What is a Certificate
Sometimes called a public key
What is a Certificate?

PUBLIC KEY

METADATA
Methods of Certification

– Certificate Authorities
  – A 3rd party will digitally sign the public key
  – Other people/systems who trust the CA can then trust you are who you claim
  – Need to be able to interact with something to determine if the trust is still valid
  – This is how most people use the web
– Simple PKI
  – Parties directly exchange their public keys, no need for additional trust points
  – Manually need to maintain trust information
  – This is how some SSH and “passwordless authentication” use cases work
– We are only discussing Certificate Authority methods today
It’s all about trust!

- A Certificate Authority (CA) guarantees the binder between a public key and another CA or an End Entity (EE)
- Each device has a trusted CA store
- Some organizations have an issuing CA off a commercial root
Example – https://www.arubanetworks.com

DigiCert Global Root CA

DigiCert SHA2 Secure Server CA

DNS: www.arubanetworks.com
Certificate Stores
"The Error"

THIS IS NORMAL!* on unconfigured devices
What Uses Certificates?

- EAP/RADIUS
- RadSec (RADIUS over TLS)
- HTTPS
- SMTP (sometimes)
- Database communications
- VPNs

- ClearPass servers
  - Supplicants
    - EAP-TLS
  - Controllers
  - Switches
  - Administrators
    - Mutual authentication HTTPS
EAP-TLS

NETWORK INFRASTRUCTURE

MUTUAL TLS

- Credentials are not stored locally on the device
- Gives the device a unique identity
- Flexible certificate properties
- Device properties stored in certificate

NO USER PASSWORD STORED!
EAP-TLS Certificates Need to be Valid

- Trusted Issuer
- Not Expired
- Not Revoked
OCSP – Is my certificate still valid

- Online Certificate Status Protocol
  - Runs over HTTP
  - Real-time check
- EAP-TLS method in ClearPass controls OCSP check for the authentication request
- Pay attention to OCSP URL for Onboard
  - Single cluster vs multi cluster
  - Multiple uses
  - Multiple CAs
Sample OCSP Response

OCSP Request Data:
- Version: 1 (0x0)
- Requestor List:
  - Certificate ID:
    - Hash Algorithm: sha1
    - Issuer Name Hash: 939E0296797407B76FB212BB47B89B99DEDF8C102
    - Issuer Key Hash: F6E04582CB0C4B0EB4588821F58E47BE24866050
    - Serial Number: 1425DCA4CC5BC2AF83A0F2D3ADE8DD20
- Request Extensions:
  - OCSP Nonce: 0410A944392A4A496241B3A5679C96DBF01

OCSP Response Data:

**OCSP Response Status: successful (0x0)**
- Response Type: Basic OCSP Response
- Version: 1 (0x0)
- Responder Id: 645ABF4899FDD84F7BE780014528059C6562E681
- Produced At: Feb 16 08:58:07 2017 GMT
- Responses:
  - Certificate ID:
    - Hash Algorithm: sha1
    - Issuer Name Hash: 939E0296797407B76FB212BB47B89B99DEDF8C102
    - Issuer Key Hash: F6E04582CB0C4B0EB4588821F58E47BE24866050
    - Serial Number: 1425DCA4CC5BC2AF83A0F2D3ADE8DD20
  - Cert Status: good
- This Update: Feb 16 08:58:07 2017 GMT
Using ClearPass Onboard
### ClearPass Recap

**ClearPass Policy Manager**
- Policy Engine
- AAA (RADIUS/TACACS)
- Device Profiling
- SSO (SAML, OAUTH)
- Device Registration/Provisioning
- Certificate Authority
- Guest Captive Portal

**Included**
- Feature Licenses

<table>
<thead>
<tr>
<th>Guest</th>
<th>Onboard</th>
<th>Onguard</th>
</tr>
</thead>
</table>

**Identity Stores**
- Active Directory
- LDAP
- Kerberos
- SAML IDP
- Multi-Factor
- OAUTH

**Context**
- Internal:
  - Device Profile
  - Posture
- External:
  - AD/LDAP
  - SQL Databases
  - MDM
  - HTTP sources

---

**NADs**
- Controllers
- APs
- Switches
- VPN
- Multivendor
- HPE Aruba
- Cisco...

**Controllers**
- APs
- Switches
- VPN

**Multivendor**
- HPE Aruba
- Cisco...

**Identity Stores**
- Active Directory
- LDAP
- Kerberos
- SAML IDP
- Multi-Factor
- OAUTH

**Context**
- Internal:
  - Device Profile
  - Posture
- External:
  - AD/LDAP
  - SQL Databases
  - MDM
  - HTTP sources
What is ClearPass Onboard

