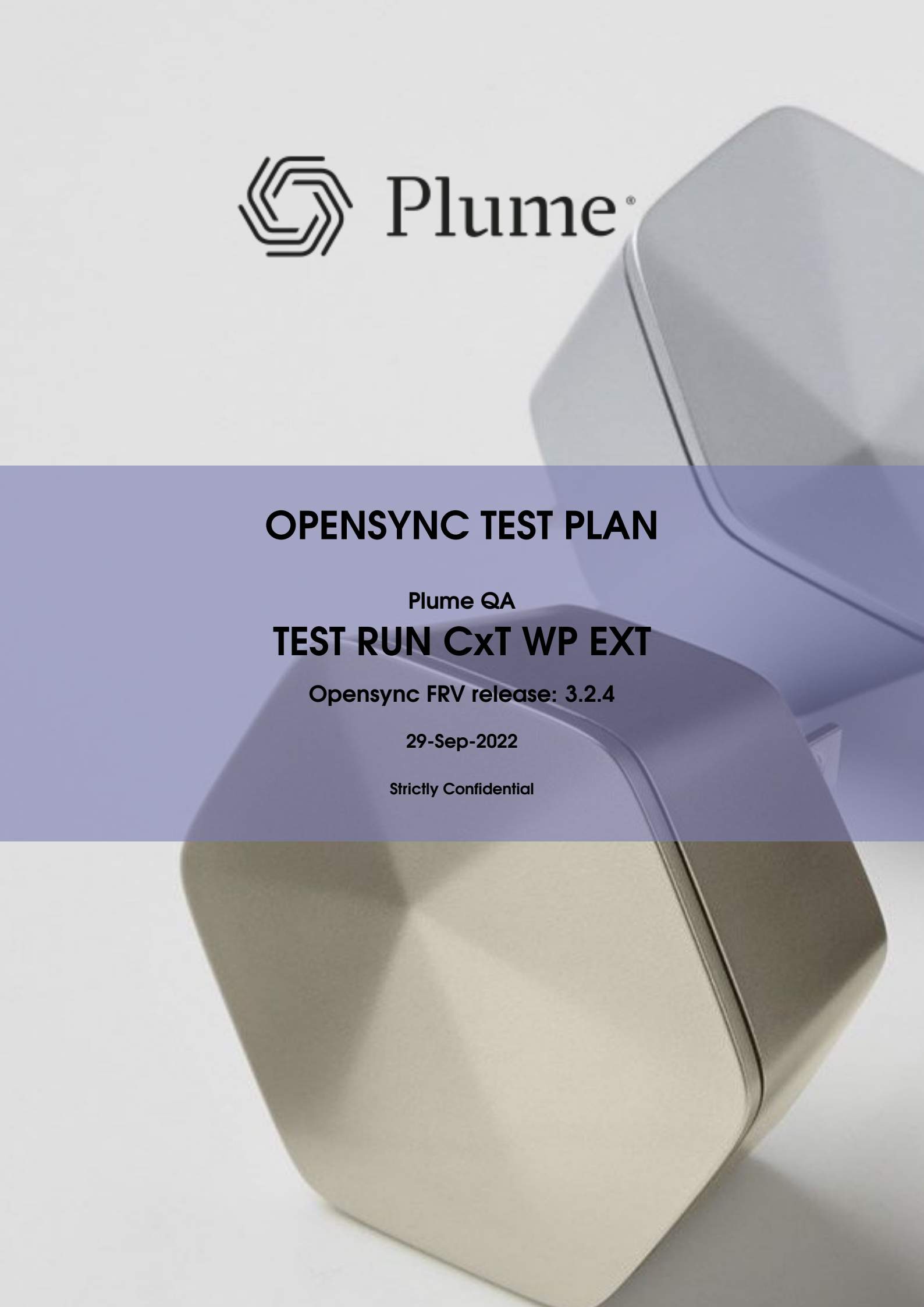


OPENSYNC TEST PLAN

Plume QA

TEST RUN CxT WP EXT

Opensync FRV release: 3.2.4

29-Sep-2022

Strictly Confidential

PUBLISHED BY PLUME
PLUME.COM

Contents

1 WorkPass 5
1.1 Onboarding iOS 5
1.2 Onboarding Android 7
1.3 Reset password - iOS 8
1.4 Reset password - Android 9
1.5 Support pages 10
1.6 Home screen information 11
1.7 Network Health 12
1.8 Login 13
1.9 Security 14
1.9.1 Online protection 14
1.9.1.1 Security Events 14
1.10 Employee zone 15
1.10.1 Adding an employee 15
1.10.2 Employee profile 17
1.10.3 Employees at work 18
1.10.4 Time at work 19
1.10.5 Most used apps 20
1.10.6 Data usage 21
1.10.7 Connection timeout 22
1.10.8 Online activity 23
1.10.9 Client information 24
1.11 Link 25
1.11.1 Networking features 25
1.11.1.1 Secure zone SSID 25

1.11.1.2 Employee zone SSID . . . 26
1.11.1.3 Networking mode . . . 27
1.11.1.4 UPnP Port Forwarding - ROUTER mode . . . 28
1.11.1.5 Port Forwarding - ROUTER mode . . . 30
1.11.2 Management . . . 31
1.11.2.1 Pinging between Zones . . . 31
1.11.2.2 Shared access between groups - Printer . . . 32
1.11.2.3 Shared access between groups - Virtual environment . . . 33
1.11.2.4 Adding an admin . . . 34
1.11.3 Bandwidth throttling . . . 35
1.11.3.1 Bandwidth throttling . . . 35
1.11.3.2 Subnet usage . . . 36
1.11.4 Devices . . . 37
1.11.4.1 Blocking clients - Secure Zone . . . 37
1.11.4.2 Blocking clients - Employee Zone . . . 38
1.11.4.3 Approving clients - Secure Zone . . . 39
1.11.4.4 Approving clients - Employee Zone . . . 40
1.12 Guest Zone . . . 41
1.12.1 Data usage statistics . . . 41
1.12.2 Repeating guest connections . . . 42
1.12.3 Guest analytics . . . 43
1.12.4 Most used apps . . . 44
1.12.5 Online activity . . . 45
1.13 Shield . . . 46
1.13.1 Content access . . . 46
1.13.1.1 Blocking websites - per employee . . . 46
1.13.1.2 Approving Websites - per employee . . . 47
1.13.1.3 Approving websites - company wide . . . 48
1.13.1.4 Blocking websites - company wide . . . 49
1.14 Secure Zone . . . 50
1.14.1 Data usage . . . 50
1.14.2 Devices . . . 51
1.14.2.1 Client groups . . . 51
1.14.2.2 Client information . . . 52
1.14.3 Timeouts . . . 53
1.14.3.1 Connection timeout . . . 53
1.14.3.2 Timeout adjustments . . . 54
1.14.4 Captive portal . . . 55
1.14.4.1 Create and edit captive portal . . . 55
1.14.5 3rd party login . . . 56
1.14.5.1 Login via Free Wi-Fi . . . 56
1.14.5.2 Login via Email . . . 57
1.14.5.3 Login via Passcode . . . 58
1.14.5.4 Login via Facebook Login . . . 59
1.14.6 Timeouts . . . 60
1.14.6.1 Connection timeout . . . 60
1.14.6.2 Timeout adjustments . . . 61

