# Lab 2 Section 3 – Black Bear Home Guardian Product Requirements

Team Red

Old Dominion University

CS411W

Professor Janet Brunelle

27 April 2021

Version II

## Table of Contents

3 Specific Requirements…………………………………………………...……...… 3-3

3.1 Functional Requirements..…………………………………………......….… 3-3

3.2 Performance Requirements..……………………………………...…....…. 3-4

3.3 Assumptions and Constraints..………………………………...…..….… 3-5

3.4 Non-Functional Requirements..………………………………………………… 3-6

## List of Figures

Figure 1: VLAN Grouping Logic………...…………………..………..…………….…. 3-4

Figure 2: Admin User Vlan Selection Modal………..……………………..……………….…. 3-7

## List of Tables

Table 1: Black Bear Access Control Table.…………………..………..…………….…. 3-3

# 3 Specific Requirements

## 3.1 Functional Requirements

**3.1.1 Cross-Platform Support.** *(Katie)* The Black Bear portal shall be built as a cross-platform application. The following requirements shall be met:

**3.1.1.1 Desktop.** The Black Bear web application portal shall be able to run on major web browsers. The following browsers shall be supported:

A. Google Chrome
B. Safari

**3.1.1.2 iOS Application.** The Black Bear iOS application portal shall be able to run on any Apple iOS device. The following devices shall be supported:

A. iPhone

**3.1.2 User Roles.** *(Katie)* Black Bear shall have three distinct user roles with corresponding distinct privilege. The following users shall be designated privileges on the network, as indicated in Table 1:

**3.1.2.1 Administrative User.** The Administrative User shall be authorized with full access to managing the network and its devices.

**3.1.2.2 Standard User.** Standard Users shall be authorized with limited access to managing the network and its devices with respect to the Administrative User.

**3.1.2.3 Guest User.** Guest Users shall have only their device(s) authorized to the Guest VLAN with no access to managing the network or its devices.

**Table 1**
*Black Bear Access Control Table*

| | USER ROLE | | |
|---|---|---|---|
| ACTION | Guest | Standard | Admin |
| Access portal from desktop or mobile device | | ✓ | ✓ |
| Provided credentials for portal access | | ✓ | ✓ |
| Access to Internet on the home network | ✓ | ✓ | ✓ |
| View & identify devices on the network | | ✓ | ✓ |
| Manage devices on the network (edit, remove) | | ✓ | ✓ |

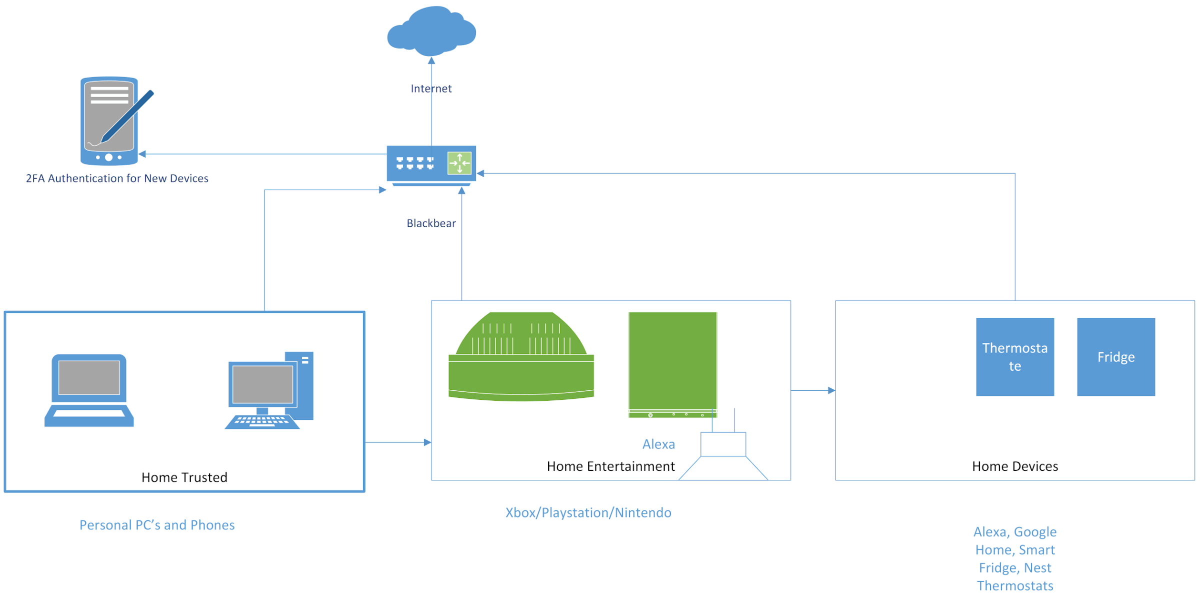
| | | | |
|---|---|---|---|
| Authorize new devices to the network | | ✓ | ✓ |
| Authorize new users to the network | | | ✓ |
| Authorize new Guest devices to the network | | ✓ | ✓ |
| Manage VLANs on the network (create, edit, remove) | | | ✓ |

**3.1.3 VLAN Segmentation.** *(Katie)* OpenWrt shall be built with custom configurations for default segmented VLANs for segmenting devices on the network.