- Automatic configuration of network settings for wired and wireless endpoints
- Provisioning of unique device credentials for BYOD and IT-managed devices
- Support for Windows, macOS, iOS, iPadOS, and Android devices
- Ability to revoke unique credentials on a specific user's device
- Set limits using context from identity stores
- ClearPass Profiler for identifying device type, manufacturer, and model
- Support for 1:1 user to device or many users to a shared device
- Self-service portal to manage enrollment and device lifecycle
ClearPass Onboard Methods
Device vs. User Registration

– ClearPass offers two options

1. Device Enrollment and unique credential provisioning – EAP-TLS certificates with policy
   – Eduroam onboarding
   – Unique certificate per user per device (provisions for shared systems)
   – Highest security
   – Requires Onboard license or subscription

2. “Headless device” registration – mac address based self-service entry with policy
   – Game systems, smart TVs, IOT devices, etc
   – mPSK option available with Aruba WLAN – unique PSK per MAC address
   – Included in ClearPass base license
Leverage your guest network!

– You don’t need a dedicated SSID for Onboarding!
– Use your guest network. It’s already there!
– Additional SSIDs add overhead and confusion
– Leverage SAML or OAuth 2.0
  – Microsoft Azure MFA
  – DUO
  – Other SSOs like OKTA
ClearPass Onboarding Workflow using Guest SSID

1. **CLIENT DEVICE**
   - Associates to open/guest SSID

2. **CONTROLLER**
   - MAC Authentication
   - Web traffic redirected to ClearPass
   - Device onboarding process
   - Onboarding complete
   - EAP-TLS authentication
   - RADIUS accept
     - Final role

3. **CLEARPASS**
   - MAC cached?
   - Valid credentials?
     - Valid credentials!

4. **IDENTITY PROVIDER**
   - Optional authorization

5. **WEB LOGIN**

6. **DISCONNECT**
   - Connects to 1X SSID
ClearPass Onboarding Process with iOS

iOS Device

User accepts provisioning profile

Install device identity certificate

Install profile and return to Safari

Switch to EAP-TLS

Network Infrastructure

Start device provisioning (signed profile payload)

Request for device provisioning

SCEP provisioning profile

Request device certificate using SCEP

ClearPass Onboard

ClearPass Policy Manager

Apple Over-the-Air Provisioning

User authenticated for device provisioning

Issue SCEP certificate for device

Generate TLS certificate and payload with Onboard settings

Device configuration profile (signed + encrypted)

Refresh device provisioning progress page

Provisioning Complete
ClearPass Onboard Configuration
Encompassing PKI options

- Support for multiple certificate authorities
  - Useful for segmentation of larger user/device bases
  - Different CA properties
- Use existing PKI already in production
- Create different expiration periods
  - Students vs lab machines
- Option for ADCS integration or proxy to a reg authority
ClearPass Onboard Configuration
Multiple options and use cases

– Support for multiple provisioning profiles
– Create profiles for wired, wireless, or both
– Only allow certain OS types to onboard
– Restrict only certain groups based on AD

<table>
<thead>
<tr>
<th>Name</th>
<th>Network Type</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>edurcam - LAB</td>
<td>Wireless</td>
<td>edurcam</td>
</tr>
<tr>
<td>edurcam - user</td>
<td>Wireless</td>
<td>edurcam</td>
</tr>
<tr>
<td>Fiemont Secure SSID</td>
<td>Wireless</td>
<td>fiemont-secure</td>
</tr>
<tr>
<td>Gonzaga Community - LAB</td>
<td>Wireless</td>
<td>Gonzaga Community</td>
</tr>
<tr>
<td>Gonzaga Community - user</td>
<td>Wireless</td>
<td>Gonzaga Community</td>
</tr>
<tr>
<td>Wired Authentication - user</td>
<td>Wired</td>
<td></td>
</tr>
</tbody>
</table>

Device Provisioning Settings

- **Android Provisioning**
  - Options control Android device provisioning.

  - **Enable Android device provisioning**: Downloads and executes an Android application on a user’s device to complete provisioning.
  - **Android rootkit detection**: Controls whether devices with a rootkit may be provisioned.
  - **Android Browser Check**: Enables browser checking for Android.

- **Chrome OS Provisioning**
  - Options control Chrome OS device provisioning.

  - **Enable Chrome OS device provisioning**: Provides a certificate to Chrome OS devices. Requires the device to be under management and the QuickConnect extension to be configured for pre-install.

- **iOS Provisioning**
  - Options control iOS device provisioning.

  - **Enable iOS device provisioning**: Provides iOS devices via Apple’s “Over-the-Air” profile delivery process.
  - **iOS Browser Check**: Enables browser checking for iOS.

- **iPadOS Provisioning**
  - Options control iPadOS device provisioning.

  - **Enable iPadOS device provisioning**: Provides iPadOS devices via Apple’s “Over-the-Air” profile delivery process.
  - **iPadOS Browser Check**: Enables browser checking for iPadOS.

- **macOS Provisioning**
  - Options control macOS device provisioning.

