**Part 1:**

Username

**“Something you know”**

Password

Employee ID Number

**“Something you have”**

Mac address (Required for off-site, not on-site) – in addition to 2 factors

Duo Authenticator or Google Authenticator

**“Something you are”**

Fingerprint Reader

**“Somewhere you are”**

Connected to organization’s on-site network (on-site)

In an authorized work location (off-site)

**MFA Framework**

Using above authentication requirements as MFA requirements:

**Off-site only requirement**

The user’s network card has the MAC address of an authorized device.

The user is connected in an authorized work location. (off-site only requirement)

**On-site only requirement**

The user is connected to the organization’s on-site network. (wired or wireless, on-site only)

**Required of all users**

The user entered an authorized username.

**Required 2 of any of the below logic statements**

The user entered an authorized employee ID.

The user authenticated their login using Duo/Google Authenticator by means of a push notification.

The user scanned an authorized fingerprint.

**Specific Technologies needed:**

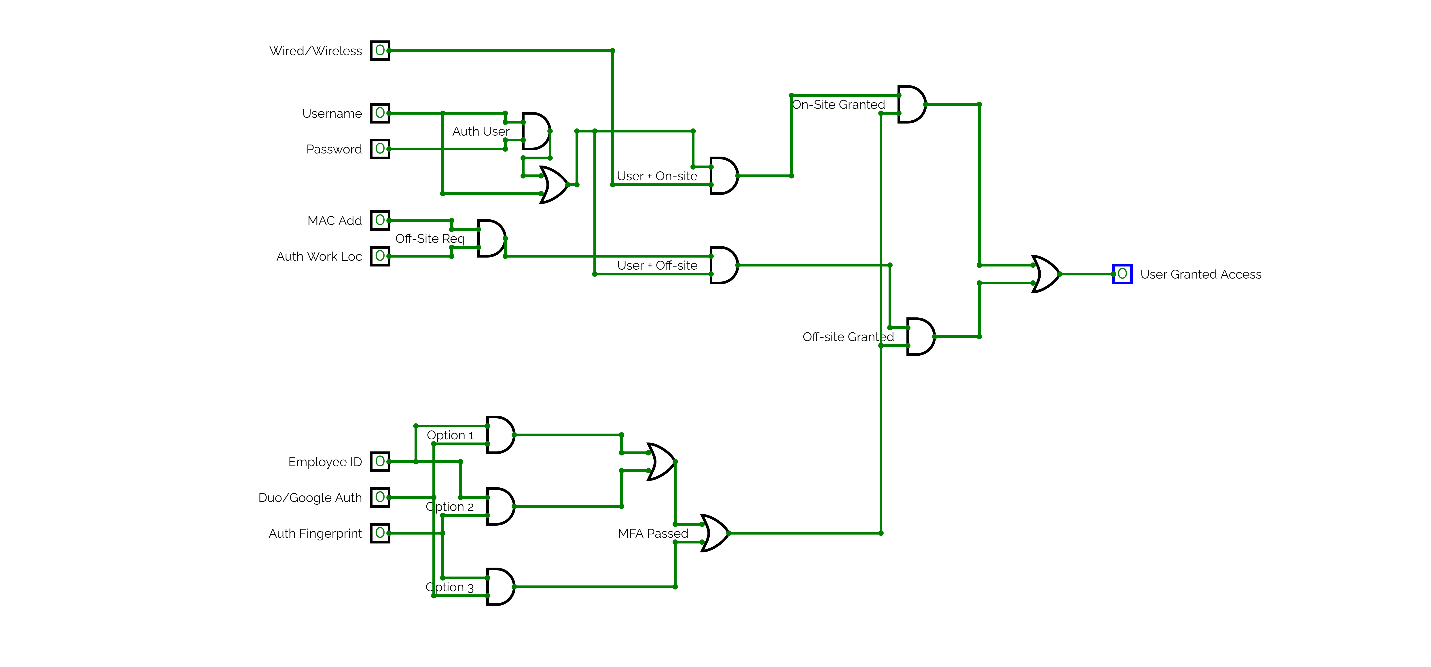
Smartphone w/Duo or Google Authenticator, Fingerprint scanner, System connected to network

**Rules for access to server on-site vs off-site**

User will be granted access if they are on-site, have an authorized username/password combination or authorized username, are connected to the organization’s network, and have 2 out of the 3 required authentication steps completed in a combination of Employee ID and Fingerprint or Employee ID and Duo/Google Push, or Duo/Google Push and Fingerprint.

