Dashboard Technical Specifications -- SaaS

Contents

- 1 Introduction
  - 1.1 Use Cases
  - 1.2 User Communities
  - 1.3 What is the Dolcera Dashboard?
  - 1.4 Workflow
- 2 Deployment Architecture
- 3 Software-as-a-Service (SaaS) Environment
- 4 Security Controls
  - 4.1 Authentication and Authorization
  - 4.2 Physical Security
  - 4.3 Redundancy
  - 4.4 Data Backups
  - 4.5 Intrusion Detection
  - 4.6 Disaster Recovery

Introduction

The Dolcera Dashboard is a web application for managing and organizing patents, product information, and scientific literature. This application is used for a variety of purposes including patent review/clearance, and by different enterprise users including attorneys, licensing professionals, engineers, and executives.

Use Cases

The typical use cases for the Dolcera Dashboard are as follows:

1. Freedom-to-practice or clearance search
2. Patent portfolio analysis
3. Competitive intelligence
4. Patent landscaping
5. Patent-to-product mapping
6. Patent-to-standard mapping

User Communities

The typical users of the Dolcera Dashboard include:

1. Patent attorneys
2. Patent managers
3. Patent searchers
4. Engineers, scientists and inventors
5. Licensing and business development professionals
6. Senior executives

What is the Dolcera Dashboard?

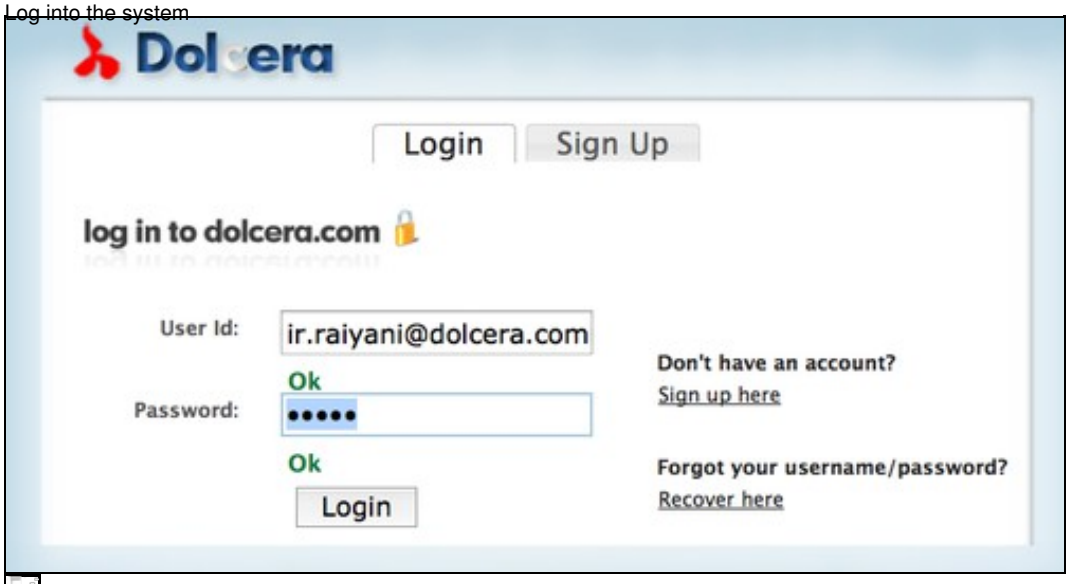
The Dolcera Dashboard is an interactive web application used to:

1. Organize large quantities of patent, scientific and product literature
2. Manage patent review workflows
3. Assist in collaboration with colleagues and partners around the world
4. Help technology teams, patent counsels, and key decision makers in monitoring the competitive landscaping and finding key partners