1. WorkPass

1.1 Onboarding iOS

Case ID

C1906027

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup – connect 1 node as GW and 2 nodes as leaf nodes
2) Clients:
– 1x iOS smartphone client with WorkPass app installed
– 1x iOS client
– 1x Linux client
– 1x Windows client
– 1x macOS client
– 1x Android client

Test Steps

1) Open the WorkPass app
2) Tap the "Set up Plume" button and start the new account setup
3) Enter your e–mail and password
4) Verify your e–mail
5) Log into the newly created account
6) Go through the onboarding procedures and claim the nodes
7) Claim the nodes through BLE
8) Once all nodes are successfully claimed, create a Secure Zone SSID and password through the app

9) Set up the employee zone SSID and password
10) Set up the guest zone SSID and bandwidth limit
11) Check that all SSID's are discoverable with your clients
12) Claim any additional nodes if required
13) Check that you can connect clients to Secure and Employee Zone
14) Check that connecting a client to Guest Zone prompts a login through captive portal

Expected Results

1, 2, 3, 4, 5) Account setup works as expected, email can be verified
6, 7) AP nodes are onboarded and come online
8) Secure zone is setup successfully
9) Employee zone is setup successfully
10) Guest zone is setup successfully
11) All 3 SSID's are discoverable
12) Any additional nodes are onboarded and come online
13) Clients can connect to all zones with network key matching SSID
14) Guest zone connection asks to log in through captive portal

1.2 Onboarding Android

Case ID

C1906028

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup – connect 1 node as GW and 2 nodes as leaf nodes
2) Clients:
– 1x Android smartphone client with WorkPass app installed
– 1x iOS client
– 1x Linux client
– 1x Windows client
– 1x macOS client
– 1x Android client

Test Steps

1) Open the WorkPass app
2) Tap the "Set up Plume" button and start the new account setup
3) Enter your e–mail and password
4) Verify your e–mail
5) Log into the newly created account
6) Go through the onboarding procedures and claim the nodes
7) Claim the nodes through BLE
8) Once all nodes are successfully claimed, create a Secure Zone SSID and password through the app
9) Set up the employee zone SSID and password
10) Set up the guest zone SSID and bandwidth limit
11) Check that all SSID's are discoverable with your clients
12) Claim any additional nodes if required
13) Check that you can connect clients to Secure and Employee Zone
14) Check that connecting a client to Guest Zone prompts a login through captive portal

Expected Results

1, 2, 3, 4, 5) Account setup works as expected, email can be verified
6, 7) AP nodes are onboarded and come online
8) Secure zone is setup successfully
9) Employee zone is setup successfully
10) Guest zone is setup successfully
11) All 3 SSID's are discoverable
12) Claim any additional nodes if required
13) Clients can connect to all zones with network key matching SSID
14) Guest zone connection asks to log in through captive portal

1.3 Reset password - iOS

Case ID

C1906031

Test type

None

Test case coverage

None

Preconditions

Preconditions:
1) Initial test environment setup
2) Clients:
– 2x iOS smartphone client with WorkPass app installed and logged in

Test Steps

On Client A:
1) Sign out under Settings–>Account, then tap sign in
2)Tap "Tap here", and then "Forgot password"
3) Enter your email and tap "Reset password"
4) Tap "Open email app" and log into your email
5) Open the email from "Plume Support" and tap "Reset now"
6) Enter the new password and tap "Submit" and then "Log in to Plume"
7) Log in to the app with the new password
On Client B:
8) Check if the 2nd phone was logged out

Expected Results

Client A:
1) The sign in screen opens
2) You are moved to the enter your email screen
3) The email input works
4) "Open email app" redirects you to the email app on your phone
5) The "Reset Password" button redirects you to the Reset Password page
6) New password is successfully accepted and saved
7) You can log into the app successfully with the new password
Client B:
8) The second phone logs out, and is able to log back again

1.4 Reset password - Android

Case ID

C2029125

Test type

None

Test case coverage

None

Preconditions

Preconditions:
1) Initial test environment setup
2) Clients:
– 2x Android smartphone client with WorkPass app installed and logged in

Test Steps

On Client A:
1) Sign out under Settings–>Account, then tap sign in
2)Tap "Tap here", and then "Forgot password"
3) Enter your email and tap "Reset password"
4) Tap "Open email app" and log into your email
5) Open the email from "Plume Support" and tap "Reset now"
6) Enter the new password and tap "Submit" and then "Log in to Plume"
7) Log in to the app with the new password
On Client B:
8) Check if the 2nd phone was logged out

Expected Results

Client A:
1) The sign in screen opens
2) You are moved to the enter your email screen
3) The email input works
4) "Open email app" redirects you to the email app on your phone
5) The "Reset Password" button redirects you to the Reset Password page
6) New password is successfully accepted and saved
7) You can log into the app successfully with the new password
Client B:
8) The second phone logs out, and is able to log back again

1.5 Support pages

Case ID

C1910042

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed

Test Steps

On each client:
1) Log into the WorkPass app
2) Go to Settings –> Support
3) Tap on all the links in the Support and About App section

Expected Results

1) The app opens successfully
2) The Support page opens
3) All links work as expected

1.6 Home screen information

Case ID

C1910069

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Android/iOS client connected to the Employee zone and assigned as a primary device of an employee.
– 1x Android/iOS client connected to the Guest zone.
3) Network has been up for at least 3 hours, and has been in regular use by users (browsing sites, using online apps)
4) Ensure that Autocheck ISP speed option in Settings – > More Is turned on
5) For the Guest zone and Employee zone clients consult the Captive portal and Employee zone section of tests if required. The Network health section only shows up after an AUTOMATIC speed test has been completed.

