

Nome do Projeto: Issues Authenticator	Data da Solicitação: 15/09/2016
Responsável: Equipe Cascavel	
Solicitante: Guilherme Horta Travassos	Clientes: Fábio Farzat, Guilherme Horta Travassos, Hilmer Neri, Talita Ribeiro

Versões e Revisões deste documento			
Data	Comentário	Autor	Versão
17/09/2017	Especificação dos requisitos de um sistema para controle de presença de usuários que atuará em conjunto com o sistema já estabelecido, o Issues Monitoring.	Equipe Cascavel	1.0
26/09/2017	Correções na especificação dos requisitos.	Equipe Cascavel	1.1
07/10/2017	Correções na especificação dos requisitos.	Equipe Cascavel	1.2
15/10/2017	Correções na especificação dos requisitos.	Equipe Cascavel	1.3
28/10/2017	Correções na especificação dos requisitos.	Equipe Cascavel	1.4
26/11/2017	Correções na especificação dos requisitos.	Equipe Cascavel	1.5

Issues Authenticator

Lista de Requisitos

1 Visão

A Equipe Cascavel é composta por estudantes da disciplina Engenharia de Software, ministrada pelo professor Guilherme Travassos.

Atualmente o sistema Issues Monitoring monitora as condições de ambiente dos laboratórios, cadastra os usuários autorizados do laboratório, monitora os usuários presentes em cada laboratório e envia alertas acerca das condições ambientais dos laboratórios. A autenticação dos usuários no laboratório é feita por um sistema de biometria, o MyDenox. Ele é um sistema de autenticação terceirizado que foi incorporado ao esquema de autenticação do Issues Monitoring. Esse sistema exige hardware para a realização da autenticação mas não há dispositivos de hardware suficientes para todos os laboratórios, o que seria custoso.

Assim, a Equipe Cascavel propõe uma solução para otimizar o processo de autenticação nos laboratórios e reduzir a dependência de hardwares externos. O Issues Authenticator deve ser um aplicativo Android de autenticação autônoma dos usuários do LENS. Com uma interface simples, ele deve permitir que o usuário controle suas preferências ambientais e visualize as mensagens de alerta recebidas do Issues Monitoring.

1.1 Escopo do Projeto

O software a ser desenvolvido deve ser capaz de se comunicar com o Issues Monitoring. Deve efetuar o login no sistema para usuários já cadastrados no Issues Monitoring, e avisar o usuário não cadastrado da necessidade de cadastro prévio. Ainda, o software deve ser capaz de informar ao Issues Monitoring as preferências do usuário acerca da temperatura e da luminosidade para o ambiente do laboratório. O software também precisa ser capaz de exibir as mensagens enviadas pelo Issues Monitoring.

1.2 Escopo Não Incluído no Projeto

O software Issues Authenticator não intenciona resolver como o Issues Monitoring irá decidir quais preferências ambientais deverão ser ativadas em um ambiente com mais de um usuário presente. O software Issues Authenticator não intenciona resolver como será feito o cadastro de usuários no sistema Issues Monitoring.

1.3 Envolvidos no Projeto

Nome	Papel
FELIPE ASSIS	Desenvolvedor
GABRIEL MORGADO	Gerente de Projeto
LUIS EDUARDO PESSOA	Desenvolvedor
PEDRO REIS	Desenvolvedor
VITOR TEIXEIRA	Product Owner

1.4 Glossário

Termo	Descrição
CT	Centro de Tecnologia
CT-2	Centro de Gestão Tecnológica
LENS	Laboratório de Engenharia de Software
Preferências ambientais	Temperatura e umidade consideradas ideais pelo usuário do sistema para o laboratório

2 REQUISITOS DO SISTEMA/SOFTWARE

2.1 Requisitos Funcionais

Código	Descrição do Requisito Funcional	Situação	Prioridade
RF01	O sistema deve avisar ao Issues Monitoring que o usuário entrou em um laboratório.	proposto	alta
RF02	O sistema deve avisar ao Issues Monitoring que o usuário saiu de um laboratório.	proposto	alta
RF03	O sistema deve ser capaz de capturar a intensidade do sinal de WiFi dos laboratórios.	proposto	alta
RF04	O sistema deve ser capaz de identificar a geolocalização do usuário.	proposto	alta
RF05	O sistema deve permitir a configuração das preferências ambientais do usuário.	proposto	alta
RF06	O sistema deve enviar as novas configurações das preferências ambientais ao Issues Monitoring.	proposto	alta
RF07	O sistema deve receber notificações enviadas pelo Issues Monitoring.	proposto	alta
RF08	O sistema deve exibir as mensagens previamente recebidas do Issues Monitoring.	proposto	alta
RF09	O sistema deve associar o usuário do Issues Authenticator ao seu respectivo cadastrado no Issues Monitoring.	proposto	alta
RF10	Cada cópia do sistema deve possuir um ID único para ser identificado pelo Issues Monitoring. Requisito não se aplica já que o identificador do usuário pode ser utilizado como ID único para comunicação. Isto permite que o usuário utilize o Issues Authenticator em mais de um dispositivo.	proposto	alta
RF11	O sistema deve permitir a desassociação dos dados que foram armazenados para as autenticações.	proposto	alta
RF12	O sistema deve retornar para o usuário uma mensagem sobre o sucesso ou a falha das solicitações.	proposto	alta