User will be granted access if they are off-site, have an authorized username/password combination or authorized username, are connected to the organization’s network from an authorized work location, have an authorized MAC address, and have 2 out of the 3 required authentication steps completed in a combination of Employee ID and Fingerprint or Employee ID and Duo/Google Push, or Duo/Google Push and Fingerprint.

**Part 2: Model the Authentication Rules – Circuit on CircuitVerse**

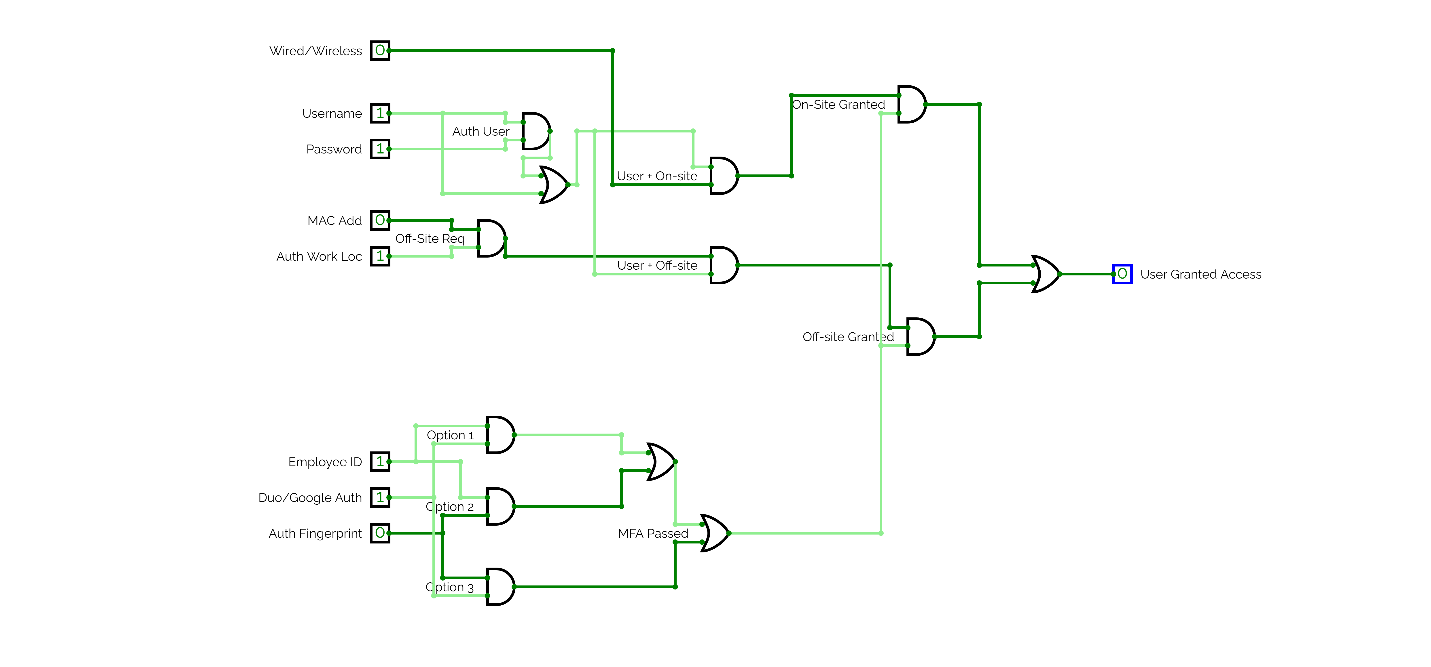


**Part 3: Prove Correctness**

1) No unauthorized user shall be able to access the protected system.

