DEPLOYMENT GUIDE

Implementing Infoblox DHCP Authentication with Captive Portal

Table of Contents

Introduction **2**

Prerequisites **2**

Configuration Instructions **2**

- Create an Authentication Server Group 2
- Configuring an Active Directory Authentication Server Group 2
- Configuring an LDAP Authentication Server Group 5
- Configuring a RADIUS Authentication Server Group 9
- Configuring Captive Portal 12
- Customizing the Captive Portal Screen 13
- Managing Captive Portal Certificates 15
- Generate Self-signed Certificates 15
- Generating Certificate Signing Requests 16
- Uploading Certificates 17
- Downloading Certificates 18
- Starting Captive Portal Service 18
- Defining the IPv4 networks and DHCP ranges 19
- Quarantine DHCP Range 19
- Authenticated DHCP Range 20
- Guest DHCP Range. 20
- Defining MAC Address Filters 21
- Configuring in the Captive Portal Wizard 21

Demonstration of Captive Portal **24**

Monitoring DHCP Authentication **29**

- Viewing the DHCP Ranges and Filters 30

Use Cases **30**

Introduction

This feature provides the ability to control access to your IPv4 networks. (This feature does not support IPv6 networks.) You can divide a network into segments for unauthenticated, authenticated and guest users, and the DHCP server assigns clients to the appropriate segment based on their MAC addresses and authentication credentials.

Prerequisites

- If the DHCP server and Captive Portal server are virtual machines, then VNIOS license must be installed.
- Grid licenses must be installed on the DHCP server and Captive Portal Server.
- DHCP licenses must be installed on the DHCP server and Captive Portal server.
- The Captive Portal member also must have DNS license installed
- The Captive Portal member only runs captive portal.

Configuration Instructions

Create an Authentication Server Group

Authentication Server Groups allow you to add one or more authentication servers in the following authentication categories:

- Active Directory
- LDAP
- RADIUS
- TACACS+
- OCSP

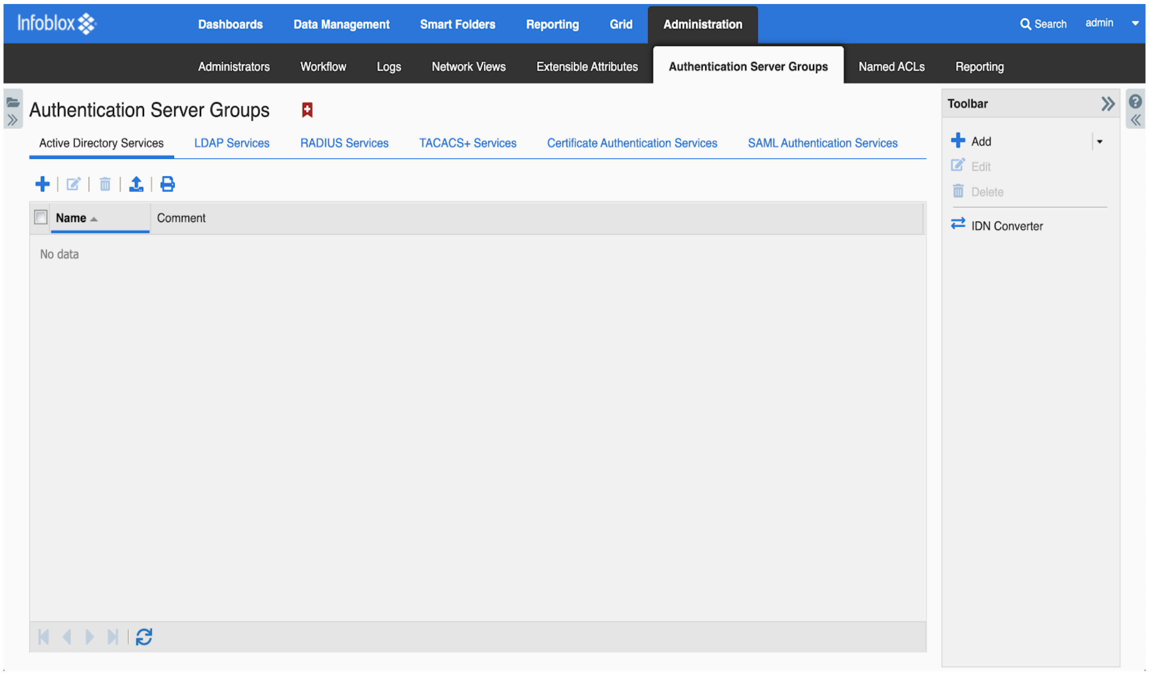
Captive Portal supports Active Directory, LDAP, and RADIUS for authenticating users.

Configuring an Active Directory Authentication Server Group

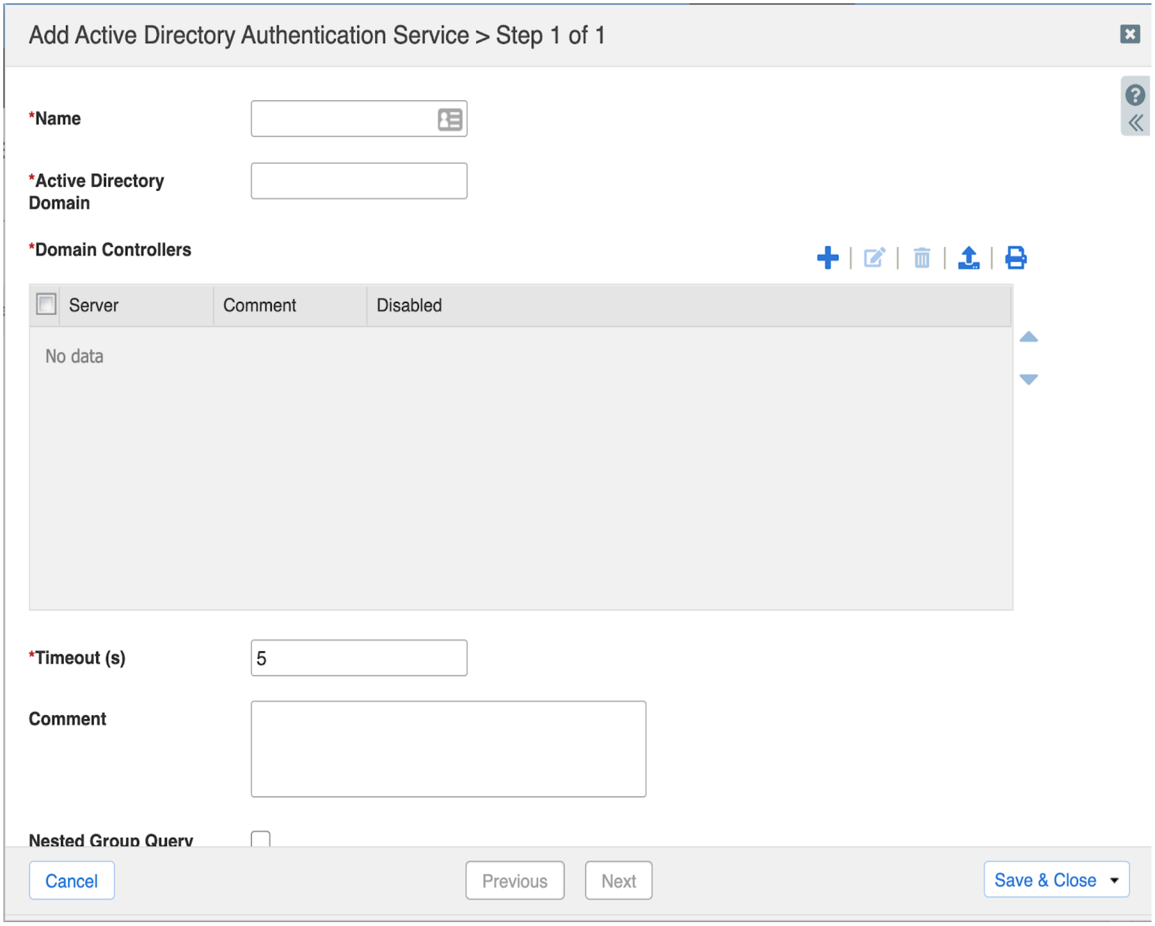
You can add multiple Active Directory servers running Windows Server 2003 or Windows Server 2008 or Windows Server 2012 to an authentication server group and prioritize the servers. When the member sends an authentication request, it always selects the first AD server in the list. It only sends authentication requests to the next server on the list if the first server does not respond.

Steps to configure an Active Directory Authentication Server Group for a captive portal server:

1. On the GUI, navigate to Administration --> Authentication Server Groups --> Active Directory Services.



2. Click on the Add icon in the main screen or toolbar to bring up the wizard and complete the following:



Add Active Directory Authentication Service > Step 1 of 1

*Name

*Active Directory Domain

*Domain Controllers

☐ Server	Comment	Disabled
No data		

*Timeout (s): 5

Comment

Nested Group Query ☐

a. Name: Enter a name for the service.
b. Active Directory Domain: Enter the AD domain name.
c. Domain Controllers: Click the Add icon and complete the following to add an AD domain controller:
   i. Server Name or IP Address: Enter the FQDN or the IP address of the AD server that is to be used for authentication.
   ii. Comment: Enter additional information about the AD server.
   iii. Authentication Port: Enter the port number on the domain controller to which the member sends authentication requests. The default is 389.
   iv. Encryption: Select SSL from the drop-down list to transmit through an SSL (Secure Sockets Layer) tunnel. When you select SSL, the appliance automatically updates the authentication port to 636. Infoblox strongly recommends that you select this option to ensure the security of all communications between the member and the AD server. If you select this option, you must upload a CA certificate from the AD server. Click CA Certificates to upload the certificate. In the CA Certificates dialog box, click the Add icon, and then browse to the certificate to upload it.
   v. Connect through Management Interface: Select this so that the member uses the MGMT port for administrator authentication connections with just this AD server.
   vi. Disable server: Select this to disable an AD server if, for example, the connection to the server is down and you want to stop the Grid member from trying to connect to this server.

vii. Click Test to test the connection to the AD server. If the Grid member connects to the domain controller using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the server, the appliance displays a message indicating an error in the configuration.

viii. Click Add to add the domain controller to the group.

d. Timeout(s): The number of seconds that the Grid member waits for a response from the specified authentication server. The default is 5.

e. Comment: Enter additional information about the service.

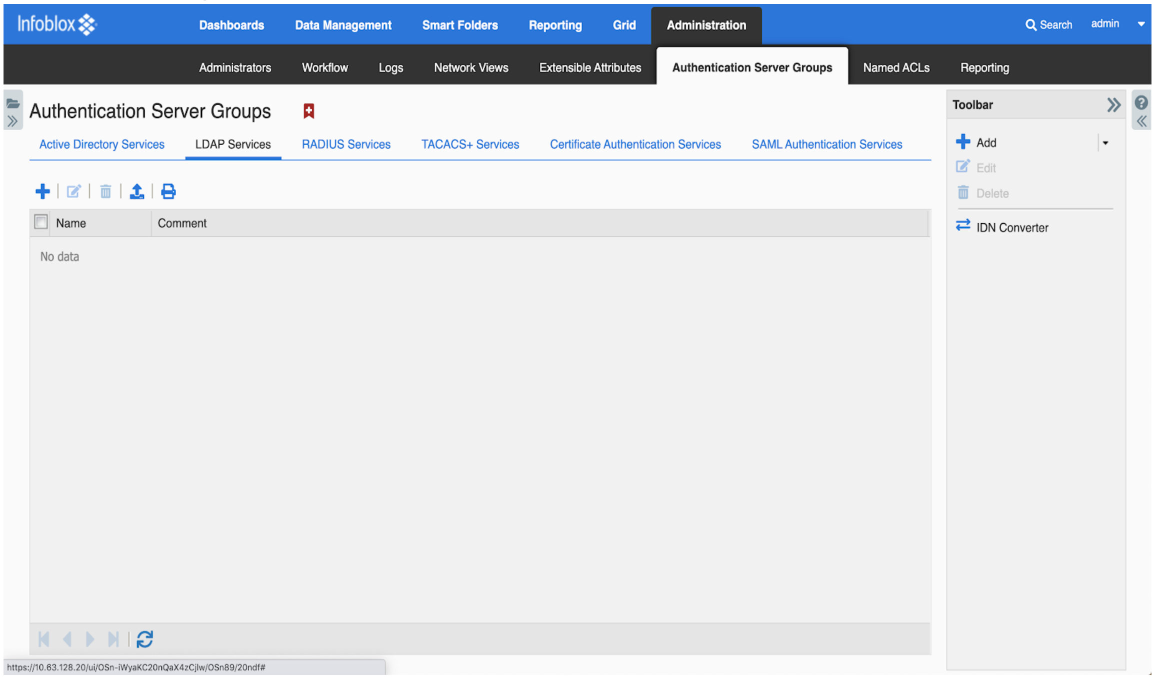
f. Disable: Select this to disable an AD authentication service profile.