Workflow

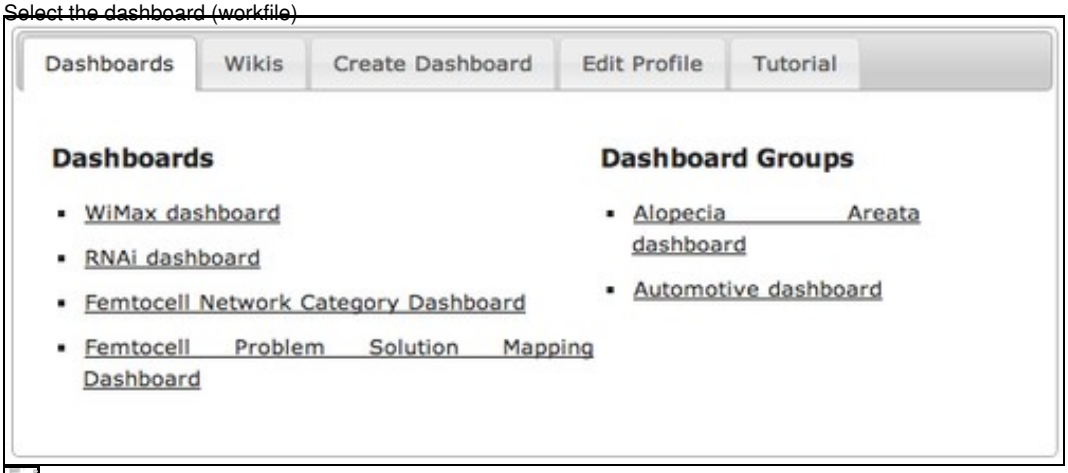
A typical workflow is described below:

1. Log into the system



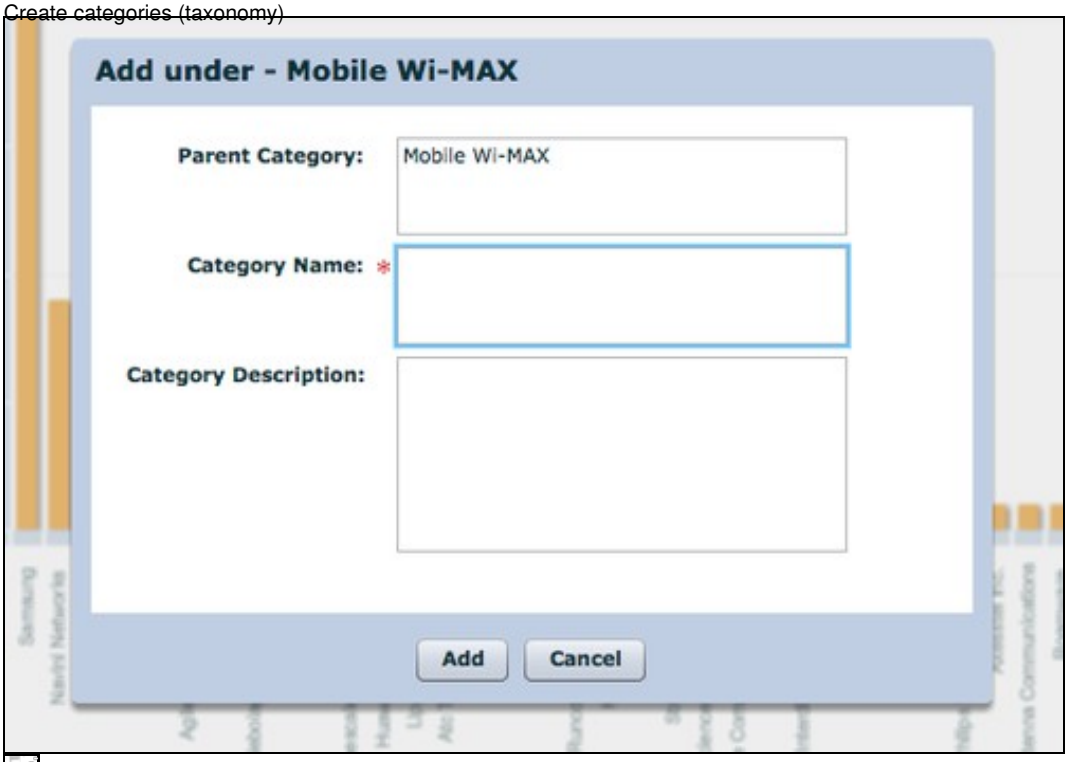
Login screen

2. Select the dashboard (workfile)



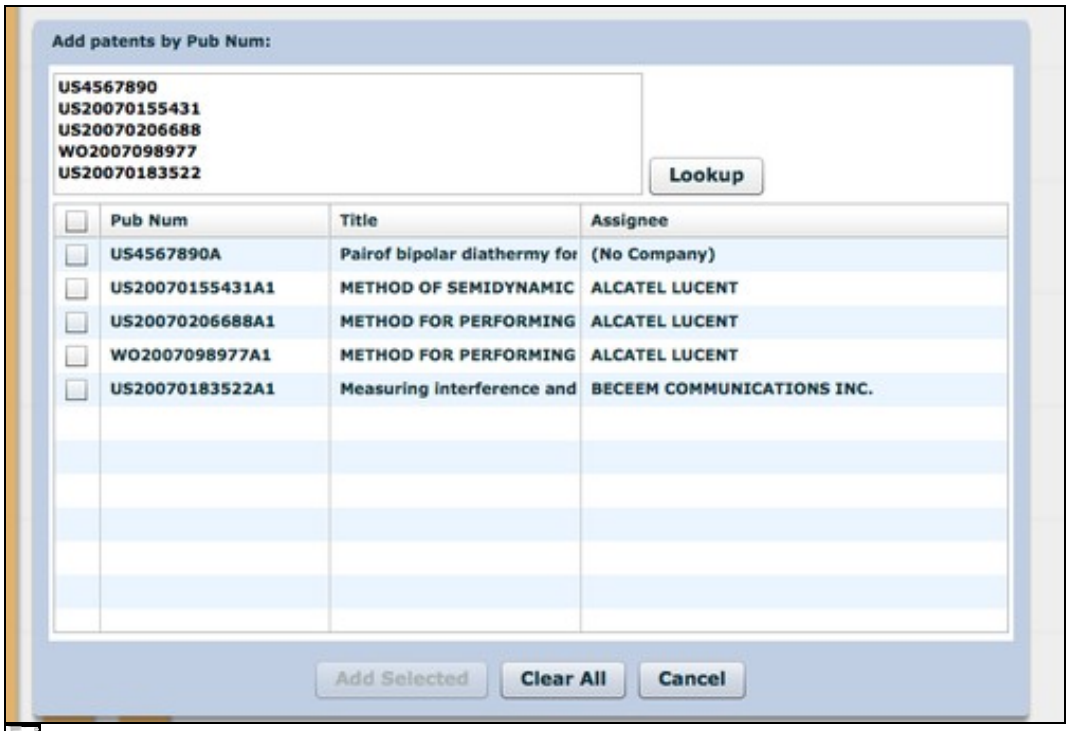
Select dashboard

3. Create categories (taxonomy)



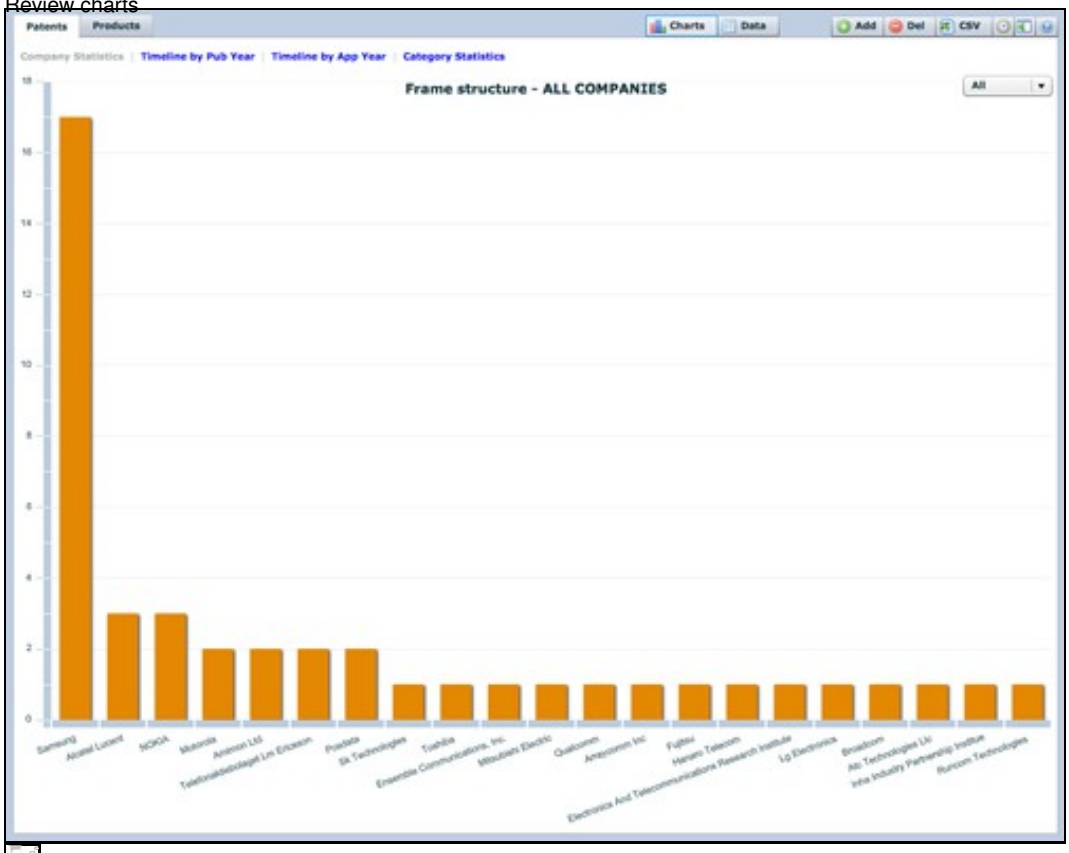
Add taxonomy categories

4. Add patents



Add patents

5. Review charts



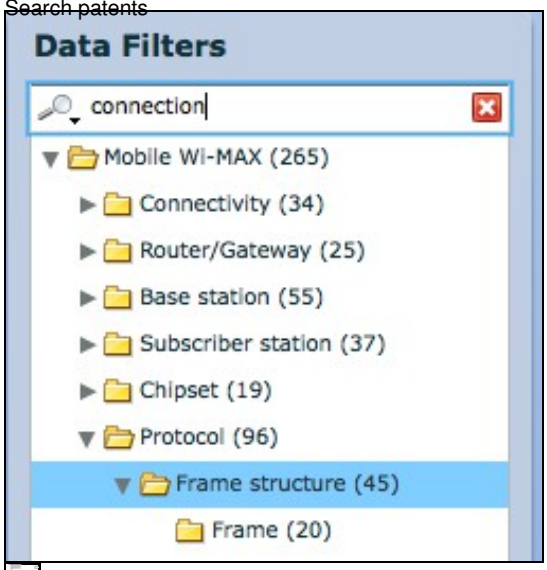
Review charts

6. Review patents



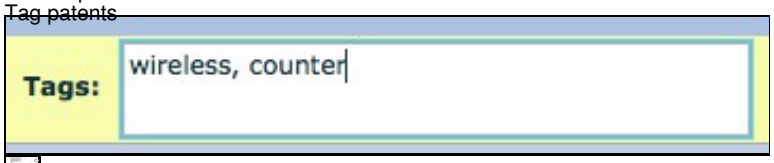
Review patents

7. Search patents



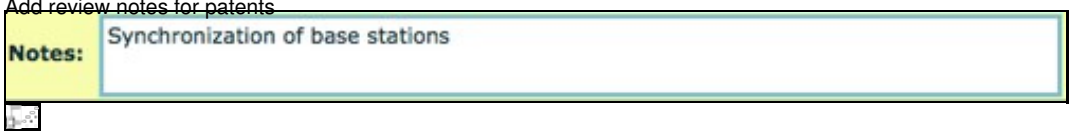
Search patents

8. Tag patents



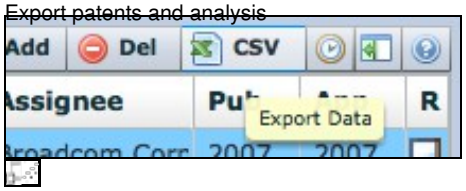
Tag patents

9. Add review notes for patents



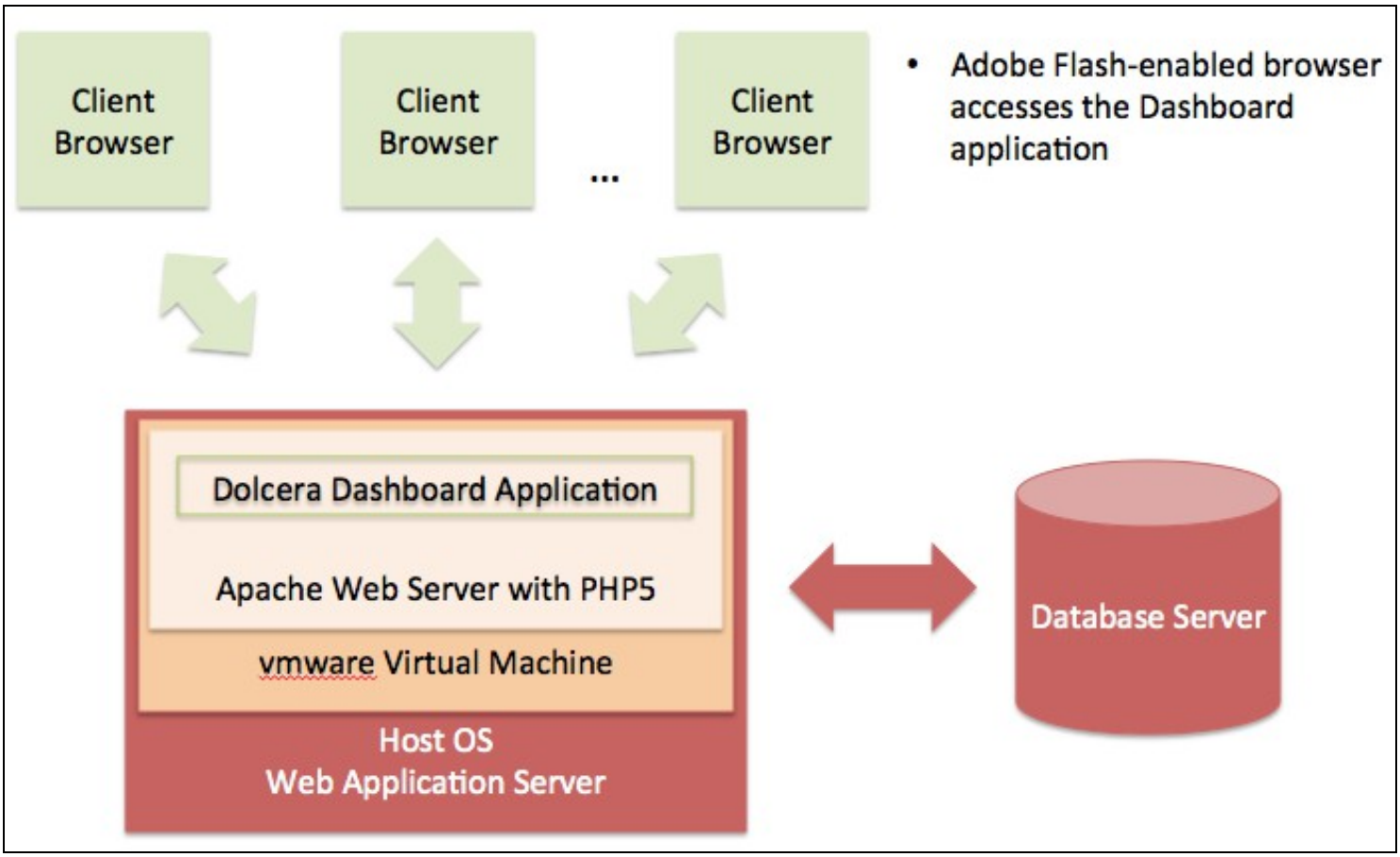
Patent notes

10. Export patents and analysis



Export patents

Deployment Architecture



Dolcera Dashboard Deployment Architecture

Software-as-a-Service (SaaS) Environment

The Dolcera Dashboard service is made available as an online service (SaaS) to the users. The users log into the application through their web browser, and can use the application online.

