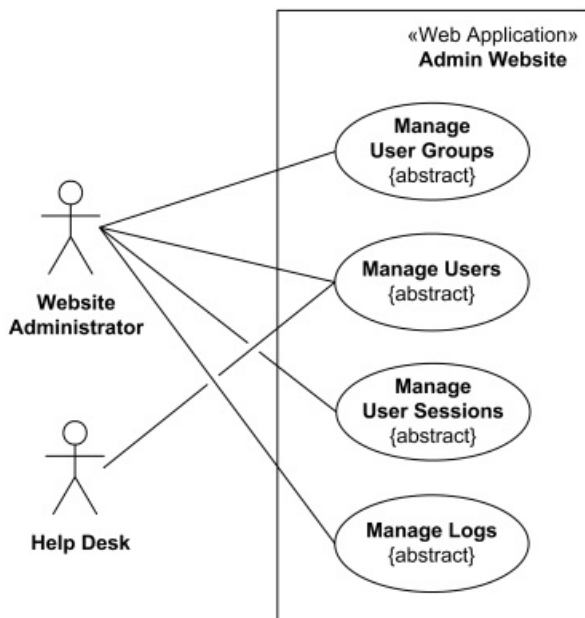# Website Administration

UML Use Case Diagram Example

Website security requirements mandate separation of administrative interfaces from common functions provided to users. This segregation, for example, is required by the Sarbanes Oxley (SOX) in US and is strongly recommended by ISO 17799.

System should have separate applications for administrators and for common users. It is recommended by *OWASP Guide 2.0* that website administration applications should not be accessible from the internet without going through some management networks, e.g. via a strongly authenticated VPN or from a trusted network operations center.

Except for administrators, some part of the administrative interfaces should be also available to the Help desk staff, as they need to be able to assist customers having issues while using the customer oriented website.

Top level use case diagram below shows some administrative functions that administration website could provide.

Two **actors** using administrative interfaces are **Website Administrator** and **Help Desk**. Help Desk uses a subset of functions available to the Website Administrator. All top level **use cases** shown are abstract as each represents some group or "package" of administrative functionality.

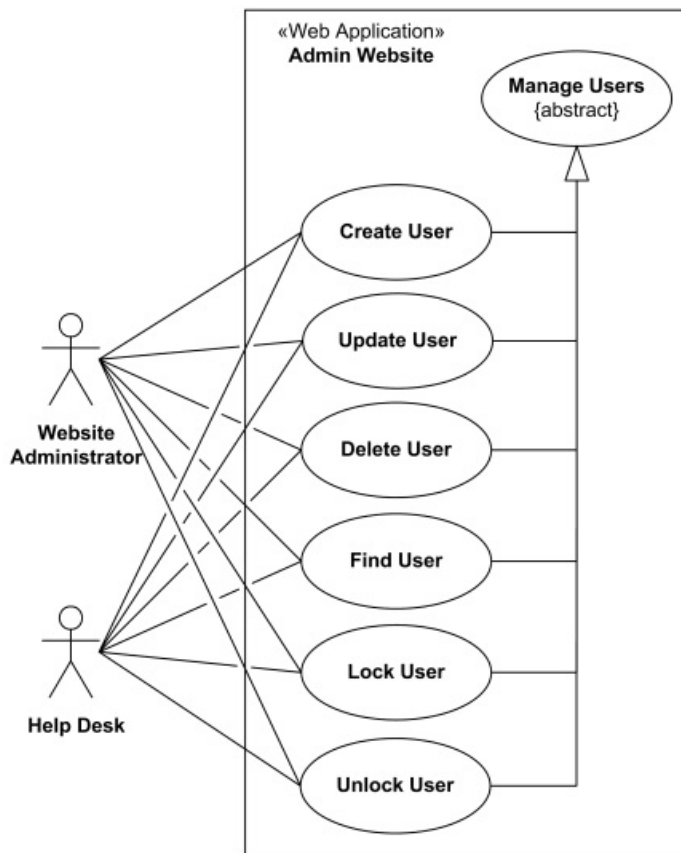*Top level use case diagram for the administration website.*

