Hewlett Packard Enterprise

04-Nov-25

Central Policy Configuration

Policies in HPE Aruba Networking Central define an organization's intent for how users and devices interact with network resources. This chapter introduces the policy framework in Central, explains the relationship between policies and roles, and demonstrates how policies are created and applied. It concludes with examples of policies used in bridged WLAN, tunneled WLAN, and User-Based Tunneling (UBT) environments.

▼ Table of contents

Feedback

Introduction

This chapter explains Central's intent-based policy framework, including available security policies, policy structure, and enforcement using roles, match criteria, and permit/deny actions.

This new approach is compared to Classic Central, where roles directly define policy behavior. The examples provided illustrate how policies are used in wireless bridged and tunneled WLANs, as well as in wired UBT environments.

Central Policy Framework

Understanding Policies, Rules, and Roles

In Central, a policy defines an organization's intent for network reachability between roles, resources, and applications. Policies capture this intent in a structured manner, describing who should have access to which resources, and under what conditions. Central's policy definition is abstracted from any device-specific configuration, so an individual policy can be applied to multiple device types. Central then translates the policy intent into device-specific configuration.

> **Note:** Some policy components cannot be applied to all device types, as described in the Network Device Considerations section.

Policies are composed of rules, which define the action a device should take for specified traffic, such as allow, deny, or prioritize. Rules use match criteria such as role, application, service, or protocol/port to identify traffic sources and destinations.

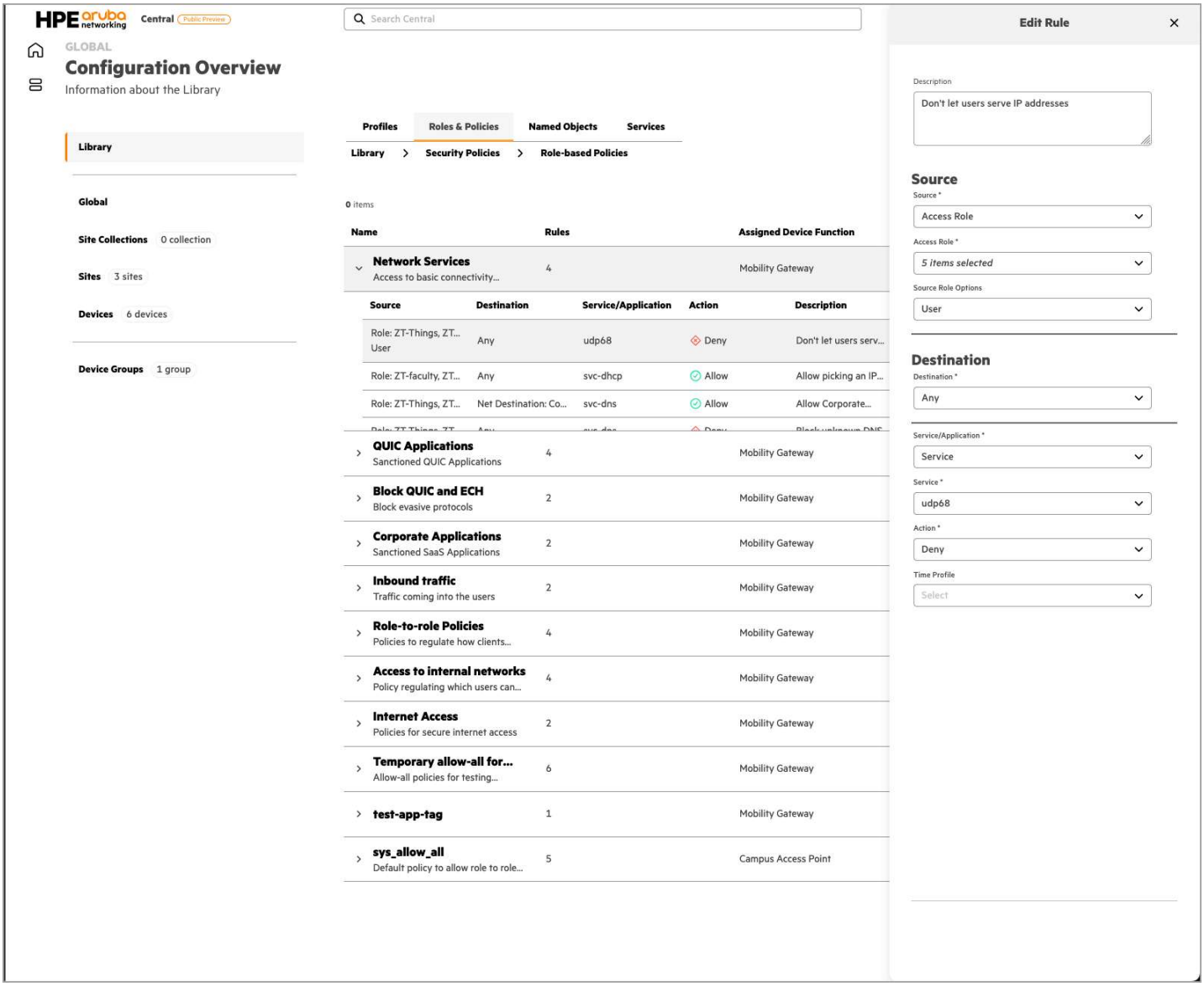
Roles represent network identities such as employees, contractors, IoT devices, or guests. Roles are referenced within a policy to define how each identity interacts within the policy's intent domain. The ability to reference multiple roles in a single policy, or even a single rule, allows simplified and flexible management of network behavior, ensuring consistency and scalability across all users and devices.

For example, a policy named "Allow Internal Access" might define how different roles can reach corporate networks:

- Employees may have full access.
- Contractors may have limited access to specific subnets or applications.
- Guests may be denied access entirely.

