

Configuring Identity & Authentication Providers

AppGateSDP
Access, evolved.

Cyxtera proprietary

Training Topics

Next...

We will take you through adding users to AppGate.

Topics:

Identity Types

Secondary Authentication

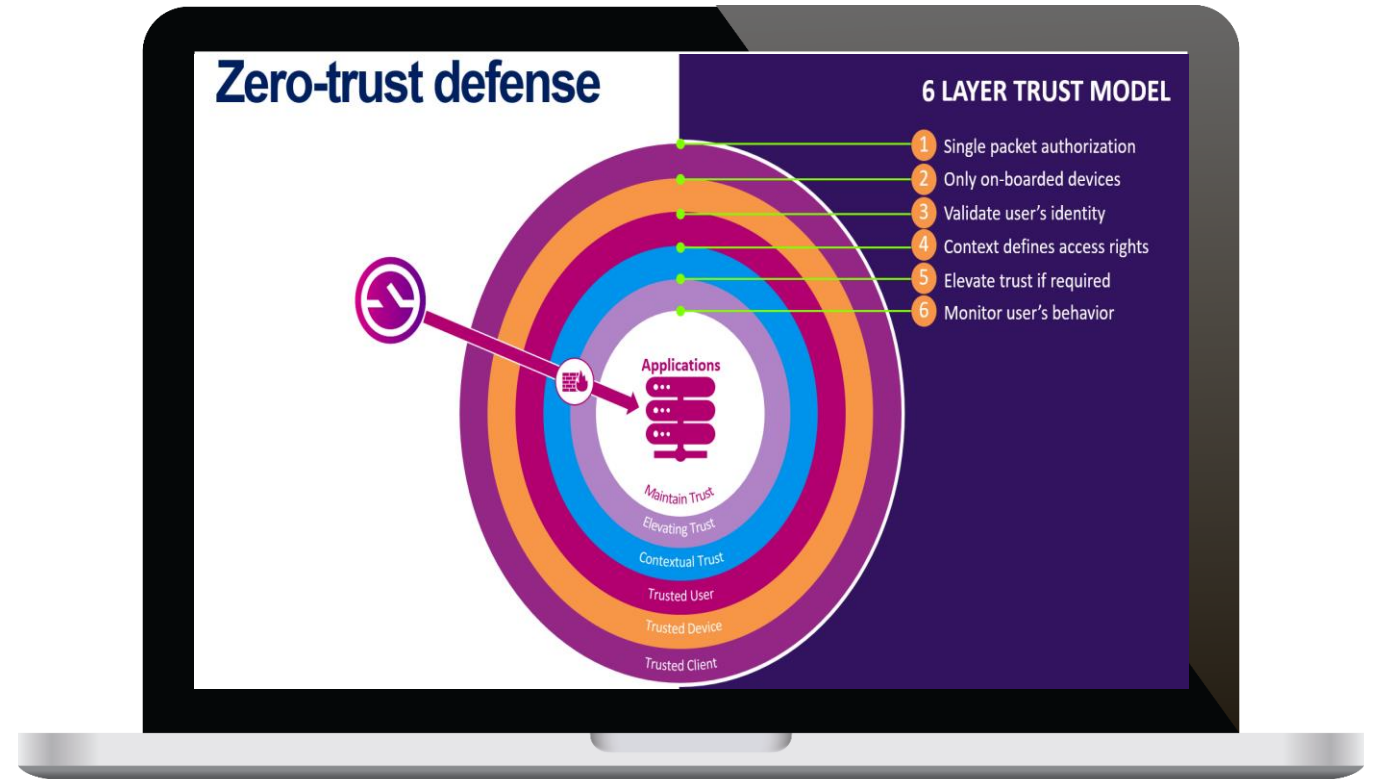
Demo: One Time Passwords

Local Users

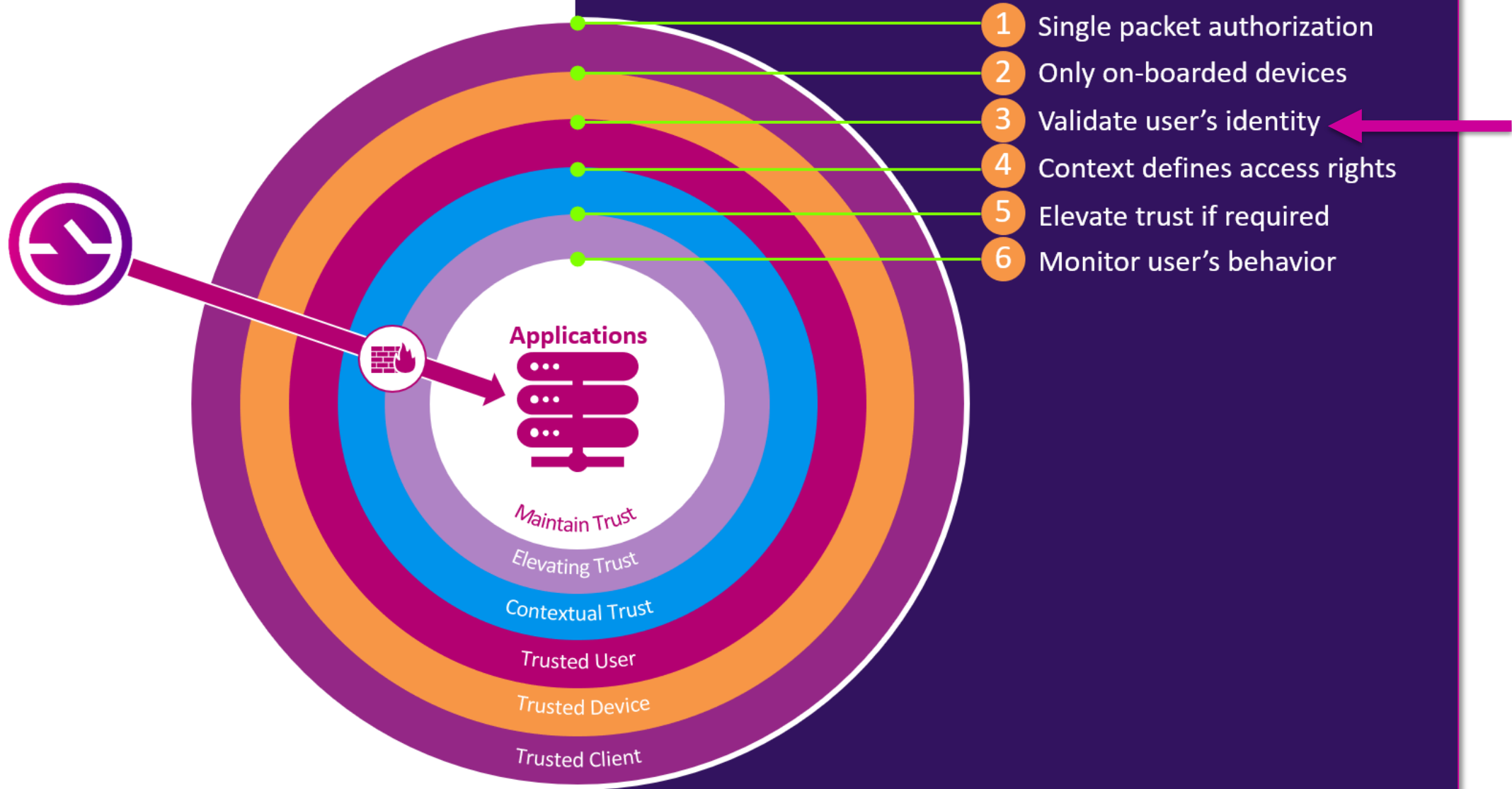
Active Directory/Radius

Demo: Onboarding

Lab: Creating a Policy for AD users

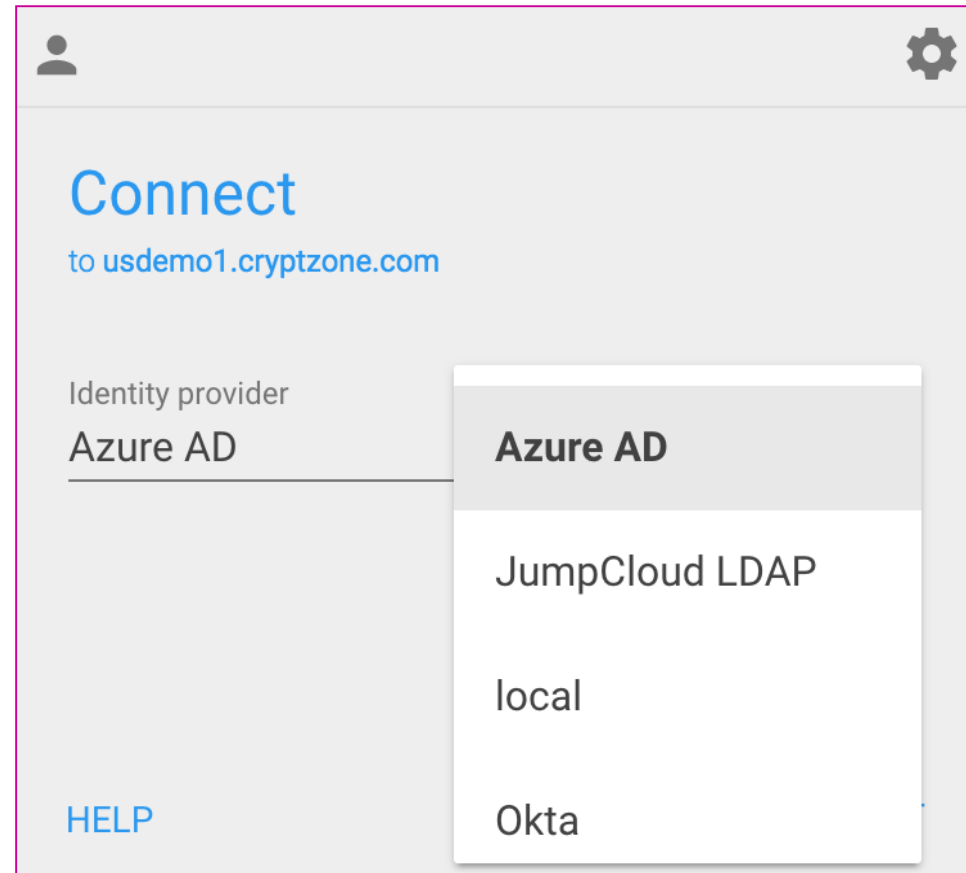


You are here



User Sources