3. Save the configuration and click Restart if it appears at the top of the screen.

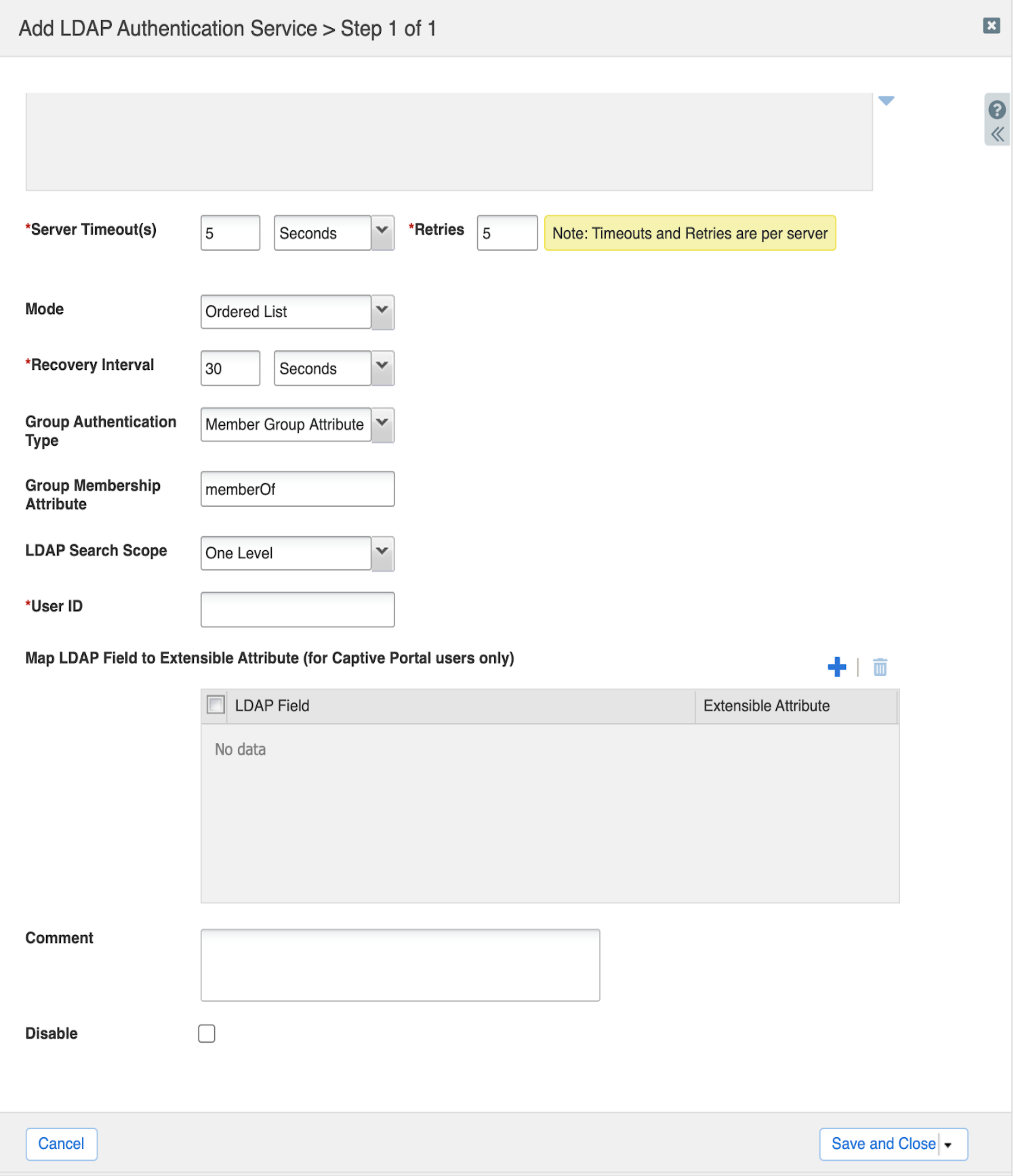
Configuring an LDAP Authentication Server Group

Steps to configure an LDAP Authentication Server Group for a captive portal server:

1. On the GUI, navigate to Administration   Authentication Server Groups   LDAP Services.



2. Click on the Add icon in the main screen or toolbar to bring up the wizard and complete the following:



Add LDAP Authentication Service > Step 1 of 1

*Server Timeout(s)	5 Seconds
*Retries	5
Mode	Ordered List
*Recovery Interval	30 Seconds
Group Authentication Type	Member Group Attribute
Group Membership Attribute	memberOf
LDAP Search Scope	One Level
*User ID	
Comment	
Disable	□

Note: Timeouts and Retries are per server

Map LDAP Field to Extensible Attribute (for Captive Portal users only)

□ LDAP Field	Extensible Attribute
No data	

a. In the Add LDAP Authentication Service wizard, complete the following:
   i. Name: Enter the name of the server group.
   ii. LDAP Servers: Click the Add icon and enter the following:
      1. Server Name or IP Address: Enter the FQDN (fully-qualified domain name) of the server or enter the IPv4/IPv6 address.
      2. LDAP Version: Select the LDAP version. The NIOS appliance supports both LDAPv2 and LDAPv3. The default LDAP version is v3.
      3. Base DN: Enter the base DN (Distinguished Name) value. All entries stored in an LDAP directory have a unique DN.

4. Authentication Type: Select the authentication type from the drop-down list. The supported authenticated types are as follows:
    a. Anonymous: Select this to connect to the LDAP server anonymously. This is selected by default.
    b. Authenticated: Select this to connect using the bind DN and bind password defined for that server.
        i. Bind User DN: Enter the bind user DN.
        ii. Bind Password: Enter the bind password.
    c. Encryption: Select the encryption type from the drop-down list.
        i. SSL: This is selected by default. All of the network traffic is encrypted using SSL (Secure Sockets Layer) protocol. The appliance automatically updates the authentication port to 636 for SSL. You must upload a CA certificate that verifies the LDAP server certificate. Click CA Certificates to upload the certificate. In the CA Certificates dialog box, click the Add icon, and then browse to the certificate to upload it.
        ii. NONE: Select this to use an unencrypted connection. Note that Infoblox strongly recommends that you select the SSL option to ensure the security of all communications between the server and the member.
    d. Network Port: Enter the authentication port number on the LDAP server to which the appliance sends authentication requests. The default value is 636. When you select NONE from the Encryption drop-down list, the appliance automatically updates the authentication port to 389.
    e. Comment: Enter useful information about the LDAP server.
    f. Connect through Management Interface: Select this so that the NIOS appliance uses the MGMT port for administrator authentication connection with just this LDAP server.
    g. Disable Server: Select this to disable the LDAP server if, for example, the connection to the server is down and you want to stop the NIOS appliance from trying to connect to this server. You cannot disable the only server in a group if it is already being used by the remote authentication policy.
    h. Click Test to test the connection. If the NIOS appliance connects to the LDAP server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the server, the appliance displays a message indicating an error in the configuration.
    i. Click Add to add the LDAP server to the group. When you add multiple LDAP servers, the appliance lists the servers in the order you added them. This list also determines the order in which the NIOS appliance attempts to contact an LDAP server. You can move a server up or down the list by selecting it and clicking the up or down arrow. You can also delete a server by selecting it and clicking the Delete icon.
5. Server Timeout(s): Specify the number of seconds that the appliance waits for a response from the LDAP server. The default value is 5 seconds.
6. Retries: Specify how many times the appliance attempts to contact an authentication LDAP server. The default value is 5. If you have configured multiple LDAP servers for authentication and the NIOS appliance fails to contact the first server in the list, it tries to contact the next server after completing the specified number of attempts, and so on.

7. Mode: Specifies the order in which a Grid member connects to an LDAP server.
    a. Ordered List: The Grid member always selects the first LDAP server in the list when it sends an authentication request. It queries the next server only when the first server is considered down. This is the default.
    b. Round Robin: The Grid member sends the first authentication request to a server chosen randomly in a group. If there is no response from the server, the Grid member selects the next server in the group. Continued attempts are performed sequentially until it selects the last server in the group. Then it starts with the first server in the group and continues the selection process until all the servers have been attempted.
8. Recovery Interval: Specify the number of seconds that the appliance waits to recover from the last failed attempt in connecting to an LDAP server. Select the time unit from the drop-down list. The default is 30 seconds. This is the time interval that NIOS waits before it tries to contact the server again since the last attempt when the appliance could not connect to the LDAP server or when the LDAP server did not send a reply within the configured response timeouts and retry attempts.
9. Group Authentication Type: Select the group authentication type for LDAP authentication service from the drop-down list. By default, Member Group Attribute authentication type is selected. When you select Member Group Attribute, you can specify custom LDAP group attribute in the Group Membership Attribute field. For example, memberOf, isMemberOf, etc. The appliance uses this attribute to retrieve the group names to which the admin belongs. When you select Posix Group, the appliance uses "memberuid" and "objectClass" to retrieve the group names to which the admin belongs.
10. Group Membership Attribute: Specify the LDAP group attribute (such as "memberOf" and "isMemberOf"). This is used to query the server and retrieve the group names to which the admin belongs. This field is enabled only when you select Member Group Attribute in the Group Authentication Type drop-down list. The default value is memberOf.
11. LDAP Search Scope: To search for an admin user name in the LDAP directory, select one of the following LDAP search scope:
    a. Base: Specify Base to perform search only on base in the LDAP directory. This is the top level of the LDAP directory tree.
    b. One Level: Specify One Level to perform search on base DN and one level below the base in the LDAP directory.
    c. Sub tree: Specify Sub tree to perform search on base and all the entries below the base DN in the LDAP directory. The default value is One Level.
12. User ID: Specify the attribute associated with the user object in the LDAP server, such as "uid" and "cn". This attribute is used to match the NIOS user name.
13. Map LDAP Field to Extensible Attribute (for Captive Portal Users only): If you configure the LDAP authentication server group to authenticate the captive portal users, you can map an LDAP attribute value to an existing extensible attribute. This mapping is optional. By doing so, the LDAP attribute value will be queried from the LDAP server once the captive portal user authentication is successful. The attribute value received from the LDAP server is mapped to the corresponding extensible attribute. NIOS updates or creates a MAC address filter depending on the captive

portal user or the client's hardware and name. Click the Add icon and enter the following:

a. LDAP Field: Enter the LDAP attribute. This attribute is queried in the LDAP directory server.
b. Extensible Attributes: Select an attribute from the drop-down list. The drop-down list displays only the extensible attributes configured with attribute type as string. Infoblox recommends that you avoid confidential data while mapping extensible attribute to an LDAP attribute because this data is visible in the extensible attribute field of the corresponding MAC address filter.

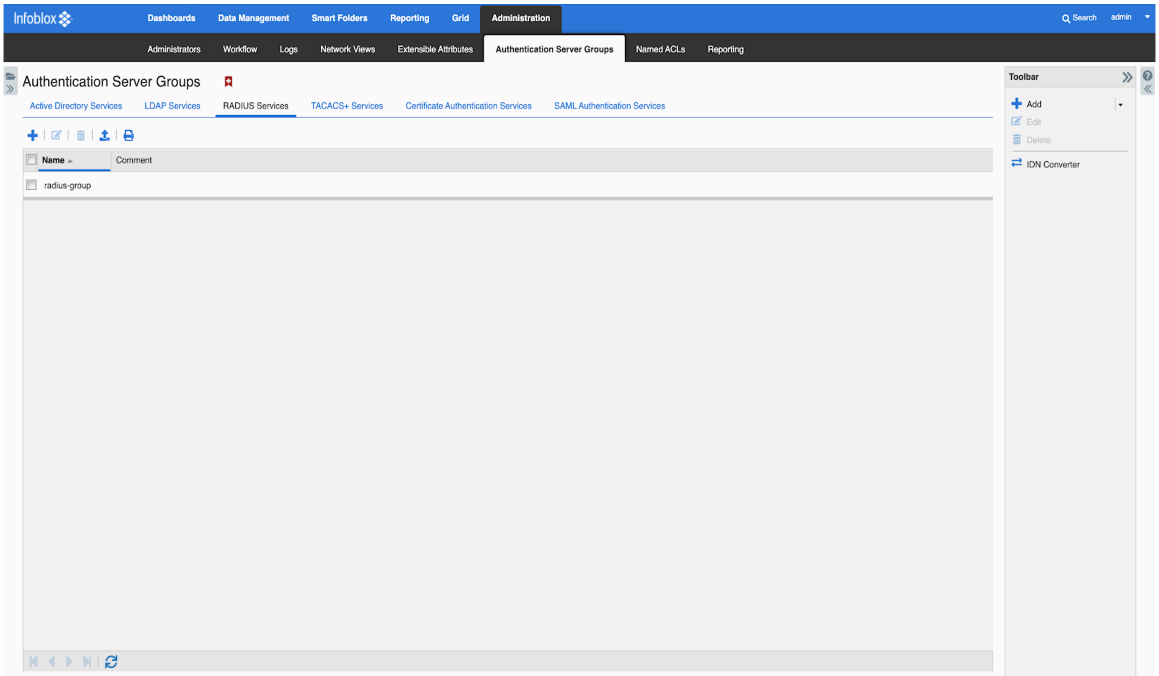
14. Comment: Enter useful information about the LDAP server group.
15. Disable: Select this to disable the LDAP authentication server group. Note that you cannot disable an LDAP group if it is already being used to authenticate one or more administrators and/or captive portal users.

3. Save the configuration and click Restart if it appears at the top of the screen.

Configuring a RADIUS Authentication Server Group

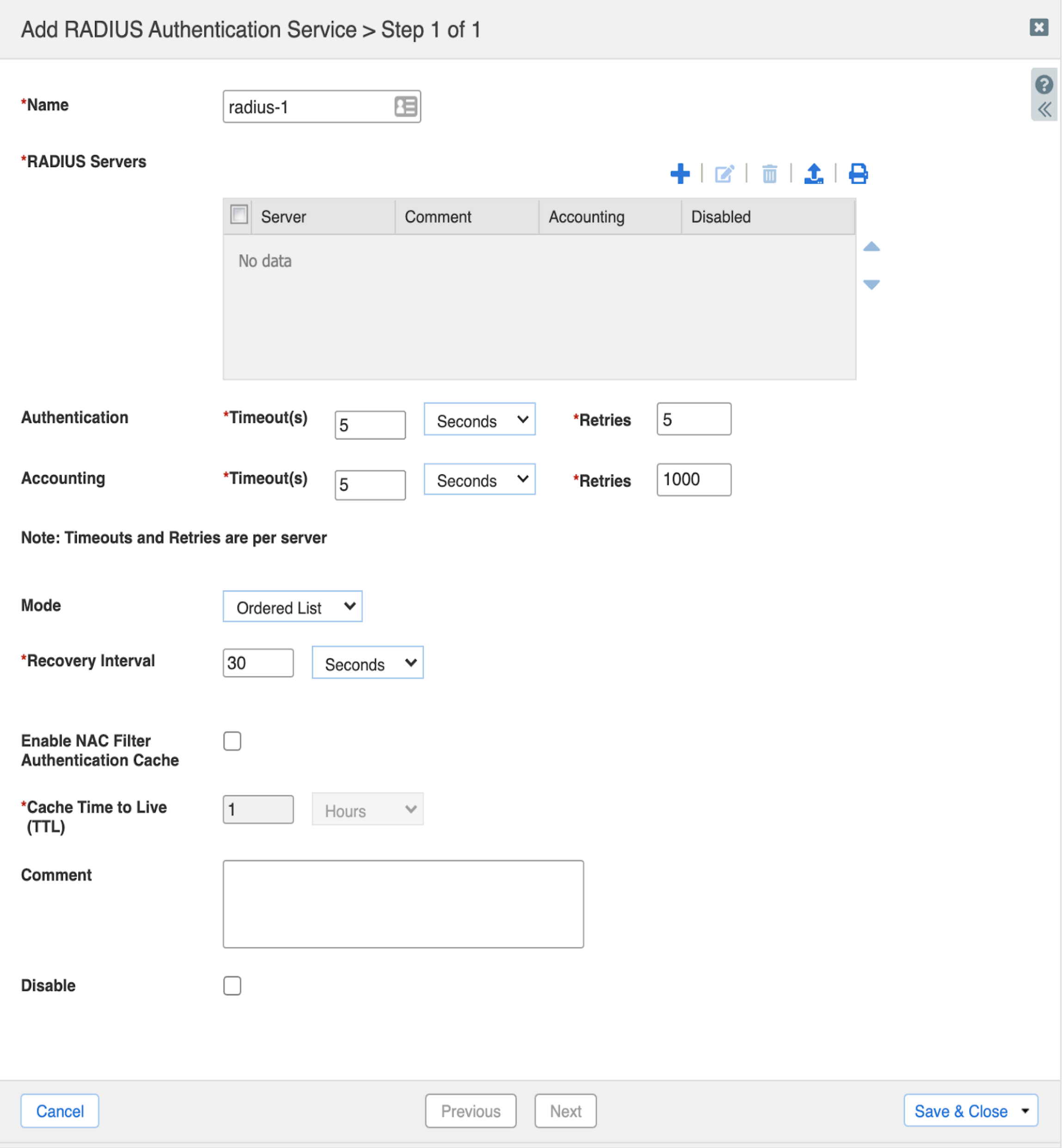
You can add multiple RADIUS servers to an authentication server group and prioritize them. When the member sends an authentication request, it always selects the first RADIUS server in the list. It only sends authentication requests to the next server on the list if the first server goes down.
To configure the RADIUS authentication server group to which a captive portal server sends authentication requests:

1. In the GUI, navigate to Administration   Authentication Server Groups   RADIUS Service.



2. Click on the Add icon to add a RADIUS server.

3. In the Add RADIUS Authentication Service wizard, complete the following:



Add RADIUS Authentication Service > Step 1 of 1

*Name: radius-1

*RADIUS Servers

□	Server	Comment	Accounting	Disabled
No data				

Authentication: *Timeout(s) 5 Seconds *Retries 5

Accounting: *Timeout(s) 5 Seconds *Retries 1000

Note: Timeouts and Retries are per server

Mode: Ordered List

*Recovery Interval: 30 Seconds

Enable NAC Filter Authentication Cache: □

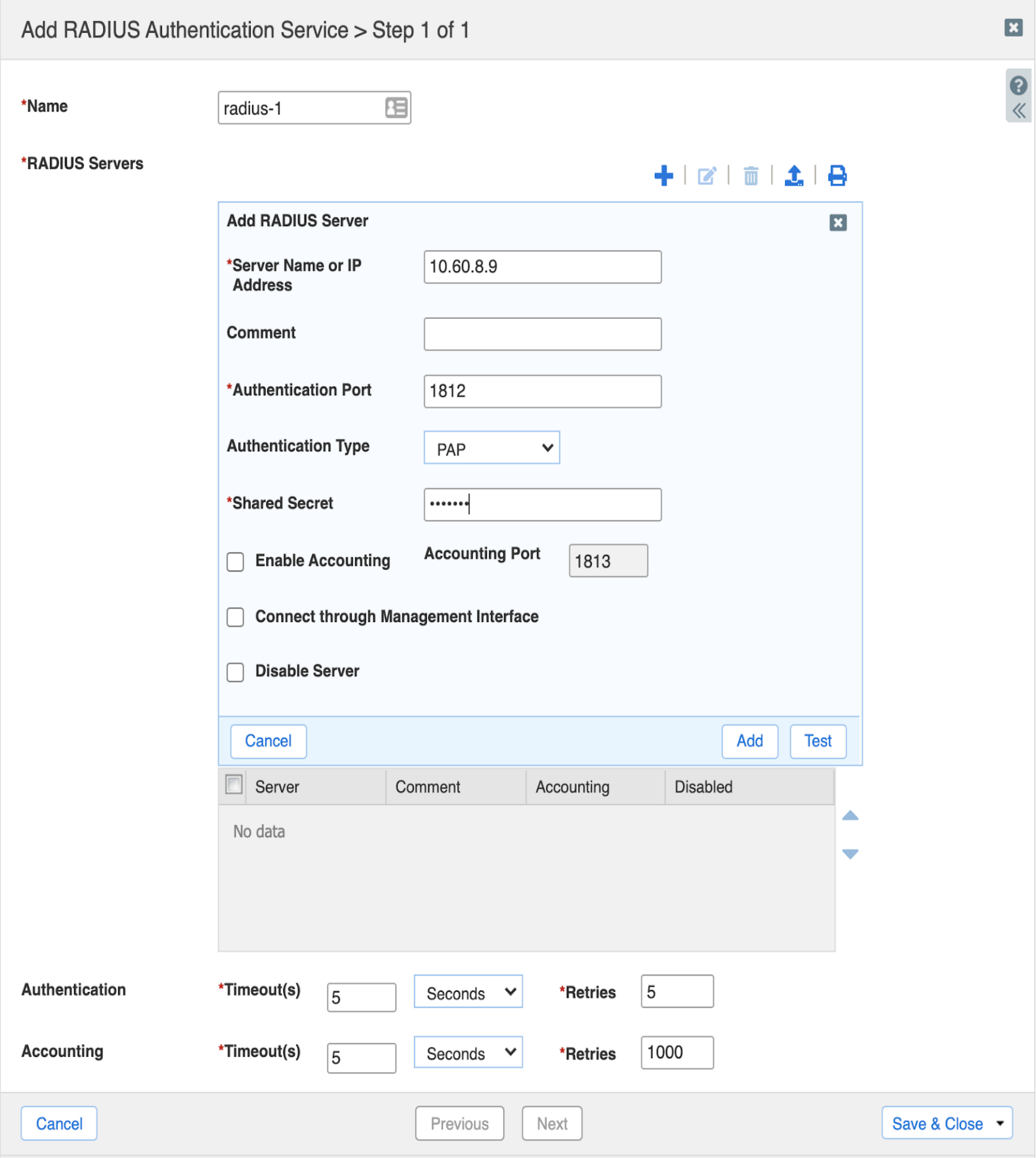
*Cache Time to Live (TTL): 1 Hours

Comment:

Disable: □

a. Name: Enter the name of the server group.

b. RADIUS Servers: Click the Add icon and enter the following:



Add RADIUS Authentication Service > Step 1 of 1

*Name	radius-1
*RADIUS Servers	

Add RADIUS Server

*Server Name or IP Address	10.60.8.9
Comment	
*Authentication Port	1812
Authentication Type	PAP
*Shared Secret	•••••••
□ Enable Accounting	Accounting Port 1813
□ Connect through Management Interface	
□ Disable Server	

□ Server	Comment	Accounting	Disabled
No data			

Authentication	*Timeout(s) 5	Seconds	*Retries	5
Accounting	*Timeout(s) 5	Seconds	*Retries	1000

i. Server Name or IP Address: Enter the RADIUS server FQDN or IP address.
ii. Comment: You can enter additional information about the server.
iii. Authentication Port: The destination port on the RADIUS server. The default is 1812.
iv. Authentication Type: Select the authentication method of the RADIUS server from the drop-down list. You can specify either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol). The default is PAP.
v. Shared Secret: Enter the shared secret that the member DHCP server and the RADIUS server use to encrypt and decrypt their messages. This shared secret must match the one you entered on the RADIUS server.
vi. Connect through Management Interface: Select this to enable the member to use its MGMT port when connecting to this server.

vii. Disable server: Select this to disable the RADIUS server if, for example, the connection to the server is down and you want to stop the DHCP server from trying to connect to this server.

viii. Click Test to validate the configuration and check that the Grid Master can connect to the RADIUS server. Before you can test the configuration though, you must specify the authentication and accounting timeout and retry values. If the Grid Master connects to the RADIUS server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the RADIUS server, the appliance displays a message indicating an error in the configuration.

ix. Click Add to add the RADIUS server to the group. When you add multiple RADIUS servers to the list, you can use the up and down arrows to change the position of the servers on the list. The member DHCP server connects to the RADIUS servers in the order they are listed.

x. Authentication Timeout: The time that the member DHCP server waits for a response from a RADIUS server before considering it unreachable. You can enter the time in milliseconds or seconds. The maximum is 10 seconds.

xi. Authentication Retries: The number of times the member DHCP server retries connecting to a RADIUS server before it considers the server unreachable. The default is five.

xii. Accounting Timeout: The time that the member DHCP server waits for a response from a RADIUS server before considering it unreachable. You can enter the time in milliseconds or seconds. The maximum is 10 seconds.

xiii. Accounting Retries: The number of times the member DHCP server retries connecting to a RADIUS server before it considers the server unreachable. The default is five.

xiv. Recovery Interval: Specifies the duration of time a RADIUS server stays inactive after being down, before becoming eligible to have RADIUS requests sent to it. The recovery interval starts when a RADIUS server is first discovered to be down.

xv. Comment: You can enter additional information about the server group entry.

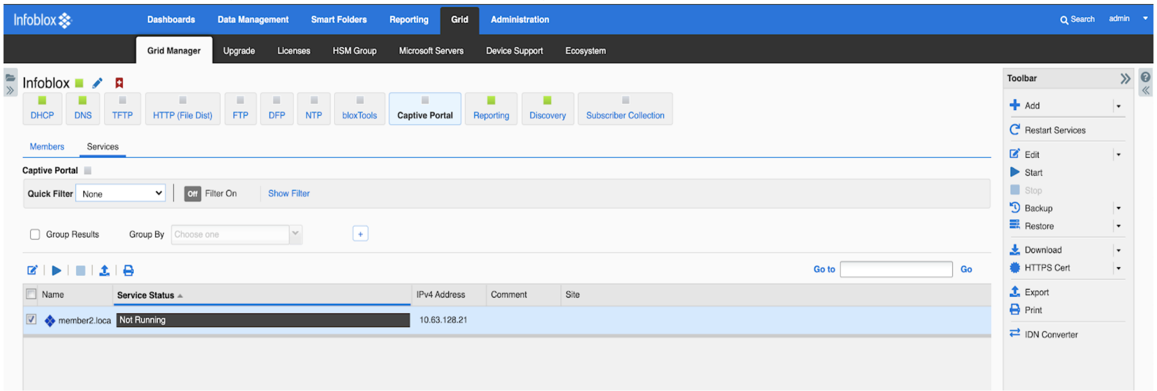
xvi. Disable: Select this to disable the authentication server group.

4. Save the configuration and click Restart if it appears at the top of the screen.

Configuring Captive Portal

The captive portal can be used to register users for authentication, guest users, or both types of users. When a DHCP client attempts to connect to the network and its MAC address is not in any of the configured MAC filters, the member DHCP server assigns it an IP address in the quarantine range. When the quarantined client tries to reach any web site, it is redirected to the captive portal. The captive portal runs a limited DNS server that is used solely to redirect queries to the captive portal web interface.

1. From the GUI, navigate to Grid --> Grid Manager → Captive Portal.



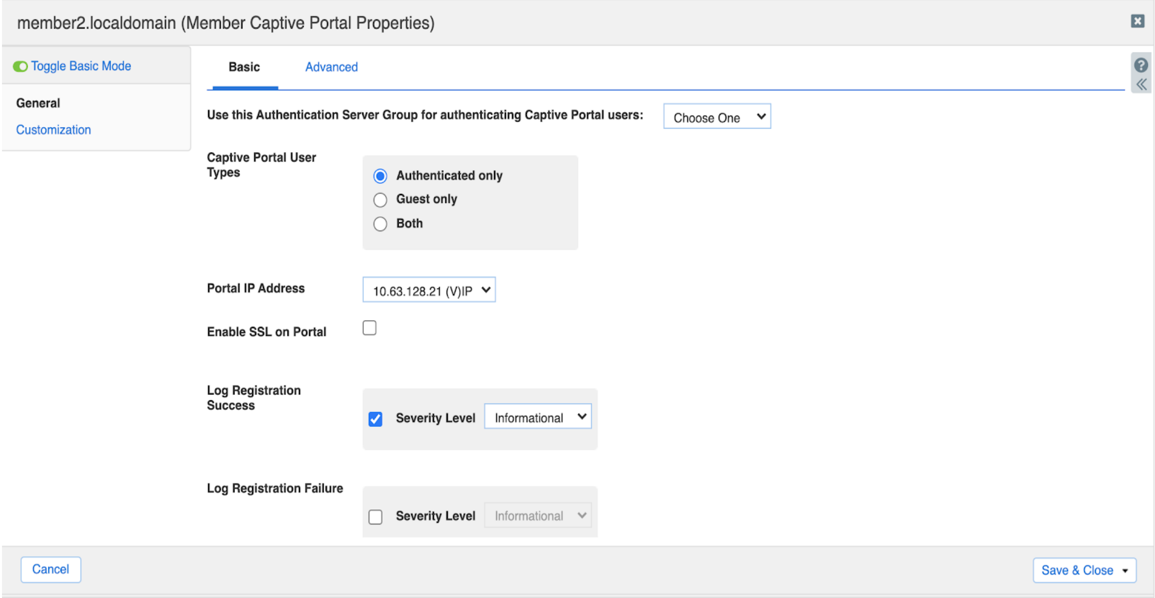
Captive Portal

Quick Filter None | Off Filter On | Show Filter

□ Group Results Group By Choose one

□	Name	Service Status	IPv4 Address	Comment	Site
☑	member2.loca	Not Running	10.63.128.21		

2. Select the member that runs the captive portal and click the Edit icon.



Use this Authentication Server Group for authenticating Captive Portal users: Choose One

Captive Portal User Types: ● Authenticated only ○ Guest only ○ Both

Portal IP Address: 10.63.128.21 (V)IP

Enable SSL on Portal: □

Log Registration Success: ☑ Severity Level: Informational

Log Registration Failure: □ Severity Level: Informational

3. In the General Basic tab of the Member Captive Portal Properties editor, complete the following:
   a. Use This Authentication Server Group for Authenticating Captive Portal Users: Select the authentication server group that authenticates users for this captive portal.
   b. Captive Portal User Types: Specify whether the captive portal is used to register Authenticated users only, Guest users only, or Both.
   c. Portal IP Address: Select the IP address of the captive portal server. The appliance lists the VIP address and the IP addresses of the loopback interface and the LAN2 port, if enabled. You can select any of these addresses as the portal IP address.
   d. Enable SSL on Portal: Select this to support encrypted web traffic through SSL/TLS. If you select this option, you must upload a certificate or generate a self-signed certificate. For information about creating and uploading a certificate for the captive portal, refer to the NIOS Administrators Guide
   e. Network View: This field displays if there are multiple network views configured. Select the network view in which the authenticated, quarantine, and guest DHCP ranges belong.
   f. Log Registration Success: Select to enable the member to log successful registrations in syslog, and then select the logging level from the drop-down list.
   g. Log Registration Failure: Select to enable the member to log failed registrations in syslog, and then select the logging level from the drop-down list.
4. In the General Advanced tab of the editor, you can specify the port on which the member listens for authentication requests redirected from the captive portal. The default port is 4433. Depending on your firewall and network policies, you can configure an unused port greater than 1 and less than 63999.
5. Save the configuration and click Restart if it appears at the top of the screen.