Test Steps

1) Open the WorkPass app
2) Check that the appropriate location name shows up
3) In Settings –> Shield enable Work appropriate Content access, Online protection and Adblocking
4) Browse the internet for a while
5) Check that the security overview shows events and that the filters work
6) Check if the device connected to Guest Wi–Fi shows up in the Guests tab
7) Check if the employee that the device is linked to shows up as ’at work’ in Employee zone

Expected Results

1) WorkPass opens
2) The Location name is correct
3) The shield settings apply successfully. If they were set per employee beforehand, they show as "custom"
4) Internet browsing works and you cannot access non–work appropriate websites
5) Security events show up and the filters display only the relevant security events
6) The connected device shows up as active on Guest Wi–Fi
7) The employee shows up as ’at work’

1.7 Network Health

Case ID

C2029128

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
3) Network has been up for at least 3 hours, and has been in regular use by users (browsing sites, using online apps)
4) Ensure that Autocheck ISP speed option in Settings – > More Is turned on

Test Steps

1) Go to the WorkPass app and run a manual speed test under the Network Health tab
2) Wait about 5–10 minutes
3) Go to the Network Health tab and check if it shows the speed test
4) Disconnect a leaf node and check if the Network Health tab updates (notices that the node was disconnected) after 60 seconds
5) Disconnect all nodes and check if the Network Health tab page updates (notices that the network is offline) after 60 seconds

Expected Results

1) Manual Speed test runs
3) Network health shows the network download/upload speed and time of last speed test
4) The Network Health tab shows how many nodes are online and offline
5) The Network Health tab shows no nodes found and network offline. The network tab shows a Network Outage warning

1.8 Login

Case ID

C1910107

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed

Test Steps

1) Log out of the WorkPass app if logged in
2) Log in via email and password
3) Log out of the WorkPass app
4) Log in via magic link

Expected Results

1) The app login page appears after log out/when opening app
2) The location successfully loads
3) The app login page appears after log out
4) The location successfully loads

1.9 Security

1.9.1 Online protection

1.9.1.1 Security Events

Case ID

C1906040

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x client, connected to the network
3) If your client visits blocked page, note the following: In case you do not get so called "police lady" or Plume message that states access was blocked, note the following in the test case result: device, OS, browser

Test Steps

1) Enable Online protection, Adblocking and set Contect access to Work appropriate in the settings
2) Block at least one website in the shield tab, that is work appropriate
3) Visit the blocked webpage, non work appropriate pages and browse the internet in general for 15 minutes
4) Check the app's Security events and make sure the events are logged (All security events, Ad blocking, Online protection, and Content Access)
5) Use the different filters and see if the chart updates

Expected Results

1) All settings apply correctly –> NOTE: In case you do not get so called "police lady" or Plume message that states access was blocked, note the following in the test case result: device, OS, browser
2) Website is blocked without an error message popping up
3) Unable to access websites and some ads are blocked
4) Events are logged (Check the filters and the timestamps – they should match with your browsing)
5) Only the filtered events are shown

1.10 Employee zone

1.10.1 Adding an employee

Case ID

C1909947

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x macOS client, connected to the Employee zone
– 1x Windows client, connected to the Employee zone
– 1x iOS/Android smartphone client, connected to the Employee zone

Test Steps

1) Open the WorkPass app
2) Move to the Employee Zone and press the plus button in the upper right corner, then Add employee
3) Add Employee photo and name
4) Select some Shield settings
5) Assign at least one client to this new employee
6) Click "Next" and select a Primary device
7) Press "Save" and check that the new Employee has been successfully created
8) Create another Employee with a different client
9) Select different Shield settings than for the first employee
10) Assign more than 1 client to this Employee
11) Press "Next" and select a Primary device, different from the first employee
12) Press "Done" and check that both Employees are successfully added
13) Check both newly created Employees' settings and confirm they match with what you selected during the creation process
14) Add a third employee and assign the third device as a primary device to this employee

Expected Results

1) The WorkPass app opens
2) The new Employee screen opens
3) The name and picture are added successfully
4) The settings show as applied on the new Employee screen
5) The client gets a green tick next to it
6) The selected client is assigned as primary
7) The employee is created and shows in the Employee zone
8) The new Employee screen opens
9) The settings show as applied on the new employee screen
10) More than one client gets a green tick next to it
11) The selected client is assigned as primary

12) The employee is created and shows in the Employee zone
13) The employee data is the same as the data used in employee creation
14) All three employees show up in the Employee zone

1.10.2 Employee profile

Case ID

C1909945

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup.
2) Clients:
– 1x smartphone client with WorkPass app installed
3) A couple of Employee profiles already created (at least three).

Test Steps

1) Open the WorkPass app with your admin account
2) Move to the Zones tab and navigate to the Employee Zone screen
3) Click on some of the existing Employees
4) Check that their information is correct (devices, name, image, time at work status and analytics)
5) Edit one of the Employee's profile
6) Save the changes and check if the changes are correctly shown in the app

Expected Results

1) The WorkPass app opens
2) Employee Zone loads
3) Employee profile opens
4) The panels on the employee profile show information
5) Editing the employee profile as admin allows you to change all the fields
6) The changes are saved to the profile

1.10.3 Employees at work

Case ID

C1909944

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x macOS client, assigned to an employee as a primary device
– 1x PC Windows client, assigned to an employee as a primary device
– 1x iOS/Android smartphone client, assigned to an employee as a primary device

Test Steps

1) Connect the clients to the Employee Zone network
2) Assign the clients to three separate employees as a primary device
3) Check if the Employees at work shows all employees whose clients are currently connected to the network with their primary device
4) Check if the timestamp under the employee name on the main screen shows the time the client connected to the Employee zone network
5) Disconnect one client and check if the change is noted in the Employees at work feature

Expected Results

1) Clients connect to the Employee Zone
2) Devices assign successfully
3) The employees show up as at work
4) The timestamp shows the correct time – the time when the device connected to the network
5) The employee no longer shows up as at work

1.10.4 Time at work

Case ID

C1909946

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x macOS client
– 1x Windows client
– 1x iOS/Android smartphone client

Test Steps

1) Join the Employee zone SSID with a client that is assigned to an Employee and has only one client assigned to them
2) Use the network for a while and then disconnect the client from the Employee Zone SSID
3) Go to the Workpass app with your admin user account
4) Move to the Zones tab and select the Employee that just disconnected from the Employee Zone SSID
5) Check if "Time at work" shows the correct time for the Employee
6) Connect an Employee to the Employee Zone SSID that has multiple clients assigned to them
7) Disconnect the Employee's primary client from the Employee Zone SSID but leave the other(s) online
8) Move to the Employees in the app, again, and check if this Employee's Time at work is correct

Expected Results

1) Employee connects to the network with only and primary assigned client
2) Employee disconnects from the network and has no clients left on the network
5) Time at work shows correct time online (at work) for this employee
6) Employee with multiple assigned clients connects to the network successfully
7) Employee disconnects their primary client from the network and the employee is now not at work anymore
8) Employees screen in the app shows correct Time at work for employee with multiple clients

1.10.5 Most used apps

Case ID

C1909948

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x PC client, connected to the Employee zone network

Test Steps

1) Connect the PC client to the Employee zone
2) Check your the Most used apps for today, the last 30 days, and the last six months
3) On the PC client, use slack and upload/download a few files on it (at least 500mb)
4) After using the web application check your location's most used apps for today, the last 30 days, and the last six months

Expected Results

1) The client successfully connects to the network
2) All of the most used apps should match the actual apps used on the network
3) The web application works
4) The web application from step #3 shows up under the most used apps

1.10.6 Data usage

Case ID

C1911157

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x PC client, connected to the Employee zone network

Test Steps

1) Connect the PC client to the Employee zone
2) Check the data usage for today, the last 7, and the last 30 days
3) On the PC client, use slack and upload/download a few files on it (at least 500mb)
4) After using the web application check your location's data usage for today, the last 7, and the last 30 days
5) Press on the employee and check the data usage

