Cyxtera™

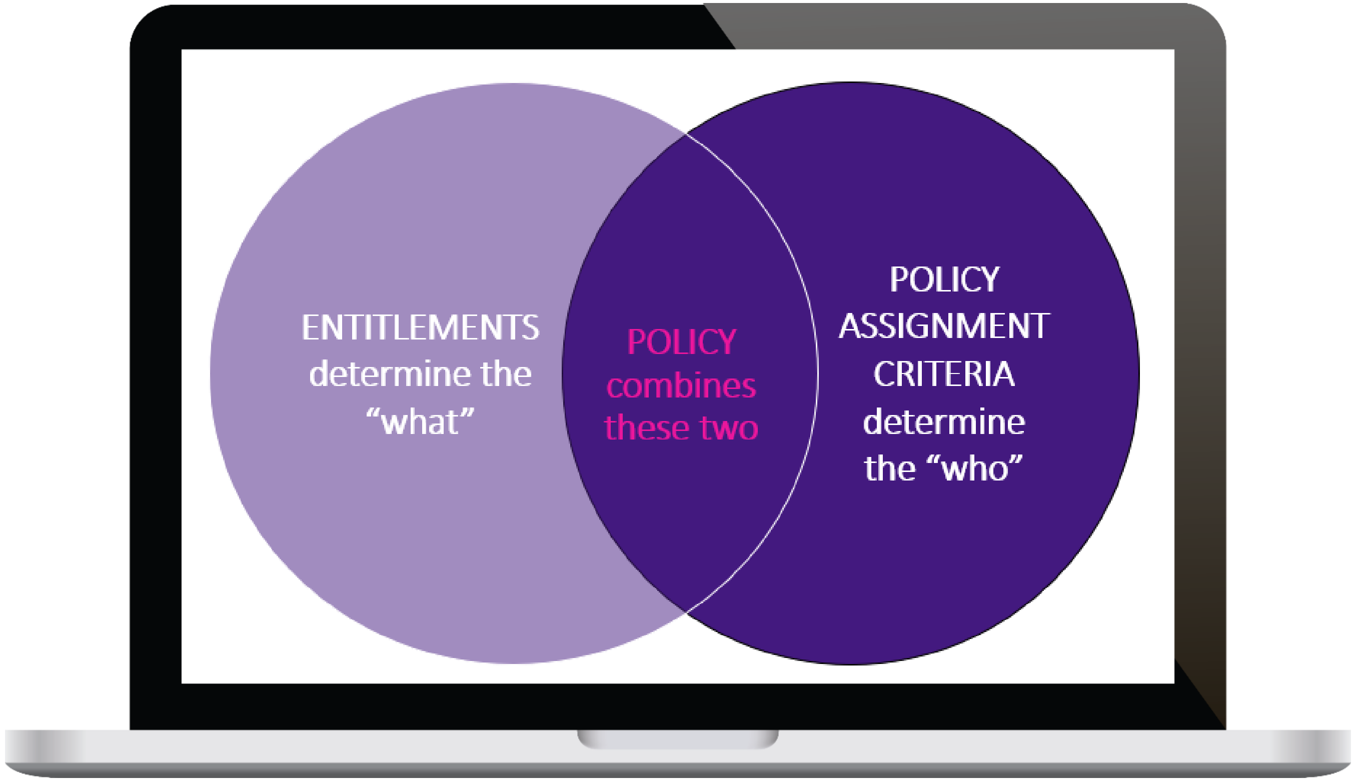
AppGate SDP
User Access Control

AppGateSDP

Access, evolved.

Training Topics

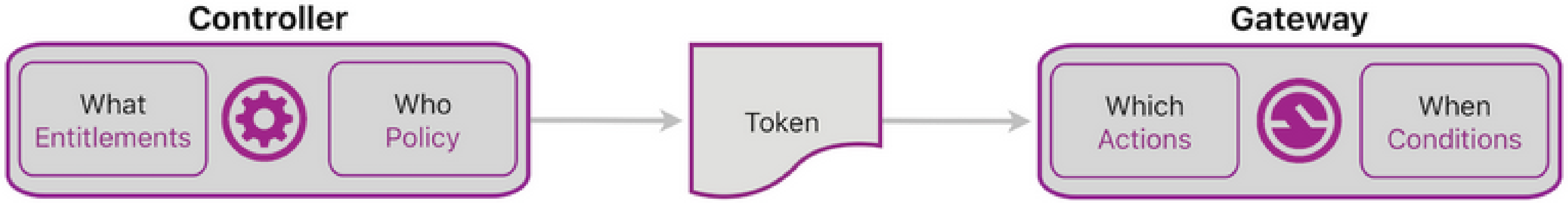
We will introduce you to the components that make up User Access (akin to firewall “rules”).


ENTITLEMENTS determine the “what”
POLICY combines these two
POLICY ASSIGNMENT CRITERIA determine the “who”

User Access Control concepts

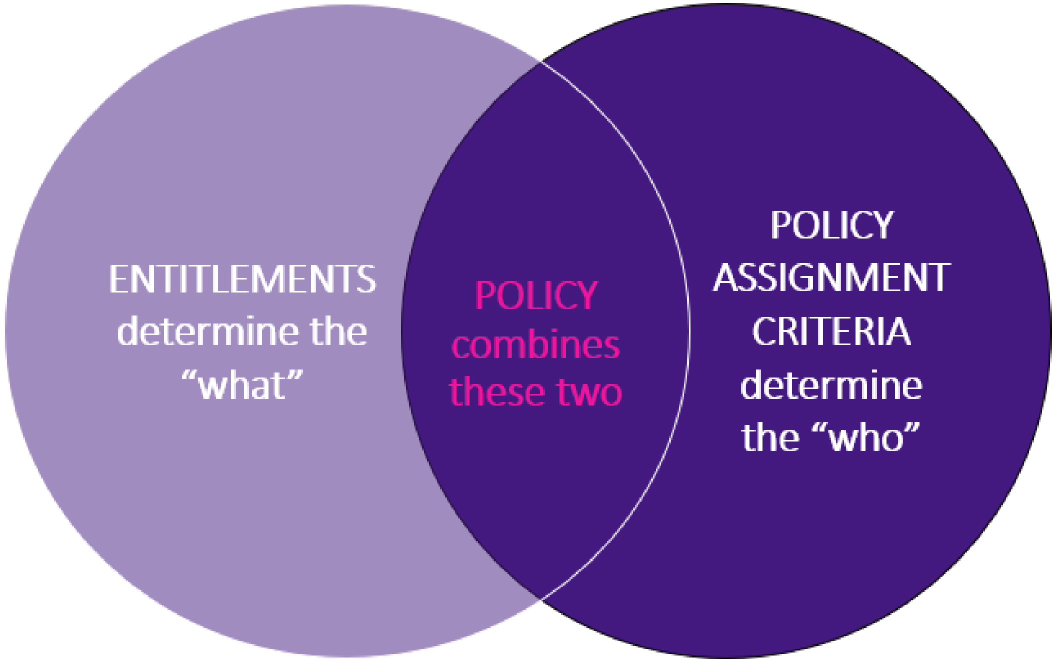
- **Policy**
  - Assigns rights to a user or group of users, such as sales, developers, consultants…
- **Policy Assignment**
  - Defines who will fit into what Policies, such as "member of Sales group"
- **Entitlement**
  - Defines an access rule, such as "access to CRM"
- **Condition**
  - Defines requirements that need to be true for Entitlements to be enabled, such as “requires OTP "