This MFA system would work with the MFA rules outlined above and can be proved by the circuit above as well. If the user was unable to provide an approved username and password, on-site with a wired/wireless connection or off-site with an approved MAC address and from an Authorized Work Location they would not be given access to the system. Also, if the user was unable to provide 2 of the 3 different MFA requirements, they would be denied access.

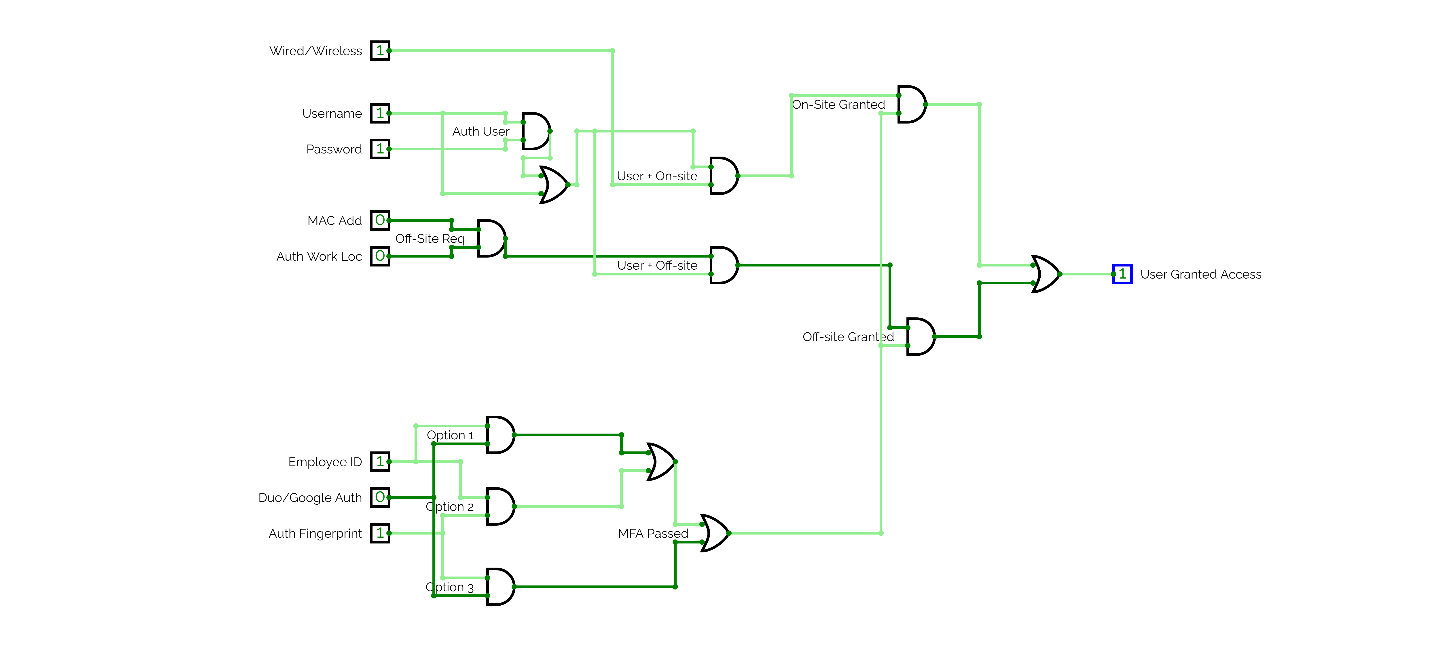
Example below: An on-site user provides an authorized username and password but does not have an approved MAC Address despite being able to provide a Duo Push, Employee ID, and being in an Authorized Work Location. This user would not be granted access to the system.



2) No user can access the system without activating at least two of the authentication methods.