Expected Results

1) The client successfully connects to the network
2) The data usage should match the actual data used on the network
3) The web application works
4) The data usage shows up in the data usage panel (increased by at least the file size)
5) The data usage increase matches on the employee screen matches the data usage increase on the employee zone screen

1.10.7 Connection timeout

Case ID

C1911154

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client

Test Steps

1) Connect all clients to the WiFi network Employee zone
2) Assign two of the clients to one of the employees
3) Timeout the assigned clients (Employee panel –> Pause button –> Set time out... –> Select timeout time)
4) Try accessing the internet on all clients
5) Cancel the timeout and timeout only one client
6) Try accessing the internet on all clients
7) Cancel the timeout

Expected Results

1) Clients connect to the Employee zone network
2) The clients are assigned successfully
3) The clients show as timed out
4) The two timed out clients cannot access the internet. The other client works as normal
5) The app shows only one assigned client as timed out
6) Only the timed out client cannot access the internet. The other two clients work as normal
7) All clients can access the internet

1.10.8 Online activity

Case ID

C1911160

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass installed
– 1x PC client, connected to the Employee zone network

Test Steps

1) Connect the PC client to the Employee zone
2) Assign the client to one of the employees
3) Check Online activity for today, the last 7 and the last 30 days for the employee with the assigned client
4) Check Most used apps for today, the last 7 and the last 30 days for the employee with the assigned client
5) On the PC client, use slack and upload/download a few files on it (at least 500mb)
6) After using the web application check the online activity for today, the last 7 and the last 30 days for the Employee with the assigned client

Expected Results

1) The client successfully connects to the network
3) The Online activity should match actual client activity for the employee
4) The most used apps should match actual client activity for the employee
5) The web application works
6) The type of web application (productivity for slack) from step #3 shows up under online activity with the correct time used

1.10.9 Client information

Case ID

C1911303

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass installed
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client connected via ethernet cable or Wi–Fi
– 1x Client, able to access Frontline
3) For clients use randomized MAC

Test Steps

1) Connect all client to the employee zone SSID
2) Check the client name, IP and mac address of the device in Frontline
3) Change the client name in the app and change to a different MAC address
4) Check the client name in the employee zone
5) Check the client name, IP Address and MAC address in Frontline
6) Repeat the steps for the other clients

Expected Results

1) All clients connect to the employee zone successfully
2) The client name, IP, and MAC Address are shown in Frontline
3) The client name and MAC Address are changed
4) The new client name shows in the employee zone panel
5) The new client name and MAC Address show in Frontline (IP may or may not change)

1.11 Link

1.11.1 Networking features

1.11.1.1 Secure zone SSID

Case ID

C1906029

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Linux PC client
– 1x macOS PC client
– 1x Windows PC client
– 1x Android smartphone client
– 1x iOS smartphone client

Test Steps

1) Connect all clients to Secure Zone SSID
2) Check if all clients connected to secure zone are shown correctly under Secure Zone section in WorkPass application
3) Change the Secure SSID password in Settings–>Secure Wi–Fi

Expected Results

1) Clients are shown in secure zone in the WorkPass App
2) All clients are shown correctly in Secure Zone section (device and device type)
3) All clients are booted off the network and are required to enter the new password

1.11.1.2 Employee zone SSID

Case ID

C1906030

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Linux client
– 1x macOS client
– 1x Windows client
– 1x Android smartphone client
– 1x iOS smartphone client

Test Steps

1) Connect all clients to employee zone
2) Check if all clients are shown and device typed correctly under employee zone section
3) Assign different clients to different employees (Also create employees, use assign to new employee... option)
4) Check if clients are correctly assigned to the employees
5) Change the Employee SSID password in Settings–>Employee Wi–Fi

Expected Results

1) Devices are shown in employee zone in the WorkPass App
2) All devices are shown in employee zone correctly
3) Clients can be assigned to employees
4) Clients are correctly shown under their assigned employee
5) All clients are booted off the network and are required to enter the new password

1.11.1.3 Networking mode

Case ID

C1910043

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup in bridge mode
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x PC or smartphone client connected to the WorkPass location
– 1x PC or smartphone client connected to the internet (can be same as above)

Test Steps

1) Log into the WorkPass app
2) Go to Settings –> Advanced Settings
3) Change networking mode from Auto(Bridge) to Router
4) Attempt to browse the internet
5) Go to settings –> advanced settings –> DNS tab
6) Change DNS (primary and secondary) to Google DNS (8.8.8.8 and 8.8.4.4) and try to connect to a website
7) Change networking mode back to Auto(Bridge)

Expected Results

1) The WorkPass app opens
2) The Advanced Settings screen opens
3) Networking mode changes successfully if you reenter the Advanced Settings screen
4) The clients can use the internet
6) The DNS Change is successful and shows in the Advanced Settings screen. Clients, connected to the location (Secure, Guest and Employee) can connect to various URLs
7) The Networking mode is set back to bridge

1.11.1.4 UPnP Port Forwarding - ROUTER mode

Case ID

C1910068

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup in router mode
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x client with access to frontline
– 1x client with Transmission app https://transmissionbt.com/ installed (Ubuntu has it by default)
– 1x client connected to the same network as the Gateway WAN connection (Not connected to network provided by Device under test)
3) Enable UPnP port forwarding:
Open Transmission then click Edit –> Preferences –> Network and check that Use UPnP / NAT–PMP port forwarding on the Advanced Settings screen is enabled, if not enable it
4) Enable Randomized port
Tick "Randomize port each time Transmission opens" –> Pick a random port whenever Transmission is started

Test Steps

1) Make sure UPnP is disabled (Settings–>Advanced settings)
2) Connect Client A to the secure/employee zone network
3) Open terminal on Client B connected to the same upstream subnet. Execute following command:
nmap –Pn <IP> –p <port>
<IP> is the WAN IP of the Node network (can be found under Pods & Nodes –> GW Pod –> WAN IP)

<port> is the port number shown in the menu in Transmission

4) Enable UPnP in the WorkPass app. (Settings–>Advanced settings)
5) Reconnect (disconnect and connect again) Client A to the plume network and reopen Transmission menu
6) Repeat step 3 – note that port is now different
7) Close Transmission
8) Repeat step 3 with port from step 6
9) Disconnect Client A and wait for 10 seconds
10) Check the port again on Client B

Expected Results

1) UPnP is disabled in WorkPass
2) Client A connects to secure/employee zone network

3) Port is filtered/closed
4) UPnP is enabled in the settings menu
5) Port used for incoming connection is different
6) Port is opened
7) Transmission closes
8) Port is filtered/closed
9) Client A disconnects
10) Port is filtered/closed