  - **Enable macOS device provisioning**: Provides macOS with secure boot and allows manual configuration.
  - **macOS Browser Check**: Enables browser checking for macOS.

  - **MacOS Devices**: Provides macOS 10.7+ (user or latest) device provisioning via Apple’s “Over-the-Air” profile delivery process.
ClearPass Onboard Configuration
Customizable user facing pages

– Full control over web page look and feel
– Customize labels, forms, HTTP/CSS code
– Use Aruba’s skins service to match current branding and web design style
– Several options to override default labels and values

**Web Login Page**
Options for the weblogin landing page for Onboard.

**Page Name:**
aruba_univ_provisioning
Enter a page name for this web login.
The web login will be accessible from "onboard/page_name.php".
ClearPass Onboard Configuration
Integrate with cloud identity and MFA

- Support MFA and cloud identity
- Based on provisioning profile – not “all or nothing”
- Several cloud and social identity sources to choose from

Multi-Factor Authentication
Require a secondary factor when authenticating.

Provider:
✓ No multi-factor authentication
  Duo Security - Two Factor Authentication
  ImageWare Systems - Solutions Powered by GoVerifyID
  SMS Verification Codes
ClearPass Onboard Lifecycle Management
Certificate expirations and inactivity

– Proactively notify users
– Optionally send to a default mailbox
– Customize the email format and content
– Expire/revoke certificates based on inactivity

Certificate Expiry:
☑ Notify users before their device credentials expire
If checked users will receive an email notification when their device’s network credentials are due to expire.

* Send Email Notification:
4 weeks prior to expiration
Select the time to send an email notification.

* If Email is Unknown:
Send a message to a fixed email address
Specify where to send emails to if the user’s certificate doesn’t have an email address recorded.

* Unknown Address:
onboard_expiration@arubauniversity.edu
Address used when no email address is known for a user.

Subject Line:
Your network credentials are about to expire
Enter a subject for the notification email.
Leave blank to use the default (Your network credentials are about to expire).

Revoke Inactive:
☑ Revoke certificates for inactive devices
If checked the certificates for devices will be revoked after a period where the device is not seen on the network.

This feature relies on data from ClearPass Insight.
You must have a primary Insight node enabled and with an appropriate data retention period configured for inactivity calculations to work correctly.

* Inactivity Period:
30 days
If a device does not authenticate on the network after this period its certificate will be revoked.
ClearPass Onboard Lifecycle Management

Management of certificates

- View by device, user, or certificate
- Revoke or delete user’s device
- Enable self-service for a user or department
- Obtain device details

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Device Name</th>
<th>Device ID</th>
<th>User</th>
<th>Status</th>
<th>Onboarded</th>
<th>Managed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>macOS</td>
<td>Seth's MacBook Air</td>
<td>udid:222798A9-999C-5B0D-8AECD569A353D86E</td>
<td>seth</td>
<td>Enrolled</td>
<td>✓</td>
<td>1 User(s)</td>
</tr>
<tr>
<td>macOS</td>
<td>Seth's MacBook Pro</td>
<td>udid:EA704D9-FB6C-556B-A394-1BDBBB97EC09</td>
<td>seth</td>
<td>Enrolled</td>
<td>✓</td>
<td>2 User(s)</td>
</tr>
<tr>
<td>iOS</td>
<td>iPhone</td>
<td>udid:00008101-0004786E3688001E</td>
<td>seth</td>
<td>Enrolled</td>
<td>✓</td>
<td>1 User(s)</td>
</tr>
<tr>
<td>iPadOS</td>
<td>iPadOS</td>
<td>udid:00008027-001224622262802E</td>
<td>seth</td>
<td>Enrolled</td>
<td>✓</td>
<td>1 User(s)</td>
</tr>
<tr>
<td>Windows</td>
<td>Windows 10</td>
<td>mac:ac:82:47:4b:10:9a</td>
<td>seth</td>
<td>Enrolled</td>
<td>✓</td>
<td>1 User(s)</td>
</tr>
</tbody>
</table>
Configuring ClearPass Onboard
ClearPass Onboard Checklist

1. Configure the Onboard Certificate Authority.
2. Configure network settings for device provisioning.
   - Set network properties – SSID name, authentication method/type
   - Set device-specific networking settings
3. Bind network settings to configuration profile
4. Configure the Onboard provisioning settings
   - Select certificate options for device provisioning
   - Select the configuration profile
   - Select which device types should be supported
   - Setup and customize the device provisioning web login page
   - Customize text for labels and messages shown before, during, and after provisioning
   - Specify options for Apple device provisioning and security
   - Customize the Onboard client for Windows and Android
   - Enable sponsorship (optional)
5. Create the Policy Manager Services
ClearPass Onboard Suggestions