**3.1.3.1 Default VLAN Groups.** The Black Bear portal shall be configured with four logical network segments for Registered Users to add devices to. The following groups shall exist in the Black Bear portal UI as default:

A. Computers/Phones
B. Smart Home
C. Gaming/TV
D. Guest

**Figure 1**
*VLAN Grouping Logic*


Internet
2FA Authentication for New Devices
Blackbear
Home Trusted
Personal PC's and Phones
Alexa
Home Entertainment
Xbox/Playstation/Nintendo
Thermosta te
Fridge
Home Devices
Alexa, Google Home, Smart Fridge, Nest Thermostats

**3.1.4 Router Hardware Independence** *(Jordan)* The Black Bear hardware demonstration shall not require one particular piece of router hardware. The following requirements will ensure hardware independence:

**3.1.4.1 Firmware Implementation** The Black Bear hardware demonstration shall be implemented as an OpenWRT firmware package. This firmware package shall exist in flashable format for flashing onto routers.

**3.1.4.2 Specific Router Independence** The Black Bear hardware demonstration firmware package shall allow installation on a router which supports necessary Black Bear features.

**3.1.5 Administrative Credential Setup** *(Jordan)* The Black Bear web portal shall require an administrative account to be set up on first use. The following requirements will ensure that the administrative credentials are created:

**3.1.5.1 Administrative Credential Customization** The Black Bear web portal shall prompt the user to set up administrative credentials when accessing the Black Bear portal when no administrative credentials exist.

**3.1.5.1.1 Credential Creation Prompt** The Black Bear web portal administrative credential prompt shall contain the following components:

A. Username entry text field
B. Password entry text field
C. Form submission button

**3.1.5.1.2 Credential Creation Prompt Success Requirements** The Black Bear web portal credential setup prompt shall be submittable to the Black Bear backend. The Black Bear credential setup prompt submission shall succeed if the following requirements are met:

A. Name, username, password, and email fields contain text entry.

**3.1.6 Login** *(Sean)* The system shall provide users with the ability to enter credentials and authenticate themselves into the Black Bear Portal. The following requirements shall be met:

**3.1.6.1 Entering a username and password.** The system shall provide users with the ability to input and submit to the backend a username and password. The following are required:

A. If the backend returns a response indicating success (3.1.7.2.a), the portal shall store the authentication token provided (3.1.7.2.b)
B. The portal shall use that authentication token in future calls to the backend for the remainder of the session.
C. If the backend returns a response indicating a failed login (3.1.7.2.c), the portal shall display an error message and prompt another attempt.

**3.1.6.2 Checking the username and password.** The system shall check if the credentials entered match a user account. The following are required:

A. If the username and password match an account stored in the database, the backend shall respond to the frontend with a message indicating a successful login.
B. The body of the response shall contain an authentication token for that user.
C. If the username and password do not match an account stored in the database, the backend shall respond to the frontend with a message indicating an unsuccessful login.

**3.1.7 Multi-Factor Authorization/Notifications** *(Sean)* Authorization is required of the Administrator in order for any new device to be given Internet access. Black Bear shall send push notifications to all Registered Users on the home network. The following requirements shall be met:

**3.1.7.1 New Devices.** A push notification requiring approval for all new devices attempting to join the home network shall be sent to all Registered User devices, if that device has not been blacklisted from joining. The following are required:

A. The notification window shall display the manufacturer and operating system of the device.
B. The notification window shall provide a button to approve the request.
C. The notification window shall provide a button to deny the request.
D. The first response to the push notification is the official response.

**3.1.7.2 Denying a request.** When a user clicks the button on the MFA notification window to deny the request, a drop-down menu shall appear in which they can indicate if the device should be denied from joining the network. The following deny options are required in the drop down menu:

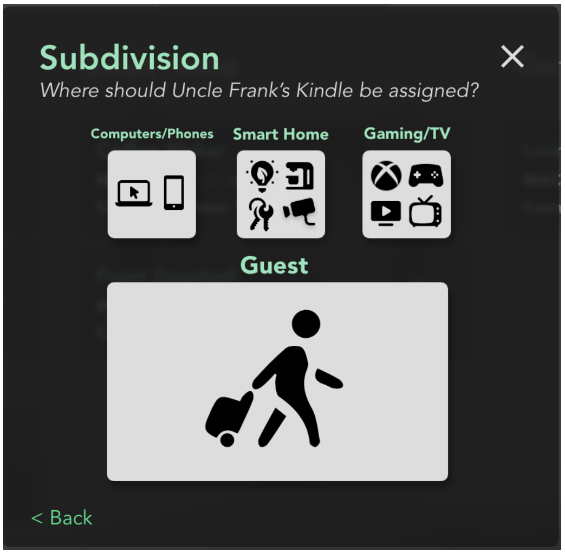
A. Deny the device access to the home network for this single request.