Customizing the Captive Portal Screen

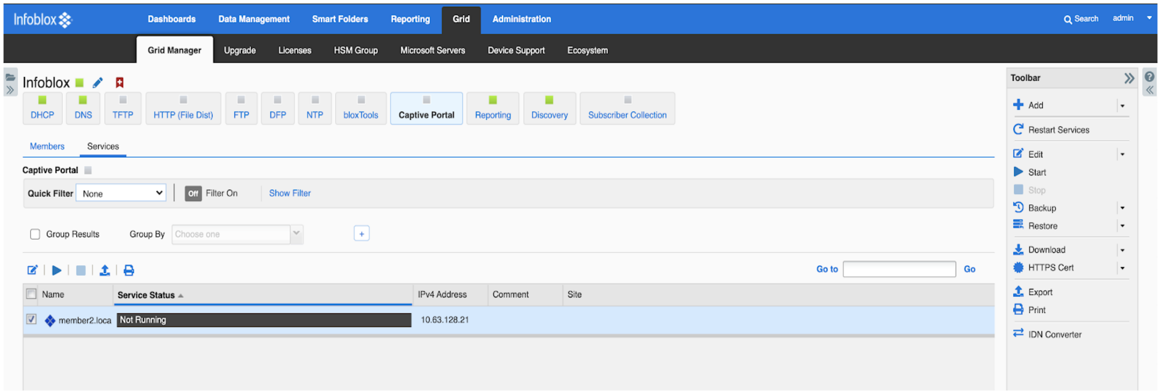
You can customize the captive portal, and if configured, the guest registration page as well. You can upload image files to the appliance and display your own logo, header and footer. In addition, you can upload the acceptable use policies that are displayed on the captive portal and guest registration page. Following are guidelines for each item you can customize:

- Logo Image: The maximum size is 200 pixels wide by 55 pixels high, and the images can be in JPEG, GIF, or PNG format. It displays on top of the header image.
- Header Image: The optimal size is 600 pixels wide by 137 pixels high. The image can be in JPEG, GIF, or PNG format. The header displays at the top of the page.

- Footer Image: The optimal size is 600 pixels wide by 20 pixels high. The image can be in JPEG, GIF, or PNG format. The footer displays at the bottom of the page.
- Acceptable Use Policy: The policy must be saved as a UTF-8 encoded file. It appears below the welcome message in the captive portal. Users can scroll through the policy when they review it. This is used in the captive portal and guest registration page. It must be a .txt file with a maximum of 8000 characters, including white space.

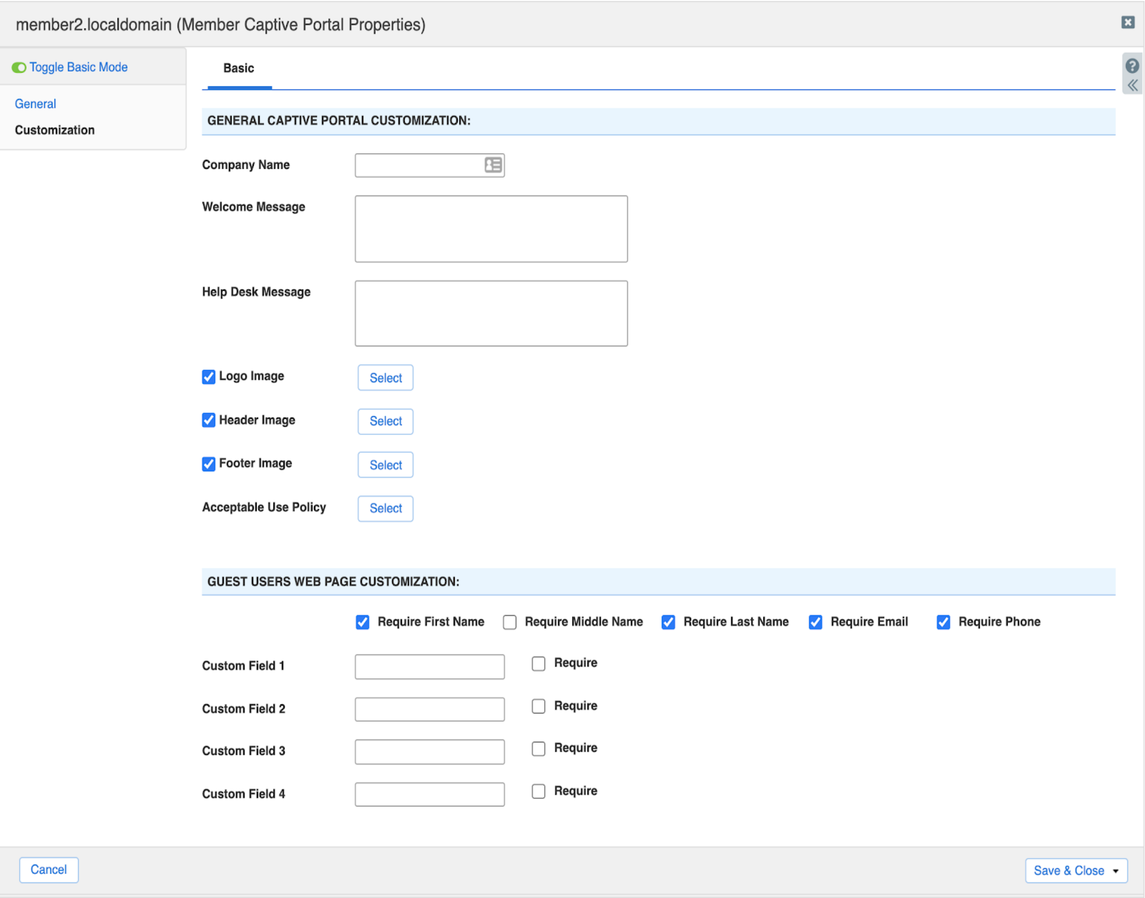
Follow the steps below to customize the captive portal screen:

1. From the GUI, navigate to Grid   Grid Manager   Captive Portal.



☐	Name	Service Status ▲	IPv4 Address	Comment	Site
☑	member2.loca	Not Running	10.63.128.21		

2. Select the member that is going to run the captive portal and then click the edit icon.


member2.localdomain (Member Captive Portal Properties)

GENERAL CAPTIVE PORTAL CUSTOMIZATION:

Company Name

Welcome Message

Help Desk Message

☑ Logo Image

☑ Header Image

☑ Footer Image

Acceptable Use Policy

GUEST USERS WEB PAGE CUSTOMIZATION:

☑ Require First Name ☐ Require Middle Name ☑ Require Last Name ☑ Require Email ☑ Require Phone

Custom Field 1 ☐ Require

Custom Field 2 ☐ Require

Custom Field 3 ☐ Require

Custom Field 4 ☐ Require

3. In the General Captive Portal Customization section, complete the following:

    a. Company Name: Enter the name of your company. The company name displays on the title bar of the browser. You can enter a maximum of 256 characters.
    b. Welcome Message: Type the message that displays on the captive portal. The message can contain a maximum of 300 characters.
    c. Help Desk Message: Type a message that provides Helpdesk information, such as contact information for technical assistance. The message can contain a maximum of 300 characters.
    d. Logo Image, Header Image, Footer Image, Acceptable Use Policy: To display the image files and the acceptable use policy on the captive portal, click Select beside the item you want to upload. In the Upload dialog box, click Select File and navigate to the image or text file. Select the file you want to display and click Upload. Note that these files have size requirements, as listed earlier in this section.

4. In the Guest Users Web Page Customization section, complete the following:
    a. The appliance displays certain fields on the guest registration page. Select the check boxes of the fields that users are required to complete: Require First Name, Require Middle Name, Require Last Name, Require Email, and Require Phone.
    b. Custom Field 1 — Custom Field 4: You can display up to four additional fields on the guest registration page. To add a field to the guest registration page, enter a label for that field. The label can have a maximum of 32 characters. Select Require to require users to complete the field. Users can enter a maximum of 128 characters in each of the fields in the captive portal login page and the guest registration page.
5. Save the configuration and click Restart if it appears at the top of the screen.

Managing Captive Portal Certificates

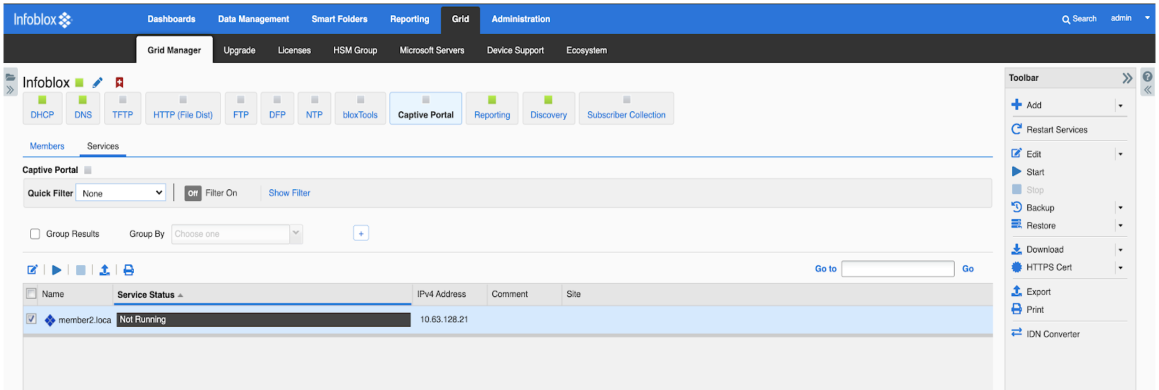
When you enable support for encrypted web traffic sent over SSL/TLS, you can do any of the following:

- Generate a self-signed certificate and save it to the certificate store of your browser.
- Request a CA-signed certificate. When you receive the certificate from the CA, upload it on the member running the captive portal.

Generate Self-signed Certificates

You can generate a self-signed certificate for the captive portal. When you generate a self-signed certificate, you can specify the hostname and change the public/private key size, enter valid dates and specify additional information specific to the captive portal. If you have multiple captive portals, you can generate a certificate for each captive portal with the appropriate hostname.
To generate a self-signed certificate:

1. From the GUI, navigate to Grid   Grid Manager   Captive Portal.

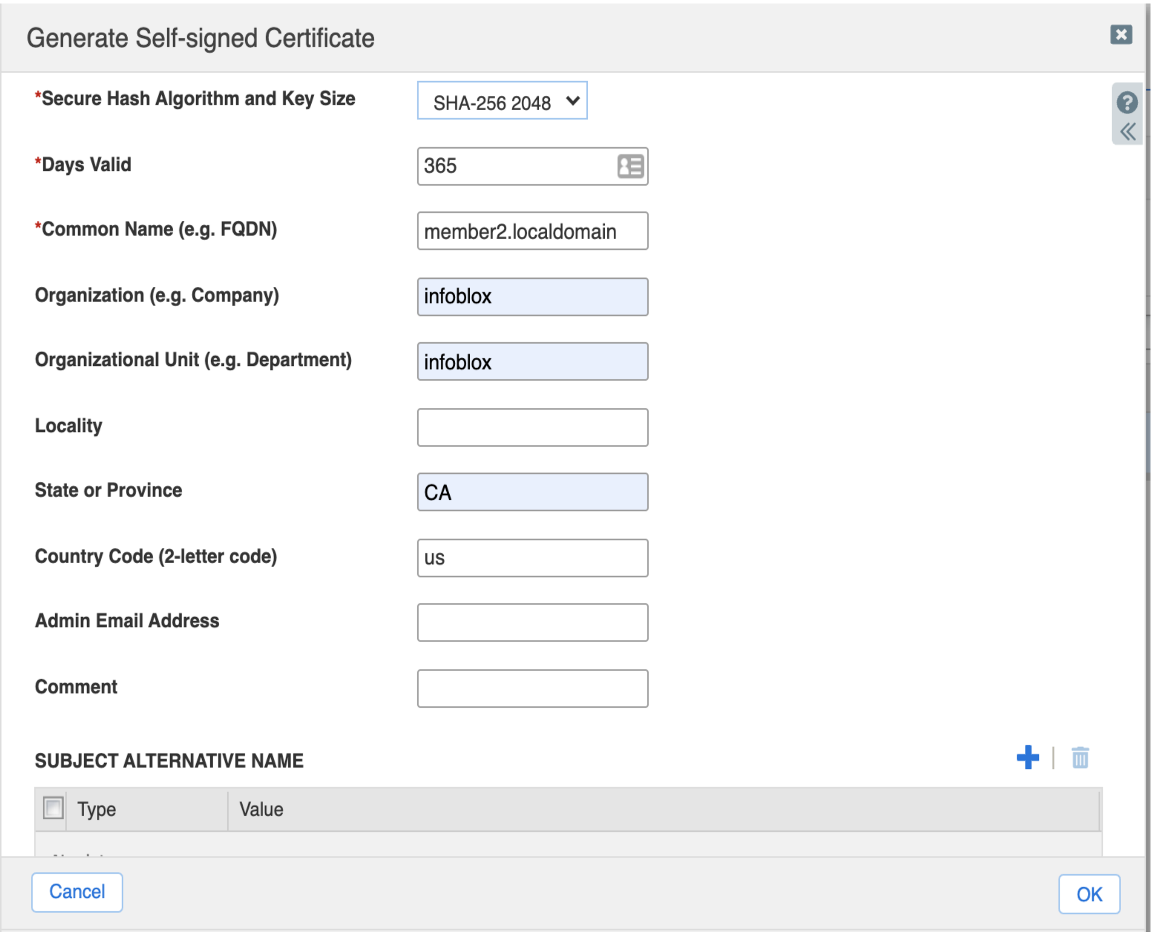


Quick Filter: None | Off Filter On

□ Group Results   Group By: Choose one

	Name	Service Status	IPv4 Address	Comment	Site
☑	member2.loca	Not Running	10.63.128.21		

2. Select the member that is running the captive portal, and then click HTTPS Cert Generate Self-signed Certificate from the Toolbar.



