**Insert Title Here**

**Introduction:**

Application Name: All Around Security Manager App

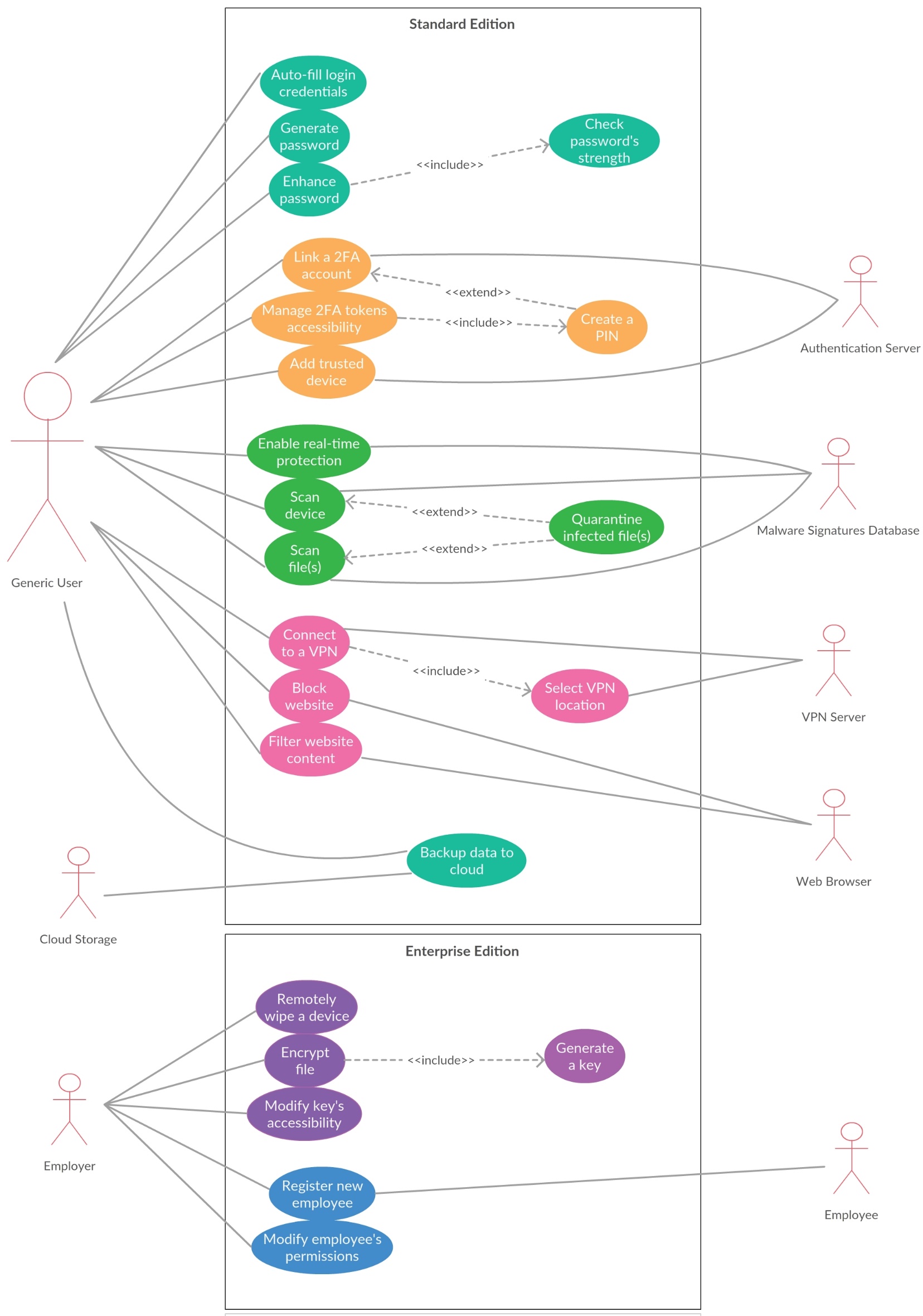
Application Description: This security manager application combines several security features into one convenient package. The app provides many key features including identity protection, multi-factor authentication, online security, and real-time protection against malicious threats. It runs on many platforms and its data is synchronized across multiple devices. In addition to the Standard Edition, this application also comes with an Enterprise Edition with new features for business security.

