Use Case Scenarios

Use case scenarios are beneficial for a team to evaluate what could potentially happen in a certain environment and what may happen when a problematic variable is introduced. The idea behind scenarios is to make the end product adaptable by using forethought in order to apply a solution for a situation that may occur.

Initially we considered who may want to use the program, this could be one of the following:

* Advanced technical user – System administrator
* Technically competent user – standard user
* Enterprises

We then questioned what the users may want to do with the program, as it is a performance monitor this can entail many different things that fall under the same scope. After some reflection, the group decided that these were the most important reasons as the why the program may be used and what it may be used for.

* Network Monitoring – monitor the throughput of the network and any potential traffic problems
* System Health – general performance overview, CPU usage, System uptime etc
* Troubleshooting – check link states, possible system issues such as RAM usage being too high
* Reporting/ Reviews/ Alerts – User notifications (implemented to admin class users) utilised for troubleshooting
* Prevention of future problems – using performance monitor to precondition the system environment

Situation Flow

Making a basic situation flow, we used the scenario that would entail a normal usage day where there would be no issues on either the programs side or the usage side.

Basic Flow

**Use Case**: Performance Monitoring

**Description**: Advanced/Standard User wants to monitor the performance of the system

**Actors**: User

**Preconditions**: Appropriate account is used; program has access to hardware monitoring sensors

1. User wants to see how system is performing.
2. Program detects user input, authenticates user.
3. Depending on user type, appropriate interface is loaded for User (basic/advanced).
4. Standard user gets basic overview of system performance, Advanced user gets reporting, reviews and separate tab for network performance.
5. User logs off from program.

Alternative Flow

In our alternative flow, we identified the issue of authenticating the user. If the user failed to authenticate themselves there needed to be a resolution and also a way to protect the system from misuse.

1. Step 2 – Failure to authenticate correctly causes the program to terminate after three bad attempts.

Exception

In an attempt for the user to regain access to the program, there were some solutions that we thought could be implemented.

* User could restart the program after it terminates and use a ‘*reset password*’ button, the problem this poses is a reset is an easy system bypass. To remedy this the group proposed an idea:
  + If password is reset, user will enter answers to two/three security questions, and possibly a randomly generated alphanumeric string that must be entered.

Post Conditions

The program should be able to identify critical changes from user input; if the user has changed their password but it was lost on the restart of the program, it is flawed. This issue reiterates when an advanced user changes some settings but they are not saved.

* On user input, password is saved and then possibly backed up?
* Admin user settings are saved whenever settings are modified.

Negative Situations

Careful consideration of the use case, allows us to identify possible negative situations that could occur at certain crucial moments of the program’s development/ operation.

Exceptions

Events occurring at normal operation of the program that would interrupt progress:

* Application does not start or crashes during operation
* Advanced/ Standard user views are not given to appropriate user i.e. Advanced user gets basic view
* Program fails to retrieve system statistics
* A password that is reset has not been saved, meaning that when the user enters the new password it is incorrect
* Settings that are changed have not been saved

Intentional Threats

Events that are caused by the action of hostile stakeholders or issues within the team:

* Stakeholders reactively change desired features of the program
* Changes are made to the program without members consulting each other

Unwanted Scenarios

Events that are undesirable:

* User correctly authenticates, but the program terminates on login or crashes
* When the user fails to authenticate correctly, but the program does not terminate
* The team does not deliver the program on time
* The team fails to meet targets and/or delivers the program with missing essential features