Generate Self-signed Certificate

*Secure Hash Algorithm and Key Size	SHA-256 2048
*Days Valid	365
*Common Name (e.g. FQDN)	member2.localdomain
Organization (e.g. Company)	infoblox
Organizational Unit (e.g. Department)	infoblox
Locality	
State or Province	CA
Country Code (2-letter code)	us
Admin Email Address	
Comment	

SUBJECT ALTERNATIVE NAME

□ Type	Value

3. In the Generate Self-signed Certificate dialog box, complete the following:
    a. Secure Hash Algorithm and Key Size: You can select SHA-1 and a RSA key size of 1024 or 2048. SHA-256 (SHA-2) can be selected together with a RSA key size of 2048 or 4096. The default value is SHA-256 2048.
    b. Days Valid: Specify the validity period for the certificate.
    c. Common Name: Specify the domain name of the captive portal.
    d. Organization: Enter the name of your company.
    e. Organizational Unit: Enter the name of your department.
    f. Locality: Enter a location, such as the city or town of your company.
    g. State or Province: Enter the state or province.
    h. Country Code: Enter the two-letter code that identifies the country, such as US.
    i. Admin E-mail Address: Enter the email address of the captive portal administrator.
    j. Comment: Enter additional information about the certificate.
4. Click OK.

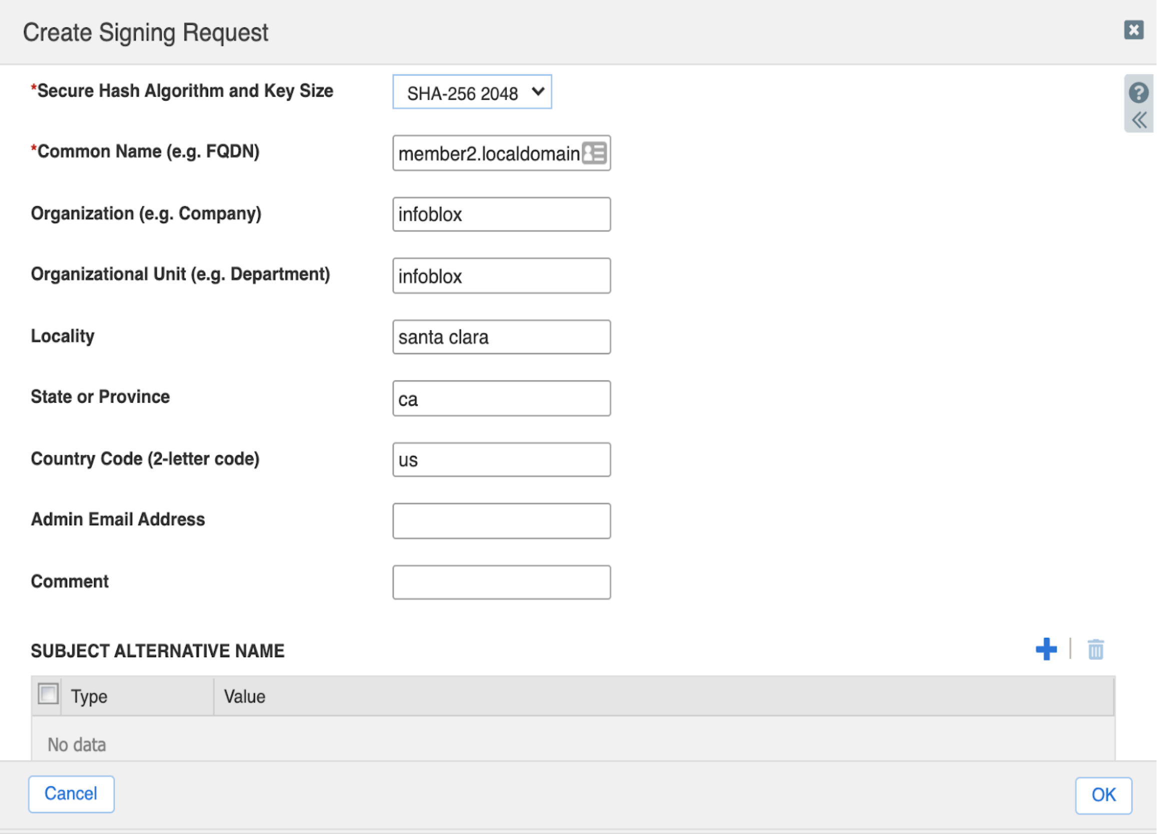
Generating Certificate Signing Requests

You can generate a CSR (certificate signing request) that you can use to obtain a signed certificate from your own trusted CA. Once you receive the signed certificate, you can import it in to the Grid member that runs the captive portal.

To generate a CSR:

1. From the GUI, navigate to Grid Grid Manager Captive Portal.

2. Select the member that is running the Captive Portal, and then click HTTPS Cert   Create Signing Request from the Toolbar.



Create Signing Request

*Secure Hash Algorithm and Key Size	SHA-256 2048
*Common Name (e.g. FQDN)	member2.localdomain
Organization (e.g. Company)	infoblox
Organizational Unit (e.g. Department)	infoblox
Locality	santa clara
State or Province	ca
Country Code (2-letter code)	us
Admin Email Address	
Comment	

SUBJECT ALTERNATIVE NAME

□ Type	Value
No data	

3. In the *Create Signing Request* dialog box, enter the following:
   a. Secure Hash Algorithm and Key Size: You can select SHA-1 and a RSA key size of 1024 or 2048. SHA-256 (SHA-2) can be selected together with a RSA key size of 2048 or 4096. The default value is SHA-256 2048.
   b. Common Name: Specify the domain name of the captive portal.
   c. Organization: Enter the name of your company.
   d. Organizational Unit: Enter the name of your department.
   e. Locality: Enter a location, such as the city or town of your company.
   f. State or Province: Enter the state or province.
   g. Country Code: Enter the two-letter code that identifies the country, such as US.
   h. Admin E-mail Address: Enter the email address of the captive portal administrator.
   i. Comment: Enter information about the certificate.
4. Click OK.

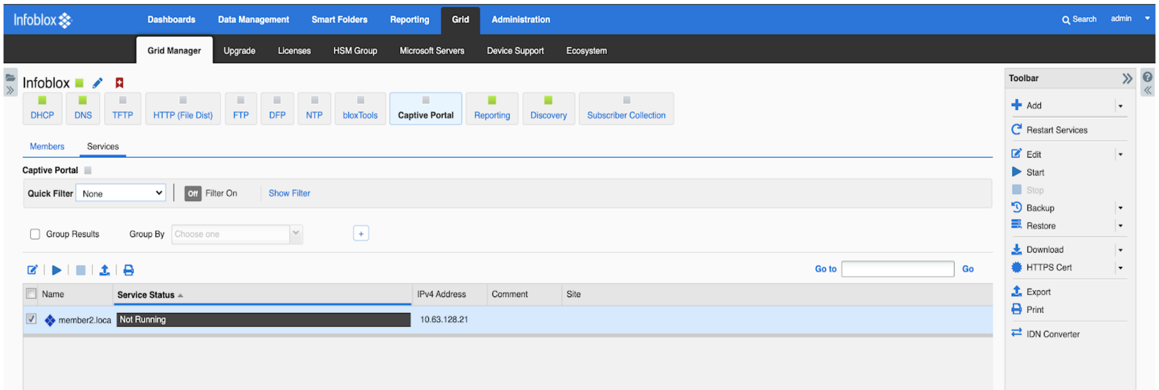
Uploading Certificates

When you upload a certificate, the NIOS appliance finds the matching CSR and takes the private key associated with the CSR and associates it with the newly uploaded certificate. The appliance then automatically deletes the CSR.

If the CA sends an intermediate certificate that must be installed along with the server certificate, you can upload both certificates to the appliance. The appliance supports the use of intermediate certificates to complete the chain of trust from the server certificate to a trusted root CA.

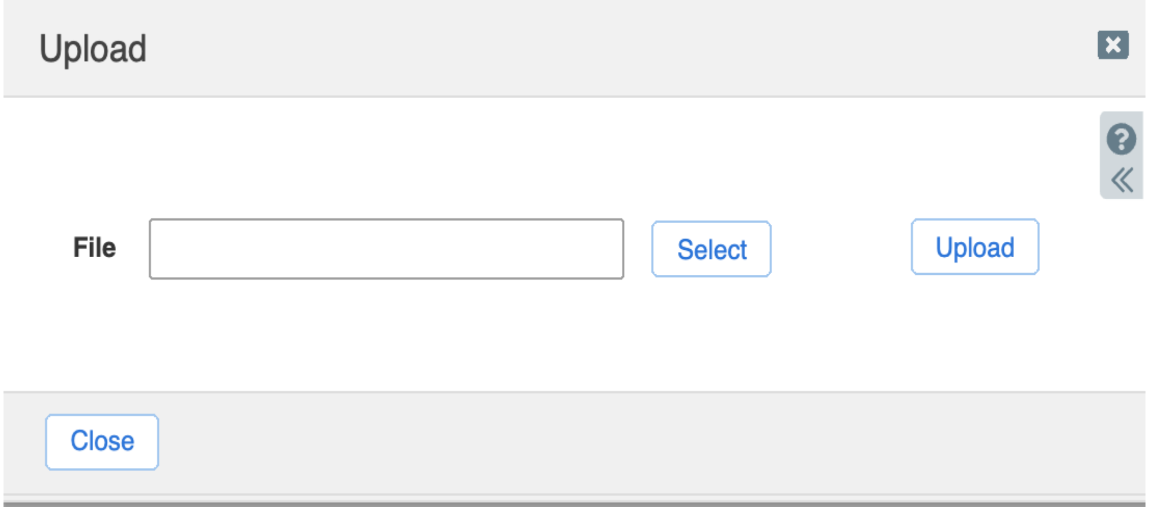
To upload a certificate:

1. From the Grid tab, select the Grid Manager tab, and then click Captive Portal.



	Name	Service Status ▲	IPv4 Address	Comment	Site
☑	member2.loca	Not Running	10.63.128.21		

2. Select the member that is running the captive portal, and then click HTTPS Cert Upload Certificate from the Toolbar.



3. In the Upload dialog box, click Select File, navigate to the certificate location, and click Open. The appliance imports the certificate. When you log in to the appliance again, it uses the certificate you imported.

Downloading Certificates

You can download the current certificate or a self-signed certificate so users can install it in their browsers.

To download a certificate:

1. From the Grid tab, select the Grid Manager tab, and then click Captive Portal.
2. Select the member that is running the captive portal, and then click HTTPS Cert -> Download Certificate from the Toolbar.
3. Navigate to where you want to save the certificate and save it.

Starting Captive Portal Service

Now that you have configured the authentication server group, configured the captive portal settings, you can start the captive portal service. Otherwise, an error will be displayed if you have not configured an authentication server group.

To start the captive portal service:

1. From the Grid tab, select the Grid Manager tab, and then click Captive Portal.
2. Select the member that is configured to run the captive portal service and click the Start icon.
3. Click on the refresh button periodically until the Service Status column turns green.

Defining the IPv4 networks and DHCP ranges

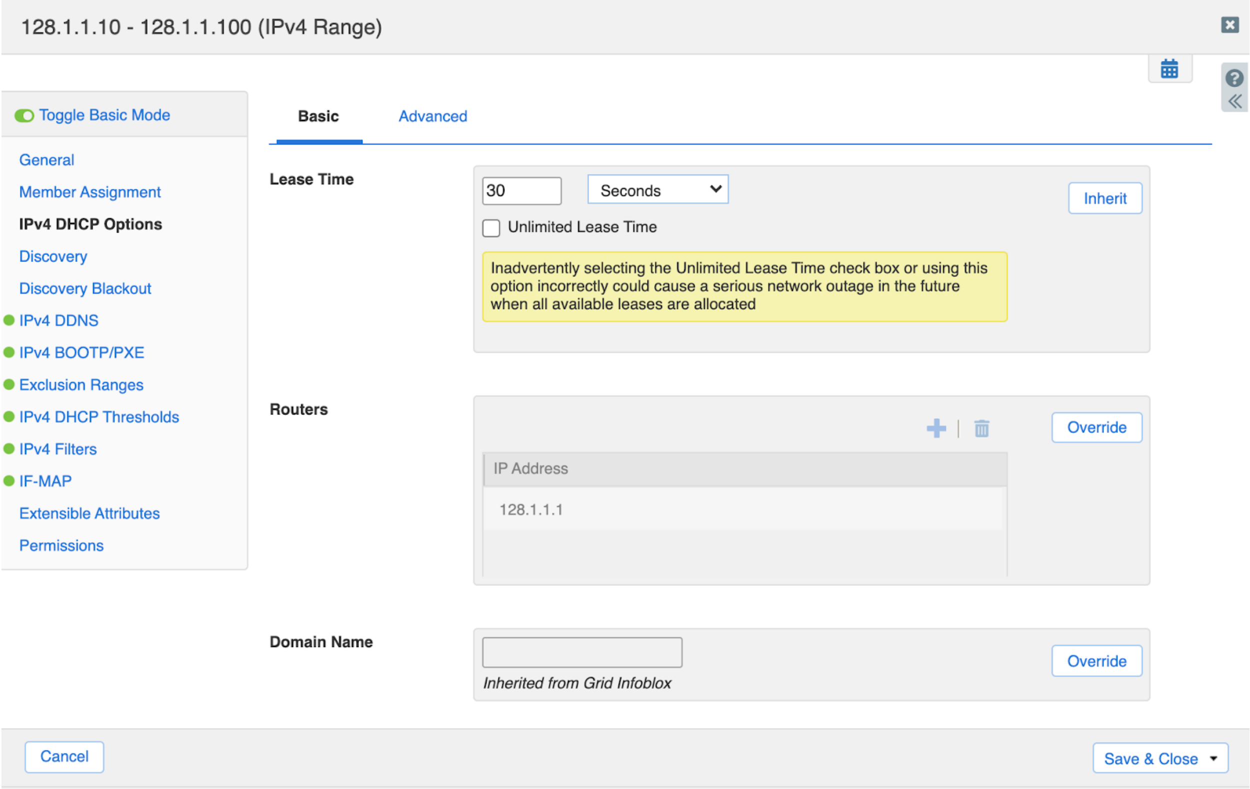
First define the IPv4 network that uses DHCP authentication, and then define the DHCP ranges and services for each access level that you want to provide on the network:

- Quarantine
- Authenticated
- Guest

Quarantine DHCP Range

You must configure a DHCP range for the quarantine level so that the member DHCP server can assign IP addresses within that range to unauthenticated DHCP clients. An unauthenticated client is allowed to access the captive portal only and must successfully pass the authentication process before it can receive an IP address from the authenticated range.