The user needs to provide at least two of the following authentication methods to gain access to the system; Employee ID, Duo/Google Push, and an authorized Fingerprint. This requirement is satisfied using the framework outline above and can be shown in the circuit.

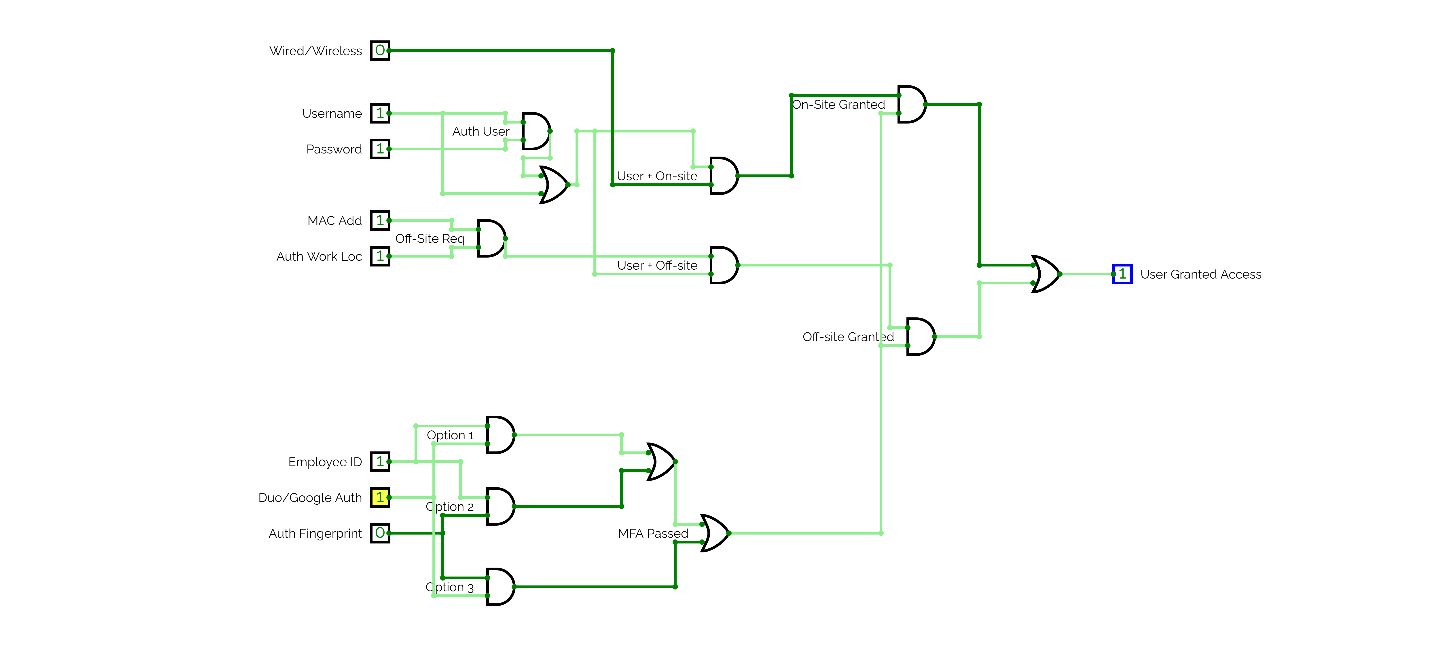
Example: The on-site user provides an authorized username and password, has a wired connection to the network, and provides an authorized Employee ID and authorized Fingerprint but not a Duo/Google Push. This user would be granted access because they have 2 out of 3 of the MFA requirements, can be any combination of the 3 or all 3 would also grant access.



3) Off-site users shall be required to have a pre-approved device, in addition to providing two or more authentication factors. The MAC address will be checked before granting access to the server. If it does not match an approved MAC address, the request will be denied.

The user is off-site and needs to provide at least 2 of the 3 authentication factors, access from an Authorized Work Location, and have a matching authorized MAC address. If these requirements are met, the user will be granted access. If any requirement is missing, the user will not be granted access.