1.11.1.5 Port Forwarding - ROUTER mode

Case ID

C1910078

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup in router mode
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x client with ssh access setup, connected to the secure/employee zone
– 1x client connected outside of test network
3) Sometimes you need to wait a while in the app for options or clients to load
4) Port forwarding in the app is done under Advanced Settings –> Reservations & Port Forwarding –> NEW IP RESERVATION –> Wait until all clients from network are visible in the list below and pick one used for test –> Add a device –> go back to Reservations & port forwarding –> select previously created reservation –>Add a Port Assignment

Test Steps

1) Connect the first client to the secure/employee zone network
2) Connect the second client to an external network
3) With the second client try to ssh to the first client > $ ssh <client_username> @WAN_IP
4) Make an IP reservation (if not already done)
5) Forward the ports to the IP reservation
6) With the second client try to ssh to the first client > $ ssh <client_username> @WAN_IP

Expected Results

1) The first client successfully connects to the WiFi network.
2) The second client is successfully connected to an external network.
3) The second client can't ssh to the first client
4) The client IP is now reserved
5) The client port is open for outside traffic
6) The second client can ssh to the first client

1.11.2 Management

1.11.2.1 Pinging between Zones

Case ID

C1906032

Test type

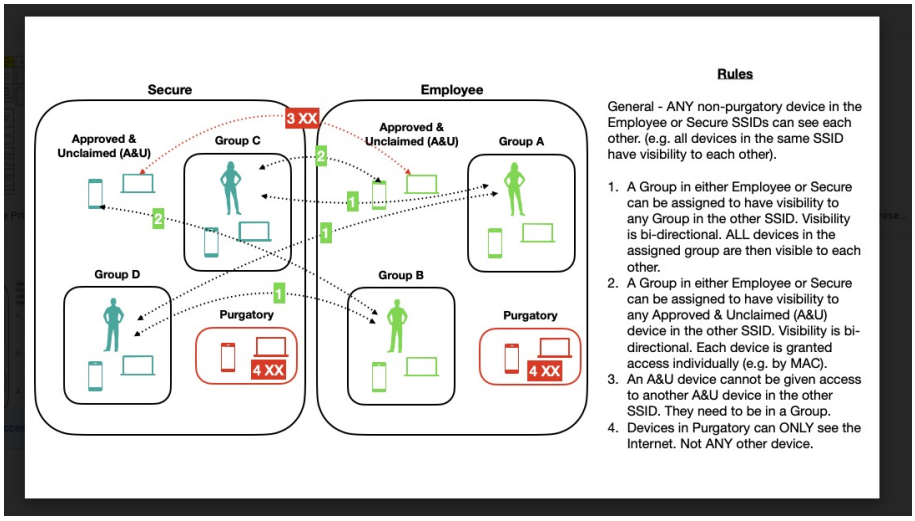
None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 3x PC or smartphone device



Test Steps

1) Connect client #1 to the Secure zone
2) Connect client #2 to the Employee zone
3) Connect client #3 to the Guest zone
4) Ping client #2 (Employee Zone) from client #1 (Secure Zone)
5) Ping client #3 (Guest Zone) from client #1 (Secure Zone)
6) Ping client #1 (Secure Zone) from client #2 (Employee Zone)
7) Ping client #3 (Guest Zone) from client #2 (Employee Zone)
8) Ping client #1 (Secure Zone) from client #3 (Guest Zone)
9) Ping client #2 (Employee Zone) from client #3 (Guest Zone)

Expected Results

1, 2, 3) Client connects successfully to the correct zone
4, 5, 6, 7, 8, 9) Clients cannot ping each other

1.11.2.2 Shared access between groups - Printer

Case ID

C1906885

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x PC client
– 1x WiFi–enabled printer client

Test Steps

1) Connect the printer client to the Secure zone
2) Connect the PC and Smartphone client to the Employee zone and assign them to an employee
3) From the smartphone and PC client (Employee zone) try pinging the printer client (Secure zone)
4) From the smartphone and PC client (Employee zone) try printing with the printer client (Secure zone)
4) Create a group with the printer client in the Secure zone and "share access" to the smartphone and PC clients in the Employee zone
5) From the smartphone and PC client (Employee zone) try pinging the printer client (Secure zone)
6) From the smartphone and PC client (Employee zone) try printing with the printer client (Secure zone)

Expected Results

1) The printer client connects to the Secure zone
2) The Smartphone and PC client connect to the Employee zone and are added to an employee
3) The ping doesn’t go through on both the smartphone and PC client
4) Both the smartphone and PC client CAN’T print with the printer
4) The group is created successfully
5) The ping goes through on both the smartphone and PC client
6) Both the smartphone and PC client CAN print with the printer

1.11.2.3 Shared access between groups - Virtual environment

Case ID

C1911159

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Windows client, connected to the secure zone
– 1x Windows client, connected to the employee zone

Test Steps

1) Connect the first Windows client, Client A to the Secure zone and the second Windows client, Client B to the employee zone
2) On Client A (in secure zone), go to Settings (write down the PC name and username –> top left in system menu) –> System –> Remote Desktop and tick Enable Remote Desktop
3) In the secure zone menu, find Client A, press on it and press MAC and IP address
4) Try to connect to Client A from Client B using the "Remote Desktop Connection" app and relevant IP
5) In Secure zone–>Devices, find Client A, click the three dots next to that device–> Share access, find Client B and select it on the left hand side and click Save
6) Try to connect to Client A from Client B using the "Remote Desktop Connection" app, relevant IP, and username

Expected Results

1) The clients successfully connect to their respective zones
2) The "Remote Desktop Connection" tick is green and says ON
3) Client A's IP and MAC Address are visible
4) The connection fails
5) Client A is successfully shared
6) The connection succeeds and Client B remotely logs into Client A

1.11.2.4 Adding an admin

Case ID

C1910041

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed. Can be the same as one of the below
– 1x iOS smartphone client
– 1x Android smartphone client

Test Steps

1) Open WorkPass and go to settings –> Account
2) Click on Invite new admin
3) Input the name and email of the new admin and press send
4) Log into the email of the new admin
5) Confirm the invitation
6) Log in as the new admin
7) Repeat for the other client

Expected Results

1) The account settings page opens
2) The Invite new admin screen opens
3) The admin shows up in the account screen with an invitation pending tag
4) The admin invitation email arrived
5) The app successfully registers the new admin
6) Log in works
7) All clients work as above

1.11.3 Bandwidth throttling

1.11.3.1 Bandwidth throttling

Case ID

C1906057

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x PC client

Test Steps

1) Go to WorkPass app and check the SpeedTest results one the home page, then navigate to Guest Zone settings
2) Set Bandwith limit to 10% of WAN speed
3) Connect clients to Guest Zone network
4) Run a speed test, stream videos
5) Disconnect clients from network and delete them in Frontline devices tab
6) Set Bandwith limit to 25% of WAN speed
7) Connect the same clients to Guest network
8) Run a speed test, stream videos