AppGate SDP - a four stage process for access control



- Policies – Policy Assignment and Entitlements
  - First we define who can access what (e.g. sales systems)
- Entitlements – Actions and Conditions
  - Then we define when access will be allowed (e.g. CRM if work hours)

Defining what access rights the user has


ENTITLEMENTS determine the “what”
POLICY combines these two
POLICY ASSIGNMENT CRITERIA determine the “who”

Prerequisites:

- Policies are used to assign rights to a user or group of users. Before we can create Policies, we must select Assignment Criteria and create Entitlements

Policies

- Policy Assignment Criteria
- Entitlements

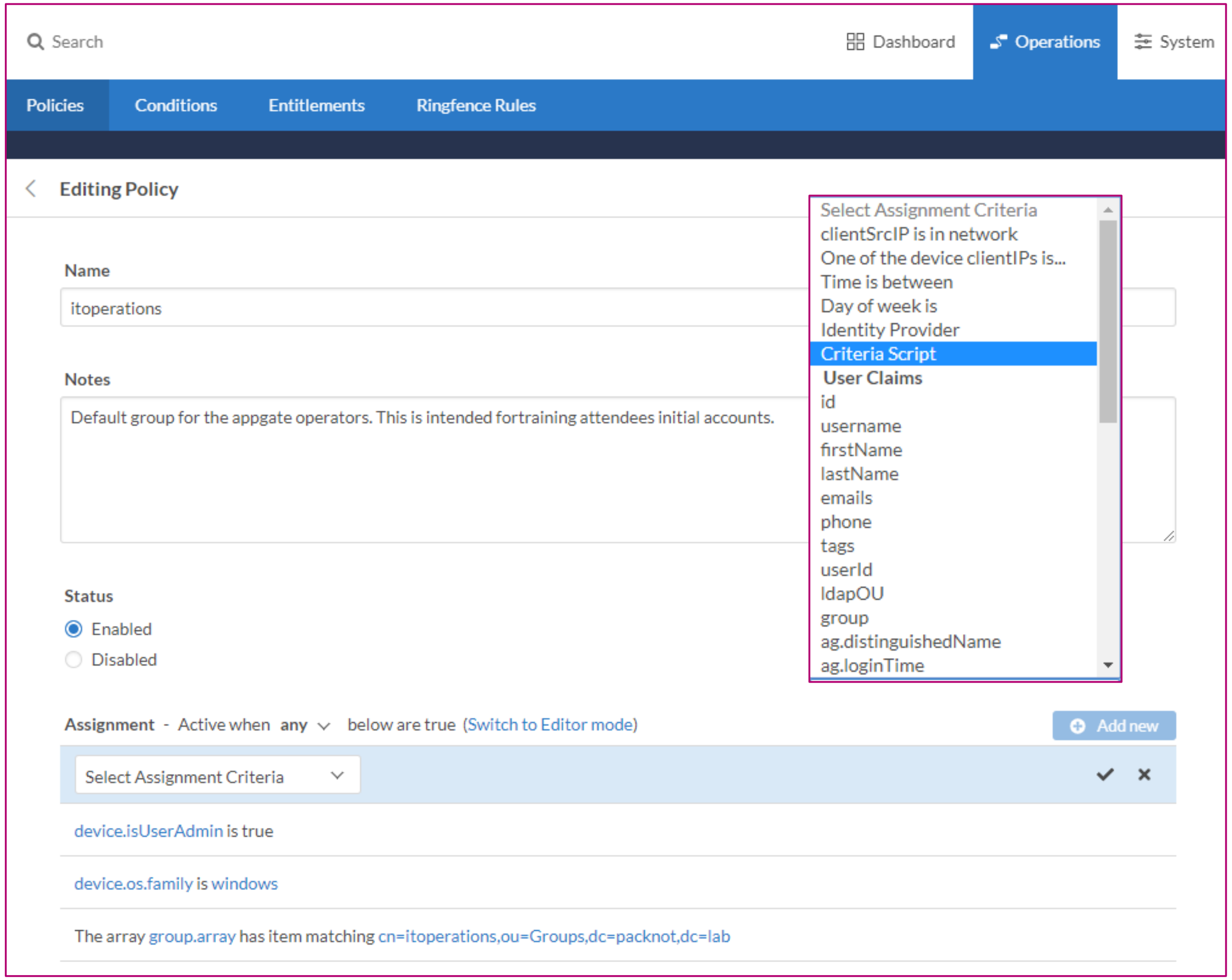
Policy Assignment Criteria decide on “who”

- Claims-based expressions defining who a Policy should be assigned to. A Policy should assign the rights that the user is likely to need during the session
- Evaluated at sign-in by the Controller or when the user's tokens are renewed
- Use static claims that are unlikely to change during the day, such as directory group membership, email address, etc.

Policy Assignment Criteria

- The Policy Assignment and its expressions are ***always*** evaluated for a true/false result
  - is user x in the AD group ‘Marketing’?
  - is user x’s device running macOS Sierra?
- Each Policy can include one or more criteria expressions
  - ‘any’ or ‘all’ expressions have to be true
- Policy Assignment Criteria expressions will be configured within the Policy itself. The builder tool provides the pick list of claims that can be used. Re-usable expressions can be created using Criteria Scripts

Policy Assignment



Editing Policy

Name

itoperations

Notes

Default group for the appgate operators. This is intended fortraining attendees initial accounts.