Lista de Requisitos

RF13	O sistema deve avisar o usuário não cadastrado da necessidade de um cadastro prévio.	proposto	baixa
------	--	----------	-------

2.2 Requisitos Não Funcionais

Código	Descrição do Requisito Não Funcional	Situação	Prioridade
Requisitos de Comunicação de Dados, Interface e Interoperabilidade:			
RNF02	O sistema deve se comunicar com o Issues Monitoring por uma API com dados no formato JSON.	proposto	alta
RNF03	O sistema deve se comunicar por um WebSocket com o Issues Monitoring para receber as mensagens de alerta quando o usuário estiver presente no laboratório.	proposto	alta
Requisitos de Confiabilidade:			
-	-	-	-
Requisitos de Desempenho e Robustez:			
RNF04	O sistema deve identificar em até um minuto a entrada ou saída do usuário do laboratório.	proposto	alta
Requisitos de Disponibilidade:			
RNF05	O sistema deve estar disponível em tempo integral durante o horário comercial, que é o período de maior fluxo de pessoas nos laboratórios.	proposto	alta
RNF06	O sistema deve rodar em tempo integral como um <i>background service</i> no dispositivo do usuário.	proposto	alta
RNF12	O sistema deve ser inicializado junto com o dispositivo para garantir que esteja disponível para realizar as autenticações de forma autônoma.	proposto	média
Requisitos de Manutenibilidade:			
-	-	-	-
Requisitos de Portabilidade:			
RNF07	O sistema deve poder ser instalado em smartphones com sistema operacional Android na versão 4.1 ou superior.	proposto	alta
Requisitos de Segurança:			
RNF08	O sistema deve ter o acesso a seus dados e funcionalidades restrito a usuários com login e senha válidos.	proposto	alta
Requisitos de Usabilidade:			
RNF09	O sistema deve realizar as autenticações de forma autônoma, utilizando as informações de WiFi e GPS do usuário para identificar sua localização.	proposto	alta
RNF10	O sistema deve forçar a ativação dos módulos GPS e Wi-Fi dos dispositivos onde está instalado.	proposto	alta

Lista de Requisitos

Restrições de Projeto e Tecnológicas:			
RNF01	O sistema deve acrescentar novas funcionalidades ao Issues Monitoring, sem interferir nas que já estão presentes.	proposto	alta
RNF11	O sistema deve funcionar paralelamente ao já operante sistema MyDenox de autenticação.	proposto	alta
Restrições Legais:			
-	-	-	-

2.3 Extensões do Issues Monitoring

2.3.1 Requisitos Funcionais

Código	Descrição do Requisito Funcional	Situação	Prioridade
RFIM01	O Issues Monitoring deve enviar as suas mensagens de alerta dos laboratórios para as cópias do Issues Authenticator dos usuários presentes no laboratório e dos responsáveis pelo laboratório.	proposto	alta
RFIM02	O Issues Monitoring deve enviar ao Issues Authenticator se os dados cadastrais do usuário estão corretos ou incorretos.	proposto	alta
RFIM03	O Issues Monitoring deve receber do Issues Authenticator as configurações de preferências ambientais do usuário.	proposto	alta
RFIM04	O Issues Monitoring deve receber do Issues Authenticator a informação de entrada ou saída de um usuário do laboratório.	proposto	alta

2.3.2 Requisitos Não Funcionais

Código	Descrição do Requisito Não Funcional	Situação	Prioridade
Requisitos de Comunicação de Dados, Interface e Interoperabilidade:			
RNFIM01	O Issues Monitoring deve fornecer API com dados no formato JSON para comunicação com o Issues Authenticator.	proposto	alta
RNFIM02	O Issues Monitoring deve se comunicar por um WebSocket com o Issues Authenticator para enviar as mensagens de alerta dos laboratórios.	proposto	alta
Requisitos de Projeto e Tecnológicas:			
RNFIM03	As modificações na API do Issues Monitoring devem ser feitas no servidor já existente, feito em Python e utilizando o framework Flask, sem comprometer o funcionamento atual.	proposto	alta

3 REFERÊNCIAS

Lista de Requisitos

Título do Documento	Versão	Onde pode ser obtido
Documento de visão e requisitos do Issues Monitoring	Final	https://moodle.cos.ufrj.br/mod/folder/view.php?id=5582

4 CONCORDÂNCIA DO CLIENTE/REPRESENTANTE DO CLIENTE

Concordo com os requisitos listados neste documento. Estou ciente de que o planejamento do projeto será realizado com base nesses requisitos aprovados.

Nome:

Cargo:

Assinatura (ou cópia de e-mail enviado):