Expected Results

1) The SpeedTest numbers are shown.
2) You are able to set the bandwidth limit
3) Clients connect to Guest Wi–Fi
4) The device should use ~10% of the bandwidth compared to the reference numbers. The combined bandwidth usage of all devices should not exceed ~10% of the reference numbers
5) Clients are removed from Frontline
6) You are able to set the bandwidth limit
7) Clients connect to Guest network
8) The device should use 25% of the bandwidth compared to the reference numbers. The combined bandwidth usage of all devices should not exceed ~25% of the reference numbers

1.11.3.2 Subnet usage

Case ID

C1906058

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x PC client, connected to the guest zone
– 1x smartphone client, connected to the employee zone
– 1x smartphone client, connected to the secure zone

Test Steps

1) Connect at least one client to each zone
2) Check secure zone/employee zone client are on a different subnet to the guest zone client

Expected Results

1) Clients connect to their respective zone Wi–Fi
2) Guest zone has its own subnet. Secure and employee zone share the same subnet

1.11.4 Devices

1.11.4.1 Blocking clients - Secure Zone

Case ID

C1906043

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client

Test Steps

1) Connect clients to the WorkPass Secure zone network
2) Access some online content with the clients
3) Block clients within the WorkPass app in Secure zone–>Devices, three dots near the device–>Block device
4) Check if clients can still access online content
5) Check if clients can ping addresses or each other

Expected Results

1) Clients connect to the Workpass network
2) Online content can be reached
3) Clients are blocked within the app
4) Clients no longer have internet access
5) Clients cannot ping each other or IPs outside the network

1.11.4.2 Blocking clients - Employee Zone

Case ID

C1910982

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client

Test Steps

1) Connect clients to the WorkPass Employee zone network
2) Access some online content with the clients
3) Block clients within the WorkPass app in Employee zone–>Devices, three dots near the device–>Block device
4) Check if clients can still access online content
5) Check if clients can ping addresses or each other

Expected Results

1) Clients connect to the Workpass network
2) Online content can be reached
3) Clients are blocked within the app
4) Clients no longer have internet access
5) Clients cannot ping each other or IPs outside the network

1.11.4.3 Approving clients - Secure Zone

Case ID

C1906044

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client

Test Steps

1) Enable Limited Network Access in the Secure Zone SSID settings
2) Connect all clients to the Secure Zone network
3) Check if push notifications for new clients are received
4) Approve one of the clients
5) Ping between an approved client and a non−approved client
6) Approve all devices
7) Ping between 2 clients that are now both approved

Expected Results

1) Limited Network Access is ON
2) All clients can connect to the Secure Zone
3) Push notifications come through successfully
4) Client is successfully approved
5) Clients cannot ping each other
6) All clients are successfully approved
7) Clients can now ping each other

1.11.4.4 Approving clients - Employee Zone

Case ID

C1910983

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client

Test Steps

1) Enable Limited Network Access in the Employee Zone SSID settings
2) Connect all clients to the Employee Zone network
3) Check if push notifications for new clients are received
4) Approve one of the clients
5) Ping between an approved client and a non−approved client
6) Approve all devices
7) Ping between 2 clients that are now both approved

Expected Results

1) Limited Network Access is ON
2) All clients can connect to the Employee Zone
3) Push notifications come through successfully
4) Client is successfully approved
5) Clients cannot ping each other
6) All clients are successfully approved
7) Clients can now ping each other

1.12 Guest Zone

1.12.1 Data usage statistics

Case ID

C1906046

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass installed
– 1x smartphone client, connected to the guest zone network
– 1x PC client, connected to the Guest zone network

Test Steps

1) Connect clients to the Guest Zone
2) Access different websites and applications (Slack, Gmail, ...) from devices through 24 and 48h
3) Check the data usage panel for today, the last 7, and the last 30 days

Expected Results

1) Clients connect to the Guest Zone
2) The guest zone network works correctly
3) The data usage panel updates and shows the data usage correctly

1.12.2 Repeating guest connections

Case ID

C1906047

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass installed
– 1x repeat smartphone client, connected to the Guest zone network
– 1x repeat PC client, connected to the Guest zone network
– 1x new smartphone client, connected to the Guest zone network
– 1x new PC client, connected to the Guest zone network

Test Steps

1) Over a period of 24 or 48h access different webpages and content with the repeat clients
2) During that time disconnect and reconnect clients a couple of times
3) Connect the other 2 clients to the Guest Zone for the first time
4) Check WorkPass Guest Zone and make sure repeated guests are marked differently than first time guests
5) Check if all devices show up in the Guest panel in the correct device group
6) Check the Devices by hour graph

Expected Results

1) The clients use the network without issues
2) The clients reconnect to the Guest network without going through the captive portal
3) The clients need to go through the captive portal to connect to the internet
4) The graph shows the new devices and the repeat devices differently
5) All devices show up in the guest panel under the correct device group
6) The graph updates with the correct amount of devices

1.12.3 Guest analytics

Case ID

C1906070

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x smartphone client, connected to the Guest zone network
– 1x PC client, connected to the Guest zone network

Test Steps

1) Connect the clients to the Guest zone network
2) Check the Average data use per session and Average session length panels in the Guest zone–>Guest analytics
3) Download a large file (100+ mb) with a client and browse the internet for a while
4) Check Avg data use per session and Average session length panels again

Expected Results

1) The clients successfully connect to the network
2) The Average data use per session and Average session length panels both show data
3) The file downloads successfully. The clients can use the network
4) Both panels show updated data compared to test step no. 2

1.12.4 Most used apps

Case ID

C1911156

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x PC client, connected to the Guest Zone network

Test Steps

1) Connect the PC client to the Guest zone
2) Check Most used apps for today, the last 30 days, and the last 6 months
3) On the PC client, use slack and upload/download a few files on it (at least 500mb)
4) After using the web application check your location's most used apps for today, the last 30 days, and the last 6 months

Expected Results

1) The client successfully connects to the network
2) All of the most used apps should match the actual apps used on the network
3) The web application works
4) The web application from step #3 shows up under the most used apps

1.12.5 Online activity

Case ID

C1911158

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x PC client, connected to the Guest zone network

Test Steps

1) Connect the PC client to the Guest zone
2) Check Online activity for today, the last 7, and the last 30 days
3) On the PC client, use slack and upload/download a few files on it (at least 500mb)
4) After using the web application check your location's online activity for today, the last 7, and the last 30 days

Expected Results

1) The client successfully connects to the network
2) Online activity should match actual client activity on the guest network
3) The web application works
4) The type of web application (productivity for slack) from step #3 shows up under online activity with the correct time used

1.13 Shield

1.13.1 Content access

1.13.1.1 Blocking websites - per employee

Case ID

C1906041

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client
3) The employee approved website list in the shield menu in the app is empty

Test Steps

1) Connect all devices to the employee zone WiFi network
2) Assign all devices to one employee
3) Try to connect to a work appropriate website (https://www.plume.com/) with all clients
4) In the shield tab, move to the block tab, press on the employee and block the website
5) Attempt to connect to the website
6) Unblock the website
7) Attempt to connect to the website again

