Captive Portal Enchantments

Guest Registration
Guest Registration

Overview

- The MAC Self Registration feature was introduced in WiNG 5.4
- The client’s MAC address and other details is stored in the internal Database on the NOC controllers after first-time registration.
- The repeat visitors are authenticated against the MAC database without the need to re-login.
- The information captured was limited to phone or email of the guest.
- WiNG5.8 provides additional mechanisms of registering guest users
  - mobile phone and email validation / social media profile etc
- The following platforms are supported:

<table>
<thead>
<tr>
<th>Controller Platforms</th>
<th># Users supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>NX 9510/NX 9610</td>
<td>2 Million</td>
</tr>
<tr>
<td>VX 9000</td>
<td>2 Million</td>
</tr>
<tr>
<td>NX 7510</td>
<td>1 Million</td>
</tr>
</tbody>
</table>
Guest Registration

Registration Methods

Device Registration (No Authentication)
- The device details are stored after Registration.
- The guest client doesn’t require authentication on subsequent visits.
- Additional registration fields have been added.

User Registration with Email or SMS validation
- On registration, Captive Portal sends a passcode to validate the user Email or Mobile number.
- Guest User can use his email or phone number along with the passcode to login on the guest network. He can use them on multiple devices.

Device Registration with One-Time-Password (OTP)
- On registration, Captive Portal sends an OTP to the client.
- Guest User will use the unique passcode to register one device.

Device Registration via Social Media Authentication (Facebook / Google+)
- Self registration via social media profile, like Facebook or Google+
- The guest client device doesn’t require authentication on subsequent visits.
Guest Registration

Device Registration (No authentication)

Device Registration (MAC Registration)
- The first time users are redirected to a registration page.
- On registration, the device MAC address and other details are added to the controller’s database.
- User details are collected based on access-type.
- On subsequent visits, the guest client device doesn’t require registration.
  - The device MAC address is authenticated against the onboard MAC database.

User connected to Guest WLAN → First time User? → Yes → Perform Registration → Add User to Database → No → Authenticate against the MAC Database → Grant Access
Guest Registration

Registration Page

- When the user connects to the Guest Wireless LAN for the first time, they are redirected to a Registration Page (registration.html).
- The Guest user will complete their registration and get access to the WiFi network.
- In WiNG 5.8, a new “Registration” page is added.
- Many new fields have been added along with the Email, Phone number:
  - Full name
  - Age Range
  - User preference for Email/SMS
  - Address
  - Zip Code
Guest Registration

Registration Page

- The administrator can customize the page by:
  - Selecting which fields to show on the page
  - Identify the fields as Mandatory or Optional for the user
  - Change the text on these fields to be displayed to the user.

  ![Registration Page Fields Table]

- New custom fields can be added to the page

  ![New Custom Fields Interface]
Device Registration

Opt-out option

- Some users do not want their data to be stored for future use
- Registration page gives the user an opt-out option
- If Selected, none of the user information is stored in the GUEST database.
- The Guest User will have to re-register every time
Guest Registration

User Registration with Email or SMS Validation

- Many retailers want some way to track the users of their guest network
- Guest users can register themselves with their email address / mobile phone number
- A **passcode** is sent to the user on their Email/mobile number.
- The Guest user can then login with the email/mobile number and the received **passcode**.
- The user is granted access to the Guest Wireless Network.
- The user can then use the same **passcode** across multiple devices.
Guest Registration

User Registration with Email / SMS notification

1. User clicks “Register Now”
2. User enters registration data along with email / phone and redirected to a Login Page.
3. Add New User.
4. User added to DB. Send out Passcode to the SMTP or SMS gateway
5. SMS / SMTP Gateway
6. Send passcode to the user
7. User will use this passcode to authenticate

Note: In this scenario each user will have a Passcode for authentication that he can use across multiple devices.
Guest Registration

User Registration with Email / SMS notification

Notification Methods

- The **passcode** is sent to the user via email or SMS Notification.
- The following notification methods are supported currently:
  - **Email**: Requires integration with the SMTP Server
    - Configure the SMTP server, credentials, email subject and content
  - **SMS (via Clickatell API)**: Requires integration with an SMS gateway
    - Clickatell is used as the SMS Gateway.
    - Configure Clickatell account details and the SMS message Body
  - **SMS via SMTP**: Some SMS gateways allow the passcode to be sent in an email to the SMS gateway.
    - The SMS gateway then forwards the passcode to the user via SMS.
    - **SMS over SMTP method can be used for customer’s on-premises SMS gateways**
Guest Registration

Email / SMS notification messages

- Users can create a format for the email and SMS messages
- Various TAGs are supported for Email / SMS messages
  - GM_NAME – Guest name.
  - GM_MOBILENUM – Guest registered mobile number.
  - GM_PASSCODE – Passcode that will be sent to guest.

When sending the actual messages, these TAGs are replaced with the actual Email or Mobile number of the user.