- Use the ClearPass Onboard Certificate Authority
  - Consider multiple CAs for different groups or functional purposes
- Use a publicly signed certificate as the code-signing cert
  - Streamlines the user experience specifically for Apple devices
    - Eliminates the root certificate download step
- Use the dual-SSID method
  - Consider the guest network or a dedicated provisioning SSID
- Customize available instructions, settings, web content
  - Provide self-help and guidance along the way
1. Create a New Certificate Authority

- Choose Root CA
- Set a user friendly name indicating intent of the CA.
  - Example: Aruba University Device Enrollment CA
  - Enter an institution specific email address
- Private Key type should be at least 2048-bit
- Expiration of the CA should be lengthy
- NOTE: This is not the expiration time of the onboarded certificates

**CA Expiration:**

3653 days

The number of days before the certificate authority's root certificate will expire.
2. Configure Onboard Network Settings

- **Access tab**
  - Create a friendly name
  - Set network type to wireless
  - Set security type to 802.1X
  - Enable checkbox to automatically connect
2. Configure Onboard Network Settings

– On the *Protocols* tab, leave all defaults to TLS

<table>
<thead>
<tr>
<th>Network Settings</th>
<th>Enterprise Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access#</td>
<td>Protocols</td>
</tr>
</tbody>
</table>

**Enterprise Protocols**
Options for 802.1X protocols supported on the network.

**iOS & macOS EAP**

**Accepted EAP Types**

- **TLS**
- **PEAP**
- **EAP-SIM**
- **TTLS**
- **EAP-FAST**

Select the authentication protocols to use when configuring an iOS or macOS 10.7+ (Lion or later) device.

**Legacy OS X EAP**

**Legacy OS X EAP:**
PEAP with MSCHAPv2
Select the authentication protocol to use when configuring
OS X 10.5/6 (Leopard/Snow Leopard) devices.

**Android EAP**

**Android EAP:**
TLS
Select the authentication protocol to use when configuring an Android device.

**Windows EAP**

**Windows EAP:**
TLS
Select the authentication protocol to use when configuring a Windows device.

**Ubuntu EAP**

**Ubuntu EAP:**
TLS
Select the authentication protocol to use when configuring an Ubuntu device.
2. Configure Onboard Network Settings
   – On the *Authentication* tab, leave all defaults for 1:1 user to device enrollment

<table>
<thead>
<tr>
<th>Network Settings » Enterprise Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enterprise Authentication</strong></td>
</tr>
<tr>
<td>Options for 802.1X authentication used on the network.</td>
</tr>
<tr>
<td><strong>Android Authentication</strong></td>
</tr>
<tr>
<td>* Certificate Store:</td>
</tr>
<tr>
<td>* Private</td>
</tr>
<tr>
<td>Select the certificate store where the client certificate will be provisioned when configuring an Android device. Installing to the system store will make certificates available for use by other applications, but may require additional security prompts during provisioning.</td>
</tr>
<tr>
<td><strong>iOS &amp; macOS Authentication</strong></td>
</tr>
<tr>
<td>* iOS &amp; macOS Credentials:</td>
</tr>
<tr>
<td>* Certificate</td>
</tr>
<tr>
<td>Select the type of credentials to provision for iOS and macOS 10.7+ (Lion or later) devices.</td>
</tr>
<tr>
<td><strong>Windows Authentication</strong></td>
</tr>
<tr>
<td>* Certificate Store:</td>
</tr>
<tr>
<td>* User</td>
</tr>
<tr>
<td>Select the certificate store where the client certificate will be provisioned when configuring a Windows device.</td>
</tr>
</tbody>
</table>
2. Configure Onboard Network Settings
   - On the *Trust* tab, leave the default settings

   - Change these settings to push additional or different RADIUS server certificates to the device for trust purposes
     - Example: ADCS workflow or non ClearPass authentication servers

   - Remaining tabs - Windows and Proxy - leave at default settings

   **Enterprise Trust**
   Certificate trust options for 802.1x protocols supported on the network.

   **Configure Trusted Servers:**
   - *Automatically configure trusted servers (recommended)*
   
   Automatic settings will trust all ClearPass servers currently in the cluster.
   You should manually enter server names if:
   - You are not using ClearPass for RADIUS authentication
   - You plan to expand your ClearPass cluster at a later date (use a wildcard rule in this case)

   **Configure Trust:**
   - *Automatically configure trust settings (recommended)*
   
   Use automatic configuration if you are using Policy Manager for authentication.
   Otherwise, select manual configuration.
3. Configure Onboard Configuration Profile

- The purpose of the Configuration Profile is to bind the Network Settings from step 2
- It is possible to provision multiple networks (SSIDs) to the enrolled devices in a single Configuration Profile
- For this walkthrough, only select the network defined in the previous step

Networks:
- Aruba University Secure SSID
- eduroam - LAB
- eduroam - user
- Fiermonti-Secure SSID
4. Configure Onboard Provisioning Settings

Putting it all together – General tab

– Give the entire profile a friendly name and description
– Enter the Organization’s name
– Under Identity, select the CA configured in Step 1
– Under Authorization, leave the default App Authentication. We will configure this next in a Policy Manager service
– Select the Configuration Profile from step 3
– Optionally configure certificate actions
4. Configure Onboard Provisioning Settings

Putting it all together – General tab - Actions

– Enable email notifications for expiring certificates
– Select 1-4 weeks prior
– If email unknown, set a general mailbox
– Enter the subject line
– Customize the email by navigating to Configuration → Receipts → Templates → Certificate Expiry
– Optionally set an email address to cc or bcc

**Actions**

These options control actions that may be taken after device provisioning.