Status

● Enabled

○ Disabled

Assignment - Active when any below are true (Switch to Editor mode)

device.isUserAdmin is true

device.os.family is windows

The array group.array has item matching cn=itoperations,ou=Groups,dc=packnot,dc=lab

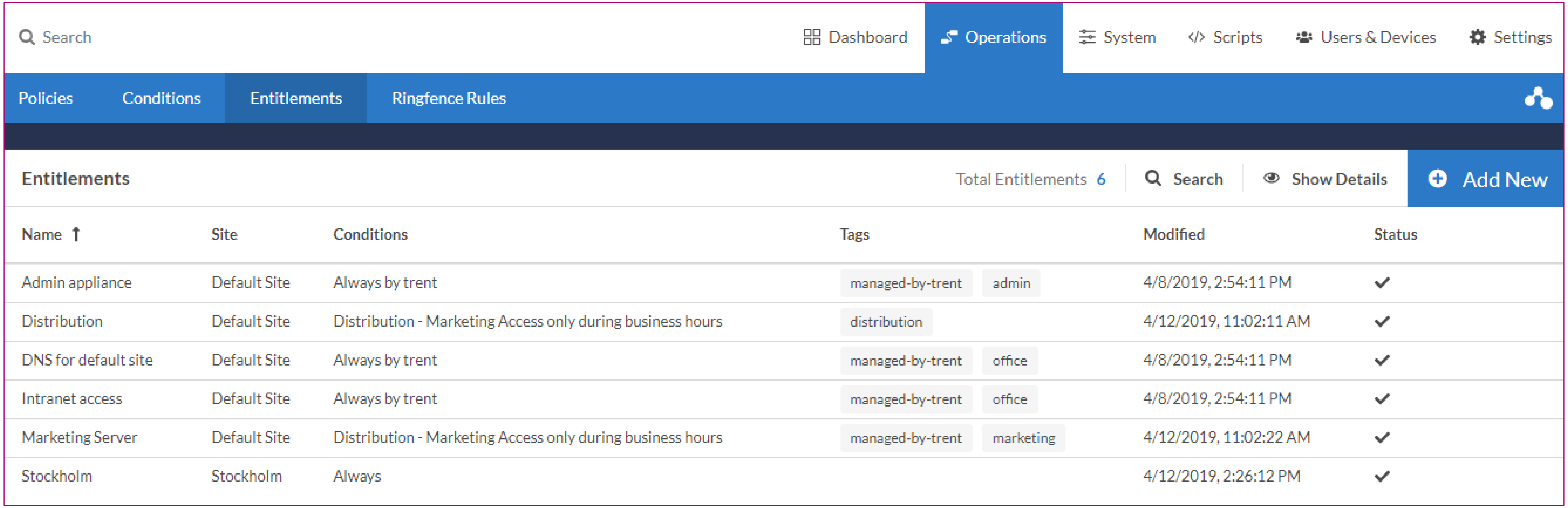
Policies

- Policy Assignment Criteria
- Entitlements

Entitlements define “what” access is granted

- Entitlements are provisioned to users via Policies
- Select the pre-defined Entitlements to be included in the Policy: you can pick Entitlements by name or by using Tags.
- Each Entitlement is linked to a particular Site and defines the rules for controlling access to network resources on that particular Site.
- The Controller will provide the Client with an Entitlement token for each Site, and a list of Gateways serving each Site. *The Client will only attempt to connect to the Gateways that it has an Entitlement token for - all other Sites in the Collective will be invisible.*