CR-NL (carriage return-new line) is the newline delimiter that should be used when composing Email messages.
Guest Registration

#3 : Device Registration Using One-Time-Passcode (OTP)

- It is similar to “Device Registration” feature, but with additional security measure to validate the user via One-Time-Passcode.
  - After the initial registration, the user access to wireless is seamless
- The guest users registers themselves with their email/mobile #
- Captive portal system sends an OTP to the Email/Phone # of user.
- Guest users needs to provide the **OTP** to validate their email/SMS, and get access to the wireless network.
- One-time-Passcode device registration is used to register **only one device**.

![Diagram](chart.png)
Guest Registration

#4. Device Registration with Social Media Authentication

- This functionality allows the guest users to register themselves using their public Facebook or Google+ profiles.
- The user’s Social Media credentials are used to validate the user.
- OAUTH 2.0 support is introduced to implement this functionality.
- Access Points or Controllers hosting Captive Portal service will be acting as intermediary and will send OAUTH requests on behalf of the user to either Facebook or Google.
- On successful authentication, the user is granted access to the wireless network.
Social Media Authentication

Device Registration through Social Media Authentication

- After successful authentication, the user is added to the onboard database.
- Subsequent visits by the user do not require the user to enter the credentials again.
- The guest user’s social media profile data is also stored on the onboard database.
  - User name, Age, etc.
- Only information that is part of the public profile of the user is stored
- Neither the user credentials or any private information about the user is collected or stored on the database.

**Note:** for iOS and Windows Phone clients it is necessary to bypass their Captive portal Detection mechanism, otherwise Social Media Authentication will not work.
Social Media Authentication

Configuration – Client IDs

- To use OAUTH, the Application needs to be registered with Google/Facebook
- This needs to be created on each site separately:
  - **Google**: Use the [Google Developer Console](#)
  - **Facebook**: Use the [App Dashboard](#) (App ID in Facebook terms)
- On registration, Google/Facebook Client ID are generated.
- These **client IDs** are used by WiNG application to identify themselves and do the Authentication on behalf of the user.
- More details at the end of this slide deck
Captive Portal UI Enhancements

Enhanced Customization Tools

- Many enhancements are added to customize the captive portal web pages
Captive Portal UI Enhancements

Enhanced Customization Tools

- Preview of the web pages is added for different device types
- Simplifies the testing while the user is customizing the pages.
Captive Portal Enhancements

Advanced Auto-Upload feature

- Prior to WiNG 5.8 it was only possible to upload Captive Portal pages files as a .tar package only for “advanced” webpage type.
  - If any particular file had to be changed we had to re-upload the whole package.

- WiNG 5.8 adds support for advanced file uploading of Captive Portal Pages:
  - It is now possible to upload a single file for a particular Captive Portal (like a logo or just a login page, etc)
  - It is possible to upload custom files for “internal” based webpages, “advanced” is no longer required.
  - It is possible to upload files into nested folders, i.e. upload a particular file into a particular destination sub-folder, for example images or js/minified.

For the **auto** upload feature to work, enable it under Web page -> Advanced tab:
Captive Portal Enhancements

Advanced Auto-Upload feature

- Uploading a single file for a particular Captive Portal:

  1) Upload the file to the main Controller (Operations -> Select Controller -> Captive Portal Pages):

{code}
vx9k-1#captive-portal-page-upload load-file UPLOAD-TEST ftp://X:X@192.168.10.187/zebra-logo.png
{code}
Captive Portal Enhancements

Advanced Auto-Upload feature

- Uploading a single file for a particular Captive Portal:

  - 2) Verify that the file has been uploaded:

```
vx9k-1#show captive-portal-page-upload load-file-status
Download of UPLOAD-TEST page file is complete
```
Captive Portal Enhancements

Advanced Auto-Upload feature

- Uploading a single file for a particular Captive Portal:

  - 3) Distribute custom files to each site via Operations Tab (go to each site -> Captive Portal Pages -> Upload)

---

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>STATUS</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>8A-F9-ED-81-08-24</td>
<td>Success</td>
<td>Added 1 rf-domain managers for captive portal page upload</td>
</tr>
</tbody>
</table>
Captive Portal Enhancements

Advanced Auto-Upload feature

- Uploading a single file for a particular Captive Portal:
  