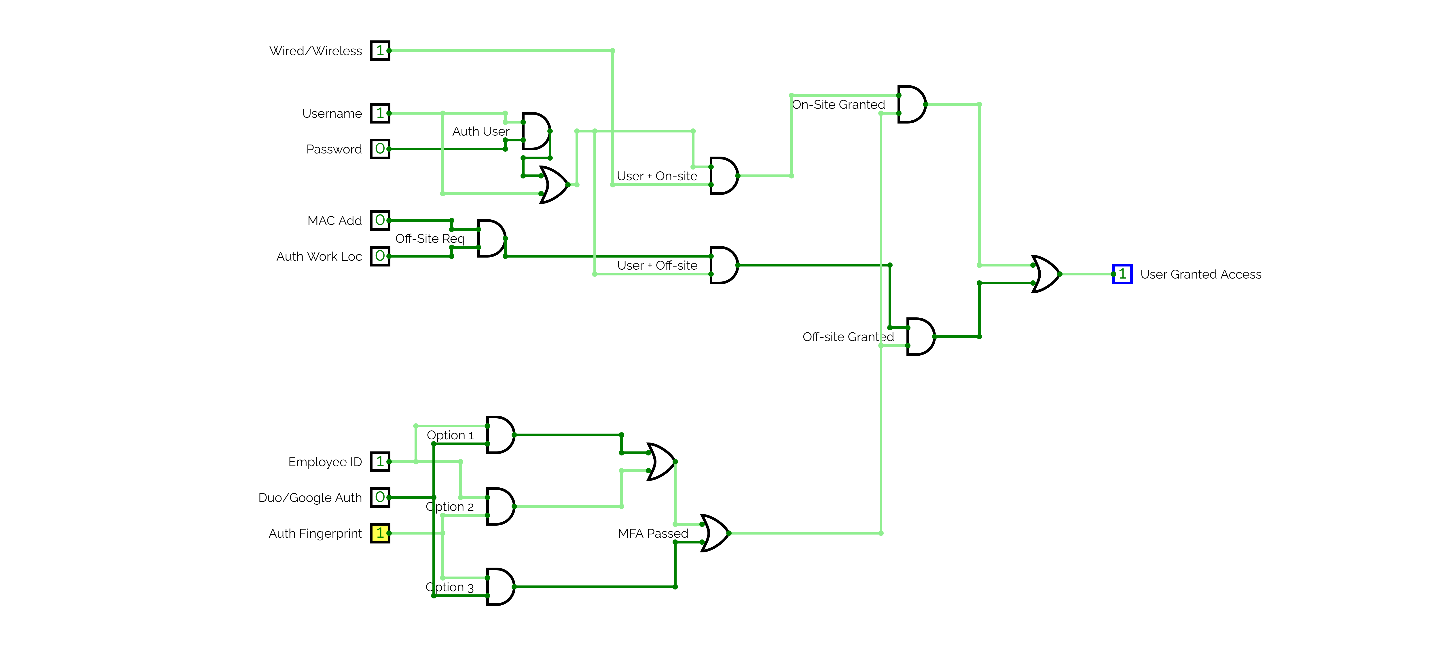
Example: The user is off-site, uses an authorized username and password, using an authorized MAC address, authenticates using their Employee ID and Duo Push, and is accessing the server from an approved work location. This user would be granted access to the server.



4) A user shall be able to access the system without a password if they provide at least two other valid authentication factors.

The user can be granted access to the system upon providing an authenticated username, are connected to the network(wired or wireless) and provide at least 2 of the 3 authentication factors. If provided, this user would be granted access to the server.