Entitlements

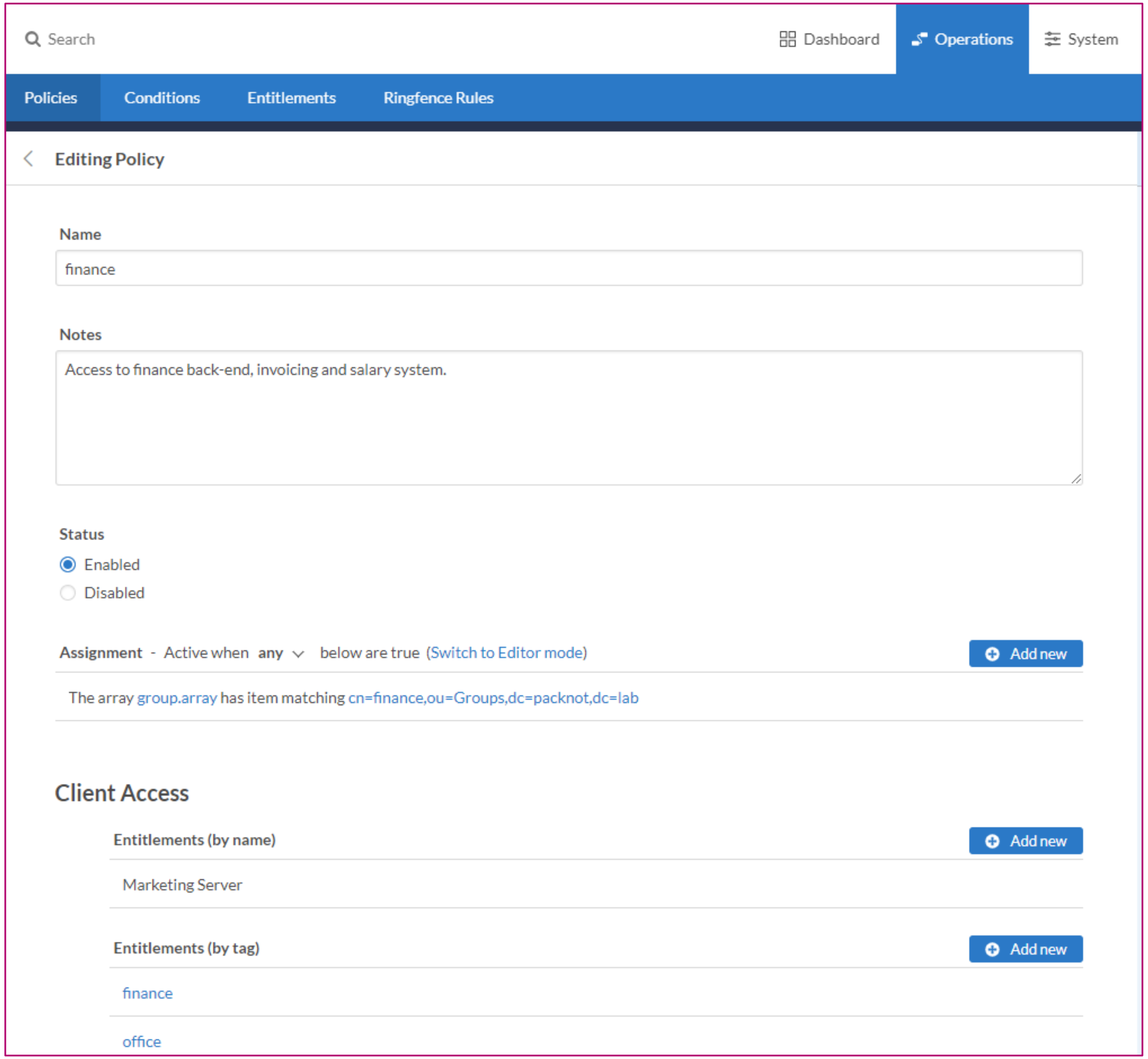


Entitlements

Total Entitlements 6

Name ↑	Site	Conditions	Tags	Modified	Status
Admin appliance	Default Site	Always by trent	managed-by-trent admin	4/8/2019, 2:54:11 PM	✓
Distribution	Default Site	Distribution - Marketing Access only during business hours	distribution	4/12/2019, 11:02:11 AM	✓
DNS for default site	Default Site	Always by trent	managed-by-trent office	4/8/2019, 2:54:11 PM	✓
Intranet access	Default Site	Always by trent	managed-by-trent office	4/8/2019, 2:54:11 PM	✓
Marketing Server	Default Site	Distribution - Marketing Access only during business hours	managed-by-trent marketing	4/12/2019, 11:02:22 AM	✓
Stockholm	Stockholm	Always		4/12/2019, 2:26:12 PM	✓

Entitlements



Editing Policy

Name

finance

Notes

Access to finance back-end, invoicing and salary system.

Status

● Enabled

○ Disabled

Assignment - Active when **any** below are true (Switch to Editor mode)

The array group.array has item matching cn=finance,ou=Groups,dc=packnot,dc=lab

Client Access

Entitlements (by name)

Marketing Server

Entitlements (by tag)

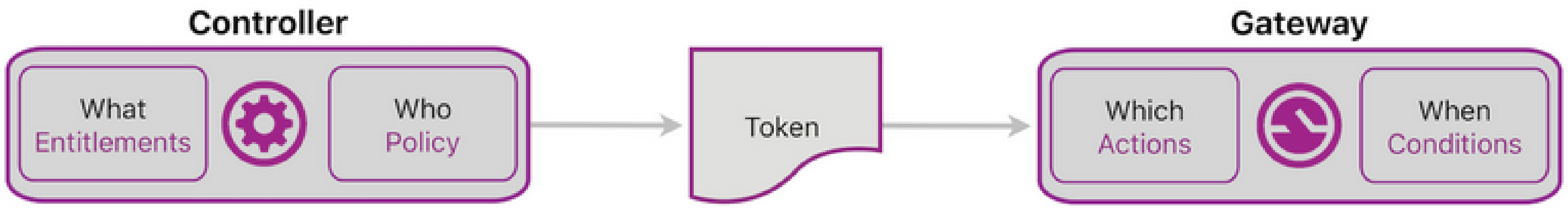
finance

office

Policies – Assignment Criteria & Entitlements Recap

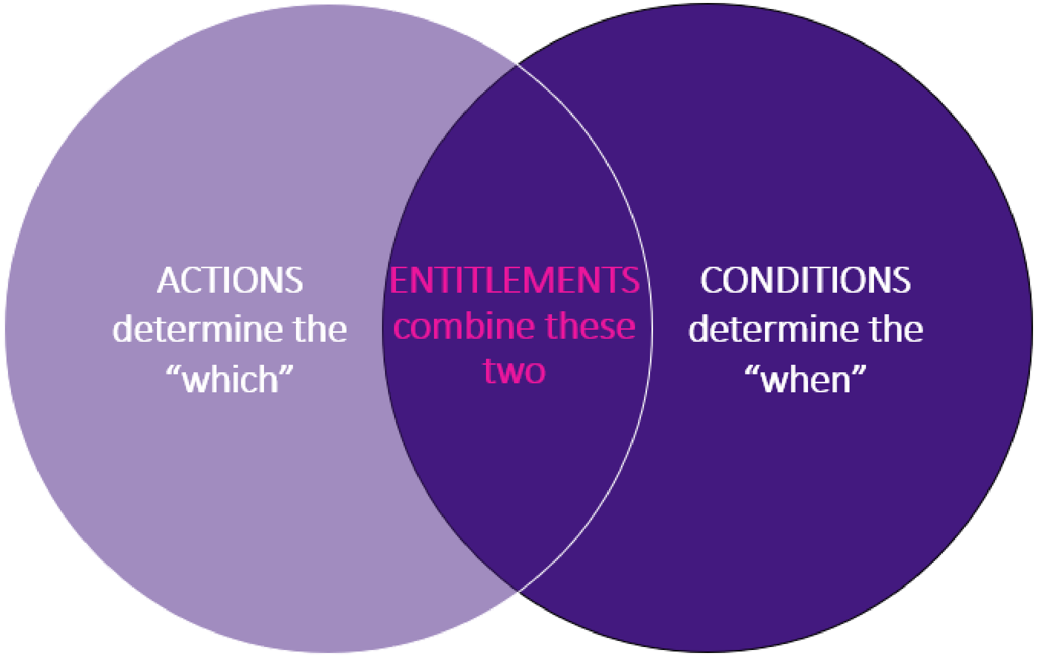
- Policies are an internal structure - within the Controller only
- They use Assignment Criteria to determine the allowed set of Entitlements
  - If the criteria expression is false, then the Policy is not enabled
- Policies can contain multiple Entitlements
- A user's resulting Entitlements may come from several Policies
- For each Site (where access is allowed) an Entitlement token is issued
- More on Entitlements coming soon…

AppGate SDP - a four stage process for access control



- Policies – Policy Assignment and Entitlements
  - First we define who can access what (e.g. sales systems)
- Entitlements – Actions and Conditions
  - Then we define when access will be allowed (e.g. CRM if work hours)

Deciding when rights can be used



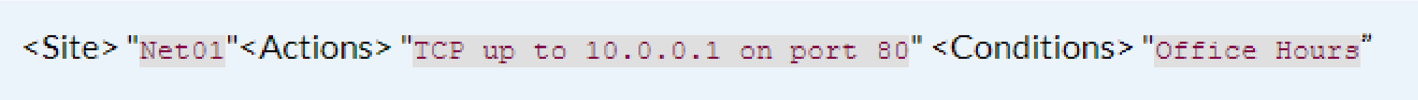
ACTIONS determine the “which”

ENTITLEMENTS combine these two

CONDITIONS determine the “when”