- Built-in
 - Local user accounts
- Integrated
 - LDAP/Active Directory
 - Radius
 - SAML



Identity Provider (IdP)

- Validates login information
 - Username & Passwords, Certificates.
- Built-in IdP for local users
- SAML, LDAP, LDAP with Certificate and Radius support
- Source for user claims
 - Attributes such email, groups, age, location are mapped as claims
- Admin can configure attribute mapping

Local User Database

AppGateSDP
Access, evolved.

Local user database

- During installation, two users are created
 - cz (ssh)
 - admin (GUI access via TCP 444)

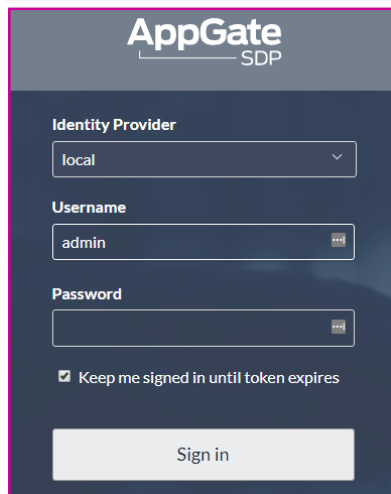
```
Configure administrator passwords

The "cz" user is a Linux user account on this particular appliance. Using this account, you can log in on the console or over SSH, and run administrative
commands with sudo.

The "admin" user is used to log in to the controller's web-based management interface.

Both passwords need to be defined.

Password for "cz" user:
Password for "admin" user:
```