Expected Results

1) Clients connect to the employee zone network
2) Clients are assigned to the correct employee
3) Connection is established successfully
4) The website is added to the blocked list for the employee
5) Attempting to connect to the website will show an "Access to this website is blocked" message only for the clients, assigned to the employee
6) The website is removed from the blocked list for the employee
7) Connection is established successfully

1.13.1.2 Approving Websites - per employee

Case ID

C1906042

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client
3) The employee approved website list in the shield menu in the app is empty

Test Steps

1) Connect all clients to the employee zone WiFi network
2) Assign all clients to 1 employee in the Employee zone
3) Make sure Content access in the employee profile settings is set to "Work appropriate"
4) Attempt to connect to a website that is not work appropriate with all clients
5) Go to the shield tab, then to the approve tab, press on the employee, and approve the website
6) Attempt to connect to the website again
7) Remove the approved website from the list
8) Attempt to connect to the website again

Expected Results

1) Clients connect to the employee zone WiFi network
2) Clients are assigned to the correct employee
3) The content access is set to "Work appropriate
4) Attempting to connect to the website will show a "Access to this website is blocked" message or fail at loading the website
5) The website is added to the approved list for the employee only
6) Only clients, assigned to the employee, can successfully access the website
7) The website is removed from the approved list
8) Attempting to connect to the website will show a "Access to this website is blocked" message or fail at loading the website

1.13.1.3 Approving websites - company wide

Case ID

C1906039

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client
3) The company approved website list in the shield menu in the app is empty

Test Steps

1) Access WorkPass app with a client that has admin access
2) Enable Work appropriate sites filter in the Settings menu
3) Connect one client to the Secure zone and try to access a non work appropriate website
4) Connect one client to Employee zone and try to access the same website
5) Connect one client to the Guest zone and try to access the same website
6) Go to the shield tab, approve tab and approve the website
7) Try to access the approved website with all clients
8) Remove the website from the approved websites list
9) Try to access the website with all clients

Expected Results

1) You can open the WorkPass app
2) The content filter shows "Work Approriate"
3) Clients in the Secure zone cannot access the website
4) Clients in Employee zone cannot access the website
5) Clients in Guest zone cannot access the website
6) The website is approved
7) All clients are able to access the approved website
8) The website is removed from the approved websites list
9) Clients in all zones cannot access the website

1.13.1.4 Blocking websites - company wide

Case ID

C1910040

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client
3) The company blocked website list in the shield menu in the app is empty.

Test Steps

1) Access WorkPass app with a client that has admin access
2) Connect one client to the Secure zone and try to access a work appropriate website (https://www.plume.com/)
3) Connect one client to Employee zone and try to access the same website
4) Connect one client to the Guest zone and try to access the same website
5) In the shield tab, move to the block tab and block the website
6) Attempt to access the blocked website with all clients
7) Remove the website from the blocked website list
8) Attempt to access the website

Expected Results

1) The WorkPass app opens
2) Clients in the Secure zone can access the website
3) Clients in Employee zone can access the website
4) Clients in Guest zone can access the website
5) The website is blocked successfully
6) All clients are unable to access the blocked website
7) The website is removed from the blocked website list
8) Clients in all zones can access the website

1.14 Secure Zone

1.14.1 Data usage

Case ID

C1910073

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with admin WorkPass access
– 1x client, connected to the secure zone
3) Write down the data usage before and after the download. Make sure the increase makes sense (matches or is close enough, accounting for other devices using the internet)

Test Steps

1) Connect devices to the secure zone network
2) Download a file with the client (100 mb+)
3) Use productivity apps with the client (slack etc.)
4) After using the internet for at least 5 minutes, check the data usage panel in the secure zone and in the device information screen

Expected Results

1) Devices connect successfully
2,3) Devices can use the internet without issues
4) Data usage updates, based one the applications used. The data usage on both screens must match

1.14.2 Devices

1.14.2.1 Client groups

Case ID

C1910074

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with admin WorkPass access
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client connected via Ethernet cable or Wi–Fi

Test Steps

1) Connect all clients to the secure zone SSID
2) Create two new client groups with the + button in the top right
3) Change the group of a client
4) Change the group of the other client to the same one
5) Move both clients to the other group
6) Bulk move all unassigned clients (devices) to a group
7) Delete the group with the devices

Expected Results

1) All clients connect successfully
2) The new client group is added
3) The client is moved to a different group
4) The client is moved to a different group
5) Both clients are in the same group
6) All clients are moved to a different group at the same time
7) All clients are moved back to the Devices group

1.14.2.2 Client information

Case ID

C1910075

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with admin WorkPass access
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client connected via ethernet cable or Wi–Fi
– 1x Client, able to access FrontLine
3) Use randomized MAC for clients

Test Steps

1) Connect the client to the secure zone SSID
2) Check the client name, IP and mac address of the device in frontline
3) In Secure zone–>Devices click one of them, three dots on the right corner–> Device settings and change the client name
4) Check the client name in the secure zone and FrontLine
5) Reconnect the client with a different MAC address
6) Check the client name, IP Address and MAC address in FrontLine

Expected Results

1) All clients connect to the secure zone successfully
2) The client name, IP, and MAC Address are shown in FrontLine
3) The client name changes
4) The new client name shows in the secure zone panel and FrontLine
5) The client MAC Address changes
6) The client shows up as a new device (sorted under the Devices group and new device on FrontLine)

1.14.3 Timeouts

1.14.3.1 Connection timeout

Case ID

C1910072

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with admin WorkPass app access
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client

Test Steps

1) Connect clients to the employee zone SSID
2) Tap on a specific client
3) Set up a Timeout for this client
4) Tap Save
5) Tap the pause button to start the time out
6) Increase/decrease the duration to 1 minute
7) Attempt to use the internet with the client on the employee zone SSID
8) Attempt to use the internet on the guest or secure SSID with other clients
9) Wait for the timeout to run out
10) Start the timeout again, but this time manually cancel it after testing
11) Edit the time out to include a different client
12) Start the time out again and attempt to access the internet with that client on the employee zone SSID
13) Attempt to access the internet with any other client on the employee zone SSID

Expected Results

1) Client connect successfully
3) Client edit screen opens
4) The duration display updates
5) Timeout starts
6) Duration gets increased/decreased to 1 minute
7) The client cannot use the internet while connected to the employee zone
8) The clients cannot use the internet while connected to the secure/guest zone
9) The time out ends and client in the employee zone can use the internet
10) The employee zone client work as above (start working when you manually end the time out)
11) The other client timeout is successfully set
12) The client cannot connect to the internet
13) The other clients can connect to the internet

1.14.3.2 Timeout adjustments

Case ID

C1953015

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with admin WorkPass access
– 4x client connected to the employee zone