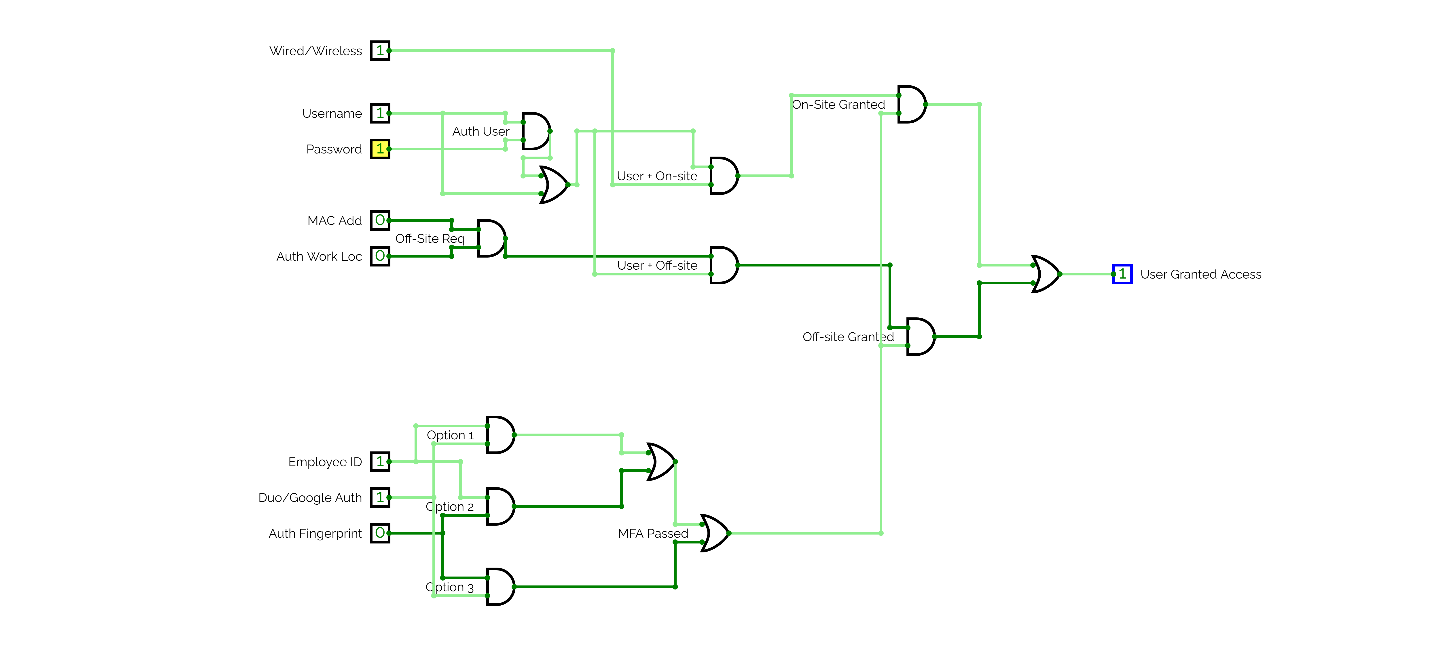
Example: The user provides an authorized username, but no password. They are connected to the network and provide their Employee ID and an authenticated Fingerprint. This user would be granted access to the server.



5) An on-site user shall be able to access the system if the fingerprint reader fails, or if they have no fingerprint available, if they provide at least two other valid authentication factors.

The user is on-site and does not have a functioning fingerprint scanner, an Employee ID and Duo Push are used to authenticate the user while connected to the network. This user is granted access to the server.

Example: The user has an authorized username and password, they are connected to the network, they provide their Employee ID and Duo Push as authentication factors and are granted access to the system.



6) The MFA framework shall provide at least one method for users to authenticate without using a personal mobile device.

The user can use their Employee ID as a method for authentication as well as a fingerprint scanner(specified in the technology needed section) without the need for a personal mobile device. Duo/Google Authentication requires a personal mobile device to confirm that access through a push notification.

Example: The user is on-site, connected to the network, with an authorized username and password. The user authenticates further using their Employee ID and Fingerprint through their fingerprint scanner on their computer. This user is granted access to the system. No personal mobile device is needed. Diagram, schematic

Description automatically generated