The image shows the AppGate SDP login web interface. It features a dark blue header with the 'AppGate SDP' logo. Below the header, there is a 'local' dropdown menu for the Identity Provider. The Username field contains 'admin' and the Password field is empty. A checkbox labeled 'Keep me signed in until token expires' is checked. A 'Sign in' button is at the bottom.

```
λ ssh cz@192.168.42.111
Authorized uses only. All activity may be monitored and reported.
cz@192.168.42.111's password:
Last login: Tue Feb  6 08:34:35 2018
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-35-generic x86_64)
AppGate 3.2.2-7203-release (image1)
Hint: run 'sudo cz-setup' for appliance management.
cz@sdp1:~$ whoami
cz
```

Local user database (Cont.)

- Users can be added/managed/removed locally
- Often used for admin accounts
- Has the same capabilities as external IdPs
- Best Practice: add admins (see [Admin Guide - Admin Roles](#))

Appliances Sites IP Pools Identity Providers MFA Providers Admin Roles					
Identity Providers					
				Total Identity Providers 3	Q Search + Add New
Name ↓	Type	Client UI	Admin UI	Tags	Modified
local	Local	✓	✓	builtin	12/15/2017, 1:23:59 PM

External User Database (Identity Providers)

AppGateSDP
Access, evolved.

External user database

- AppGate supports
 - LDAP/Active Directory (AD)
 - Radius
 - Security Assertion Markup Language (SAML)

Appliances	Sites	IP Pools	Identity Providers	MFA Providers	Admin Roles
Identity Providers			Total Identity Providers 3		Q Search + Add New
Name↓	Type	Client UI	Admin UI	Tags	Modified
local	Local	✓	✓	builtin	12/15/2017, 1:23:59 PM
LDAP	Ldap	✓	✓		12/15/2017, 2:35:27 PM
Free-Radius	Radius	✓	✓		4/12/2018, 1:28:55 PM

External user database

- AppGate SDP Supports
 - LDAP/Active Directory (AD)
 - Radius
 - Security Assertion Markup Language (SAML)

External user database – LDAP/AD

< Editing Identity Provider

Name
LDAP

Display name
LDAP

Notes

DNS Servers + Add new
192.168.42.43 **will be used by AppGate Client**

DNS Search Domains + Add new
appgate.lab

☐ Block Local DNS Requests

IPv4 Pool
42_network **will be used by AppGate Client**

IPv6 Pool
Select an IP Pool

External user database – LDAP/AD cont'd

Required items

- On-boarding Mode
- Where to use

On-boarding mode

☐ Enabled - No cookie verification

☒ Enabled

☐ Require Multi-factor authentication

☐ Disable on-boarding for new devices

Multi-factor authentication configuration (Select "Require Multi-factor authentication" to enable)

On-boarding MFA Provider

Select an MFA Provider ▼

On-boarding MFA Message

Administrative authorization requires two-factor authentication. Please use your device to log in.

Where to use

☒ Client

☒ Admin UI

☐ Use as default

External user database – LDAP/AD cont'd

LDAPS (recommended) is supported via X.509 Certificate

Where to use

☒ Client

☐ Admin UI

☐ Use as default

Hostnames or IP Addresses

192.168.42.43

Add new

Port

636

☒ Enable SSL

Certificate

-----BEGIN CERTIFICATE-----
MIIFZzCCA0+gAwIBAgIQGj6XweSPhZIH zdeLY7E/AzANBgkqhkiG9w0BAQ0FADBG
MRMwEQYKCZImiZPyLQG BGRYDbGF iMRcwFQYKCZImiZPyLQG BGRYHYXBwZ2F0ZTEW
MBQGA1UEAxMN YXBwZ2F0ZS1BRC1DQTAeFw0xNzAxMTYwOTA4MzlaFw0yMjAxMTYw
OTE4MzdaMEYx EzARBgoJkiaJk/IsZAEZFgNsYWVx FzAVBgoJkiaJk/IsZAEZFgdh
-----END CERTIFICATE-----

Choose a file...