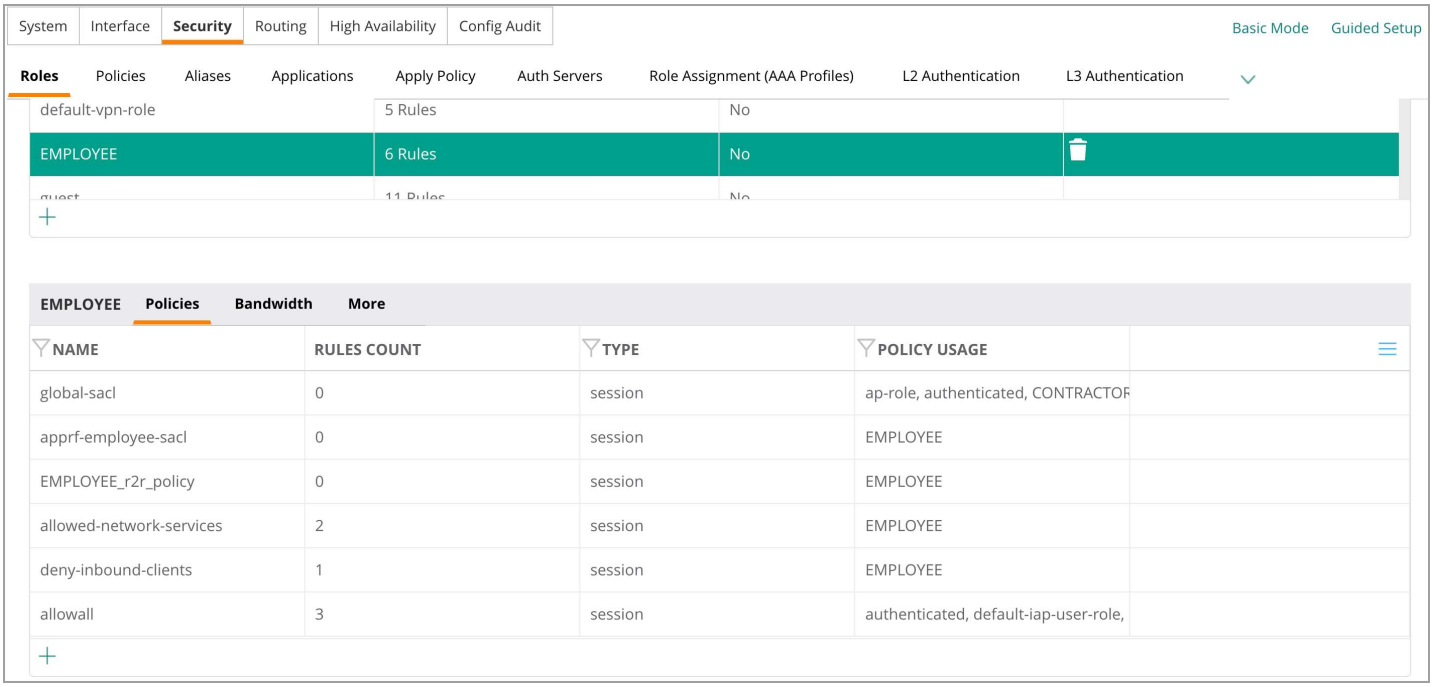
The figure below shows an example of a comprehensive policy library. The policy library contains multiple policies, each composed of rules that may reference different roles. These policies are then applied to various scopes (such as Sites or Site Collections) and device functions (such as gateways, access points, or switches) to enforce the intended behavior at the appropriate point in the network.

This framework enables network operators to maintain a unified, intent-based view of access control across the organization. Policies can be modified, reused, and applied easily and consistently where needed.



Comparison to Classic Central

In Classic Central, the role was the primary configuration object. Each role contained its own ACLs and permissions, creating a tight coupling between the identity and its access rules. This meant every new role required its own ACL set, even when multiple roles shared similar access behavior.



In the new model, policies are intent-based and can reference multiple roles within them. The administrator defines intent once, such as internal access or guest Internet access, and maps roles to that intent with the appropriate access level.

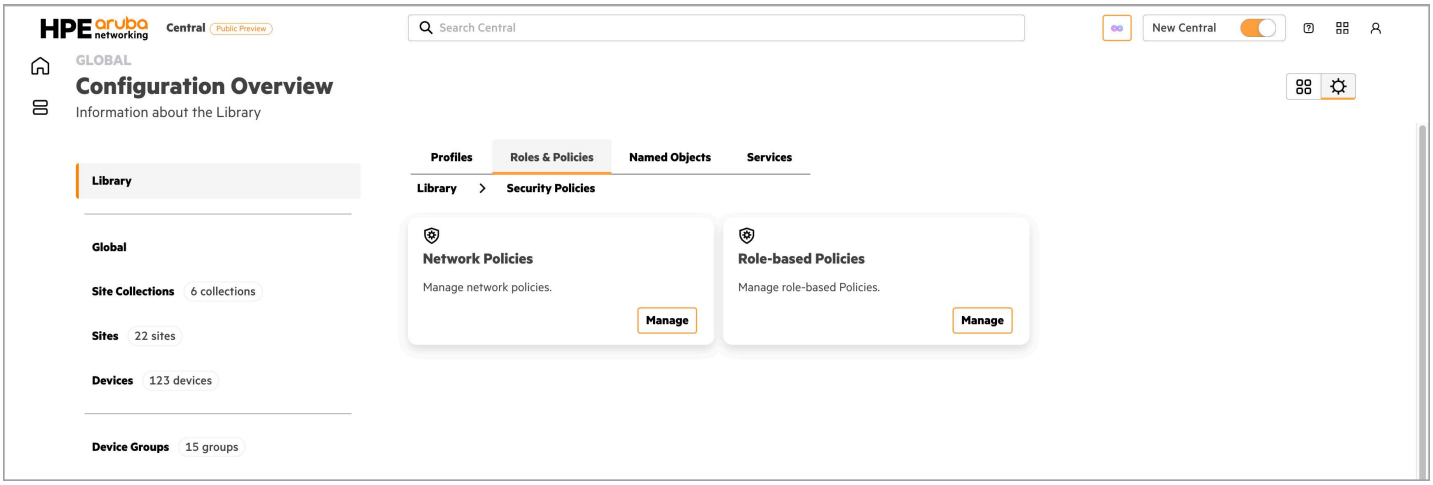
This change offers several points of differentiation:

Aspect	Classic Central	Central (Intent-Based Model)
Configuration model	Role-centric. Each role includes its own ACLs and rules.	Policy-centric. Each policy defines an intent domain and references roles within it.
Example	Create an *Employee* role and define ACLs for internal access directly within that role.	Create an *Internal Access* policy and reference *Employee*, *Contractor*, *Guest*, and *IoT* roles with different access outcomes.
Scope and reuse	Rules are repeated across multiple roles that share similar access needs.	A single policy describes shared intent for all roles, avoiding duplication.
Change management	Modifying a rule requires editing each role individually.	Updating a policy automatically affects all roles that reference it.
Conceptual model	Identity first: ACLs define behavior within the role.	Intent first: roles define to whom the intent applies.
Visibility	Rules are distributed across multiple roles.	Policies consolidate intent and simplify troubleshooting.