  3) Monitor the status in GUI or CLI (history at the NOC will only be shown for RFDMs):

```
vx9k-1#show captive-portal-page-upload history on HOMEAPS
---+--------------+-------+----------+-----------------+-------------------------+
<table>
<thead>
<tr>
<th>AP</th>
<th>RESULT</th>
<th>TIME</th>
<th>RETRIES</th>
<th>UPLOADED-BY</th>
<th>LAST-UPLOAD-ERROR</th>
</tr>
</thead>
<tbody>
<tr>
<td>birch-2</td>
<td>done</td>
<td>2015-06-30 20:00:40</td>
<td>0</td>
<td>84-24-8D-85-1F-EC</td>
<td>-</td>
</tr>
<tr>
<td>birch-2</td>
<td>done</td>
<td>2015-06-30 20:02:51</td>
<td>0</td>
<td>84-24-8D-85-1F-EC</td>
<td>-</td>
</tr>
</tbody>
</table>
Total number of entries displayed: 2
```

```
vx9k-1#show captive-portal-page-upload history
---+--------------+-------+----------+-----------------+-------------------------+
<table>
<thead>
<tr>
<th>AP</th>
<th>RESULT</th>
<th>TIME</th>
<th>RETRIES</th>
<th>UPLOADED-BY</th>
<th>LAST-UPLOAD-ERROR</th>
</tr>
</thead>
<tbody>
<tr>
<td>birch-1</td>
<td>done</td>
<td>2015-06-30 20:10:20</td>
<td>0</td>
<td>vx9k-1</td>
<td>-</td>
</tr>
<tr>
<td>birch-1</td>
<td>done</td>
<td>2015-06-30 20:10:20</td>
<td>0</td>
<td>vx9k-1</td>
<td>-</td>
</tr>
</tbody>
</table>
Total number of entries displayed: 2
```
Captive Portal Enhancements

Advanced Auto-Upload feature

- Uploading a single file into a nested subfolder (**CLI only**):

```
vx9k-1# captive-portal-page-upload load-file UPLOAD-TEST ftp://X:X@192.168.10.187/zebra-logo.png ?
  destination-dir For non archive file, optionally specify the relative path
  of the destination directory. The default destination is
  the root directory of the captive portal.
<cr>
```

```
vx9k-1# captive-portal-page-upload load-file UPLOAD-TEST ftp://X:X@192.168.10.187/zebra-logo.png
  destination-dir ?
  WORD Relative path of existing or new destination directory. Examples:
  images, js/minified
```

```
vx9k-1# captive-portal-page-upload load-file UPLOAD-TEST ftp://X:X@192.168.10.187/zebra-logo.png
  destination-dir images ?
<cr>
```

- Optionally check all custom files uploaded for a given Captive Portal:

```
vx9k-1# show captive-portal-page-upload list-files UPLOAD-TEST
+-------------------------------+-------+---------------------+---------------------+
| NAME                          | SIZE  | LAST MODIFIED       |
|-------------------------------+-------+---------------------+---------------------|
| images/zebra-logo.png         | 3220  | 2015-06-30 20:17:46 |
| zebra-logo.png                | 3220  | 2015-06-30 19:28:41 |
| zebstras.jpg                  | 325891| 2015-06-28 20:54:12 |
+-------------------------------+-------+---------------------+---------------------+
```
Guest Registration
Analytics: User Demographics

User Trend

Visitor

Age Range

Gender
Guest Registration
Analytics: User Device Types

- **Browser**:
  - Chrome (37.97%)
  - Firefox (24.40%)
  - Safari (24.31%)
  - Internet Explorer (13.62%)

- **Operating System**:
  - Windows 7 (24.93%)
  - Windows 8 (22.53%)
  - Apple iOS (21.19%)
  - Macintosh (19.15%)
  - Android (12.28%)

- **Device**:
  - Windows PC (47.46%)
  - Apple iPad (21.19%)
  - Macintosh (10.15%)
  - Motorola Droid (6.23%)
  - Android Mobile (5.97%)
Guest Registration
Statistics : Social Media
Guest Registration

User Search

- Users can be searched against the database on various parameters

<table>
<thead>
<tr>
<th>Search Criteria</th>
<th>User MAC</th>
<th>User Name</th>
<th>Email</th>
<th>Mobile #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filtered based on</td>
<td>Time of Access</td>
<td>RF-Domain</td>
<td>WLAN</td>
<td></td>
</tr>
</tbody>
</table>

**Guest Access**

- Fill the field to retrieve data, i.e., mac, email, mobile, or name

<table>
<thead>
<tr>
<th>MAC</th>
<th>Name</th>
<th>Email</th>
<th>Mobile</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC-FA-00-B3-F6-AC</td>
<td>Viacheslav Dementyev</td>
<td></td>
<td></td>
<td>Details</td>
</tr>
<tr>
<td>9C-F3-B7-0B-9C-40</td>
<td>Maria Antunova</td>
<td></td>
<td></td>
<td>Details</td>
</tr>
<tr>
<td>2C-F0-EE-DC-07-01</td>
<td>Piotr Lewandowski</td>
<td><a href="mailto:poiew@gmail.com">poiew@gmail.com</a></td>
<td></td>
<td>Details</td>
</tr>
</tbody>
</table>
Captive Portal Enchantments