**Certificate Expiry:**
- Notify users before their device credentials expire
  If checked users will receive an email notification when their device's network credentials are due to expire.
- *Send Email Notification:*
  - 4 weeks prior to expiration
  - Select the time to send an email notification.
- *If Email is Unknown:*
  - Send a message to a fixed email address
  - Specify where to send emails to if the user's certificate doesn't have an email address recorded.
- *Unknown Address:*
  - onboard_expiration@arubauniversity.edu
  - Address used when no email address is known for a user.

**Subject Line:**
- Your network credentials are about to expire
  - Enter a subject for the notification email.
  - Leave blank to use the default (Your network credentials are about to expire).
- *Email Message:*
  - Certificate Expiry
  - The plain text or HTML print template to use when generating an email message.
- *Email Skin:*
  - (Use Default: Use the default skin)
  - The format in which to send email receipts.
- *Send Copies:*
  - Always send using “Bcc:”
  - Specify when to send to the recipients in the Copies To list.

**Copies To:**
- onboard_expiration@arubauniversity.edu
  - An optional list of email addresses to which copies of expiry notifications will be sent.
4. Configure Onboard Provisioning Settings

Putting it all together – Supported Devices tab

– Select the devices available to be onboarded
– Under iOS and iPadOS, recommend enabling forcing the use of Safari to provide the best user experience
– Recommend setting the device detection to “Always” to allow users to select their device type should browser detection fail
4. Configure Onboard Provisioning Settings

Putting it all together – Web Login tab

- Set the page name. This is the URL that will be given to users or used in a captive portal
- Customize look and feel of the login page
  - edit the title, HTML, apply a skin

<table>
<thead>
<tr>
<th>Web Login Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options for the weblogin landing page for Onboard.</td>
</tr>
</tbody>
</table>

- **Page Name:**
  - device_enrollment
  - Enter a page name for this web login.
  - The web login will be accessible from '/onboard/page_name.php'.

- **Skin:**
  - Aruba ClearPass Skin
  - Choose the skin to use when this web login page is displayed.

<table>
<thead>
<tr>
<th>Title:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba Student Device Registration</td>
</tr>
<tr>
<td>The title to display on the web login page. Leave blank to use the default (Register Your Device).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Header HTML:</th>
</tr>
</thead>
<tbody>
<tr>
<td>{nwa_text id=16344}In order to connect to this network, your device must be registered with Aruba University ITS. This wizard will guide you through the configuration process. {/nwa_text} {/nwa_loopcontext}</td>
</tr>
<tr>
<td>{capture assign=organization_name}{nwa_mdps_configname=organization_name}{/capture}</td>
</tr>
<tr>
<td>{nwa_text id=14462}Login below using your RC credentials. {/nwa_text}</td>
</tr>
</tbody>
</table>
4. Configure Onboard Provisioning Settings

Putting it all together – Web Login tab

– See below color coding for config to UX mappings based on MacOS

OS Specific messages - configured in Pre-Login section on the Instructions and Messages tab

macOS Instructions
These options control messages shown during macOS device provisioning.

Pre-Login:
Use custom message

Instructions shown to the user before they log in using an macOS device.

Pre-Login Message:
For your Apple Mac, Aruba University network provisioning is a multi-step process. In order to configure your device you must follow this process to completion.
4. Configure Onboard Provisioning Settings

Putting it all together – Instructions and Messages tab

– Use this tab to create customized and detailed messaging and instructions throughout the onboarding process

– Create custom messages for denied, expired, reprovisioned, or unsupported devices

– Override default messages for specific OSs
  – Android
  – iOS
  – iPadOS
  – MacOS
  – Windows
  – Web-based
4. Configure Onboard Provisioning Settings

Putting it all together – Instructions and Messages tab

- Use this tab to create customized and detailed messaging and instructions throughout the onboarding process
- See below for color coded config to UX mappings based on MacOS
- Profile Download Page - This is the **FIRST** page post login

**Message for ALL OS types**
(Will be displayed at the top of all post-login pages)

**Provisioning Device:**
- Use custom message

Message shown to the user during the provisioning process (after login).