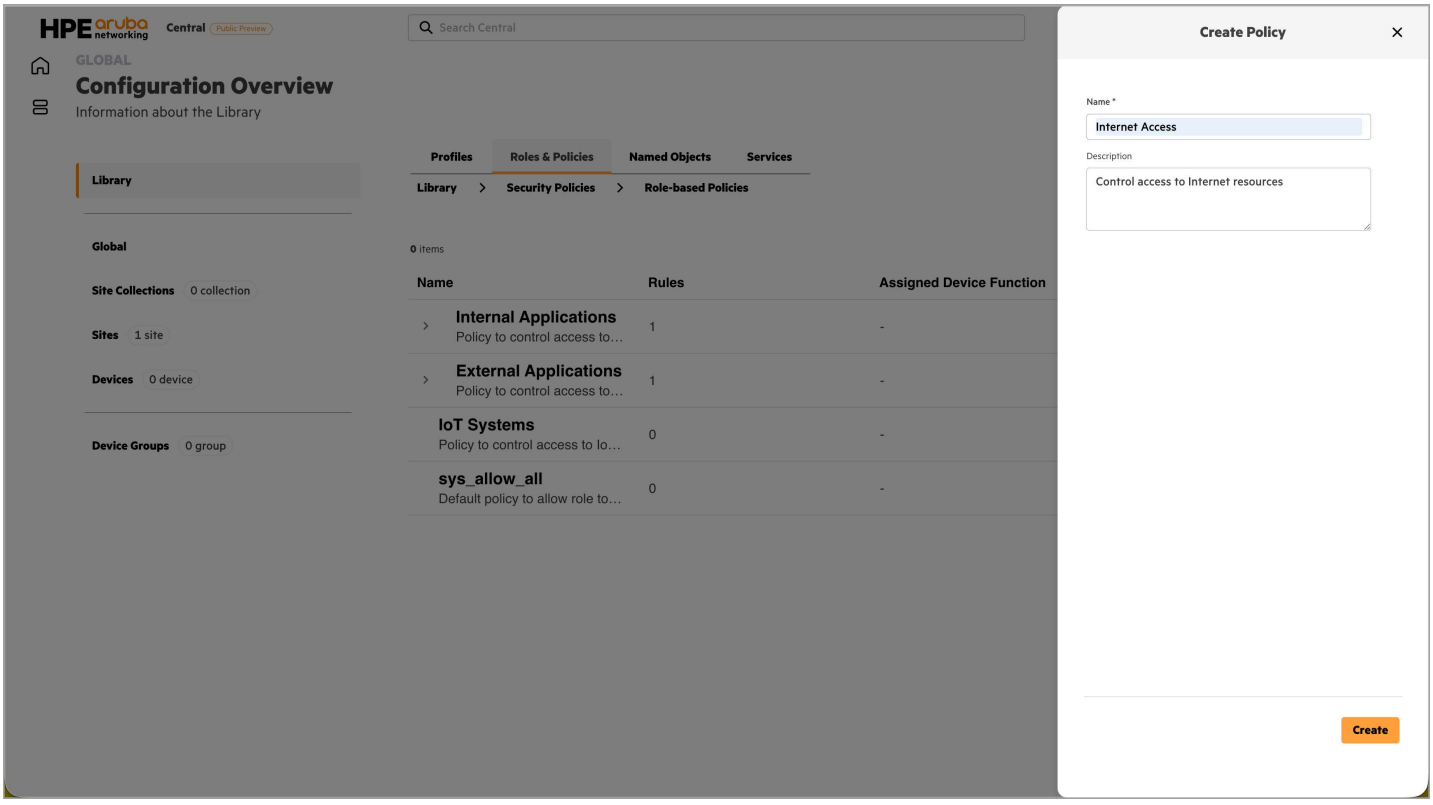
Constructing a Policy

Policies in Central fall into two major categories:

- **Network-based policies** operate as traditional access lists. They are typically applied to VLAN interfaces on switches.
- **Role-based policies** define intent for specific user or device roles. They are applied across gateways, access points, and switches.



Each policy created should have an intent, such as governing access to internal applications or applying a consistent Internet policy. The example below shows the creation of an Internet access policy.