By reducing the amount of different service you need to use, this application provides great convenience and is guaranteed to be the optimal solution to your security needs.

**Diagram drafting:**

|  |  |
| --- | --- |
| FUNCTIONS | USE CASES |
| Passwords Management | |
| - Stores & manages login credentials  - Generates & enhances passwords | - Autofill login credentials  - Generate a password  - Enhance a password  + Check password strength |
| Authentication & Authorization | |
| - Manages two-factor authentication tokens  - Tracks activities across devices | - Link a 2FA account  + Create a PIN  - Manage 2FA tokens accessibility  + Create a PIN  - Add a trusted device |
| Device Protection | |
| - Provides real-time protection against malwares & infiltrations  - Identifies & quarantines suspicious files | - Enable real-time protection  - Scan the device  + Quarantine infected file(s)  - Scan a file/folder  + Quarantine infected file(s) |
| Online Privacy & Security | |
| - Enables private browsing with VPNs  - Filters & blocks malicious websites | - Connect to a VPN  + Select a location  - Block a website  - Filter website content |
| Other | |
| - Synchronizes information across devices | **-** Backup data to cloud |
| Enterprise Features | |
| - Manages devices & enables remote wipes to prevent data leakage  - Encrypts data & manages encryption keys  - Manages identities & accessibilities | - Remotely wipe a device’s data  - Encrypt a file/folder  + Generate a key  - Modify key’s accessibility  - Register a new employee’s information  - Modify an employee’s permissions |

**Use Case Diagram and Description: (next pages)**

****

|  |  |
| --- | --- |
| Use Case Title | Connect to a VPN |
| Primary Actor | User |
| Level | Sea/Blue level (user goal) |
| Stakeholders | User, VPN Server |
| Precondition | User must have an active and stable Internet connection. |
| Minimal Guarantee | Unexpected error occurs; system displays and logs the error, then shows a link for user to submit a support ticket. |
| Success Guarantee | A stable VPN connection is correctly and fully established. |
| Trigger | User selects the option to enable VPN connection. |
| Main Success Scenario | 1. System begins searching for available VPN servers.  2. System displays available VPN servers along with their locations, traffic, and speed.  3. User selects the preferred attribute among ID, location, traffic, and speed to sort the list.  4. User selects “Refresh” to refresh and update the list.  5. User selects a specific VPN to view its details.  6. User selects “Connect to this VPN” to manually connect to the selected VPN.  7. User selects “Connect Automatically” to automatically find and connect to the optimal VPN.  8. User selects “Terminate Connection” to end connection to the current VPN and browse other options.  9. User selects “Disable VPN” to disable the function. |
| Extensions | 1.a. System fails to perform the search.  1.a.1. System displays a searching error message and notifies user to check the Internet connection.  1.a.2. User makes sure there is a stable Internet connection and hits “Refresh.”  1-8.a. No available VPN servers can be found.  1-8.a.1. System displays a “No available VPN” message.  1-8.a.2. User hits “Refresh” until there are results.  6-7.a. The connection cannot be established.  6-7.a.1. System displays a “Failed to connect” message.  6-7.a.2. User attempts to connect again and succeeds.  6-7.a.3. User attempts to connect again and fails; user browses other options.  6-7.b. The connection is established but data cannot be transferred.  6-7.b.1. System displays a “High traffic on current server” message and suggests user to connect to a different VPN.  6-7.b.2. User remains on the connection and waits until data is transferred.  6-7.b.3. User terminates the connection and browses other options. |