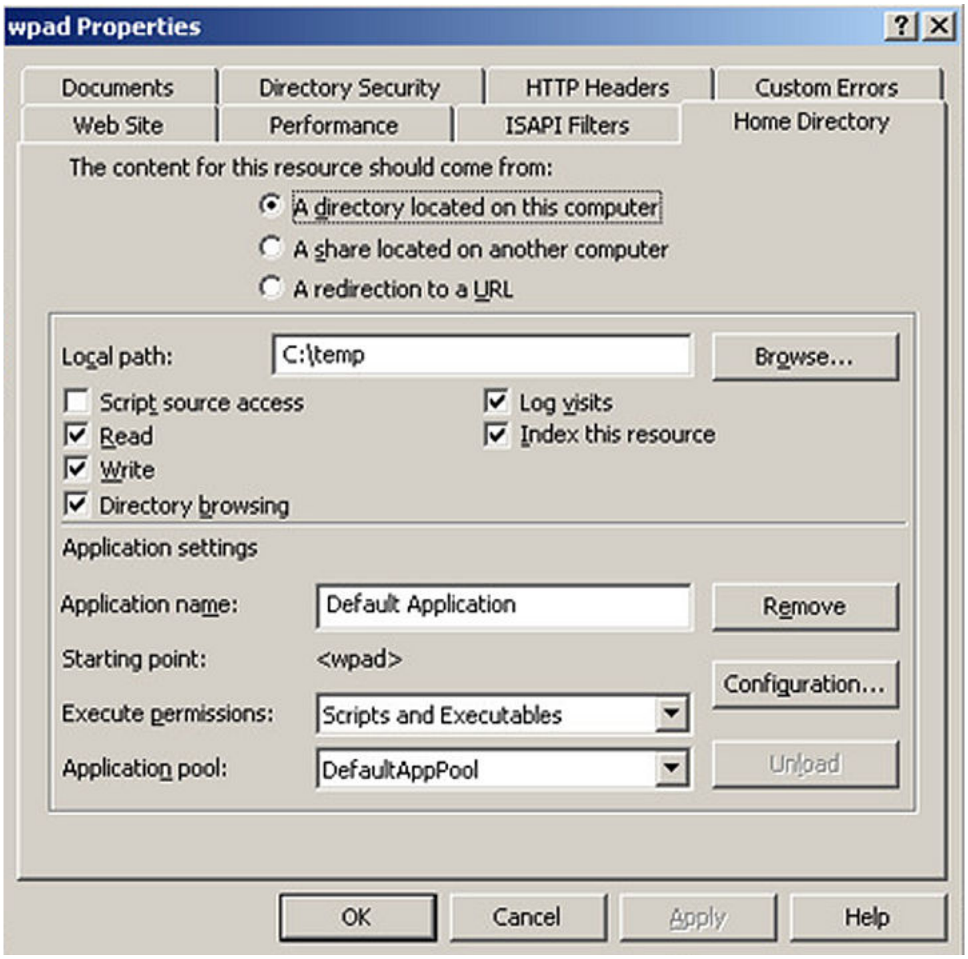
Registered MIME types (file extensions):
.dat application/x-ns-proxy-autoconfig

MIME Type

Extension: .dat

MIME type: application/x-ns-proxy-autoconfig

12. Store the .dat file in the home directory of the web server (in this example “C:\temp”).



The content for this resource should come from:

● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local path: C:\temp

□ Script source access
☑ Read
☑ Write
☑ Directory browsing
☑ Log visits
☑ Index this resource

Application settings

Application name: Default Application

Starting point: <wpad>

Execute permissions: Scripts and Executables

Application pool: DefaultAppPool

Test the proxy server functionality:

13. Configure one zone named “Zone_BANGALORE_GUEST”.
14. Associate one IN interface to this zone.
15. Enable DHCP Server on the IN interface and configure the DHCP server 252 option.
16. Configure Zone_BANGALORE_GUEST with one Access Portal Access Group named “Internet”.
17. Connect a client on the Zone_BANGALORE_GUEST network.
18. From the client, execute `ipconfig release/renew`.
19. Open and configure a browser for “auto configure proxy setting”.
20. Enter the client host URL in the browser. If the proxy server is reachable, the Client should get redirected to the portal page with a redirection URL of http://<webserver>/wpad.dat.