Rules within a Policy

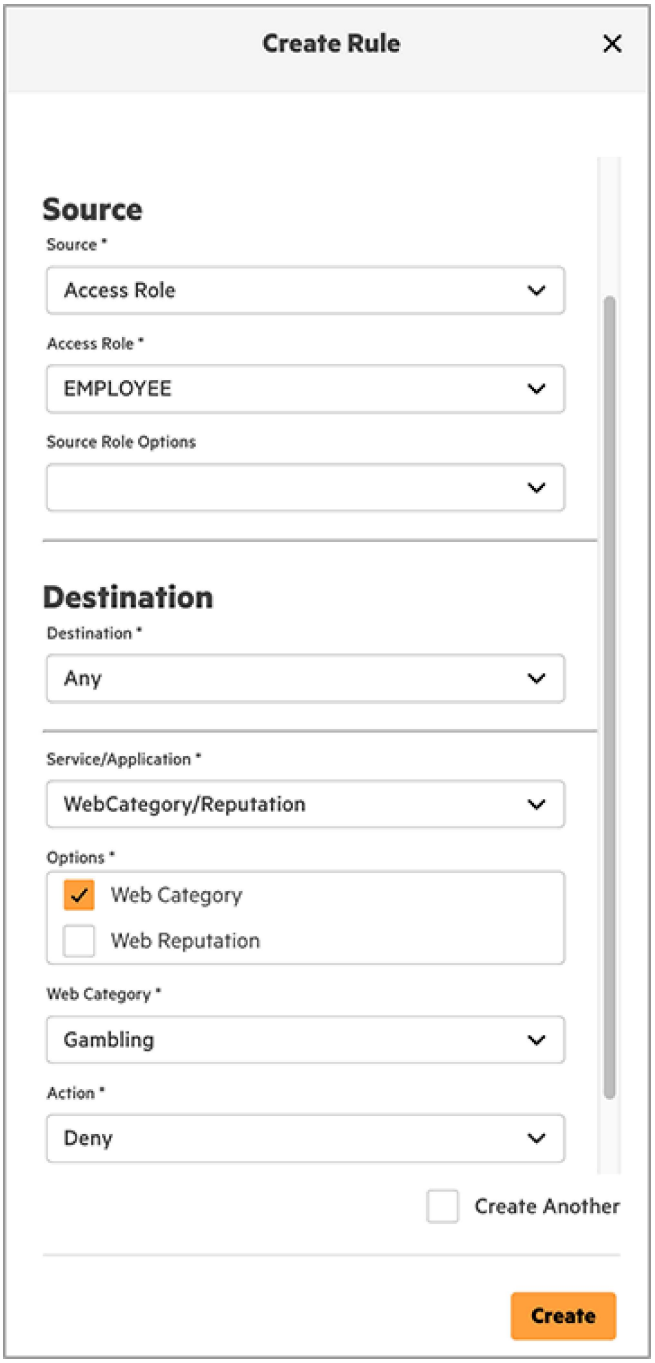
Rules within a policy consist of a source, a destination, and an action. Typical source match criteria include role, network, host, and any. Destination match criteria include many of the same options but can also reference services, applications, web categories, and reputation. When matching on roles for source or destination, multiple roles can used in a single rule to streamline policy creation.

The most common match criteria include:

- **Roles**: Define who or what is sending or receiving the traffic.
- **Applications**: Identify traffic by application or category such as Office 365, YouTube, or Social Media.
- **Networks or Subnets**: Target traffic destined for specific internal or external networks.
- **Services or Ports**: Provide precise matching for protocols or custom services.
- **Web Category or Reputation**: Evaluate traffic based on risk or content classification.

Each rule specifies an enforcement action such as *Allow* or *Deny* that determines if traffic is permitted or blocked.

For example, an Internet Access policy might deny employees access to gambling websites while allowing other users normal Internet connectivity.



These enforcement options allow a single policy to define multiple access outcomes across different roles. For instance, a policy could allow guests and employees to visit reputable websites while restricting high-risk categories for internal roles.

Internet Access... 3

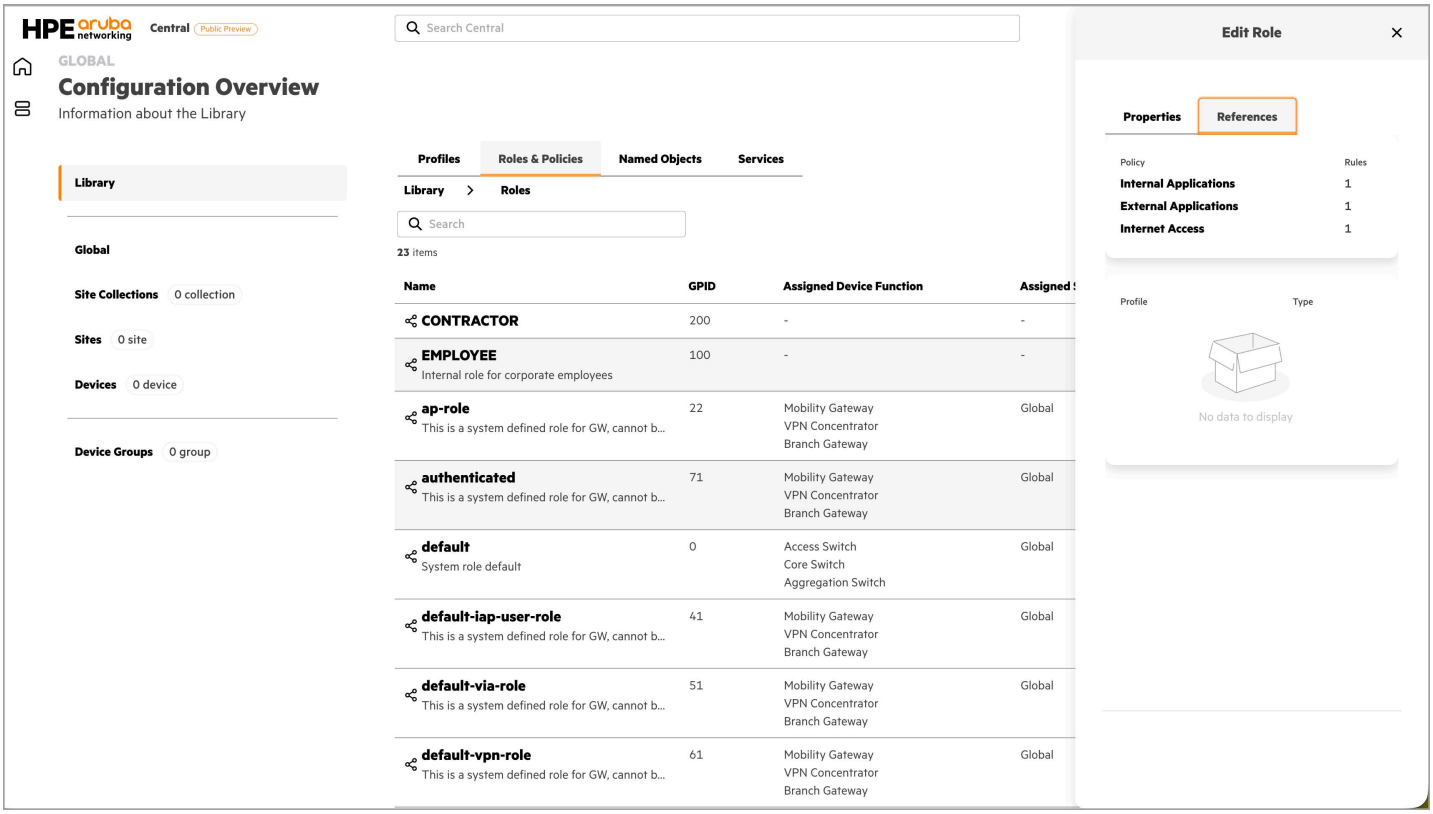
Source	Destination	Service/Application	Action
Role: EMPLOYEE	Any	Trustworthy	Allow
Role: guest	Any	Trustworthy	Allow
Role: EMPLOYEE, C...	Any	Gambling	Deny