External user database – LDAP/AD cont'd

Service Account DN	<input type="text" value="cn=sdp,OU=AppGate admins,dc=appgate,dc=lab"/>
Service Account Password	<input type="password" value="•••••"/>
Base DN	<input type="text" value="dc=appgate,dc=lab"/>
Object Class	<input type="text" value="user"/>
Username Attribute	<input type="text" value="sAMAccountName"/>
Membership Filter	<input type="text" value="(objectCategory=group)"/>
Membership Base DN	<input type="text" value="Distinguished Name of group search base in Active Directory. Leave empty to use Base DN."/>

External user database – LDAP/AD cont'd

Test your access!

1. LDAP(S)

DeleteCloneTest connectionCancelSave

AppliancesSitesIP PoolsIdentity ProvidersMFA ProvidersAdmin Roles

< Editing Identity Provider

Test succeeded

Name

LDAP

Identity Providers

Total Identity Providers 3SearchAdd New

Name ↑	Type	Client UI	Admin UI	Tags	Modified
Free-Radius	Radius	✓	✓		4/12/2018, 1:28:55 PM
LDAP	Ldap	✓	✓		6/1/2018, 12:35:22 PM
local	Local	✓	✓	builtin	12/15/2017, 1:23:59 PM

Test

2. Test a User

External user database – LDAP/AD cont'd

Test your access!

Test Users

Provide an username and it will be tested using LDAP

Username

zahir

Identification test succeeded

The user **zahir** is able to authenticate using provider **LDAP**. Once logged in, the following attributes will be mapped and available within Policies, Criteria Scripts, Conditions and Entitlement Scripts.

Mapped

firstName	zahir
groups	["CN=third party,CN=Users,DC=appgate,DC=lab"]
userId	69c0d0ea-0cf6-42e9-a23f-a56f5fcf3908
ag	{"identityProviderId": "49d078ea-a3e4-46db-a56a-0255002769ba"}
username	zahir

External user database

AppGate SDP supports

- LDAP/Active Directory (AD)
- **Radius**
- Security Assertion Markup Language (SAML)

External user database – Radius cont'd

Required items:

- Name/Display Name
- DNS
- IP Pool

The screenshot shows a configuration page for an external user database named 'Free-Radius'. The page includes fields for Name, Display name, and Notes. Below these are sections for DNS Servers and DNS Search Domains, each with an 'Add new' button. There is also a checkbox for 'Block Local DNS Requests'. At the bottom, there are dropdown menus for 'IPv4 Pool' (set to 'AppGate-Lab') and 'IPv6 Pool' (set to 'Select an IP Pool').

Name

Free-Radius

Display name

Free-Radius

Notes

DNS Servers

192.168.42.43

+ Add new

DNS Search Domains

appgate.lab

+ Add new

☐ Block Local DNS Requests

IPv4 Pool

AppGate-Lab

IPv6 Pool

Select an IP Pool

External user database – Radius cont'd

Required items

- On-boarding Mode
- Where to use

On-boarding mode

☐ Enabled - No cookie verification

☒ Enabled

☐ Require Multi-factor authentication

☐ Disable on-boarding for new devices

Multi-factor authentication configuration (Select "Require Multi-factor authentication" to enable)

On-boarding MFA Provider

Select an MFA Provider ▼

On-boarding MFA Message

Administrative authorization requires two-factor authentication. Please use your device to log in.