Manage User Groups abstract use case is specialized by **Create Group**, **Update Group**, and **Delete Group** use cases. The idea is that website administrator could create different user groups, for example, having different privileges or options, and later some user groups could be modified or even deleted.
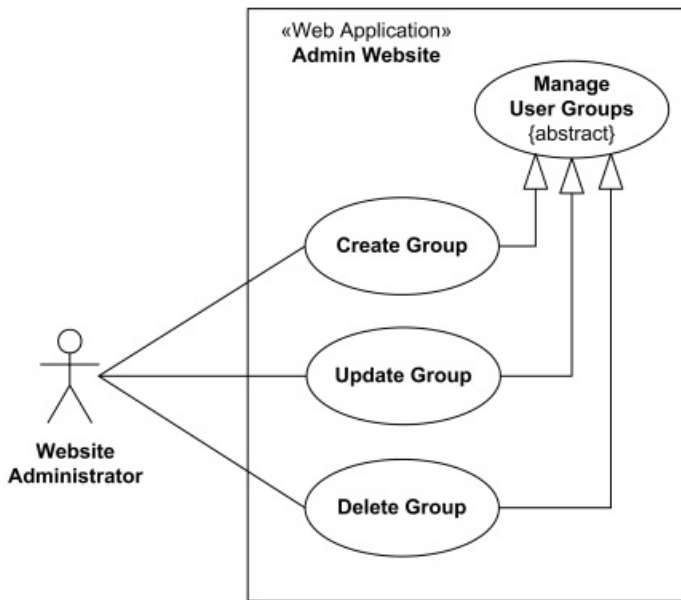
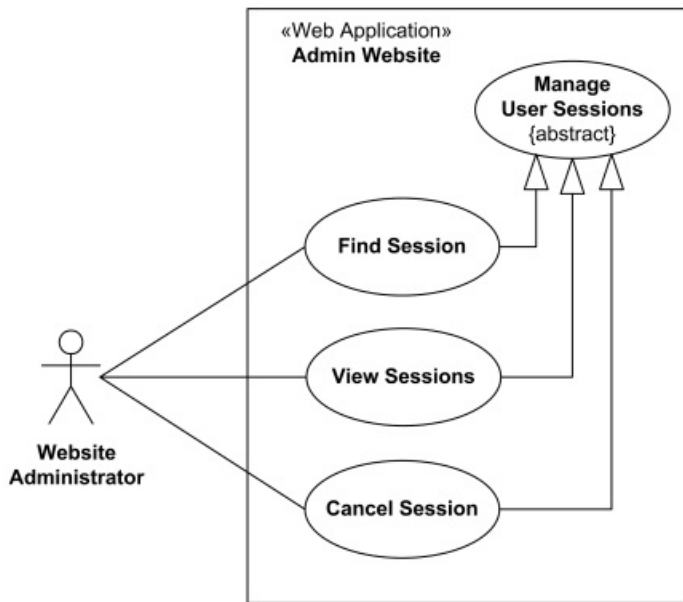*User group management use case diagram for the administration website.*

User management use cases are available both to the **Website Administrator** and to the **Help Desk**. There is standard user CRUD (Create, Retrieve/Find, Update, Delete) functionality set.

Two other use cases, **Lock User** and **Unlock User** are specific to website security. For example, if during some predefined period of time there were several unsuccessful login attempts using wrong user password, user account should be locked for some predefined time to prevent possible brute force password guessing attack. This locking and unlocking is usually done automatically by intrusion detection or website authentication subsystem, but this functionality needs to be available in the manual mode too, just in case. For example, some user might call and ask to lock his or her account.

User management use case diagram for the administration website.

User session is created either for each new incoming request that is not yet part of a session, or/and after user was authenticated. Website administrator should have ability to see how many sessions were created, including some statistics about sessions, to find some specific session and see status of that session, and to cancel (delete) some session, if required.
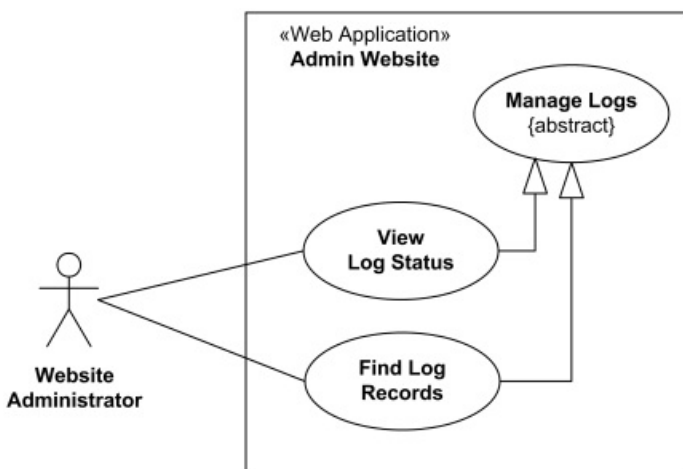
User sessions management use case diagram for the administration website.

List of administrative functions included in the **log management** depend on the security requirements supported and implemented by the website.

It is a standard security requirement (e.g., see **OWASP Guide 2.0**) for the logs that new records can be only appended while older log records should not be rewritten or deleted. It could be implemented e.g. by writing logs to a write once / read many (WORM) device such as a CD-R.

Website administrator should be able to see status of logs. The status could include verification that logging is still functional (there is enough space on disk and/or connection to database is not stale), and that older log files are on schedule being moved to a permanent storage for archiving.

Logs management use case diagram for the administration website.

It is also common requirement to allow website administrator to find and see some log records related to a specific user or an exceptional situation.

Shopping domain

Noticed a spelling error? Select the text using the mouse and press Ctrl + Enter.