Entitlements

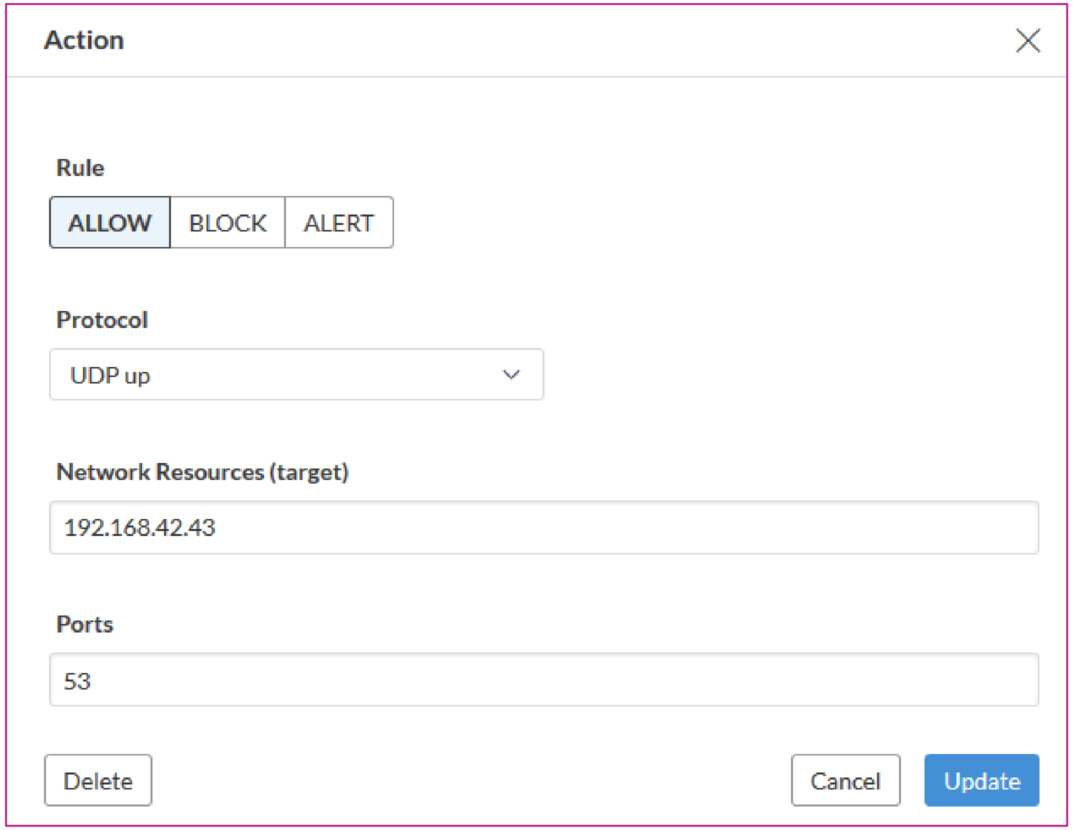
- Each Entitlement defines the rules for controlling access to network resources on a particular Site.
- The main elements of an Entitlement are:
  - The Site
  - Actions (traffic protocols, target hosts, ports)
  - any Conditions that must be met for those Actions to be allowed at the Gateway.
- The default Condition for an Entitlement is *'Always'* i.e. unrestricted unless a specific Condition has been included.
- Example of a user Entitlement to allow *IP Access to 10.0.0.1 server on port 80* only *if the time is between 09.00 and 17.00* :



```
<Site> "Net01"<Actions> "TCP up to 10.0.0.1 on port 80" <Conditions> "Office Hours"
```

Actions define “which” rules are applied

- Think of Actions as firewall rules:
  - Type - allow, block or alert
  - Protocol (tcp, udp, icmp, ah, esp, gre)
  - Network Resources (hostnames, IPs, subnets)
  - Ports
- Entitlements can have multiple Actions
- Normally, Entitlements will be used to <ALLOW> user traffic to network resource. However, an Entitlement can <BLOCK> traffic to a service or be used to trigger an <ALERT> if traffic is sent to a particular host.



Action

Rule: ALLOW

Protocol: UDP up

Network Resources (target): 192.168.42.43

Ports: 53

Conditions decide “when”

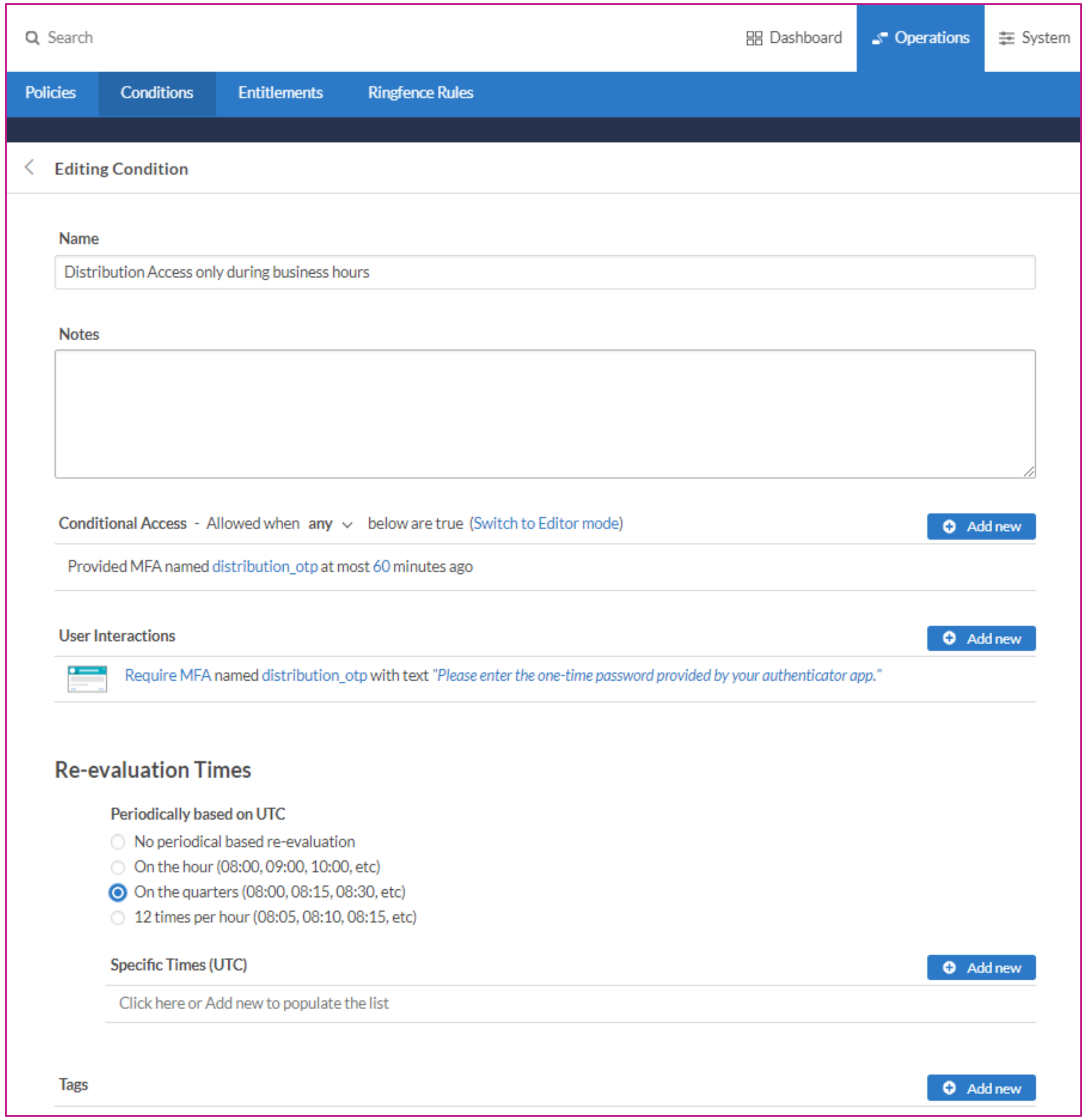
- Each Entitlement can include one or more Conditions to provide real-time control over how the Entitlement is used: for example, only allowing access to a service during working hours, or requiring the user to re-enter their password before gaining access to sensitive resources.
- Condition access criteria are passed to the Gateway(s) protecting a Site in the Entitlement token. The Gateway will evaluate claims and configure firewall rules according to the Condition criteria.
- Entitlements are re-evaluated periodically by the Gateway e.g. if a token is updated or a target IP address is changed by a name resolver. Additional re-evaluations can be included in the Condition.
- Conditions needs to be pre-defined