Where to use

☒ Client

☒ Admin UI

☐ Use as default

External user database – Radius cont'd

Required items

- Hostname/IP
- Shared Secret
- Authentication protocol

Hostnames or IP Addresses

+ Add new

192.168.42.42

Port

1812

Shared secret

.....

Authentication Protocol

☒ PAP☐ CHAP

Map Attributes to User Claims

+ Add new

User-Name mapped to claim username

Map On-demand Device Claims

+ Add new

Click here or Add new to populate the list

Tags

+ Add new

Click here or Add new to populate the list

DeleteCloneTest connection

CancelSave

External user database – Radius cont'd

Test your access!

The screenshot displays the 'Editing Identity Provider' page in the Cyxtera management console. The top navigation bar includes links for Appliances, Sites, IP Pools, Identity Providers (selected), MFA Providers, and Admin Roles. A green success banner at the top of the form area reads 'Test succeeded' with a checkmark icon. The form contains three fields: 'Name' with the value 'Free-Radius', 'Display name' with the value 'Free-Radius' and a toggle icon, and a large empty 'Notes' text area.

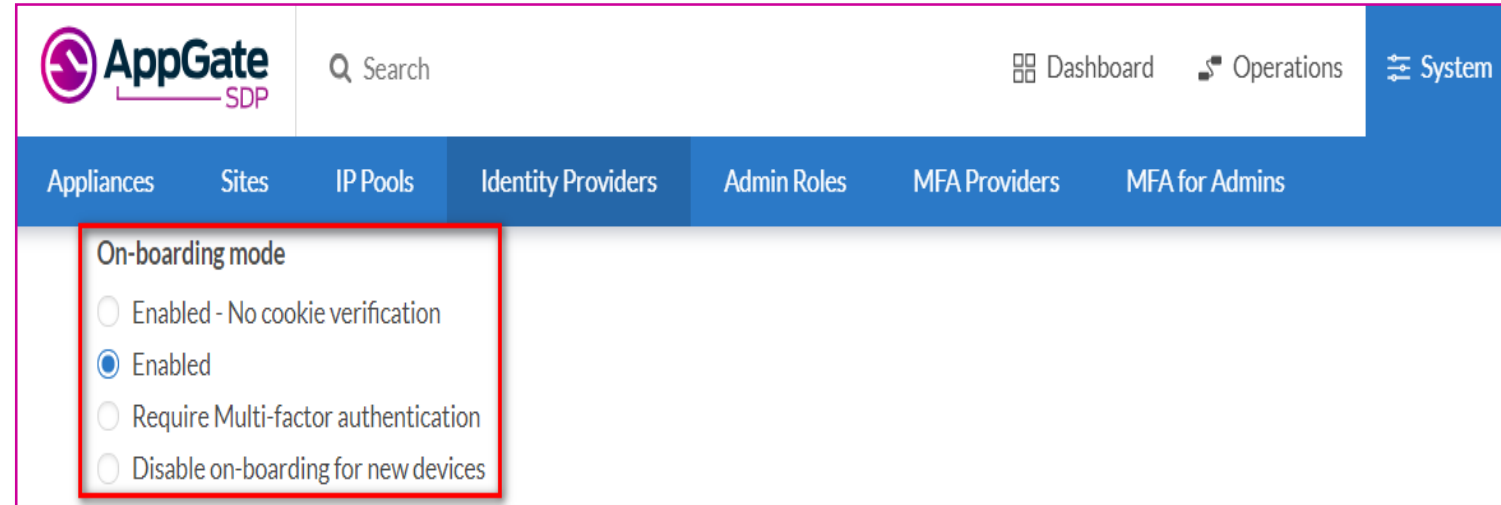
Appliances	Sites	IP Pools	Identity Providers	MFA Providers	Admin Roles
<p>< Editing Identity Provider</p> <p>Test succeeded</p> <p>Name Free-Radius</p> <p>Display name Free-Radius</p> <p>Notes</p>					

On-Boarding

AppGateSDP
Access, evolved.