Security Controls

Dolcera has extensive security controls in place to protect client confidential information and to share the results of Dolcera's research and analysis in a secure manner with our clients.

The Dolcera IT team has implemented secure procedures at its facilities in the US and India, and at its data centers in the US.

Authentication and Authorization

- All access to client-specific information is obtained after authentication via a username and password
- Client users who require access to data and systems at Dolcera must be authorized by the Dolcera account management team in consultation with the appropriate client management.
- Only those Dolcera team members who are directly involved with a particular client are authorized to access client-related data.
- Dolcera regularly reviews and updates the authorizations of team members as appropriate, based on their work assignments.
- Infrastructure logs and audit trails contain information about security-related events including logins, IP address, date and time of access.

Physical Security

- US data center facilities are protected by the highest level of physical and biometric access controls.

Redundancy

- Dolcera systems have several levels of redundancy, including multiple servers, multiple storage and backup solutions, multiple network connections and multiple levels of physical and data security.

Data Backups

- Data is backed up on a nightly basis or in real time as appropriate, and is securely synchronized to the Dolcera servers located in the US data center.

Intrusion Detection

- Intrusion detection systems have been installed on Dolcera servers and are monitored by the Dolcera team.

Disaster Recovery

- Dolcera has a disaster recovery plan and the necessary technology and systems (including data backups and alternative designated work sites) to implement the disaster recovery procedures in case of need.