Resultant Role Policy

HPE Aruba Networking devices still enforce policy using a role-centric policy strategy, where each role has its own uniquely assigned policy set. This requires Central to translate intent-based policy definitions into role-based policy. Central compiles intent-based policies for each device based on assigned scopes and device functions, evaluates the roles referenced within each policy, and generates a resultant role-based policy for each role, such as *EMPLOYEE* or *CONTRACTOR*. The resultant role-based policies are pushed to managed devices.

Administrators can define policy using an intent-based model, while Central automatically assembles a device-enforceable rule set for each role. The resultant policy represents the cumulative access intent for an identity, based on all applied policies in Central.

When reviewing a role in the **Library** → **Roles** section, the **References** tab displays the policies that contribute to its resultant configuration. Each listed policy includes the number of rules that apply to that role. This view provides valuable insight into how Central constructs the final rule set.



Policy Order and Match Behavior

Administrators must carefully consider both policy and rule order to ensure organizational intent is enforced. Central constructs a resultant policy rule set from intent-based policy rules in the following manner:

- Policies that appear higher in the policy have their rule sets evaluated first. The complete rule set of the first policy that applies to a role is inserted into a resultant policy before any of the rules in the next policy that applies to a role.
- When building resultant policy rules, Central inserts rules in the order they appear in a Central intent-based policy.

To ensure proper enforcement:

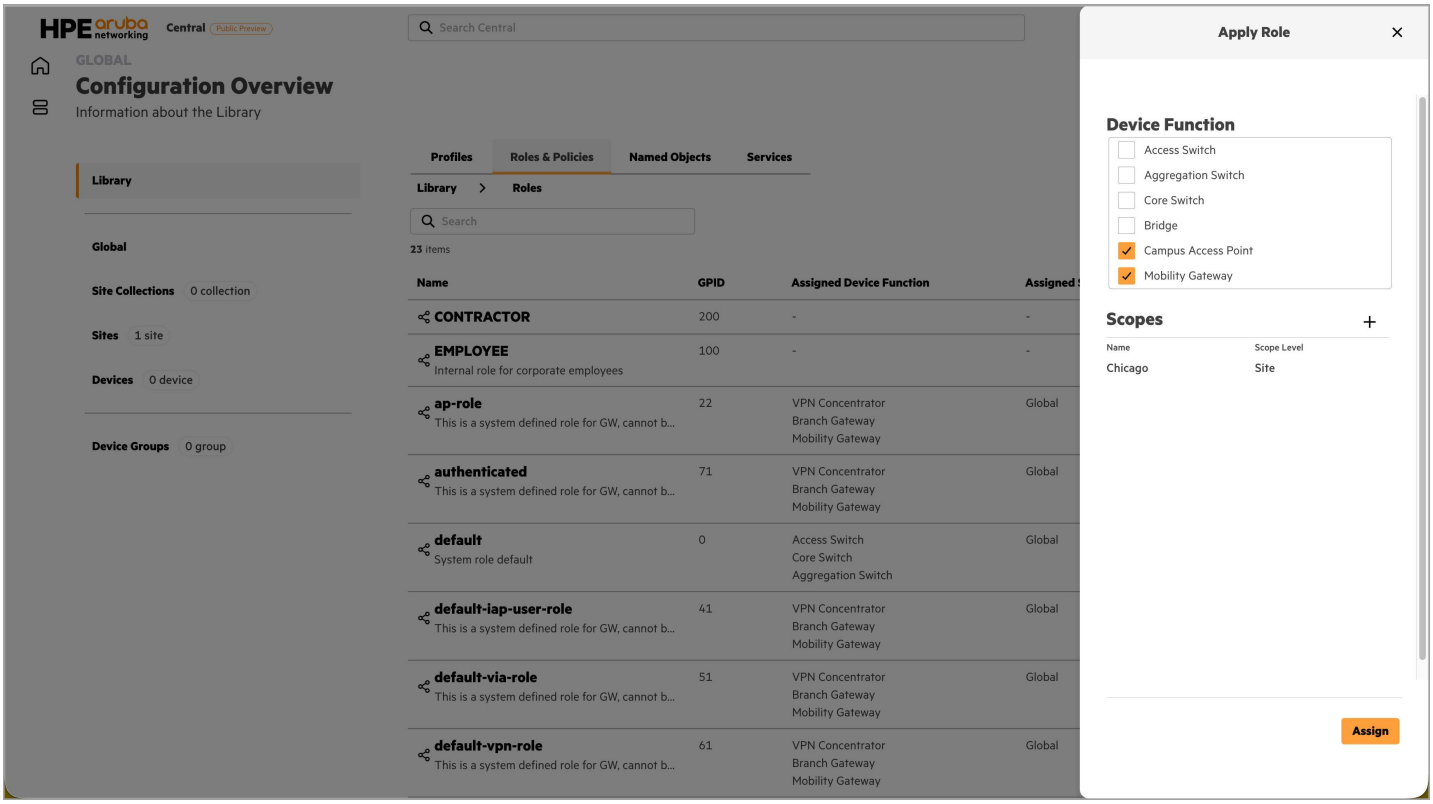
- Review the order in which policies are applied.
- Place specific rules (for example, role- or application-based) before broader ones.
- Avoid redundant broad rules across multiple policies.
- Review policies applied to roles using the References pane.
- Develop and test use cases to verify that rules interact correctly.

When constructing policy, administrators must ensure that broad match criteria are not used in Central policies that appear at or near the top of the policy list. This ensures that subsequent policy intent is evaluated. Broad match criteria should be used only in policies that appear near or at the bottom of the policy list to provide consistent fallback behavior without suppressing granular access control.