Device On-Boarding

- Configured per IdP
 - One group of users (admins) might be allowed to use any devices while others require on-boarded devices
- Controls the inventory of allowed devices
- Controller sends a cookie to the device
 - Added Security with optional 2FA allows self-registration
- Environment lockdown possible



The screenshot displays the AppGate SDP web interface. The top navigation bar includes the AppGate SDP logo, a search bar, and links for Dashboard, Operations, and System. Below this is a secondary navigation bar with tabs for Appliances, Sites, IP Pools, Identity Providers, Admin Roles, MFA Providers, and MFA for Admins. The 'Identity Providers' tab is selected, and a configuration panel for 'On-boarding mode' is shown. This panel contains four radio button options: 'Enabled - No cookie verification', 'Enabled' (which is selected), 'Require Multi-factor authentication', and 'Disable on-boarding for new devices'.

On-boarding mode
<input type="radio"/> Enabled - No cookie verification
<input checked="" type="radio"/> Enabled
<input type="radio"/> Require Multi-factor authentication
<input type="radio"/> Disable on-boarding for new devices

Device On-Boarding (Cont'd)

- **Enabled - No cookie verification**
 - Controller will send another cookie if the client doesn't have one
- **Enabled**
 - First login, controller will silently send the cookie
 - Controller will require cookie in following connections
- **2FA Required**
 - First login, controller will require 2FA to send the cookie
- **Disabled**
 - Controller will not issue any **new cookie**
 - Existing cookies will work
- **Cookies stored on OS User Context**
 - Credential manager or Keychain

On-Boarding Demo

AppGateSDP
Access, evolved.

Multi-Factor Authentication (MFA)

AppGateSDP
Access, evolved.

Multi-Factor Authentication Providers

- Validates MFA input
- Built-in Time Based OTP and Radius support
- Not full Radius implementation?
 - But works with Nordic Edge, SecurID

Built-in Time Based OTP

- SDP has a built-in time-based OTP
- 30 seconds window to enter OTP
 - <https://time.is> good way to check sync
- Compatible with almost every OTP app
 - Google Authenticator, Microsoft Authenticator, 100x other app
- Max drift between OTP device and system (5 min)

OTP First Time Use Demo

AppGateSDP
Access, evolved.

Setup MFA Provider

PolicesConditionsEntitlementsRingfence Rules

< Editing Condition

Name

OTP

Notes

2 Factor Authentication for accessing CRM resources

Conditional Access

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

Provided MFA named OTP at most 60 minutes ago

Time is between 08:00 and 17:00 in UTC 24H format

User Interactions

Require MFA named OTP with text "Please Enter your OTP token "

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

Click here or Add new to populate the list

DeleteCloneTestCancelSave

Cyxtera

CYXTERA PROPRIETARY

CYXTERA TECHNOLOGIES CONFIDENTIAL | PROVIDED UNDER NDA 38

Attach OTP Condition to Entitlement

PoliciesConditionsEntitlementsRingfence Rules

< Editing Entitlement

Name

Distribution

Display name

Distribution

Notes

Status

Enabled

Disabled

Site

Default Site

Actions

#0 - ALLOW TCP up to distribution.packnot.lab on port 80

Add new

Condition

If all of the following conditions are true, then the entitlement is applied:

OTP

Add new

Tags

Click here or Add new to populate the list

Add new

Delete

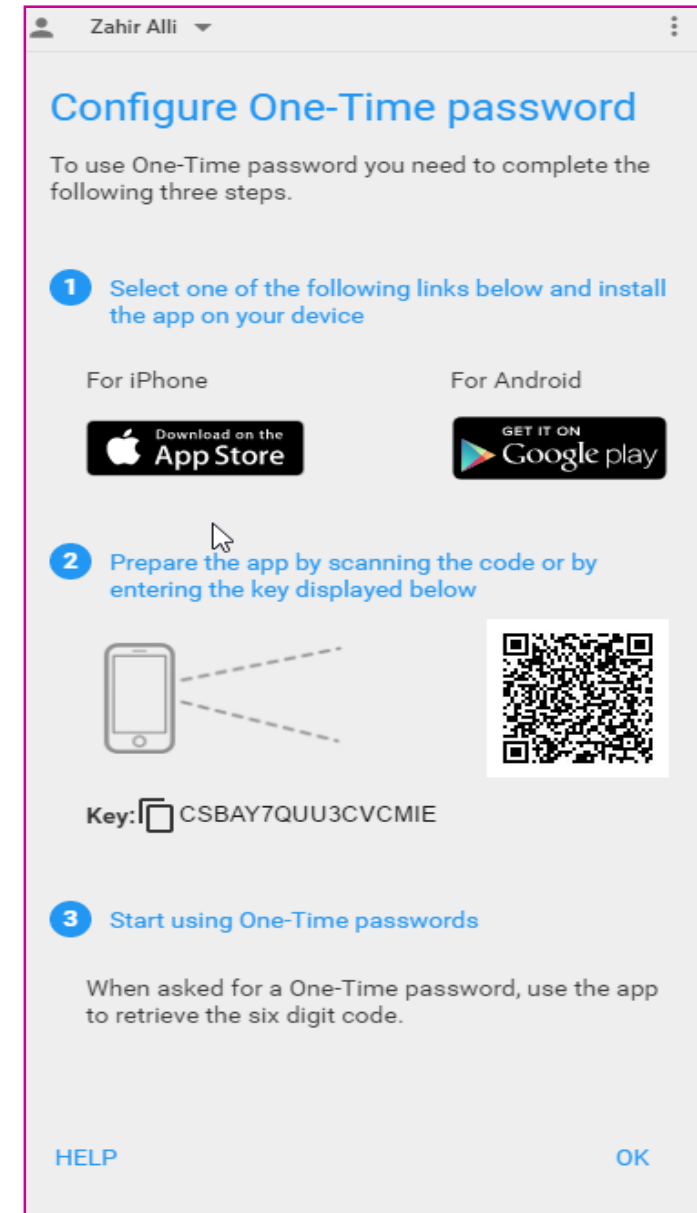
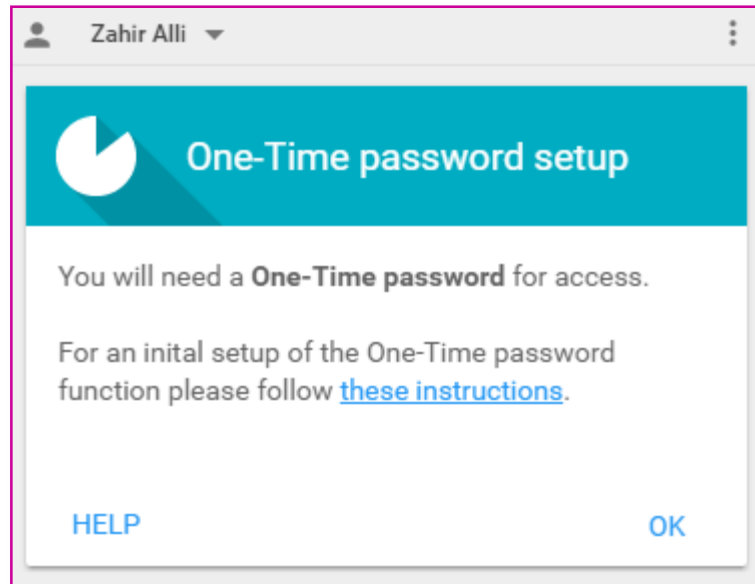
Clone

Cancel

Save

Verify OTP Condition

- Connect with the AppGate SDP Client



Labs 3 and 4

AppGateSDP
Access, evolved.

Configuring Identity & Authentication Providers

AppGateSDP
Access, evolved.

Cyxtera proprietary