Creating Conditions

There are 3 parts to a Condition:

- Set the Conditional Access criteria
- Set (optional) User Interaction/Remedy if Condition not met
- Set when you would like this Condition re-evaluated

Let’s look at each in turn…



Editing Condition

Name

Distribution Access only during business hours

Notes

Conditional Access - Allowed when any below are true (Switch to Editor mode)

Provided MFA named distribution_otp at most 60 minutes ago

User Interactions

Require MFA named distribution_otp with text *"Please enter the one-time password provided by your authenticator app."*

Re-evaluation Times

Periodically based on UTC

○ No periodical based re-evaluation
○ On the hour (08:00, 09:00, 10:00, etc)
● On the quarters (08:00, 08:15, 08:30, etc)
○ 12 times per hour (08:05, 08:10, 08:15, etc)

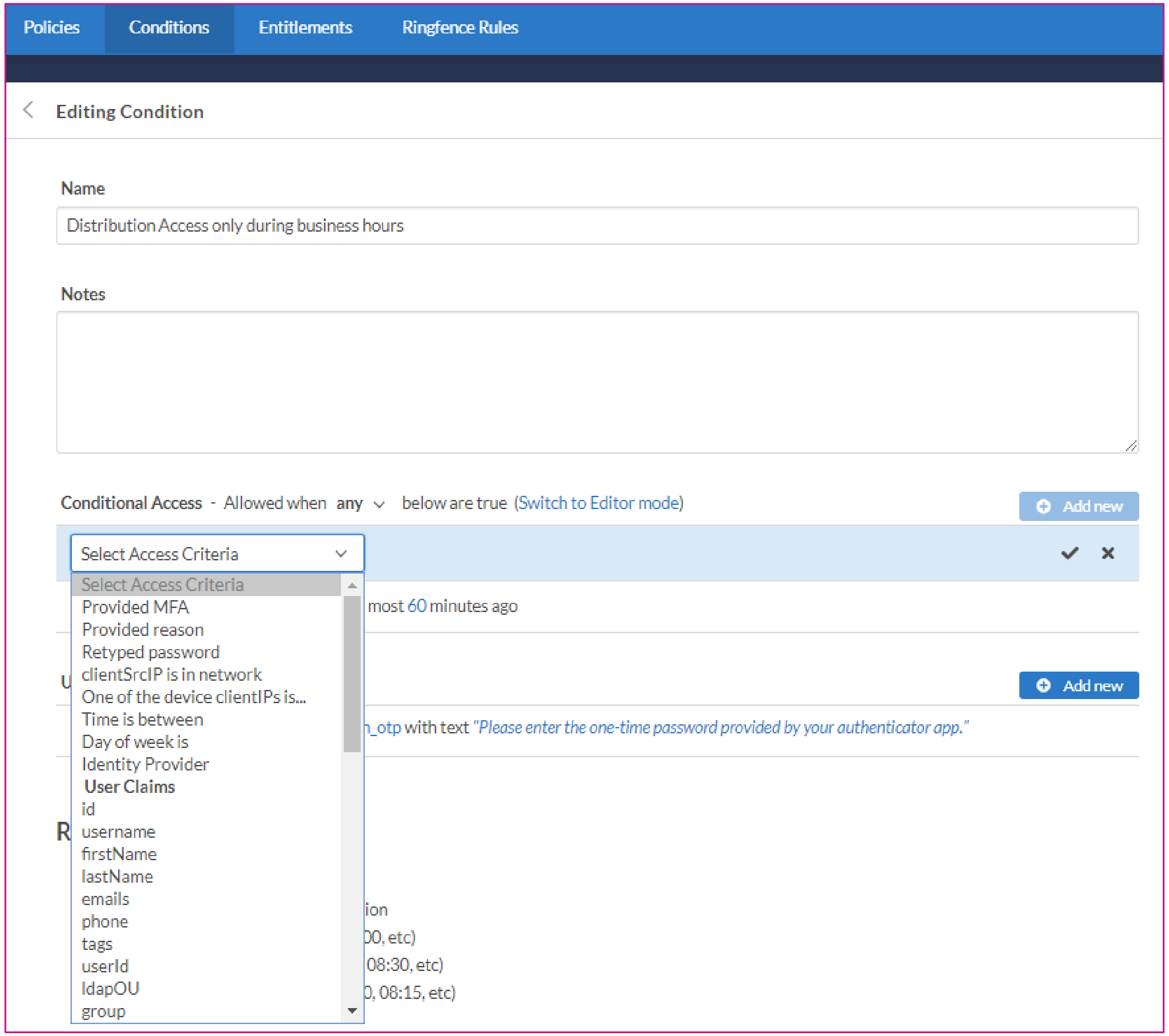
Specific Times (UTC)

Click here or Add new to populate the list

Tags

Conditional Access Criteria Expression

- The expression is comprised of access criteria: claims and associated value(s). You select whether any or all of the criteria must be true for the Condition to pass at the Gateway.
- The expression builder provides a pick list of available claims that can be used - User, system, device, onDemand claims