Assigning Roles and Policies

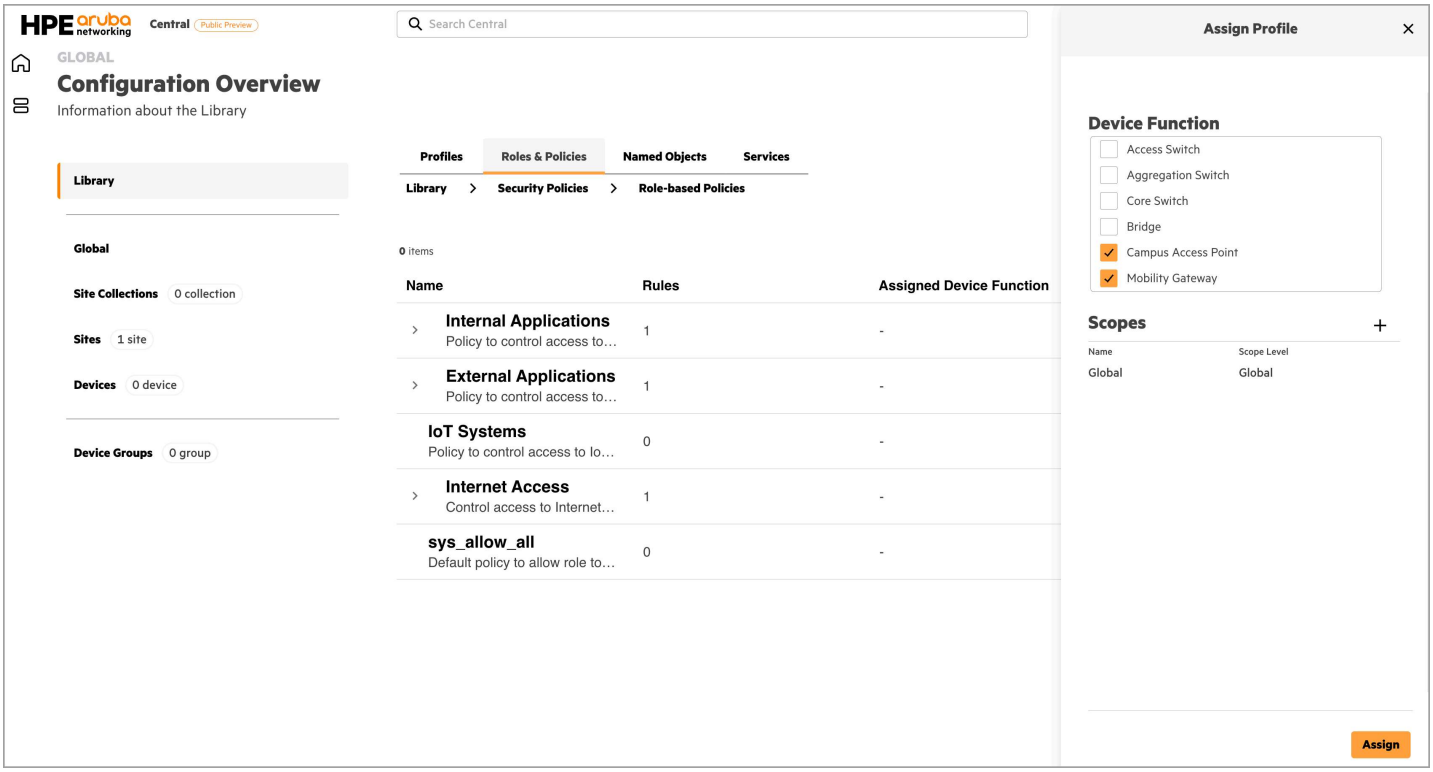
Roles and policies are pushed to devices based on their **scope** assignment in Central, such as site, device group, or global level.

The assignment of scopes to roles is the primary method of controlling where both role and policy configuration are pushed to devices. Roles should be assigned only to scopes that contain devices that enforce policy for the role (i.e., where devices and users associated with the role will connect). Keeping the scope limited conserves resources on network devices.



Policy scope assignment can be applied more broadly because policies are pushed only to devices where a relevant role is also assigned. This behavior enables role scope assignments to govern where policies are pushed. As a result, it is generally recommended to scope policies globally. This provides consistent availability across the network while reducing administrative effort.

Multiple policies can be applied to the same scope, which is often the norm rather than the exception. Each policy represents a distinct intent, such as internal access, external access, or application optimization. When multiple policies are applied, Central evaluates them collectively based on their priorities and role matches to generate the resultant policy sent to the enforcing device.



Network Device Considerations

Different devices support different enforcement capabilities. For example, gateways can use service definitions such as DNS or HTTP, but access points cannot. Similarly, CX switches support network-based access control lists (ACLs), but have limited application awareness compared to gateways.

When assigning policies, administrators must ensure that the enforcement logic aligns with the device type.