Configuration
Guest Registration

Topology
Guest Registration

Guest Registration Flow

Captive Portal

Onboard RADIUS

Onboard Database

SMS / SMTP GW

1. Redirect to Registration.html
2. Complete Registration
3. Internet Access
4. Authentication
5. Welcome!
6. RADIUS lookup
7. RADIUS Access-ACCEPT
8. RADIUS validation with database
9. Send PassCode to the User via SMS or Email
10. Register User Data
11. Send PassCode to SMS / SMTP Gateway
12. Complete Registration
13. Welcome!
Captive Portal Enchantments

Device Registration
Guest Registration
Device Registration – No authentication / Terms & Agreement

1. MAC auth will FAIL. Device will be redirected to the Captive Portal.
2. Captive Portal Redirect
3. After failed MAC authentication, Guest device will be redirected to the Terms & Agreement Page.
4. Upon successful Captive Portal authentication, Access Point will send a request to add a new device to the NOC controller (cluster master).
5. NX will check if his own database status is primary. If not NX shall forward it to the primary database controller to add device record. See Note*
6. Guest Device roams to another Access Point
7. AP will perform MAC auth through the RFDM
8. Client is found in the Database, AP will receive ACCESS-ACCEPT and client is associated, Captive Portal AUTH is skipped!

*Note: Depending on the database status, the access point will either send the request to the primary database controller or to the backup database controller.
Device Registration

Configuration – Captive portal policy

```plaintext
! aaa-policy CENTRALLIZED-NX
   authentication server 1 onboard centralized-controller
!
captive-portal DEVICE-REG
   access-type no-auth
   terms-agreement
   use aaa-policy CENTRALLIZED-NX
!
profile ap7522 OAK
no autoinstall configuration
no autoinstall firmware
interface radio1
   no dynamic-chain-selection
interface radio2
   wlan REG-ME bss 1 primary
   no dynamic-chain-selection
interface ge1
   switchport mode access
   switchport access vlan 3010
interface vlan3010
   ip address dhcp
   ip dhcp client request options all
interface pppoe1
   use firewall-policy default
   use captive-portal server DEVICE-REG
service pm sys-restart
router ospf
   traffic-shape total-bandwidth 10 Mbps
!
```

Select access type as “No authentication”
Device Registration
Configuration – Config steps

1. Create a RADIUS group for Guest Users
2. Create a RADIUS Server Policy.
3. Assign the Policy to the NX profile.
Device Registration

Configuration – WLAN

1. Enable MAC authentication
2. Enable Captive Portal with fallback
3. Enable Device Registration
4. Configure a RADIUS group name

```
! wlan REG-ME
 ssid REG-ME
 vlan 3010
 bridging-mode local
 encryption-type none
 authentication-type mac
 use aaa-policy CENTRALLIZED-NX
 use captive-portal DEVICE-REG
 captive-portal-enforcement fall-back
 registration device group-name GUESTS expiry-time 1500
!
profile ap7522 OAK
 no autoinstall configuration
 no autoinstall firmware
 interface radio1
   wlan REG-ME bss 1 primary
   no dynamic-chain-selection
 interface radio2
   wlan REG-ME bss 1 primary
   no dynamic-chain-selection
 interface ge1
 switchport mode access
 switchport access vlan 3010
 interface vlan3010
 ip address dhcp
 ip dhcp client request options all
 interface pppoe1
 use firewall-policy default
 use captive-portal server DEVICE-REG
 service pm sys-restart
 router ospf
 traffic-shape total-bandwidth 10 Mbps
```
Captive Portal Enchantments

User Registration using Email/SMS
User Registration using Email/SMS

Configuration

! aaa-policy CENTRALIZED-NX
   authentication server 1 onboard centralized-controller
!
captive-portal DEVICE-REG
   access-type registration
   use aaa-policy CENTRALIZED-NX
!
profile ap7522 OAK
   no autoinstall configuration
   no autoinstall firmware
   interface radio1
      no dynamic-chain-selection
   interface radio2
      no dynamic-chain-selection
   interface ge1
      switchport mode access
      switchport access vlan 3010
   interface vlan3010
      ip address dhcp
      ip dhcp client request options all
   interface pppoe1
      use firewall-policy default
use captive-portal server USER-REG-EMAIL-SMS
service pm sys-restart
router ospf
traffic-shape total-bandwidth 10 Mbps
!

Set Server Mode to “Internal”, create and select AAA Policy pointing to the NOC controller, select access type as “registration”. Assign this policy to the AP profile.
User Registration using Email/SMS