**3.1.7.4 MFA requests handled by Admin User.** Admin Users shall have extra privileges when approving MFA requests. The following are required:

A. When the button to approve is clicked, the MFA notification window shall display the four default VLANs of the network.
B. The button for the Guest VLAN shall be larger than the buttons for the other VLANs (see Figure 3).
C. If the button for the Guest VLAN is clicked, The device shall be connected to the Guest VLAN.
D. If a button other than the Guest VLAN is clicked, the system shall display a confirmation modal with a warning message.
E. If the Admin User clicks the button to confirm on the confirmation modal, the device shall be connected to the VLAN specified.
F. If the Admin User clicks the button to confirm on the confirmation modal, a confirmation notification shall be displayed.
G. The confirmation notification shall disappear five seconds after it appears.

**Figure 2**

*Admin User Vlan Selection Modal*



Subdivision

Where should Uncle Frank's Kindle be assigned?

**3.1.8 Manage Devices (Edit / Remove)** *(Jeremy)* Black bear shall allow administrative and standard users to edit the network configuration or remove devices from the network. The following requirements shall be met:

**3.1.8.1 Edit Device Network Configuration** Black Bear shall allow users to edit network attributes of devices on the network. The following configurable device specific network attributes shall be implemented:

A. Assigned VLAN supporting both pre-configured default VLANs (i.e. Computers / Phones, Smart Home, Gaming / TV, and Guest) and user-defined custom VLANs.

**3.1.8.2 Remove Device From Network** Black Bear shall allow users to remove connected or known devices from the network through a device-specific detail page.

**3.1.9 VLAN Management** *(Carlos)* Black bear separates several networks on a logical base with the utilization of VLANs and allows users to manage adding and removing new or existing VLANs. The following features shall be implemented to ensure the management of those VLANs:

**3.1.9.1 Adding New VLAN Network** Black bear shall allow users the ability to add new VLAN Networks.

**3.1.9.2 Renaming New VLAN Network** Black bear shall allow administrative users the ability to rename new or existing VLAN Networks.

**3.1.9.3 Removing New VLAN Network** Black bear shall allow administrative users to remove existing VLAN Networks.

**3.1.10 Basic Router Configuration** *(Carlos)* Black bear shall allow the user to manage their firewall configurations.

**3.1.10.1 Deny Traffic** Black bear shall allow administrative users the ability to block traffic from specific IP addresses, regions, and/ or specific ports.

**3.1.10.2 Permit Traffic** Black bear shall allow administrative users the ability to allow traffic from specific IP addresses, and/or specific ports. Default will be to allow any IP and to any port.

**3.1.10.3 Set Explicit Firewall Rules** Black bear shall allow administrative users the ability to modify(add, change, or remove) and manage their firewall rules.

**3.1.11 Continuous Monitoring** *(Carlos)* Black bear shall allow the user to manage their alert notifications and logs for auditing traffic analysis. The following requirements shall be met:

**3.1.11.1 Firewall Logs** Black bear shall allow administrative users the ability to modify and manage their firewall logs reporting for traffic analysis.

**3.1.11.2 Immutability of logs.** Black Bear shall not allow non-administrative users to modify logs.

**3.1.11.3 Firewall Alerts** Black bear shall allow administrative users the ability to modify and manage their firewall alerts.

**3.1.12 Viewing Profile Information** *(Jordan)*

**3.1.12.1 Profile Information Page** The Black Bear Web Portal shall contain a user profile information page that displays:

A. The registered name of the user
B. The user's role
C. The registered email of the user
D. The phone number of the user

**3.1.13 Account Creation** *(Sean)* The system shall allow Admin users to create additional Admin or Standard User accounts. The following functional requirements shall be met:

**3.1.13.1 Ability for existing Admins to create accounts.** The following are required:

A. The Admin shall be provided with a feature to create an additional account.
B. The Admin shall be able to choose whether the additional account should be an Admin or Standard User account.
C. The Admin shall be able to provide an email address of the additional user.

D. If the email address does not match the JavaScript regular expression /\S+@\S+\.\S+/, an error message shall be displayed.

**3.1.13.2 Confirming a new Account.** Given the Admin user has specified the details of the new account in 3.1.4.1.1 and submitted the request, the following are required:

A. A random username and password shall be generated for the account.
B. A new account shall be stored in the database.
C. The account shall be stored with the generated username.
D. The account shall be stored with the generated password.
E. The account shall be stored with the user role matching that specified in 3.1.6.1.b.
F. An email containing the username and password shall be sent to the email address specified in 3.1.6.1.c.