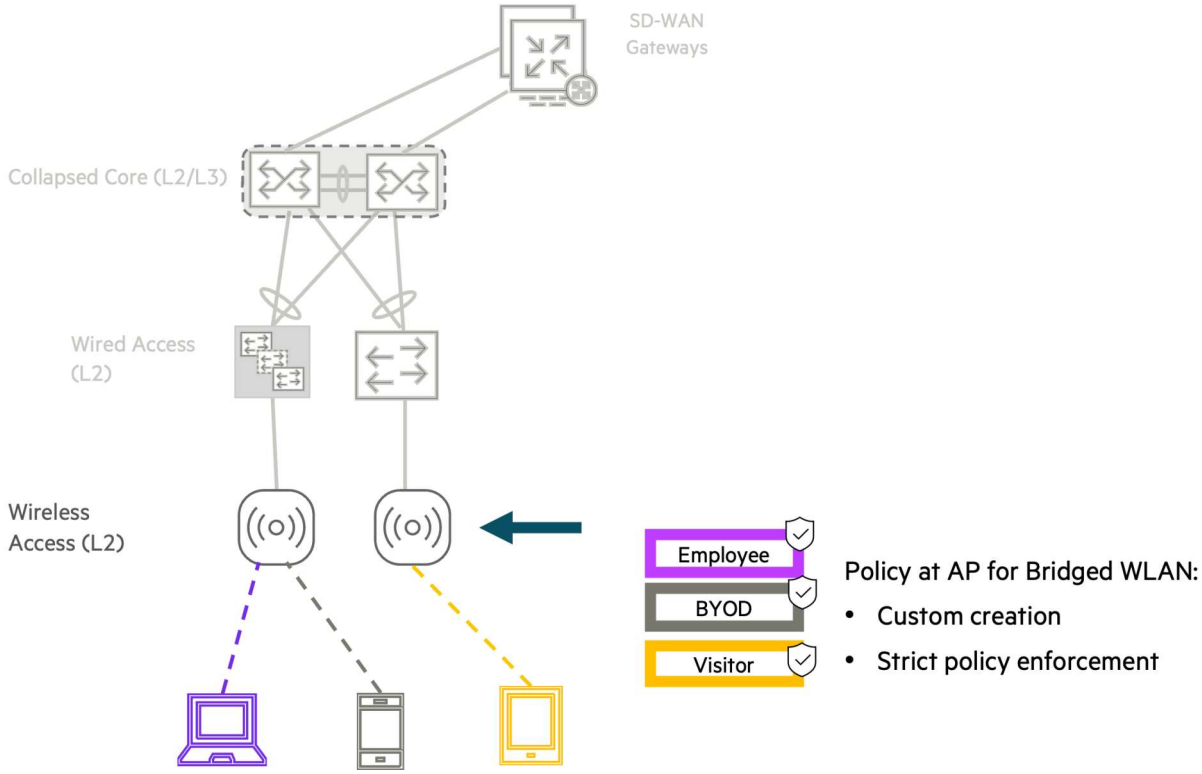
Example Use Case

This section describes how policies are applied in different deployment types, including bridged WLANs, tunneled WLANs, and User-Based Tunneling (UBT) environments. Each use case has unique scoping and enforcement considerations that determine where policies and roles should be applied.

The wireless examples refer to a simple 802.1X enabled WLAN using RADIUS returned user roles.

Bridged WLAN Policy

In a bridged WLAN, policy is applied at the access point. Each connected client is assigned a role through authentication or local assignment, and the access point enforces the policies associated with the assigned role.



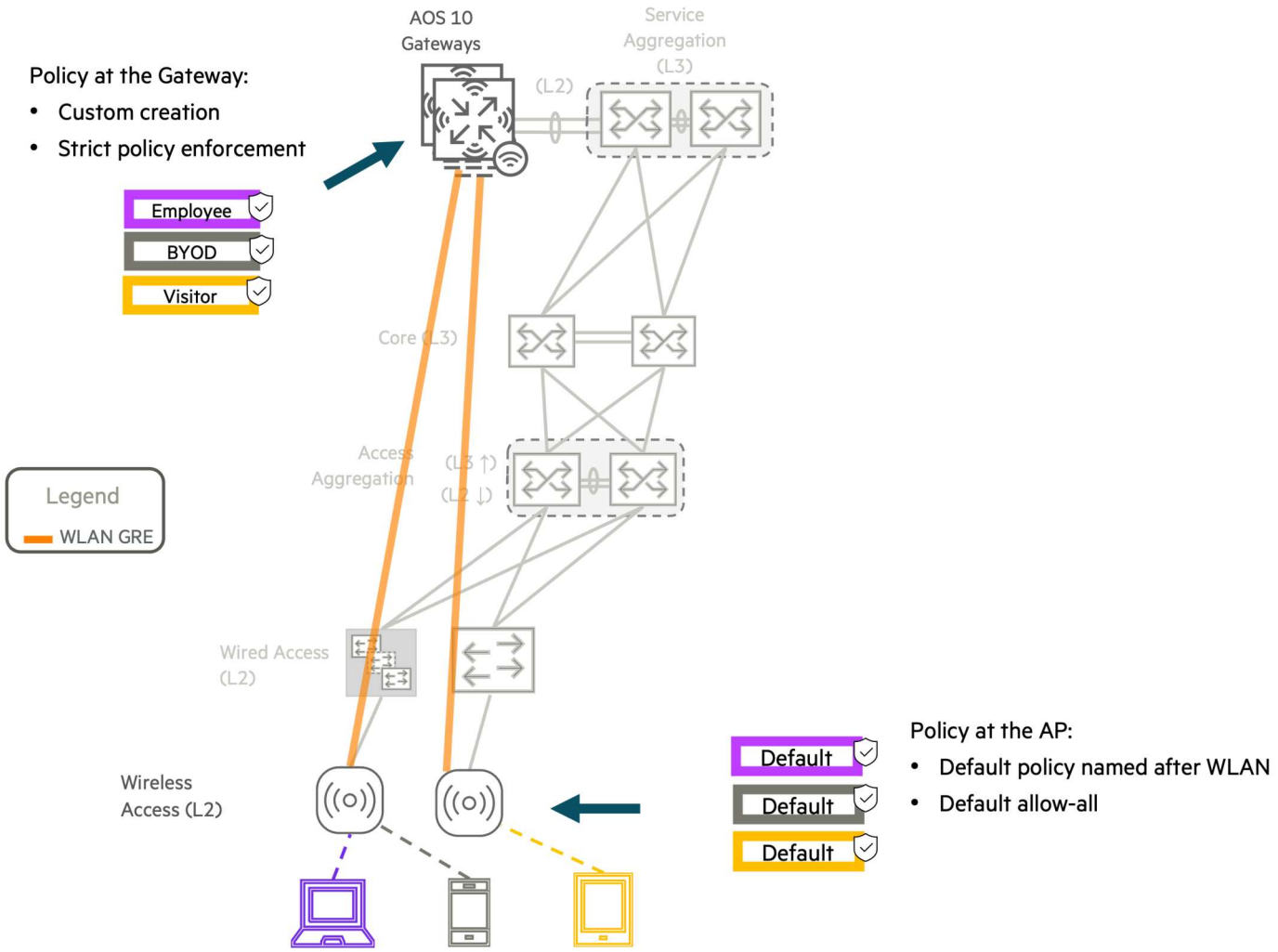
In this model, enforcement is on the local AP (no gateway involvement). Roles assigned to bridged WLANs should be scoped in Central so only access points broadcasting the WLAN receive the role. Limiting the role's scope conserves AP resources and ensures that only relevant roles and policies are downloaded.