Configuration - Radius

```plaintext
! radius-group GUESTS
guest
!
radius-server-policy ONBOARD-NX
  use radius-group GUESTS
profile nx9600 NUXI
  no autoinstall configuration
  no autoinstall firmware
  no device-upgrade auto
  use radius-server-policy ONBOARD-NX
  crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  crypto ikev1 remote-vpn
  crypto ikev2 remote-vpn
  crypto auto-ipsec-secure
  crypto load-management
  crypto remote-vpn-client
  interface xge1
  interface xge2
  interface xge3
  interface xge4
  interface ge1
  interface ge2
  use firewall-policy default
  service pm sys-restart
  traffic-shape total-bandwidth 10 Mbps
!```

Create a RADIUS group for Captive Portal Users named “GUESTS” and assign it to our RADIUS Server Policy. Assign the Policy to the NX profile.
User Registration using Email/SMS

Configuration – Wireless LAN

! wlan USER-REG
  ssid USER-REG
  vlan 3010
  bridging-mode local
  encryption-type none
  authentication-type none
  use captive-portal USER-REG-EMAIL-SMS
  captive-portal-enforcement
  registration user group-name GUESTS expiry-time 1500
! profile ap7522 OAK
  no autoinstall configuration
  no autoinstall firmware
  interface radio1
    wlan USER-REG bss 1 primary
    no dynamic-chain-selection
  interface radio2
    wlan USER-REG bss 1 primary
    no dynamic-chain-selection
  interface ge1
    switchport mode access
    switchport access vlan 3010
  interface vlan3010
    ip address dhcp
    ip dhcp client request options all
  interface pppoe1
    use firewall-policy default
    use captive-portal server USER-REG-EMAIL-SMS
    logging on
    service pm sys-restart
    router ospf
    traffic-shape total-bandwidth 10 Mbps

Configure a WLAN, enable Captive Portal Authentication and select Captive Portal Policy. Enable User Registration and set a RADIUS group name.
User Registration using Email/SMS

Configuration – Guest Management Policy

Configuration -> Services -> Guest Management -> <name>:

- guest-management GM
  - email host smtp.gmail.com sender
  - wing5dot8demo@gmail.com security ssl username
  - wing5dot8demo password AB12_***
  - email subject WiNG 5.8 BETA
  - email message Hello GM_NAME, Thanks for registering with Zebra CaptivePortal Access. Your Passcode for accessing the Internet: GM_PASSCODE.
- sms host clickatell username zebra-demo password
  - fh44BAX0lkee api-id 3540370 user-agent pyclickatell
  - sms message Hello GM_NAME, your Zebra Internet Passcode is: GM_PASSCODE.
- sms-over-smtp host smtp.gmail.com sender
  - wing5dot8demo@gmail.com security ssl username
  - wing5dot8demo password AB12_*** recipient
  - sms@messaging.clickatell.com
  - sms-over-smtp subject sms-smtmp passcode
    - sms-over-smtp message api-id:3541608 CR-NL
  - user:zebra-demo CR-NL password:fh44BAX0lkee

MO:1

profile nx9600 NOC-NX9600

use radius-server-policy ONBOARD-NX

... use guest-management GM
Captive Portal Enchantments

Device Registration with One-Time-Password Validation
User Registration using OTP

Configuration – Wireless LAN

wlan USER-REG
ssid USER-REG
vlan 3010
bridging-mode local
encryption-type none
authentication-type none
use captive-portal USER-REG-EMAIL-SMS
captive-portal-enforcement
registration user group-name GUESTS expiry-time 1500
!
profile ap7522 OAK
no autoinstall configuration
no autoinstall firmware
interface radio1
    wlan USER-REG bss 1 primary
    no dynamic-chain-selection
interface radio2
    wlan USER-REG bss 1 primary
    no dynamic-chain-selection
interface ge1
    switchport mode access
    switchport access vlan 3010
interface vlan3010
    ip address dhcp
    ip dhcp client request options all
interface pppoe1
use firewall-policy default
use captive-portal server USER-REG-EMAIL-SMS
logging on
service pm sys-restart
router ospf
traffic-shape total-bandwidth 10 Mbps

1. Enable MAC Auth,
2. Enable Captive Portal with Fallback
3. Select device-OPT for User Registration and set a RADIUS group name.
User Registration using Email/SMS

Configuration – Guest Management Policy

```bash
! guest-management GM
  email host smtp.gmail.com sender
  wing5dot8demo@gmail.com security ssl username
  wing5dot8demo password AB12_xxx
  email subject WiNG 5.8 BETA
  email message Hello GM_NAME, CR-NL Thanks for registering with Zebra CaptivePortal Access, CR-NL Your Passcode for accessing the Internet: GM_PASSCODE CR-NL Zebra Technologies
  sms host clickatell username zebra-demo password
  fh44BAX0lk3 api-id 3540370 user-agent pyclickatell
  sms message Hello GM_NAME, your Zebra Internet Passcode is: GM_PASSCODE
  sms-over-smtp host smtp.gmail.com sender
  wing5dot8demo@gmail.com security ssl username
  wing5dot8demo password AB12_xxx recipient
  sms@messaging.clickatell.com
  sms-over-smtp subject sms-smtp passcode
  sms-over-smtp message api_id:3541608 CR-NL
!
profile nx9600 NOC-NX9600
  use radius-server-policy ONBOARD-NX
...
  use guest-management GM
!
```

Configure Guest Management Policy for Email / SMS / SMS over SMTP Notification. Assign the Policy to the NX / VX
Guest Registration

Device-OTP Registration – Email / SMS validation

1. On the Registration Page user must fill in email / phone # or both to get registered and select preferred communication method for receiving OTP.

2. Navigate to "Register Now" section

3. After user will enter registration data AP will send a request to add new user to the NX / VX database.

4. VX will send out a notification with a Passcode to the SMTP or SMS gateway based on user preference.

5. SMS or SMTP gateway will send out notification to the user with the passcode that will be used for login.

6. User will enter his mobile or email and received passcode to authenticate. Passcode will be validated by RADIUS.

Note: In this scenario each device will have a unique Passcode for authentication.
Captive Portal Enchantments

Guest Registration with Social Media Authentication
Social Media Authentication

Application Registration

- **Google:**
- Go to the *Google Developer Console*
- Edit the Consent Screen on the Developer Console
- Create a new Client ID under *Credentials tab* and configure *Web-Origin* and *Redirect URL*
- Copy Client ID into the WiNG Captive Portal Configuration

*Note: Detailed instructions are provide at the end of the slide deck*
Social Media Authentication

Configuration – Captive Portal