**Provisioning Message:**

{nwa_icontext:type=info}

(nwa_text id=16344)In order to connect to this network, your device must be registered with ITS. This wizard will guide you through the configuration process. Remember to complete all steps! (/nwa_text)

**Message for SPECIFIC OSs**
(Based on browser detection or user specified from dropdown list)

**Profile Download:**
- Use custom message

Instructions shown to the user when asked to download the macOS profile.

**Profile Download Message:**

{nwa_text id=16443}For your Apple Mac, Aruba University network provisioning is a multi-step process. In order to configure your device you must download and install this provisioning profile which will configure your device to connect to the network. (/nwa_text)
4. Configure Onboard Provisioning Settings

Putting it all together – Instructions and Messages tab

- Use this tab to create customized and detailed messaging and instructions throughout the onboarding process
- See below for color coded config to UX mappings based on MacOS
- Installing Profile page - This is the SECOND page post login

Message for ALL OS types
(Will be displayed at the top of all post-login pages)

Message for SPECIFIC OSs
(based on browser detection or user specified from dropdown list)

Provisioning Device:
- Use custom message
- Message shown to the user during the provisioning process (after login).

Provisioning Message:
- (nwa_context type=info)
- (nwa_text id=16344)In order to connect to this network, your device must be registered with ITS. This wizard will guide you through the configuration process. Remember to complete all steps! (nwa_text)

Installing Profile:
- Use custom message
- Instructions shown to the user while the macOS profile installs.

Installing Profile Message:
- <p>
- (nwa_text id=16442)You're almost done! Check your download folder and click on the mobileconfig file that was just downloaded and open System Preferences. Click the Profiles icon and find the downloaded profile. Click install to finalize the registration process. (nwa_text)
- </p>
4. Configure Onboard Provisioning Settings

Putting it all together – Instructions and Messages tab

- Use this tab to create customized and detailed messaging and instructions throughout the onboarding process
- See below for color coded config to UX mappings based on MacOS
- Complete page - This is the FINAL page post login

Message for SPECIFIC OSs (based on browser detection or user specified from dropdown list)
4. Configure Onboard Provisioning Settings

Putting it all together – Apple Profiles tab

– Apple devices use SCEP to enroll and install certificates

– The configuration profiles are downloaded and installed by the user
  – The Organization name from the General tab is used to name the downloaded .mobileconfig file

– Use a publicly signed cert as the profile signing cert!
  – Avoids the root certificate step
  – Marks the profile as “verified”

![Downloads](image_url)
4. Configure Onboard Provisioning Settings

Putting it all together – Apple Profiles tab

– See below for color coded config to UX mappings based on MacOS

![Profile settings in MacOS System Preferences](image)

Publicly signed certificate!
4. Configure Onboard Provisioning Settings

Putting it all together – Apple Profiles tab

– What happens when you install the profile (MacOS)

Install the profile

**Trusted server certs**

**Personalized TLS cert**

**Network Settings**

**SCEP Process**

**NOTE:** Certificate Authority configured in step 1

**Wi-Fi Network Settings**

Note: EAP-TLS as EAP type

Result

<table>
<thead>
<tr>
<th>Settings</th>
<th>Certificate Authority configured in step 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Authority</td>
<td>ClearPass Onboard Local Certificate Authority (Signing)</td>
</tr>
</tbody>
</table>

**SCEP Enroll**

<table>
<thead>
<tr>
<th>Description</th>
<th>SCEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td><a href="https://clearpass.fiernont.net/onboard/mdps_scep.php/tls/7bde340d991f5b5b08ba2beea23e3">https://clearpass.fiernont.net/onboard/mdps_scep.php/tls/7bde340d991f5b5b08ba2beea23e3</a></td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>ClearPass Onboard Local Certificate Authority (Signing)</td>
</tr>
<tr>
<td>Expires</td>
<td>Jan 31, 2023 at 10:07 AM</td>
</tr>
<tr>
<td>Issuer</td>
<td>ClearPass Onboard Local Certificate Authority (Signing)</td>
</tr>
</tbody>
</table>

**Wi-Fi Network**

<table>
<thead>
<tr>
<th>Description</th>
<th>eduroam - user</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>eduroam</td>
</tr>
<tr>
<td>Encryption</td>
<td>WPA2 Enterprise</td>
</tr>
<tr>
<td>Enterprise Profile ID</td>
<td>A51D9B9E-42EB-4D14-B77C-073B9A4C2B5</td>
</tr>
<tr>
<td>EAP Type</td>
<td>EAP-TLS</td>
</tr>
<tr>
<td>Auto Join</td>
<td>True</td>
</tr>
<tr>
<td>Proxy Type</td>
<td>None</td>
</tr>
</tbody>
</table>
4. Configure Onboard Provisioning Settings

Putting it all together – Onboard Client tab

– Used for Windows and Android onboarding
  – via ArubaQuickConnect.exe for Windows
  – via ClearPass QuickConnect app in Google Play
– Customized logo displayed in the app
  – Upload files to Configuration ➔ Content Manager ➔ Public Files
– Set a provisioning address
– Configure a title, password recovery and/or helpdesk URL

Options for Windows, Android and Legacy OS X (10.6/8) device provisioning.
These settings are not used for iOS, iPadOS or macOS 10.7+ (Lion or later) devices.