Editing Condition

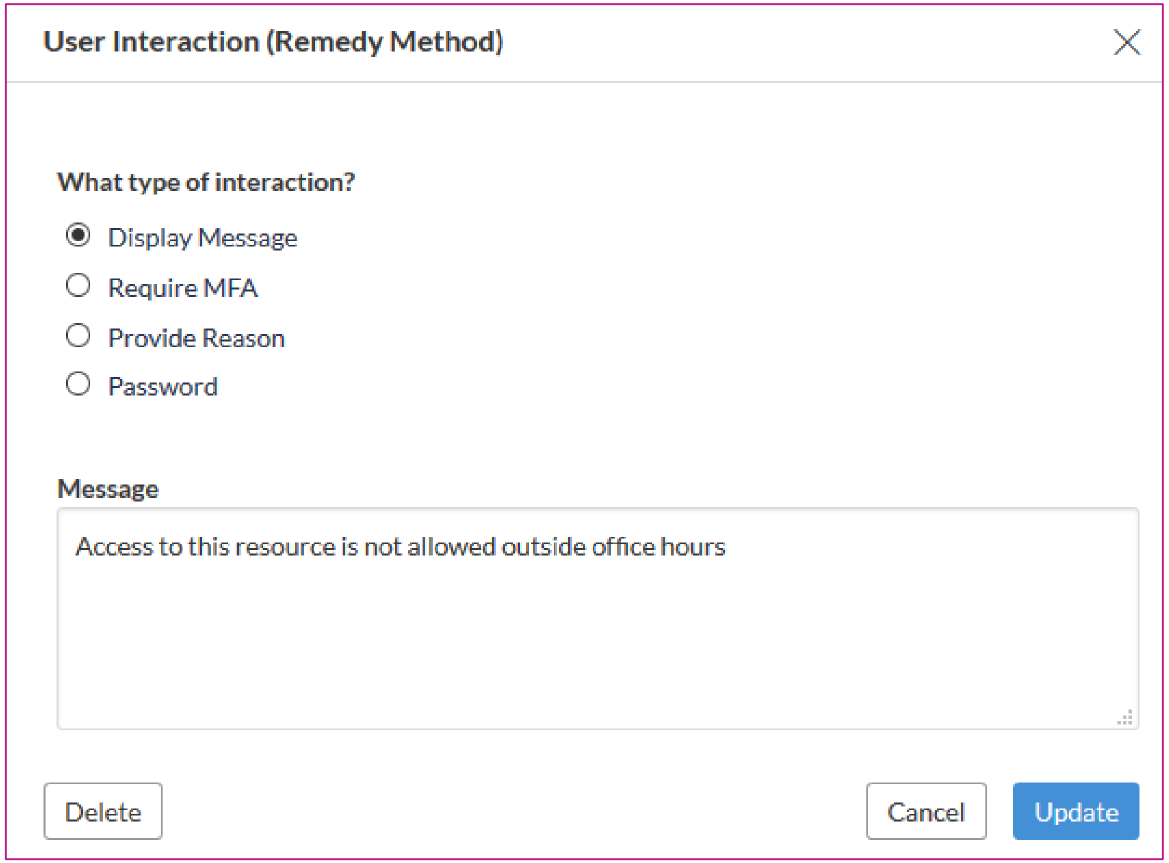
Name: Distribution Access only during business hours

Notes

Conditional Access - Allowed when any below are true (Switch to Editor mode)

User Interaction

- When a Condition is false – User Interactions/Remedies inform the user about why access has been denied and/or any action they can take to be granted access
- 4 types can be specified:
  - Display Message
  - Require MFA
  - Provide Reason
  - Password



User Interaction (Remedy Method)

What type of interaction?

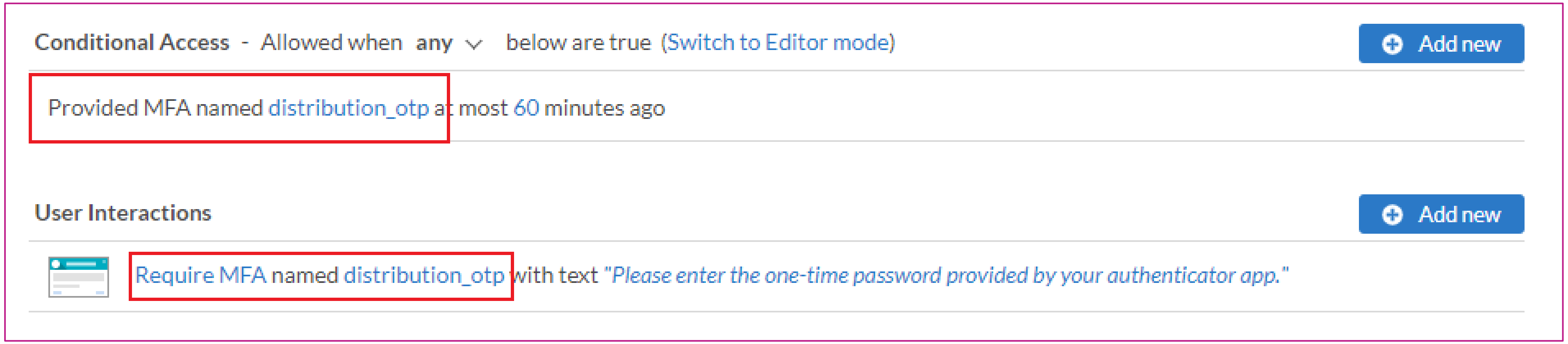
● Display Message
○ Require MFA
○ Provide Reason
○ Password

Message

Access to this resource is not allowed outside office hours

User Interaction

- If you have…
  - “Provided MFA or Provided Reason or Retyped Password" as Access Criteria in the Condition
- You **MUST** have the relevant User Interaction/Remedy method:
  - Otherwise the condition will fail
- When creating a Condition using a remedy method expression, you will be prompted for a name - this will create a new internal claim with #name# as the suffix.