```plaintext
! captive-portal OAuth
  access-type registration
  server host virtual.captive.org
  oauth
  oauth client-id Google 253638723891-bsim9dcmg51einn3v7sd496s1767hjsf.apps.googleusercontent.com Facebook 1576296242634490
  use aaa-policy CENTRALIZED-NX
  use dns-whitelist EnableOAuth
!
dns-whitelist EnableOAuth
  permit fbstatic-a.akamaihd.net
  permit connect.facebook.net
  permit facebook.com suffix
  permit google.com suffix
  permit ssl.gstatic.com
  permit googleapis.com suffix
  permit googleusercontent.com suffix
!
profile ap7522 OAK
... use captive-portal server OAuth ...
!
```

Configure DNS whitelist to allow Google / Facebook for OAuth authentication. Assign this whitelist to the Captive Portal Policy.
Social Media Authentication

Configuration – Wireless LAN

1. Enable MAC Authentication
2. Enable Captive Portal with fallback.
3. Select Device registration and configure the Radius Group GUESTS

```bash
wlan SOCIAL-REG
ssid SOCIAL-REG
vlan 3010
bridging-mode local
crypt-type none
authentication-type mac
use aaa-policy CENTRALIZED-NX
use captive-portal OAuth
use captive-portal-enforcement fall-back
registration device group-name GUESTS expiry-time 4320
profile ap7522 OAK
no autoinstall configuration
no autoinstall firmware
interface radio1
  wlan SOCIAL-REG bss 1 primary
  no dynamic-chain-selection
interface radio2
  wlan SOCIAL-REG bss 1 primary
  no dynamic-chain-selection
interface ge1
  switchport mode access
  switchport access vlan 3010
interface vlan3010
  ip address dhcp
  ip dhcp client request options all
interface pppoe1
  use firewall-policy default
  use captive-portal server OAuth
```
Captive Portal Enchantments

Guest Registration CLI commands
Guest Registration

CLI: Verification for SMS / SMTP Gateways

# show guest-registration notification-status

NOC-NX9600# show guest-registration notification-status
Clickatell Gateway:
  Status: Yes
  Available Credit: 390.000
  Last SMS Sent Time: 2015-05-11 14:50:55.185324
  Last SMS to Mobile number: 420737208506
  Last SMS Auth Status: OK, Session ID: f2eeb862c840741fd3dc4e066bdfe392
  Last SMS Sent Status: OK, Message ID: 0d2fddbe94f9df64b48695545a53a6ae
Email Gateway:
  Last EMail Time: 2015-05-11 14:50:58.089818
  Last EMail To: cgj864@zebra.com
  Last EMail Status: Success
SMS to SMTP Gateway:
  Last EMail Time: 2015-05-11 14:50:56.901852
  Last EMail To: 420737208506
  Last EMail Status: Success

Guest Access

Clickatell Gateway
- Status: Yes
- Available Credit: 390.000
- Last SMS to Mobile number: 420737208506
- Last SMS Auth Status: OK, Session ID: f2eeb862c840741fd3dc4e066bdfe392
- Last SMS Sent Status: OK, Message ID: 0d2fddbe94f9df64b48695545a53a6ae

Email Gateway
- Last EMail To: cgj864@zebra.com
- Last EMail Status: Success

SMS to SMTP Gateway
- Last EMail Time: 2015-05-11 14:50:56.901852
- Last EMail To: 420737208506
- Last EMail Status: Success

EMail Gateway
- Last EMail To: cgj864@zebra.com
- Last EMail Status: Success
## Guest Registration

### CLI: Search Registered Guest Users

**show guest-registration <option> time <30-Mins|2-Hours|5-Hours|1-Day|1-Week|1-Month|all> [rfdomain <rfdomain>] [wlan <wlan>]**

<table>
<thead>
<tr>
<th>Description</th>
<th>Shows guest registration statistics based on the option and time entered. If RF Domain and / or WLAN are entered, shows the statistics for the RF Domain and / or WLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>age-range – Age ranges logged in</td>
</tr>
<tr>
<td></td>
<td>browsers – Browsers logged in</td>
</tr>
<tr>
<td></td>
<td>devices – Devices logged in</td>
</tr>
<tr>
<td></td>
<td>gender – Genders logged in</td>
</tr>
<tr>
<td></td>
<td>os – Operating systems logged in</td>
</tr>
<tr>
<td></td>
<td>social – Social sites logged in</td>
</tr>
<tr>
<td></td>
<td>user-trends – User trends</td>
</tr>
<tr>
<td></td>
<td>visitors – Type of visitors logged in</td>
</tr>
<tr>
<td></td>
<td>The time values are with respect to the latest segment of time, e.g., specifying “time 30-Mins” will show statistics for the most recent 30 minutes.</td>
</tr>
</tbody>
</table>

**show guest-registration client <option> <value>**

<table>
<thead>
<tr>
<th>Description</th>
<th>Shows client(s) matching the input.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>email – Email address</td>
</tr>
<tr>
<td></td>
<td>mac – MAC address</td>
</tr>
<tr>
<td></td>
<td>member – Member ID</td>
</tr>
<tr>
<td></td>
<td>mobile – Mobile phone number</td>
</tr>
<tr>
<td></td>
<td>name – Full name</td>
</tr>
<tr>
<td></td>
<td>time – Timeline(30-Secs, 2-Mins, 5-Mins, 10-Mins, 15-Mins, 30-Mins, or 1-Hour)</td>
</tr>
<tr>
<td></td>
<td>NOTE; If the time option is specified, an RF Domain and/ or WLAN can also be specified, i.e. show guest-registration client time &lt;timeline&gt; [rfdomain &lt;rfdomain&gt;] [wlan &lt;wlan&gt;]</td>
</tr>
</tbody>
</table>
Guest Registration

Database Operations – Import Export DB

- Export the Guest Registration Database: in CSV or JSON format

