

NOTE: The configuration steps listed below assume the ACS is already setup for use with Active Directory, and provides either Read-Write or Read-Only authorization based on the account used.

- An Identity Search Sequence named "User Search Sequence" has been configured to check Active Directory first, then check the local ACS user list for valid accounts.
- Two ACS Identity Groups have been configured, one for ReadWrite permissions named "Network Admin", and another for ReadOnly permissions named "Read-Only".
 - Active Directory and local ACS user account are assigned to one of the Identity Groups depending on their required level of access to enterprise network devices.

Configure the PacketShaper

1. Login to the BlueCoat PacketShaper webGUI

- Open a web browser and navigate to the <https://> address of the PacketShaper.
 - Leave the username field blank, and enter only the admin password in the password box.
 - This grants 'touch' (read-write) access to the PacketShaper
- At the top right side of the screen, click the [Legacy UI](#) link to configure the device.
- Select the [Setup](#) tab near the top center of the screen.

2. Select RADIUS client from the Choose Setup Page: drop-down box.

- Configure the RADIUS client settings as follows, enabling both **Authentication** and **Accounting**, and using the correct **Authentication method**, **Authentication Host** (ACS IP address), and **Shared Secret**:

Top Ten Monitor Manage Report Xpress Setup Info

SETUP

Choose Setup Page: RADIUS client

RADIUS Client settings

apply changes ... reset form

RADIUS Authentication will be used if **Authentication** is turned on *and* an **Authentication Host** is entered.
RADIUS Accounting will be used if **Accounting** is turned on *and* an **Accounting Host** is entered.

Authentication: on
Authentication method: MSCHAP
Primary Authentication Host: 192.168.1.100 **Port:** 1812 **Shared Secret:** CiscoACsv5
Secondary Authentication Host: **Port:** *default: 1812* **Shared Secret:**

Accounting: on
Primary Accounting Host: 192.168.1.100 **Port:** 1813 **Shared Secret:** CiscoACsv5
Secondary Accounting Host: **Port:** *default: 1813* **Shared Secret:**

Retry limit: 3
Retry interval (seconds): 5

- Click the [apply changes ...](#) button.

3. Click the [LOG OUT](#) link at the top right of the page.

Configure the Cisco ACS v5.x (GUI)

1. Login to the Cisco ACS web GUI
2. Navigate to **System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA**
 - a. **Create the BlueCoat Vendor**
 - i. Click the **Create** button at the bottom of the page and use the following information:

System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA >

Name: BlueCoat
Description: Vendor-Specific Attributes for PacketShaper
Vendor ID: 2334
Attribute Prefix: Packeteer-

▶ Use Advanced Vendor Options

⚙ = Required fields

Click the **Submit** button at the bottom of the page

3. Navigate to **System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA > BlueCoat**
 - a. **Create the required custom attribute for ACS permissions**
 - i. Click the **Create** button at the bottom of the page and use the following information:

System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA > BlueCoat >

General

Attribute: Packeteer-AVPair
Description: Used to specify access level

RADIUS Configuration

Vendor Attribute ID: 1
Direction: OUTBOUND
Multiple Allowed: False
 include attribute in log

Attribute Type

Attribute Type: String

⚙ = Required fields

Click the **Submit** button at the bottom of the page

4. **Navigate to Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**a. **Create the BlueCoat Read-Write authorization profile**i. Click the **Create** button at the bottom of the page

- Select the **General tab**

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles >

General Common Tasks RADIUS Attributes

Name: BlueCoat-RW

Description: BlueCoat Read-Write Authorization

= Required fields

- Select the **RADIUS Attributes tab**

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles >

General Common Tasks **RADIUS Attributes**

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value

Add ^ Edit V Replace ^ Delete

Dictionary Type: RADIUS-BlueCoat

RADIUS Attribute: Packeteer-AVPair Select

Attribute Type: String

Attribute Value: Static

access=touch

= Required fields

Click the **Add ^** button above the Attribute fieldii. Click the **Submit** button at the bottom of the page

b. **Create the BlueCoat Read-Only authorization profile**i. Click the **Create** button at the bottom of the page

- Select the **General** tab

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles >

General Common Tasks RADIUS Attributes

Name: BlueCoat-RO

Description: BlueCoat Read-Only Authorization

= Required fields

- Select the **RADIUS Attributes** tab

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles >

General Common Tasks RADIUS Attributes

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value

Add ^ Edit V Replace ^ Delete

Dictionary Type: RADIUS-BlueCoat

RADIUS Attribute: Packeteer-AVPair

Attribute Type: String

Attribute Value: Static

access=look

= Required fields

Click the **Add ^** button above the Attribute fieldii. Click the **Submit** button at the bottom of the page

5. **Navigate to Access Policies > Access Services > Service Selection Rules**a. **Filter by Device IP Address**