Conditional Access - Allowed when any below are true (Switch to Editor mode)

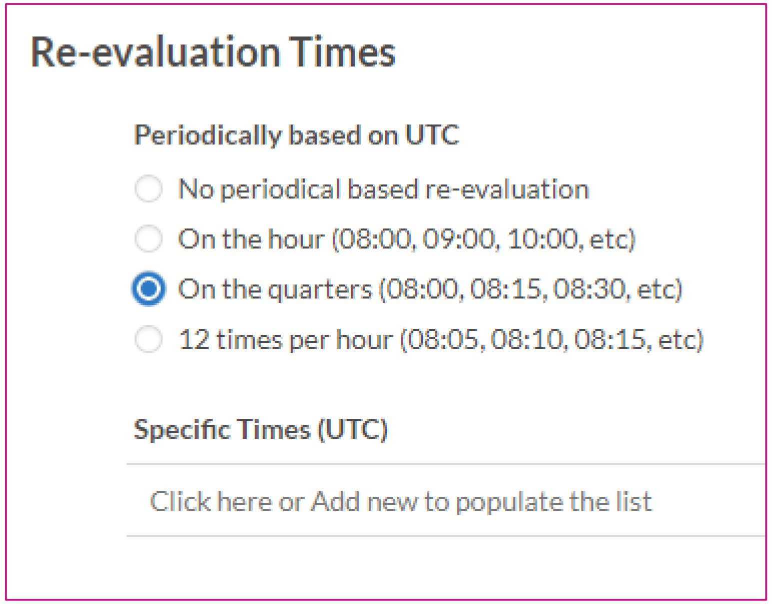
Provided MFA named distribution_otp at most 60 minutes ago

User Interactions

Require MFA named distribution_otp with text *"Please enter the one-time password provided by your authenticator app."*

Time based re-evaluations

- There are two options to force the Gateway to re-evaluate the Conditions within an Entitlement:
  - Periodic re-evaluation times: The Gateway will re-evaluate a user's entitlements at this frequency. Mainly required when using password and MFA remedy types to check if they have expired.
  - The Gateway will re-evaluate a user's entitlements at this time. Required if a condition includes a temporal element such as 'only after 17.00’.
- The system actually has a 5 minute warning event; so for time based events, the Gateway checks whether the condition still passes and during this 5 minute window will trigger the remedy method before the Condition fails preventing the users session being lost by the change in the firewall rules.



Re-evaluation Times

Periodically based on UTC

○ No periodical based re-evaluation

○ On the hour (08:00, 09:00, 10:00, etc)

● On the quarters (08:00, 08:15, 08:30, etc)

○ 12 times per hour (08:05, 08:10, 08:15, etc)

Specific Times (UTC)

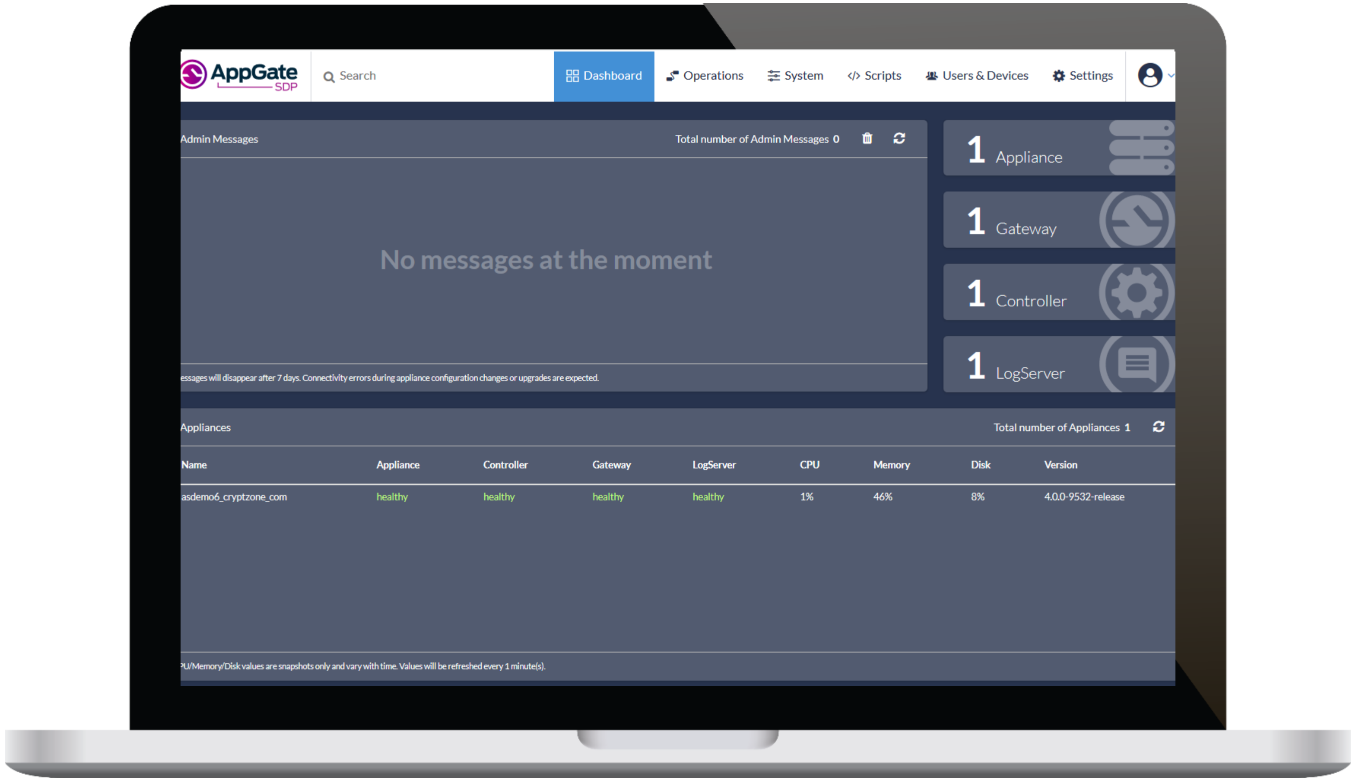
Click here or Add new to populate the list

Entitlements – Actions & Conditions Recap

- Controller sends one Entitlement token per-site and are the means by which access rules are passed to the Gateway (via the Client).
- Entitlements use Conditions to determine the allowed set of Actions
  - Entitlements should contain at least one Action
  - Conditions will be evaluated at time of use and a preset re-evaluation time
  - User Interaction/Remedy actions can be applied to Conditions

Lab: Provision access to distribution

- The people working within distribution should be provisioned access - Lab 1
- Access should be during working hours time - Lab 2



Admin Messages

Total number of Admin Messages 0

No messages at the moment

essages will disappear after 7 days. Connectivity errors during appliance configuration changes or upgrades are expected.

1 Appliance

1 Gateway

1 Controller

1 LogServer

Appliances

Total number of Appliances 1

Name	Appliance	Controller	Gateway	LogServer	CPU	Memory	Disk	Version
asdemo6_cryptzone_com	healthy	healthy	healthy	healthy	1%	46%	8%	4.0.0-9532-release

PU/Memory/Disk values are snapshots only and vary with time. Values will be refreshed every 1 minute(s).

Cyxtera™

AppGate SDP
User Access Control

https://www.cyxtera.com/secure-access

AppGateSDP

Access, evolved.