Note: Infoblox recommends 30-second leases for addresses in the quarantine DHCP range. This provides enough time for the user authentication process, so when the client attempts to renew the lease at the midpoint of its lease time, the member can then assign the client a new IP address, depending on the result of the authentication process. Here is a screenshot of that configuration:



128.1.1.10 - 128.1.1.100 (IPv4 Range)

Lease Time: 30 Seconds

□ Unlimited Lease Time

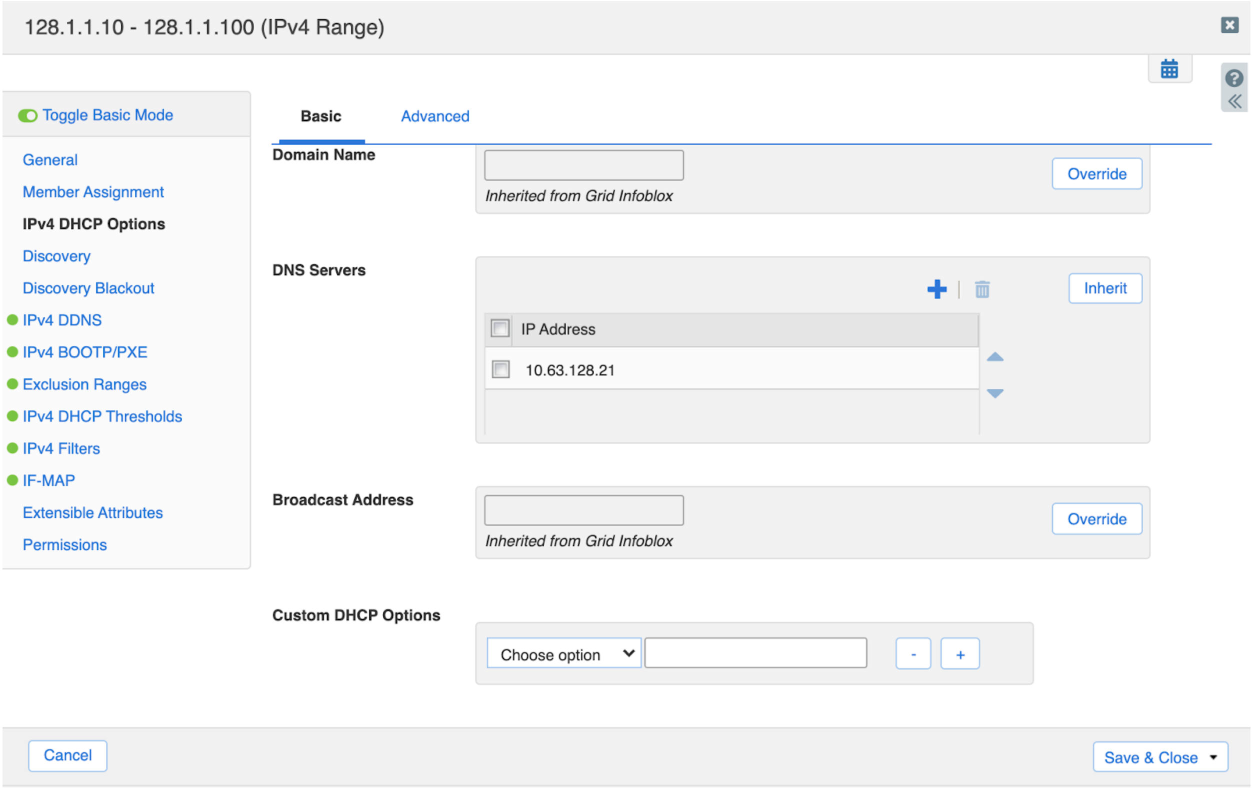
Inadvertently selecting the Unlimited Lease Time check box or using this option incorrectly could cause a serious network outage in the future when all available leases are allocated

Routers

IP Address
128.1.1.1

Domain Name: Inherited from Grid Infoblox

When you configure the quarantine DHCP range, you must specify the captive portal IP address as the DNS server for the address range. The captive portal runs a limited DNS server that resolves all queries with the IP address assigned to the web interface on the captive portal. Here is a screenshot of that configuration:



128.1.1.10 - 128.1.1.100 (IPv4 Range)

Domain Name: (empty) — Inherited from Grid Infoblox

DNS Servers:

□ IP Address
□ 10.63.128.21

Broadcast Address: (empty) — Inherited from Grid Infoblox

Custom DHCP Options: Choose option

Note that you can run the Captive Portal wizard to automatically set the lease time of the quarantine range to 30 seconds and to add the captive portal IP address as the DNS server. Alternatively, you can set the lease time and the DNS server IP address in the DHCP tab of the DHCP Range editor.

To ensure that clients can reach the captive portal, you must specify a route to the captive portal. On a network where all systems can reach each other without going through a router, that is, all IP addresses are on the same subnet, you must configure Option 33 for the quarantine DHCP range. This option specifies a list of static routes that the client should install in its routing cache. The routes consist of a list of IP address pairs. For clients to reach the captive portal, specify the portal IP address first (destination address), and the LAN address of the NIOS appliance second. When the appliance assigns an IP address from the quarantine DHCP range, it also includes the static route that you specified in option 33. On a routed network, you must configure a default route via the router on the subnet. See the above screenshot.

Authenticated DHCP Range

Configure a DHCP range for authenticated users if you want the Grid member to assign IP addresses within that range to authenticated DHCP clients. Users that receive an IP address in this range typically are allowed full access to the network.

When a client successfully passes authentication, the member automatically stores its MAC address in the corresponding MAC address filter. When the client attempts to renew the lease at the midpoint of its lease time, the member matches the source MAC address in the request with a MAC address in the filter for the authenticated DHCP address range. The member then assigns the client a new IP address from the authenticated DHCP range.

Guest DHCP Range.

Configure a guest DHCP range if you want the client to be assigned an IP address from a different DHCP range such as one which may have limited/restricted access on your network. You can configure and customize a guest registration page when you configure the captive portal.

Defining MAC Address Filters

After you configure the network and DHCP ranges, you must then configure the MAC address filters and add them to the appropriate DHCP ranges. If you configured DHCP ranges for authenticated and guest users, you must configure MAC address filters for each range with an action of Allow. You must also add those filters to the quarantine range with an action of Deny, to ensure that the member does not allocate an address from the quarantine range to a host whose MAC address matches an entry in the MAC filters for the authenticated and guest DHCP ranges.

When you create the filters, you also specify whether the MAC address entries expire. The member automatically deletes expired MAC address entries from the filter. If a client that registered earlier attempts to renew its IP address or to register after its MAC address has expired, it is redirected to the captive portal because its MAC address is no longer in the filter.

Configuring in the Captive Portal Wizard

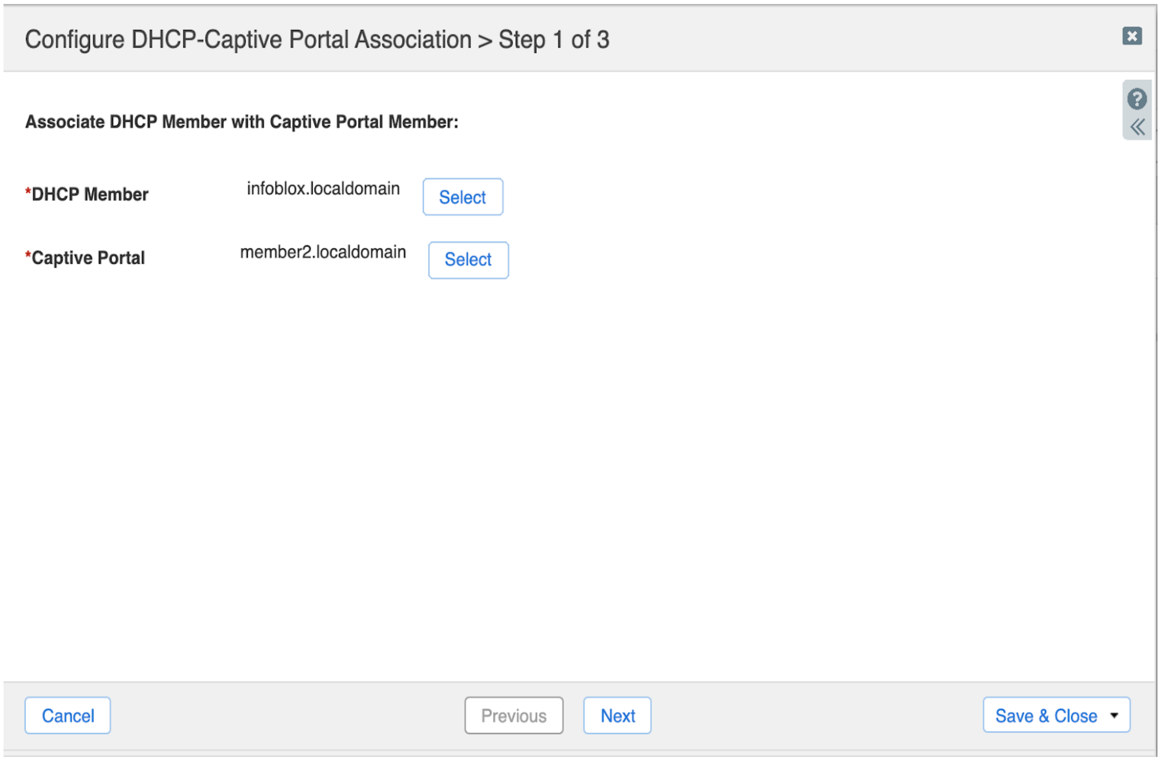
After you configure the captive portal and the DHCP ranges for each access level, you can use the Captive Portal wizard to accomplish the following tasks:

- Associate the captive portal member with the member that serves the DHCP ranges you configured.
- Create MAC address filters and add them to the appropriate DHCP ranges. The wizard allows you to create MAC address filters for the quarantine DHCP range, and for the authenticated and guest DHCP ranges, depending on whether the captive portal is used to register users for authentication, guests, or both. For example, if you indicated that the captive portal is used for authenticated users only, then the wizard allows you to create a MAC filter for the authenticated DHCP range only.
    - If the captive portal is used to register users for authentication, the wizard allows you to create a MAC address filter for the authenticated range. The wizard then automatically adds the filter to the authenticated DHCP range with an action of Allow. It also adds the filter to the quarantine range with an action of Deny. This ensures that the member does not allocate an address from the quarantine range to a host whose MAC address matches an entry in the MAC filter.
    - If the captive portal is used to register guest users, the wizard allows you to create a MAC address filter for the guest DHCP range. The wizard then automatically adds the filter to the guest DHCP range with an action of Allow. It also adds the filter to the quarantine range with an action of Deny. This ensures that the member does not allocate an address from the quarantine range to a host whose MAC address matches an entry in the MAC filter.
- Add the captive portal IP address as the DNS server for the quarantine address range.
- Set the lease time of the quarantine range to 30 seconds.

To use the Captive Portal wizard to complete the tasks for the DHCP authentication feature:

1. From the Data Management tab, select the DHCP tab, or from the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and click Configure Captive Portal.

3. In the Captive Portal wizard, complete the following and click Next:



Configure DHCP-Captive Portal Association > Step 1 of 3

Associate DHCP Member with Captive Portal Member:

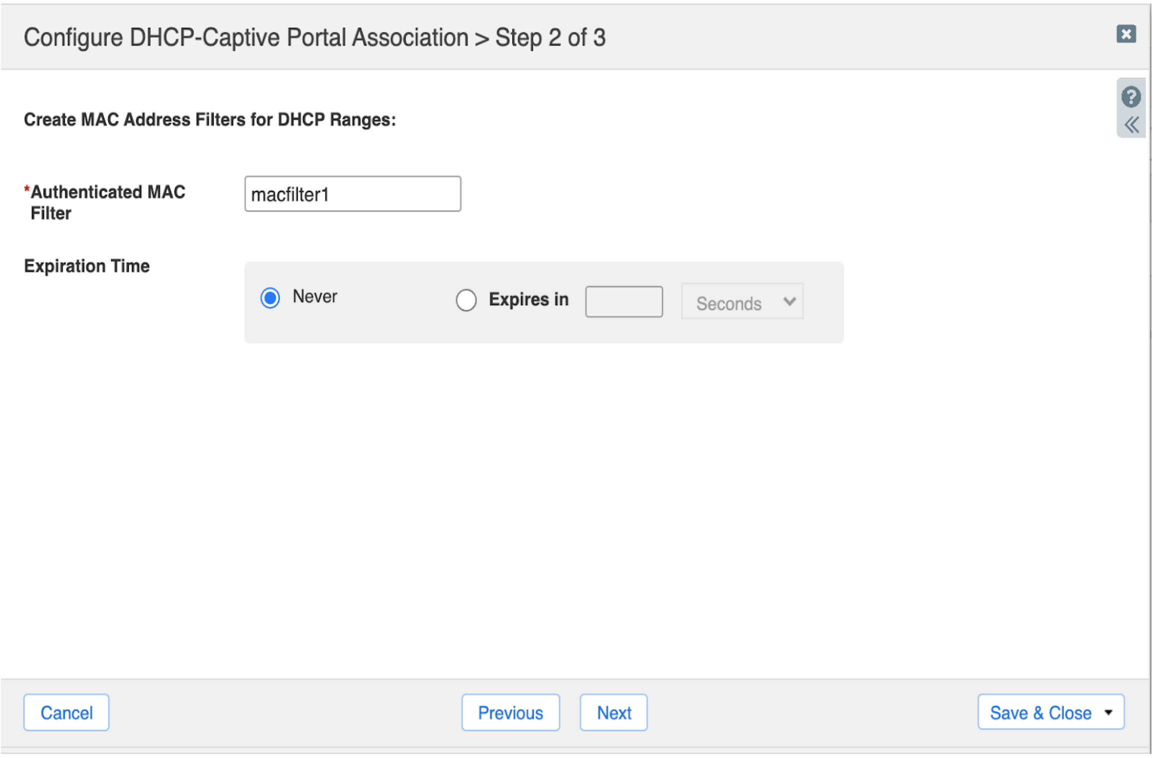
*DHCP Member infoblox.localdomain

*Captive Portal member2.localdomain

   a. Member DHCP: Select the member DHCP server that uses this captive portal to authenticate users.
   b. Captive Portal: Select the member that runs the captive portal. Note that the member that runs the captive portal cannot run any other service, such as DHCP or DNS, and cannot be the Grid Master or Grid Master candidate.