Test Steps

1) Connect all devices to the employee zone SSID
2) Navigate to the employee zone and set up a timeout
3) Tap the pause button to start the timeout
4) Try to use the internet with all clients
5) Tap on one client under the employee zone devices panel and cancel the timeout
6) Try to use the internet with all clients
7) Tap on another client under the employee zone devices panel and shorten the timeout and wait out the duration
8) Try to use the internet with all clients
9) Wait for the main timeout to run out
10) Try to use the internet with all clients

Expected Results

1) The devices connect to the employee zone network
2) The timeout panel shows the timeout duration and respective icons
3) The timeout starts
4) None of the four devices can use the internet
5) The device no longer shows as timed out
6) The internet works on only the device, which had the timeout canceled
7) The device no longer shows as timed out
8) The internet works on two devices (2 devices whose timeout has finished)
9) The timeout ends for all four devices
10) The internet works on all devices

1.14.4 Captive portal

1.14.4.1 Create and edit captive portal

Case ID

C1906034

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x client, not connected to the guest Wi–Fi

Test Steps

1) Test the Captive portal without any changes
2) In the WorkPass app, go to Settings–>Guest Wi–Fi–>Set up guest login portal
3) Go to the Business info tab, change the values and upload a logo
4) Tap publish and check the changes in the app and on a client
5) Disable the toggles in the Business info page
6) Press publish and check if the changes have been applied

Expected Results

1) The Captive portal works as expected
2) The Captive portal shows in the app
3) You are able to change the values inside the Business info page and upload a logo
4) The changes have been applied
5) You are able to turn off the features
6) The changes have been applied

1.14.5 3rd party login

1.14.5.1 Login via Free Wi-Fi

Case ID

C1906035

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x client with Wi–Fi access and randomized MAC ON
3) Under Settings, click on Guest Wi–Fi and click the toggle to enable it, then set it up and publish it

Test Steps

1) In the portal setup, go to Login options, enable Free W–Fi Login toggle
2) Tap publish
3) Log into the Guest Wi–Fi
4) Disable Free Wi–Fi login options and Free Wi–Fi
5) Attempt to connect to the Guest Wi–Fi

Expected Results

1) You are able to enable the toggle button
2) The changes appear in the portal landing page when attempting to connect to the Guest Wi–Fi
3) You are able to log in
4) You are able to disable the toggle button
5) You cannot log into the guest network via Free Wi–Fi button

1.14.5.2 Login via Email

Case ID

C2029130

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x client with Wi–Fi access and randomized MAC ON
3) Under Settings, click on Guest Wi–Fi and click the toggle to enable it, then set it up and publish it

Test Steps

1) In the portal setup, go to Login options, enable Email Login toggle
2) Tap publish
3) Log into the Guest Wi–Fi
4) Disable Email login options and Free Wi–Fi
5) Attempt to connect to the Guest Wi–Fi with your real name and email

Expected Results

1) You are able to enable the toggle button
2) The changes appear in the portal landing page when attempting to connect to the Guest Wi–Fi
3) You are able to log in
4) You are able to disable the toggle button
5) You log into the Guest Wi–Fi successfully

1.14.5.3 Login via Passcode

Case ID

C2029131

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x client with Wi–Fi access and randomized MAC ON
3) Under Settings, click on Guest Wi–Fi and click the toggle to enable it, then set it up and publish it

Test Steps

1) In the portal setup, go to Login options, enable Passcode Login toggle
2) Tap publish
3) Log into the Guest Wi–Fi
4) Disable Passcode login options and Free Wi–Fi
5) Attempt to connect to the Guest Wi–Fi with your real name and email

Expected Results

1) You are able to enable the toggle button
2) The changes appear in the portal landing page when attempting to connect to the Guest Wi–Fi
3) You are able to log in
4) You are able to disable the toggle button
5) You log into the Guest Wi–Fi successfully

1.14.5.4 Login via Facebook Login

Case ID

C2029132

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with WorkPass app installed
– 1x client with Wi–Fi access and randomized MAC ON
3) Under Settings, click on Guest Wi–Fi and click the toggle to enable it, then set it up and publish it

Test Steps

1) In the portal setup, go to Login options, enable Facebook Login toggle
2) Tap publish
3) Log into the Guest Wi–Fi
4) Disable Facebook login options and Free Wi–Fi
5) Attempt to connect to the Guest Wi–Fi with your real name and email

Expected Results

1) You are able to enable the toggle button
2) The changes appear in the portal landing page when attempting to connect to the Guest Wi–Fi
3) You are able to log in
4) You are able to disable the toggle button
5) You log into the Guest Wi–Fi successfully

1.14.6 Timeouts

1.14.6.1 Connection timeout

Case ID

C2029133

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with admin WorkPass app access
– 1x Android smartphone client
– 1x iOS smartphone client
– 1x PC client

Test Steps

1) Connect all devices to the secure zone SSID
2) Tap the pencil next to Set time out
3) Select all devices by tapping the checkmark next to Devices
4) Tap Save
5) Tap the pause button to start the time out
6) Increase/decrease the duration to 1 minute
7) Attempt to use the internet with the devices on the secure zone SSID
8) Attempt to use the internet on the guest or employee SSID
9) Wait for the timeout to run out
10) Start the timeout again, this time, manually cancel it after testing
11) Edit the time out to include only 1 device
12) Start the time out again and attempt to access the internet with that device on the secure zone SSID
13) Attempt to access the internet with any other device on the secure zone SSID

Expected Results

1) Devices connect successfully
2) The edit time out screen opens
3) All devices are selected
4) The duration display updates
5) Timeout starts
6) Duration is decreased to 1 minute
7) The devices cannot use the internet while connected to the secure zone
8) The devices cannot use the internet while connected to the employee/guest zone
9) The time out ends and devices in the secure zone can use the internet
10) The secure zone devices work as above (start working when you manually end)
11) Only one device shows as selected in the edit time out screen
12) The device cannot connect to the internet
13) The other devices can connect to the internet

1.14.6.2 Timeout adjustments

Case ID

C2029134

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smartphone client with admin WorkPass access
– 4x client, connected to the secure zone

Test Steps

1) Connect all devices to the Secure zone SSID
2) Navigate to the secure zone and set up a timeout
3) Tap the pause button to start the timeout
4) Try to use the internet with all clients
5) Tap on one client under the secure zone devices panel and cancel the timeout
6) Try to use the internet with all clients
7) Tap on another client under the secure zone devices panel and shorten the timeout and wait out the duration
8) Try to use the internet with all clients
9) Change the network to the employee zone for one client
10) Try to use the internet with all clients
11) Wait for the main timeout to run out
12) Try to use the internet with all clients

Expected Results

1) The devices connect to the Secure zone network
2) The timeout panel shows the timeout duration and respective icons
3) The timeout starts
4) None of the four devices can use the internet
5) The device no longer shows as timed out
6) The internet works on only the device, which had the timeout canceled
7) The device no longer shows as timed out
8) The internet works on two devices
9) The client connects to the employee zone
10) The internet works on two devices (2 devices which timeout has been finished), but not on the other two
11) The timeout ends for all four devices
12) The internet works on all devices

Plume