**Code-Signing Certificate:**

Name — Use Aruba factory signature
Select a code signing certificate for signing the Windows provisioning application.

**Provisioning Address:**
clearpass.fiormonti.net (requires DNS resolution)
Select the hostname or IP address to use for device provisioning.

**Provisioning Access:**

To be provisioned, devices must be able to access clearpass.fiormonti.net via HTTPS.

**Validate Certificate:**

No, do not validate this web server's certificate
Specify whether the web server's certificate is to be validated during device provisioning.
When testing with the default self-signed web server certificate, you may need to disable validation.
This option applies to Windows, Android, and OS X 10.5/6 devices only.

**Bypass Proxy:**

[ ] Bypass proxy server
If checked, the proxy server configured on the client will not be used during the Onboard enrollment process.

**Logo Image:**

Select an image to use in the provisioning wizard. New images can be uploaded using the Content Manager.

**Wizard Title:**

[ ] Aruba University Device Enrollment Wizard
Enter a title for the wizard used on Windows and Legacy OS X (10.6/8) devices.

**Password Recovery URL:**

Enter the URL displayed to users who have forgotten their password.

**Helpdesk URL:**

[ ] https://www.arubauniversity.edu/content/it-web/offices/lts/support1
Enter the URL displayed to users who require helpdesk assistance.
4. Configure Onboard Provisioning Settings

Putting it all together – Onboard Client tab

![Aruba University Device Enrollment Wizard]

**Device Provisioning**
Options for Windows, Android, and Legacy OS X (10.5/8) device provisioning.
These settings are not used for iOS, iPadOS, or macOS 10.7+ (Lion or later) devices.

- **Code-Signing Certificate:**
  - None — Use Aruba factory signature

- **Provisioning Address:**
  - clearpass.fiormonti.net (requires DNS resolution)
  - Select the hostname or IP address to use for device provisioning.

- **Provisioning Access:**
  - To be provisioned, devices must be able to access clearpass.fiormonti.net via HTTPS.

- **Validate Certificate:**
  - No, do not validate this web server’s certificate
  - Specify whether the web server’s certificate is to be validated during device provisioning.

- **Bypass Proxy:**
  - Bypass proxy server
  - If checked, the proxy server configured on the client will not be used during the Onboard enrollment process.

**Logo Image:**
Select an image to use in the provisioning wizard. New images can be uploaded using the Content Manager.

**Wizard Title:**
Aruba University Device Enrollment Wizard
Enter a title for the wizard used on Windows and Legacy OS X (10.5/8) devices.

**Password Recovery URL:**
Enter the URL displayed to users who have forgotten their password.

**Helpdesk URL:**
https://www.arubauniversity.edu/content/hr-web/offices/fts/support/
Enter the URL displayed to users who require helpdesk assistance.

**Downloads**
ArubaQuickConnect.exe
Open file
Optional Onboard Provisioning

Shared Computers

- Focus on Windows and MacOS
  - Restrict to these OS types
- Create a different provisioning page
- Use a shared resource identity account
  - This will become the username on the network
    - sciencelab@arubauniversity.edu
    - it_testing@arubauniversity.edu
- Create policy to only allow the shared resource accounts to onboard a device
- Use Machine certificate store in Windows
  - Configured in Onboard Network Settings
- Use System store for MacOS
  - Configured in Onboard Provisioning Settings
Onboard Services in Policy Manager

Use Wizard to setup the two services

- Navigate to Configuration → Service Templates & Wizards
  - Bottom of the list
- Select “Onboard Services Only”
- Creates two services
  1. A pre-auth service used at the web login page
  2. Authorization service used when generating and enrolling the certificate
Onboard Services in Policy Manager

Configure the Onboard Pre-Auth and Authorization services

- Add a line to service rule to granularly apply policy to a specific onboard web login page
- Page-Name equals the web login page name configured in the Onboard provisioning settings
- Edit the services post wizard to add AD as an authentication source
Customizing the Web Pages
How to brand and create a familiar UX for users
BONUS: Editing the Galleria Skin

What is the Galleria Skin?

– Every installation of ClearPass includes 2 Galleria Skins.
– Easy to customize modern and professional looking web designs
– Can be applied to both user facing and administrative back end pages
– Advanced editing of HTML and CSS possible
– Turnkey service provided with Aruba Skin service
BONUS: Editing the Galleria Skin

Edit Options – Colors
– See how color options relate to web pages
– See if organization has a style or branding guide
BONUS: Editing the Galleria Skin

Edit Options – Title, Logo, Icons, Copyright
– See how options relate to web pages

Title Prefix:
Galleria Wi-Fi
The prefix for the browser page title. For example: <title>Galleria Wi-Fi</title>

Favicon:
[default]
Select the favicon to use.