4. This panel allows you to create MAC address filters for the authenticated and guest DHCP ranges. The MAC filters you can create depend on your entry in the Captive Portal properties of the Grid member. For example, if you indicated that the captive portal is used for authenticated users only, then this panel allows you to create a MAC address filter for the authenticated DHCP range only. You can also specify existing MAC filters, if you want to apply them to the

authenticated and guest DHCP ranges. Complete the following and click Next:



Configure DHCP-Captive Portal Association > Step 2 of 3

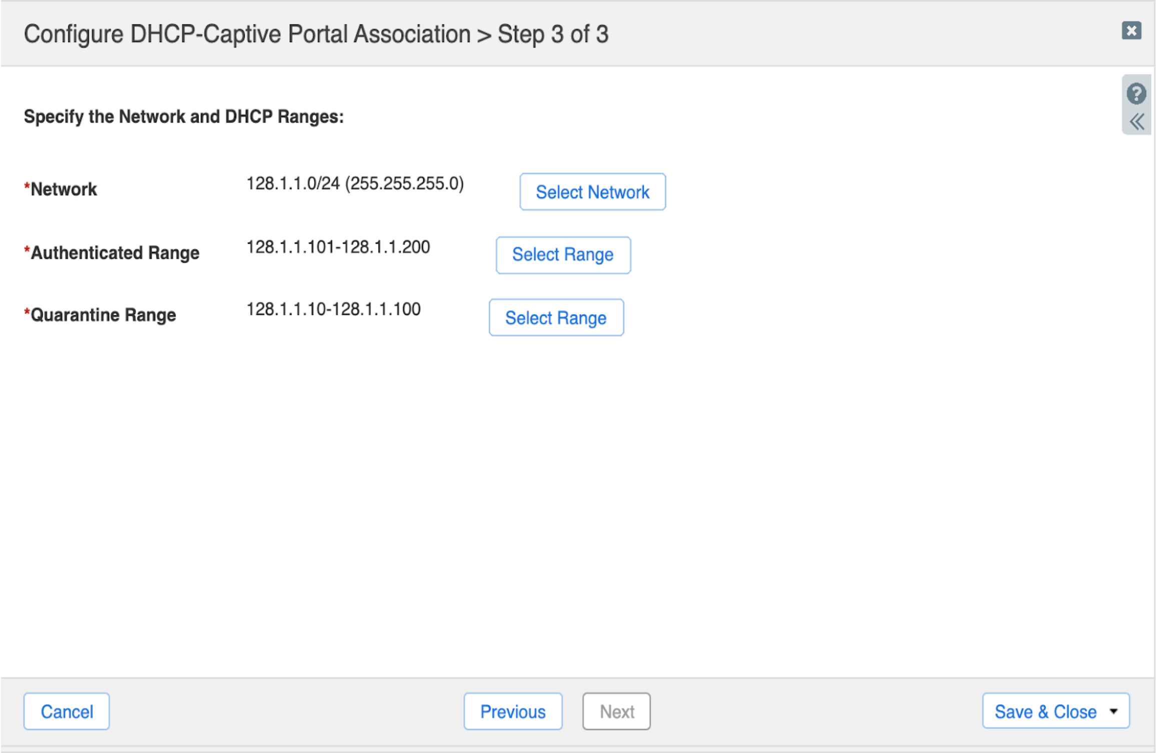
Create MAC Address Filters for DHCP Ranges:

*Authenticated MAC Filter: macfilter1

Expiration Time: ● Never ○ Expires in [ ] Seconds

a. Authenticated MAC Filter: Specify a name for the MAC filter that is used for authenticated users.
b. Expiration Time: Specify how long a MAC address is stored in the MAC address filter for authenticated users.
    i. Never: Select this option to store MAC addresses in the MAC address filter until they are manually removed.
    ii. Expires in: Select this option to store MAC addresses in the MAC address filter for the specified period of time.
c. Guest MAC Filter: Specify a name for the MAC filter that is used for guest users. NOTE: This field will only appear if you have configured the Captive Portal User Types to either Guest only or Both (i.e. Authenticated and Guest).
d. Expiration Time: Specify how long a MAC address is stored in the MAC address filter for guest users.
    i. Never: Select this option to store MAC addresses in the MAC address filter until they are manually removed.
    ii. Expires in: Select this option to store MAC addresses in the MAC address filter for the specified period of time.

5. In this panel, you specify the network and address ranges, so that the wizard can apply the MAC address filters to the appropriate ranges. Complete the following:



Configure DHCP-Captive Portal Association > Step 3 of 3

Specify the Network and DHCP Ranges:

*Network	128.1.1.0/24 (255.255.255.0)	Select Network
*Authenticated Range	128.1.1.101-128.1.1.200	Select Range
*Quarantine Range	128.1.1.10-128.1.1.100	Select Range

a. Network: Select the network that uses DHCP authentication.
b. Authenticated Range: Select the IP address range that the appliance uses for authenticated users. The wizard applies the authenticated MAC address filter you specified in the preceding step to this DHCP range with an action of Allow. This effectively allows the member to assign an IP address from the address range to a requesting host whose MAC address matches the MAC address in the filter.
c. Quarantine Range: Select the IP address range that the appliance uses for quarantined addresses. The wizard applies the authenticated and guest MAC address filters to the quarantine DHCP range with an action of Deny. This effectively denies an address request from a host whose MAC address matches an entry in the MAC filters for the authenticated and guest DHCP ranges.

6. Save the configuration and click Restart if it appears at the top of the screen.

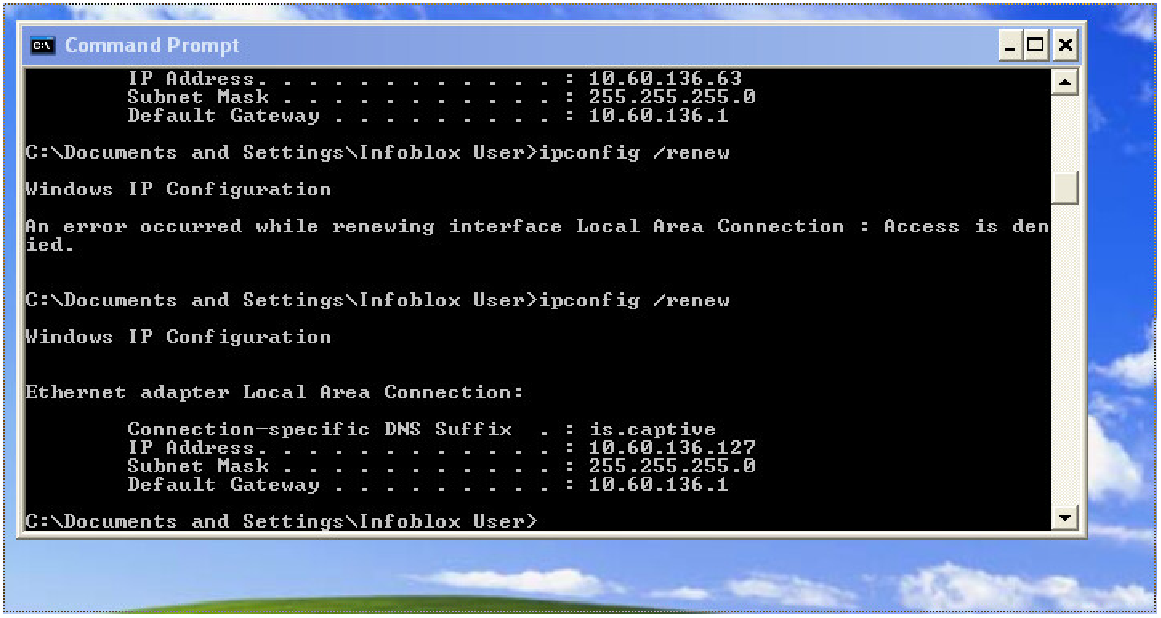
Demonstration of Captive Portal

Configuration of the DHCP ranges

- Quarantine Range: 10.60.136.96-10.60.136.127
- Authenticated Range: 10.60.136.32-10.60.136.63

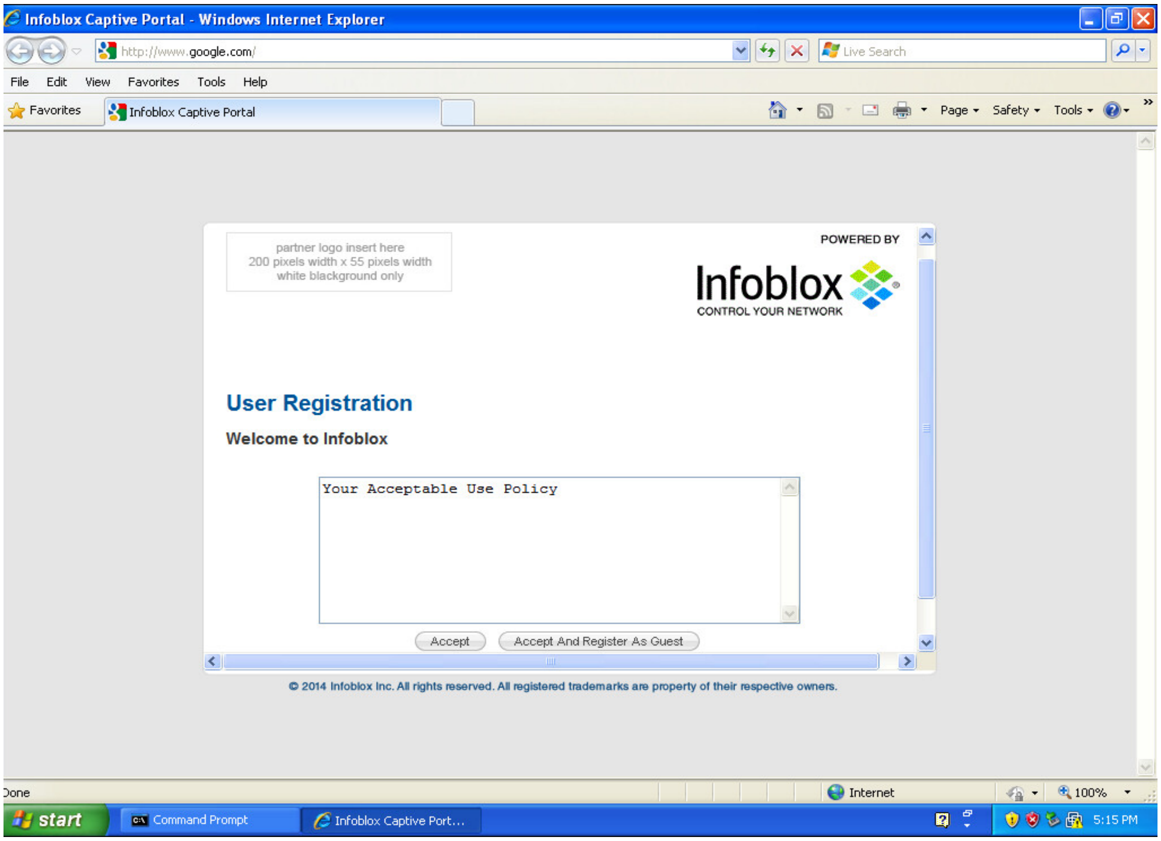
The following screen shots will show captive portal at work.

