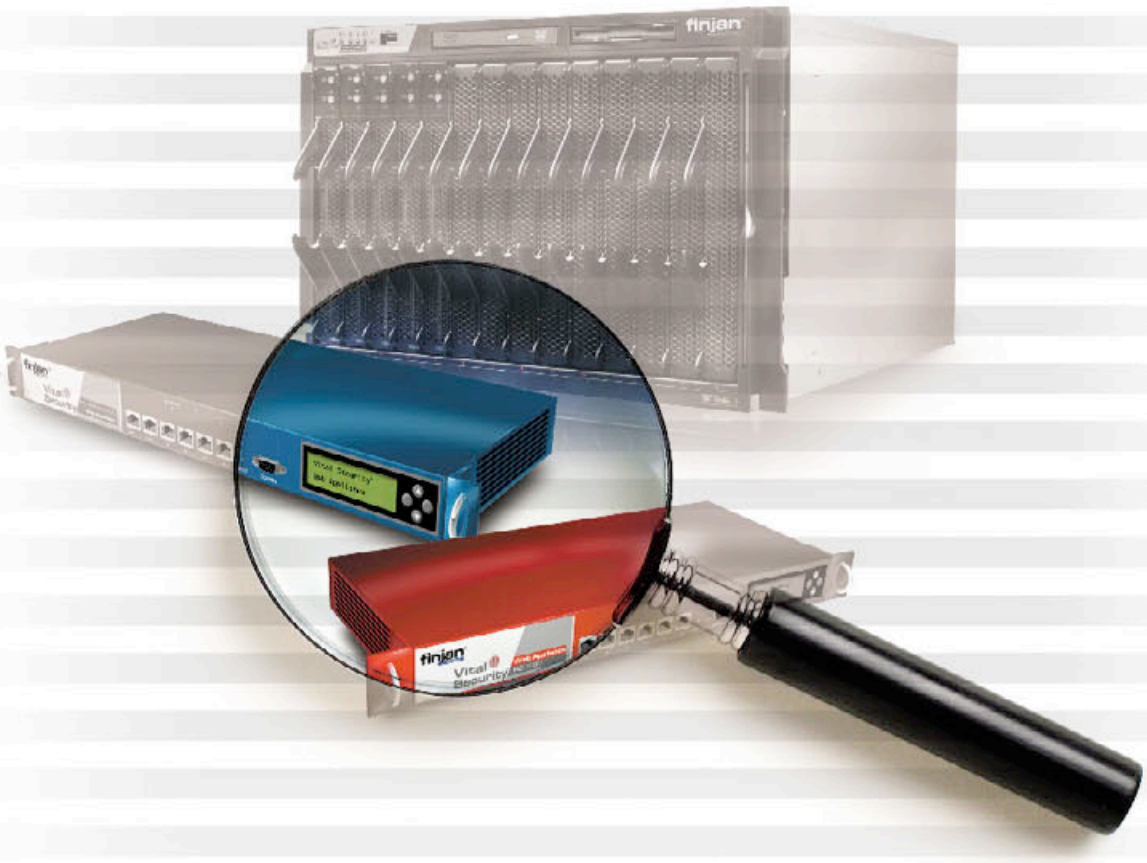
finjan
Vital Security™
securing your web

Technical Brief

Multiple Administrators



Vital Security™ Web Appliances NG-1100/NG-5100/NG-8100 Tech Brief: Multiple Administrators

For additional information, please visit www.finjan.com or contact one of our regional offices:

San Jose, USA
Toll Free: 1 888 FINJAN 8 (1 888 346 5268)
Tel: +1 408 452 9700
Email: salesna@finjan.com

New York, USA
Tel: +1 212 681 4410
Email: salesna@finjan.com

Asia Pacific
Tel: +972 (0)9 864 8200
Email: salesapac@finjan.com

United Kingdom
Tel: +44 (0)1252 511118
Email: salesuk@finjan.com

Germany
Tel: +49 (0)89 673 5970
Email: salesce@finjan.com

Israel
Tel: +972 (0)9 864 8200
Email: salesis@finjan.com

Catalog number: VSNG_TB2
Email: support@finjan.com
Internet: www.finjan.com

CONTENTS

Introduction **4**
The basics of multiple administrator support **4**
Super Administrators **5**
Multiple Administrator Scenarios **6**
Conclusion **16**

Introduction

Enterprises and SMBs often need to enable multiple network and security administrators with different access rights on the Management Console. This need derives from several reasons:

Security – the chances of misuse, not only by unauthorized, but also by authorized personnel, decreases when multiple administrator accounts are defined with distinct passwords. In fact, every administrator can be defined with different levels of management rights. Hence, the overall system security increases.

Audit Trail / Accountability – enforcing each administrator to use their own account provides efficient and targeted audit capabilities via the logging mechanism, which shows a detailed list of all actions performed through the Management Console. The information includes both the actions, and the administrator that performed these actions.

Role based administration – the Management Console provides control over a magnitude of tasks associated with different domains, such as, security, user management, IT and more. Therefore, it can be very convenient to aggregate the management tasks according to their specific domain. Providing an administrator with permissions on a subset of tasks is equivalent to defining administration roles, e.g. security administrator, IT administrator etc.