```
NX9610# service guest-registration export
   format (json|csv) <File-URL>
   [time <30-Mins-to-1Month| all>
   [rfdomain <rfdomain>] [wlan <wlan>]]
```

- Import the Guest Registration Database: from a file in CSV format

```
NX9610# service guest-registration import
   format json <File-URL>
```
Guest Registration

Database Operations – Delete User/s

- A user can be deleted from the database.
- **service guest-registration delete:**
- This command is used to delete either a particular user or all the users in the users collection.

```
NX9610# service guest-registration delete
   <email/mac/mobile/name/All> <value>
```

Example:
```
NX9610# service guest-registration delete
   mobile 14085549636
```
Guest Registration

Database Operations – Internal Auto Backup

- By default guest user database will be backed up every 24 hours for the past 7 days. Backup time is configurable.
- Several snapshots will remain in the system in case a database restore will be needed.
- Automatic backup can be optionally disabled.

```
vx9k-1(config-guest-management-GM)#show context include-factory | grep database
  guest-database-backup enable 00:00

vx9k-1(config-guest-management-GM)#guest-database-backup enable 23:59 ?
<cr>

vx9k-1(config-guest-management-GM)#no guest-database-backup enable ?
<cr>
```
Guest Registration

Database Operations – Internal Auto Backup

- Show internal backup snapshots:

```bash
tax9k-1#show guest-registration backup-snapshots
```

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Creation Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>users_20150624-0000.json</td>
<td>2025</td>
<td>06-24-2015 00:00</td>
</tr>
<tr>
<td>users_20150625-0000.json</td>
<td>2025</td>
<td>06-25-2015 00:00</td>
</tr>
<tr>
<td>users_20150626-0000.json</td>
<td>2025</td>
<td>06-26-2015 00:00</td>
</tr>
<tr>
<td>users_20150627-0000.json</td>
<td>2025</td>
<td>06-27-2015 00:00</td>
</tr>
<tr>
<td>users_20150628-0000.json</td>
<td>2025</td>
<td>06-28-2015 00:00</td>
</tr>
<tr>
<td>users_20150629-0000.json</td>
<td>660</td>
<td>06-29-2015 00:00</td>
</tr>
<tr>
<td>users_20150630-0000.json</td>
<td>660</td>
<td>06-30-2015 00:00</td>
</tr>
</tbody>
</table>

- Operations on internal backup snapshots:

```bash
tax9k-1#service guest-registration backup ?
  delete   Delete all backup snapshots
  restore  Restore all backup snapshots
```
Guest Registration

Database Operations – External Backup

- Optionally for backup purposes whole guest user database can be exported via FTP or SFTP. **On-Demand Backup** example:

```
vx9k-1#database-backup database captive-portal ?
URL  Destination of backup
URLs:  ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz
       sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz
```

- **Scheduled Backup** can also be configured under controller profile:

```
vx9k-1#database-backup database captive-portal ?
URL  Destination of backup
URLs:  ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz
       sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file.tar.gz
```
Guest Registration

Troubleshooting

• Following debug modules will provide detailed information when troubleshooting issues related to guest registration:

  • `debug cfgd guest-management`
  • `debug wireless client radius`
  • `debug captive portal all`

• *Note:* In order to see any debug information, logging on the device must be set to debug level.
Guest Registration

Configuration parameters summary

- Please take note of the following parameters for the various guest registration configuration options:

<table>
<thead>
<tr>
<th>Registration Method</th>
<th>Access Type (CP)</th>
<th>Type of Registration (WLAN)</th>
<th>Auth</th>
<th>CP Failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Auth</td>
<td>None</td>
<td>Device</td>
<td>MAC</td>
<td>Y</td>
</tr>
<tr>
<td>User Auth</td>
<td>Registration</td>
<td>User</td>
<td>No-Auth</td>
<td>N</td>
</tr>
<tr>
<td>OTP</td>
<td>Registration</td>
<td>Device-OTP</td>
<td>MAC</td>
<td>Y</td>
</tr>
<tr>
<td>Social Auth</td>
<td>Registration</td>
<td>Device</td>
<td>MAC</td>
<td>Y</td>
</tr>
</tbody>
</table>
Guest Registration

Database Operations

- Database statistics and operational status (CLI only):

```
NOC-NX9600#show database status

+----------------+---------------+-----------------+-------------------+
<table>
<thead>
<tr>
<th>MEMBER</th>
<th>STATE</th>
<th>ONLINE TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>localhost (self)</td>
<td>PRIMARY</td>
<td>1 days 3 hours 27 min 22 sec</td>
</tr>
</tbody>
</table>

NOC-NX9600#show database statistics

+----------------+-------+--------+-------+-------+----------+----------+
<table>
<thead>
<tr>
<th>DATABASE</th>
<th>FILE SIZE</th>
<th>STORAGE SIZE</th>
<th>DATA SIZE</th>
<th>INDEX SIZE</th>
<th>DISK FREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>mart</td>
<td>64M</td>
<td>9.8M</td>
<td>4.0M</td>
<td>2.3M</td>
<td>5.0T</td>
</tr>
<tr>
<td>captive_portal</td>
<td>64M</td>
<td>24k</td>
<td>4.3k</td>
<td>47.9k</td>
<td>5.0T</td>
</tr>
</tbody>
</table>
```
Social Media Authentication Configuration – Google Client IDs

- Edit the consent screen on Google Dev Console:

  ![Google Dev Console Screenshot]

  - Email address: wing5dot5demo@gmail.com
  - Product name: CaptiveOAuth

  - Consent screen:
    - The consent screen will be shown to users whenever you request access to their private data using your client ID.
    - Note: This screen will be shown for all of your applications registered in this project.
Social Media Authentication

Configuration – Google Client IDs

- Create a new Client ID under Credentials tab and configure Web-Origin and Redirect URL:

  - **Application type**: Web application
    - Accessed by web browsers over a network.
    - Cannot contain a wildcard (http://*.example.com) or a path (http://example.com/subdir).
  
  - **Authorized JavaScript origins**
    - http://virtual.captive.org:880

  - **Authorized redirect URIs**
    - http://plus.google.com
Social Media Authentication
Configuration – Google Client IDs

• Copy Client ID into the WiNG Captive Portal Configuration:

Client ID: 2536387323891-bsim9dcmg51einn3v7sd496sl767hjsf.apps.googleusercontent.com
Email address: 2536387323891-bsim9dcmg51einn3v7sd496sl767hjsf@developer.gserviceaccount.com
Client secret: pviEkkTkSIO37auWgGe14cl
Redirect URLs: http://plus.google.com
JavaScript origins: http://virtual.captive.org:880

No keys found.
Social Media Authentication
Configuration – Google Client IDs

- Enable Google+ API to be able to obtain user’s profile information
Social Media Authentication

Configuration – Facebook Client IDs


- Set both Site URL and Mobile URL to point to Access Point or Controller hosting the captive portal server, as it will be sending OAuth request on behalf of the user:

  Tell us about your website

  Site URL
  http://virtual.captive.org:880

  Mobile Site URL
  http://virtual.captive.org:880
You should add your contact email under Settings->Contact Email and App Domain to match your Captive Portal URL:
Social Media Authentication
Configuration – Facebook Client IDs

- Make this App available to everyone. Navigate to Status & Review Tab:

![OAuth](image)

**Status**

Do you want to make this app and all its live features available to the general public?

- [ ] YES
- [ ] NO

**Submit Items for Approval**

Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our Platform Policy and Review Guidelines.

[Start a Submission]
Social Media Authentication

Configuration – Facebook Client IDs

- Get Facebook Client ID (App ID) under Dashboard to later use it for WiNG Captive Portal:
THANK YOU