1. Below is a PC that just booted up and you see the IP address being in the quarantined range.



```
        IP Address. . . . . . . . . . . . : 10.60.136.63
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.60.136.1

C:\Documents and Settings\Infoblox User>ipconfig /renew

Windows IP Configuration

An error occurred while renewing interface Local Area Connection : Access is den
ied.

C:\Documents and Settings\Infoblox User>ipconfig /renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : is.captive
        IP Address. . . . . . . . . . . . : 10.60.136.127
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.60.136.1

C:\Documents and Settings\Infoblox User>
```

2. Below is the PC screen when an internet browser is started up.



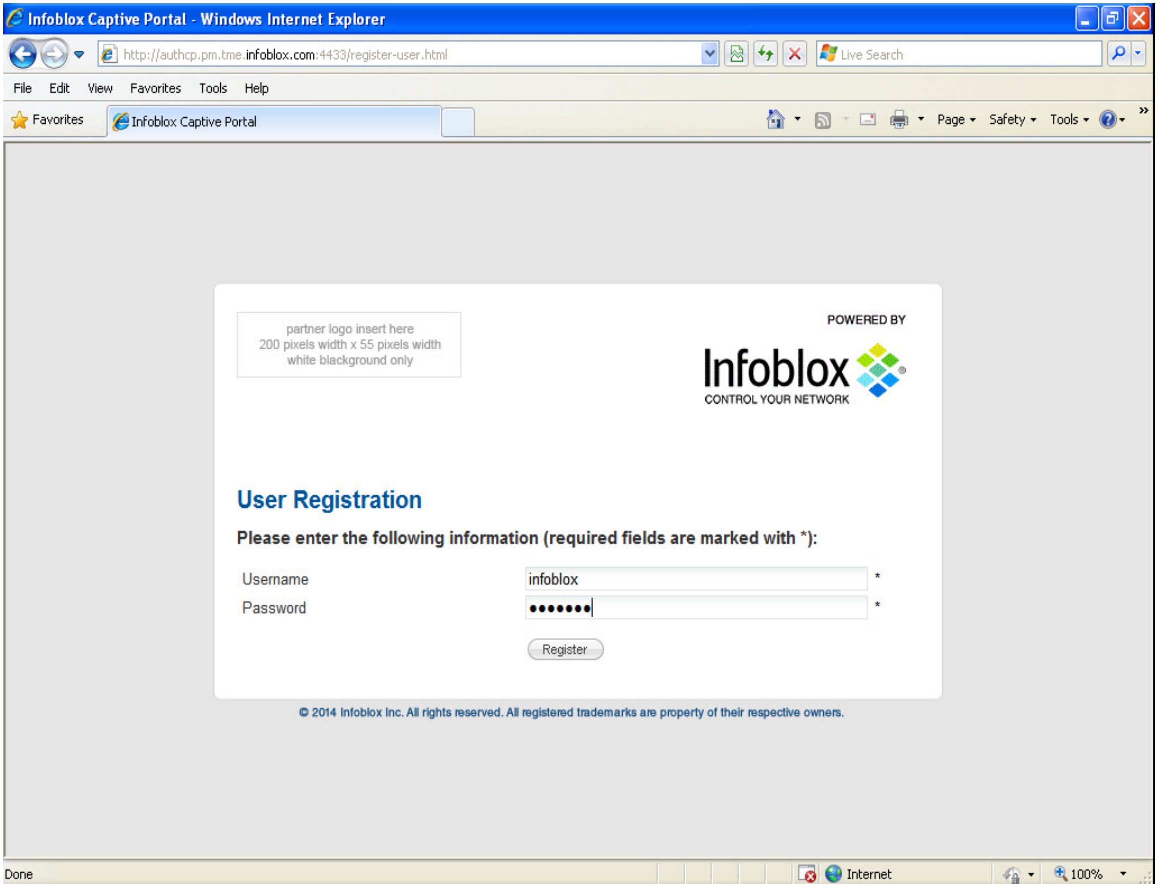
User Registration

Welcome to Infoblox

```
Your Acceptable Use Policy
```

© 2014 Infoblox Inc. All rights reserved. All registered trademarks are property of their respective owners.

3. Click on the Accept button to accept the policy and then register with username and password.



Infoblox Captive Portal - Windows Internet Explorer
http://authcp.pm.tme.infoblox.com:4433/register-user.html
Live Search
File Edit View Favorites Tools Help
Favorites
Infoblox Captive Portal
Page Safety Tools
partner logo insert here
200 pixels width x 55 pixels width
white blackground only
POWERED BY
Infoblox
CONTROL YOUR NETWORK

User Registration

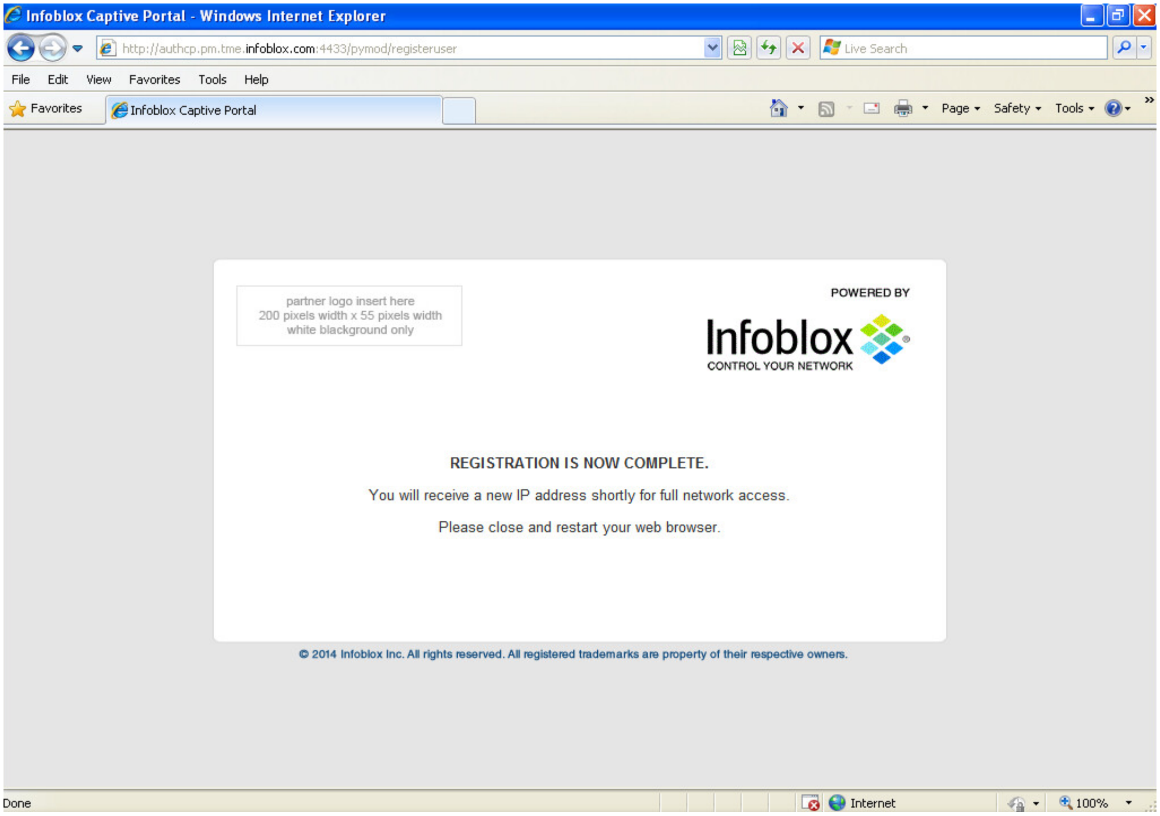
Please enter the following information (required fields are marked with *):

Username infoblox *

Password ••••••• *

Register
© 2014 Infoblox Inc. All rights reserved. All registered trademarks are property of their respective owners.
Done
Internet
100%

4. Click on the Register button and the following screen appears.



Infoblox Captive Portal - Windows Internet Explorer
http://authcp.pm.tme.infoblox.com:4433/pymod/registeruser
Live Search
File Edit View Favorites Tools Help
Favorites
Infoblox Captive Portal
Page Safety Tools
partner logo insert here
200 pixels width x 55 pixels width
white blackground only
POWERED BY
Infoblox
CONTROL YOUR NETWORK
Done
Internet
100%

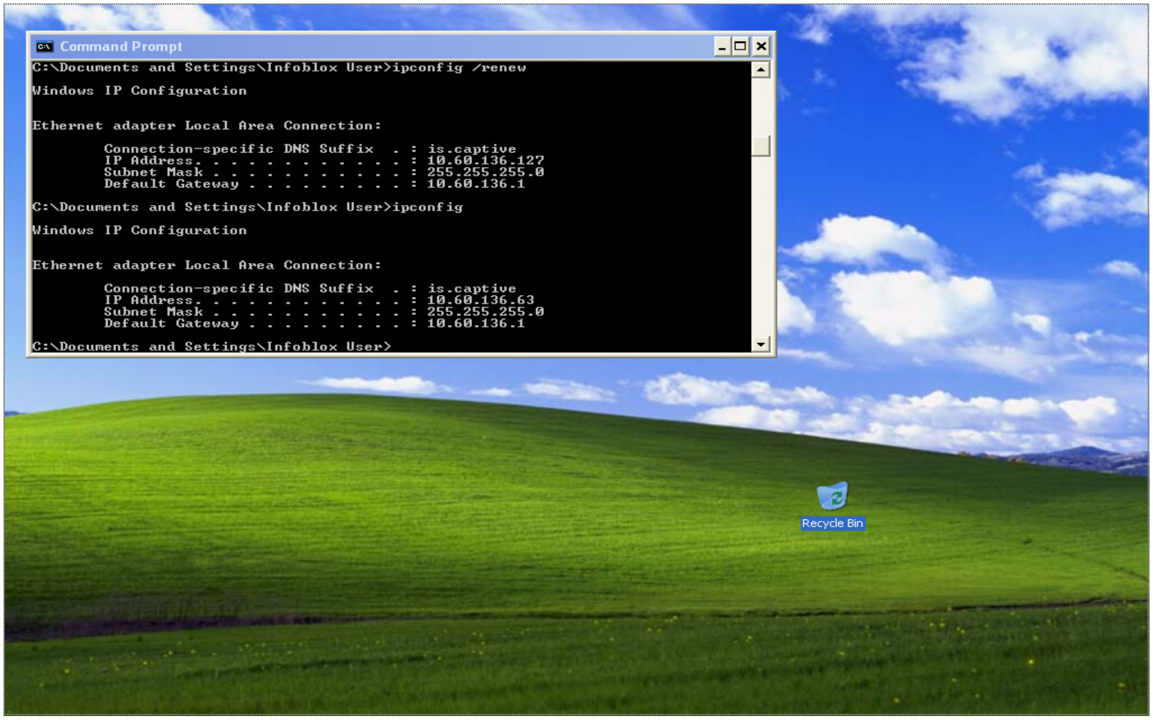
REGISTRATION IS NOW COMPLETE.

You will receive a new IP address shortly for full network access.

Please close and restart your web browser.

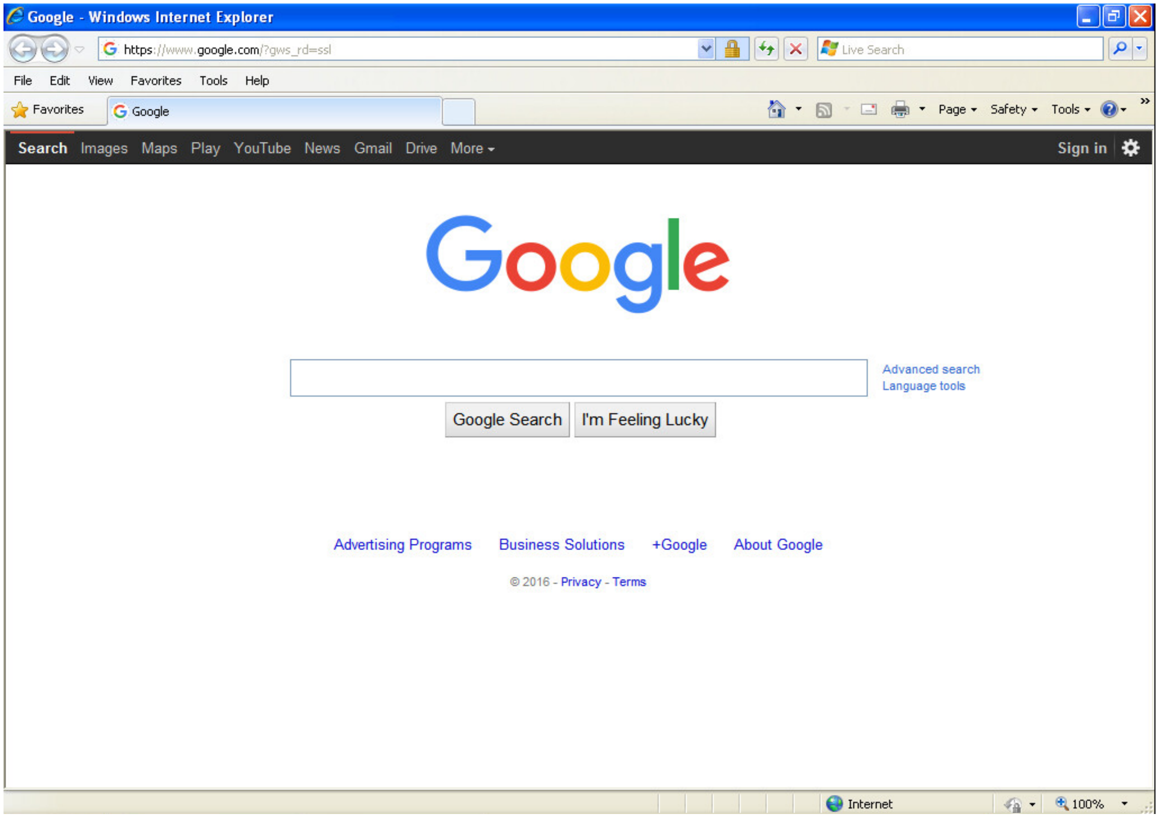
© 2014 Infoblox Inc. All rights reserved. All registered trademarks are property of their respective owners.

5. Check the IP configuration to verify you are now on the authenticated DHCP IP range.



```
C:\Documents and Settings\Infoblox User>ipconfig /renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : is.captive
        IP Address. . . . . . . . . . . . : 10.60.136.127
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.60.136.1

C:\Documents and Settings\Infoblox User>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : is.captive
        IP Address. . . . . . . . . . . . : 10.60.136.63
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.60.136.1

C:\Documents and Settings\Infoblox User>
```

6. Startup your internet browser.



Monitoring DHCP Authentication

You can monitor the captive portal service on the Dashboard by checking the status on the Grid Status and Member Status widget.

More specifically, you can also view the MAC addresses that are in the MAC address filters for the authenticated, guest, and quarantine range.

Viewing the DHCP Ranges and Filters

To view the newly created MAC address filters:

1. Navigate to Data Management   DHCP   IPv4 Filters. Grid Manager lists all the configured filters.
2. You can select a filter and view or configure its properties, such as extensible attributes.

To view the DHCP ranges and the newly added filters:

1. Navigate to Data Management   DHCP   Networks tab   Networks section   network .
2. Select the DHCP range you want to view and click the Edit icon.
3. If the editor is in Basic mode, click Toggle Advanced Mode.
4. Click the Filters tab to view the filters.

To verify that the captive portal is the DNS server in the quarantine range:

1. Navigate to Data Management   DHCP   Networks   Networks section   network.
2. Select the quarantine DHCP range and click the Edit icon.
3. In the DHCP Range editor, click the IPv4 DHCP Options tab. The captive portal IP address is listed in the DNS Servers table.

Use Cases

Infoblox's Captive Portal can be used to:

- Authenticate regular users
- Authenticate guest users

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com