Each WLAN includes a default role, assigned to clients that do not receive a role from an authentication server or local role-assignment rules. By default, the default role uses the same name as the WLAN, but it is best practice to specify a custom default role in the WLAN profile. This enables policy rules to reference a single default role consistently, improving policy reusability and reducing the number of policy rules required. When using a custom default role for WLANs, it is best practice to assign a device function of Campus Access Point.

In most designs, the default role is used when 802.1X does not assign a more specific role. By default, the default role allows all traffic, but it can be modified using policy to be more restrictive.

Tunneled WLAN Policy

In a tunneled WLAN, all user traffic is forwarded in a GRE tunnel between an AP and a Gateway. Both the access point and gateway are potential policy enforcement points; however, it is best practice to apply user traffic policy at gateways as described below.



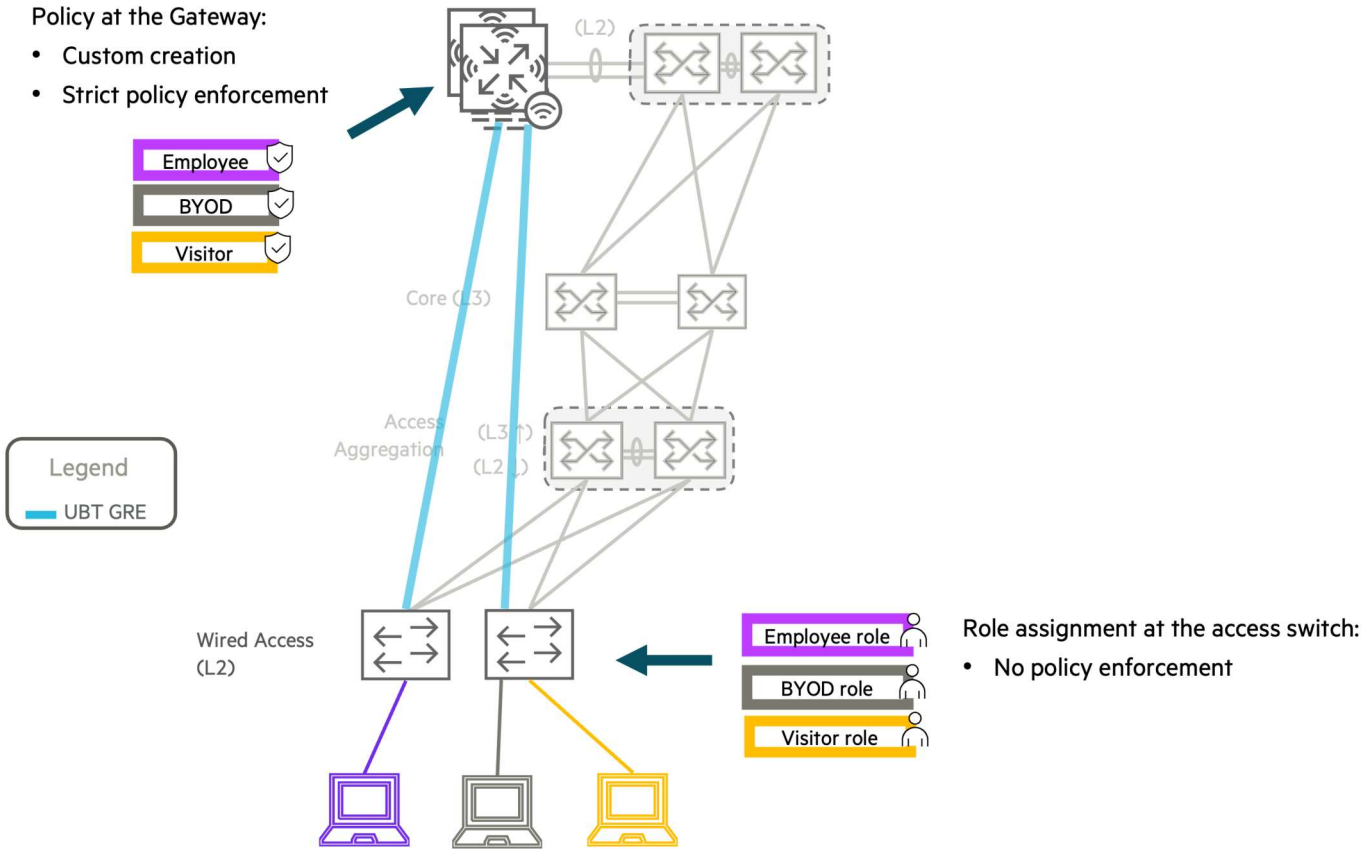
In Central, each WLAN element profile creates a default role automatically, and Central assigns it to campus access point and gateway device functions. This role generally has an allow-all policy to allow all traffic to flow from the access point to the gateway. Administrators also can select a custom role as the default, if desired.

All other user-defined roles should be scoped only to the gateways participating in the WLAN. This ensures that gateways have the role definitions needed for policy enforcement without unnecessarily downloading the role and associated policy to access points.

This separation ensures that the AP handles wireless transport while the gateway enforces access intent. If user-defined roles are also scoped to access points in a tunnel WLAN, Central will attempt to apply policies associated with the roles to those access points, which can cause unexpected behavior and potential resource overhead.

User-Based Tunneling (UBT)

User-Based Tunneling (UBT) extends centralized policy enforcement to wired clients by applying role-based access controls through Mobility Gateway clusters. In a UBT deployment, wired devices connected to access switches are assigned roles dynamically. Central defines the appropriate role-based policies based on these assignments, and the gateways enforce them.



UBT requires additional configuration on the switches and gateways to operate correctly. This configuration is out of scope for this chapter. See the User-Based Tunneling Design chapter in the VSG for more information.

For UBT to function correctly, the role must be defined in Central and scoped to the appropriate access switch. Within the role definition, switch-specific parameters also must be configured. The authentication mode should be set to Client, User-Based Tunneling should be enabled, the Gateway Zone must match the configuration in the UBT element profile for the corresponding switch, and the Gateway Role should be set appropriately, typically matching the role defined on the switch.

The image below shows an example of a role configured for UBT. The fields displayed have been reduced for clarity.