- i. Click the **Customize** button at the bottom right of the page and set the following:

Click **OK**

b. **Create the BlueCoat RADIUS rule**

- i. Click the **Create** button at the bottom of the page and set the following, using the correct **BlueCoat IP** :

Click the **OK** button at the bottom of the page

- c. Check the box next to the **BlueCoat** service selection policy, then use the **▲** button near the bottom of the page to move the policy to position #1 (top) in the list.
- d. Click the **Save Changes** button at the bottom of the page

6. **Navigate to Access Policies > Access Services > Default Network Access**a. **Configure Group Mapping for the policy**

- i. Select the **General** tab
 - Check the box next to Group Mapping (Applies to Active Directory configurations)

Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"

General Allowed Protocols

General

Name: Default Network Access

Description: Default Network Access Service

Service Type: Network Access

Policy Structure

Identity

Group Mapping

Authorization

- ii. Select the **Allowed Protocols** tab and check the following boxes:

Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"

General **Allowed Protocols**

Process Host Lookup

Authentication Protocols

Allow PAP/ASCII

Allow CHAP

Allow MS-CHAPv1

Allow MS-CHAPv2

- Click **Submit**

7. **Navigate to Access Policies > Access Services > Default Network Access > Identity**a. **Set the ACS to authenticate using the User Search Sequence (Active Directory and Local Users)**

- i. Ensure the radio button next to **Single result selection** is selected, then set to whatever Identity Source you are currently using. In this example, we have setup an Identity Store Sequence that checks Active Directory and local ACS user accounts, and have named it "User Search Sequence" :

Access Policies > Access Services > Default Network Access > Identity

Single result selection Rule based result selection

Identity Source: **User Search Sequence** **Select**

▶ Advanced Options

- ii. Click the **Save Changes** button at the bottom of the page

NOTE: This section only applies if you use Active Directory integration:

8. **Navigate to Access Policies > Access Services > Default Device Admin > Group Mapping**

- a. Select the radio button for **Rule based result selection**, and click **OK** on the pop-up dialog box.

b. **Create the Read-Write Rule**

- i. Click the **Create** button at the bottom of the page

- Under **General**, name the new rule **Read-Write**, and ensure it is Enabled
- Under **Conditions**, check the box next to **Compound Condition**, then set **Dictionary: AD-AD1**, **Attribute: ExternalGroups**, and **Value: <Active Directory Domain>/ReadWrite** group as shown:

- Click **Add V** to add the condition to the **Current Condition Set**
- Under **Results**, set the **Identity Group** field to the **All Groups: Network Admin** group

5. Click the **OK** button at the bottom of the page

c. **Create the Read-Only Rule**

- i. Click the **Create** button at the bottom of the page and repeat the steps with the highlighted changes:

- Under **General**, name the new rule **Read-Only**, and ensure it is Enabled
- Under **Conditions**, check the box next to **Compound Condition**, then set **Dictionary: AD-AD1**, **Attribute: ExternalGroups**, and **Value: <Active Directory Domain>/ReadOnly** group:
- Click **Add V** to add the condition to the **Current Condition Set**
- Under **Results**, set the **Identity Group** field to the **All Groups: Read-Only** group
- Click the **OK** button at the bottom of the page

- d. Click the **Save Changes** button

9. **Navigate to Access Policies > Access Services > Default Network Access > Authorization**a. **Use Identity Groups**

- i. Click the **Customize** button at the bottom right of the page
 - Under **Customize Conditions**, select **Identity Group** from the left window, click the **>** button to add it, then click the **OK** button to close the window

b. **Create the BlueCoat-RW Authorization Rule**

- i. Click the **Create** button at the bottom of the page
 - Under **General**, name the new rule **BlueCoat-RW**, and ensure it is Enabled
 - Under **Conditions**, check the box next to **Identity Group**, and set it to **All Groups: Network Admin**
 - Under **Results**, set the **Authorization Profile** to **BlueCoat-RW**

General
Name: **BlueCoat-RW** Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions
 Identity Group: in All Groups: Network Admin Select

Results
Authorization Profiles:
BlueCoat-RW
Select Deselect

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

- Click the **OK** button at the bottom of the page to close the window

c. **Create the BlueCoat-RO Authorization Rule**

- i. Click the **Create** button at the bottom of the page and repeat the steps with the highlighted changes:
 - Under **General**, name the new rule **BlueCoat-RO**, and ensure it is Enabled
 - Under **Conditions**, check the box next to **Identity Group**, and set it to **All Groups: Read-Only**
 - Under **Results**, set the **Authorization Profile** to **BlueCoat-RO**
 - Click the **OK** button at the bottom of the page to close the window

- d. Verify that both rules are listed before the 'Default' rule at the bottom, then click **Save Changes**

10. **Verify successful configuration by logging into the BlueCoat web GUI using an Active Directory account.**