Logo:
logo-public.png (128 x 100)
The logo image to use for the skin. Recommended: Use a high-resolution image.

Copyright:
&copy; Copyright ("Y")[date]
Insert...
Override the copyright text for the license.

Include Logo on Guest Login:
- Show Logo
  Include the logo on guest-facing pages.
- Include Copyright on Guest Login:
  - Show Copyright
    Include the copyright information on guest-facing pages.
BONUS: Editing the Galleria Skin

Edit Options – Background Images

– By default, the Galleria skin includes 6 images taken by Aruba employees
– Images can be edited and replaced
– Upload images to Configuration → Content Manager → Public
– Recommend creating a folder to upload images
– Larger file sizes can create a delay in rendering
– Set path in the Background Images text box
  – Path example “/guest/public/<foldername>/<imagename>”
  – Optionally set a transition delay
BONUS: Editing the Galleria Skin

Edit Options – Guest form display

– Boxed vs Floating

– Light vs Dark (only available with Boxed option)

– Labels vs Placeholders
Advanced Onboard Policies

Use identity to change Onboard workflows and settings
BONUS: AD Based Onboard Policies

Customize ClearPass Policy Manager Services

- As mentioned previously, there are 2 ClearPass services created for Onboard - pre-auth and authorization
- The sample request shown shows some of the details ClearPass knows about a user requesting a certificate
- Using this context, we can change onboard policies and certificates
- Following workflow will create this policy
  - New student device == 4 year certificate expiration
  - Renewed student device == 6 month certificate expiration
  - Limit students to 3 devices each
BONUS: AD Based Onboard Policies
Edit the Certificate Authority – Increase Validity Period

- The certificate authority must have a certificate validity period greater than any value in the enforcement profile
- Set to a maximum value in days to leverage policies up to this limit
- Default value is 365 days
**BONUS: AD Based Onboard Policies**

Create new Enforcement Profiles – Certificate Expiration using Time Source

- Profile template is “Generic Application Enforcement”
- New Onboard device will receive a 4 year certificate expiration
  - Use Session-Timeout in seconds
    - ClearPass:Session-Timeout = 126144000
- Renewed Onboard device will receive a 6 month certificate expiration
  - Use Session-Timeout in seconds
    - ClearPass:Session-Timeout = 15780000
**BONUS: AD Based Onboard Policies**

Create new Enforcement Profiles – max allowed devices

- Profile template is “Generic Application Enforcement”
- Create a new profile to limit Onboarded devices per user to 3
BONUS: AD Based Onboard Policies

Edit the Onboard AppAuth Enforcement Policy

- Create new rules to map identity structure to the created enforcement profiles

<table>
<thead>
<tr>
<th>Summary</th>
<th>Enforcement</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules Evaluation Algorithm:</td>
<td>Select first match</td>
<td>Select all matches</td>
</tr>
<tr>
<td>Enforcement Policy Rules:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Actions</th>
</tr>
</thead>
</table>
BONUS: AD Based Onboard Policies
Customize the Onboard Authorization Service

- Edit the service rules
  - add the Page-Name to granularly apply policy to a specific Onboard URL
- Add identity sources as AuthZ sources
- Confirm the edited Enforcement Policy is applied to the service
Creating the Onboard Self-Service Portal

Allow users to self-manage their own devices and certificates
**BONUS: Self-Service Enablement**

Portal for Onboarded device lifecycle management

- Ability for users to self-manage their own devices
- Uses Operator Profiles already pre-built in ClearPass
- Customize new Operator Profiles to suit organization's needs
- Ability to see only one's own devices, any devices shared between a common group, or administrative access for complete visibility
- Actions to mark a device lost or delete a device/user
**BONUS: Self-Service Enablement**

Portal for Onboarded device lifecycle management

- Controlling access to guest/onboard is done via Administration ➔ Operator Logins ➔ Profiles

- BYOD Operator is the pre-built profile
  - Duplicate this profile to build your own custom access like “Student”
  - Example shown to the right
BONUS: Self-Service Enablement
Portal for Onboarded device lifecycle management

– Map Operator Profile to Policy
– In Enforcement Profile, use the attribute “admin_privileges”
– Tie Enforcement Policy to these new Profiles

Enforcement Profiles - Guest Student User

Enforcement Profiles - Guest Admin User

Services - Guest Operator Login to AD

Enforcement Policy Details
Description: [Deny Application Access Profile]
Rules Evaluation Algorithm: first-applicable

Conditions
1. (Authentication:Username \text{\_EQUALS\_IGNORE\_CASE} \text{seth}) Guest Admin User
2. (Tips:Role \text{\_EQUALS} \text{Student}) Guest Student User