Compartmentalization – the security solution is often deployed in a multi-department or multi-company environment, where each has its own security requirements and separate administrators. In this case, it may be essential to provide administrators with permissions only for their managed group.

The basics of multiple administrator support

Vital Security provides multiple administrator functionality that addresses all of the above requirements. In order to understand the full scope of this feature, and how to use it in your environment, it is necessary to understand the basic building blocks behind it:

- **Permission**: Write: can add and edit data through the Management Console, Read Only: can only view data through the Console and None: cannot gain access to the data through the Console.
- **Functionality**: a collection of tasks within the same domain. Examples for **functionalities** are “Security Policies”, “Device Settings” and “User Management”. Most **functionalities** are correlated with a top level tab in the GUI, although this is not mandatory and may change in future releases.

- **Objects**: specific components that can be manipulated, for example a specific security policy, a specific URL list, etc. An **object** is either pre-defined by Finjan (e.g. Default Security Policy) and therefore is not editable, or customer defined in which case it is "owned" and editable only by one **Administrator Group**.
- **Administrator**: any individual who has access to the Management Console via a unique username and password. Each **administrator** belongs to a single **administrator group** and has **permissions** to various **functionalities;** hence defining his / her role.
- **Administrator group**: a collection of **administrators** that share common **permissions** on specific **objects**. When a new **administrator** is created, he inherits his **permissions** on **objects** (but not on **functionalities**) from the **administrator group** he belongs to.

The following instructions highlight the information given above:

1. An administrator will be able to create an object (e.g. a new security policy) only if he has "Write" permissions for the relevant functionality (e.g. Security Policies).
2. An administrator will be able to edit or delete an object (e.g. an existing security policy) only if he has "Write" permissions for the relevant functionality (e.g. Security policies) AND his administrator group has "Write" permissions for the specific object.
3. An administrator will be able to view an object (e.g. an existing security policy) only if he has "Write" or "Read Only" permissions for the relevant functionality (e.g. Security Policies) AND his administrator group has "Write" or "Read Only" permissions for the specific object.
4. An administrator will be able to view logs and reports only related to users and user groups his administrator group has "Write" permissions for.

Super Administrators

Super Administrators are administrators who are part of the predefined Super Administrator group. All Super Administrators have predefined "Write" permissions on all functionalities and objects.

Super Administrators are useful in the following scenarios:

- Provide a preconfigured solution for simple deployments
- Create new administrator groups
- Create new administrators in different administrator groups
- Define permissions for both administrator groups as well as administrators

- Provide override capabilities on top of existing administrators and their permissions

Multiple Administrator Scenarios

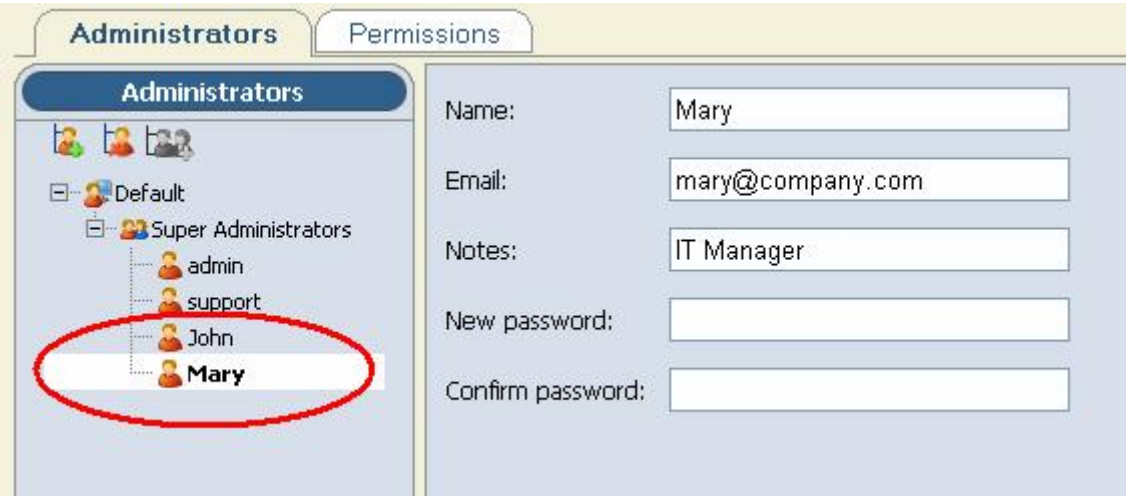
Support for multiple administrators within Vital Security can be done in numerous ways. To achieve the most out of this functionality, we recommend defining the deployment requirements, and then following the suggested guidelines. The following sections provide detailed examples to illustrate the various scenarios.

Accountability

In this example, 2 additional administrators will be created; both have full access to all functionality, yet each one logs in to the Management Console with his/her credentials.

⇨ **To create multiple administrators for accountability purposes:**

1. Create additional administrators, John and Mary, under the Super Administrator group. Do not create any additional administrator groups.



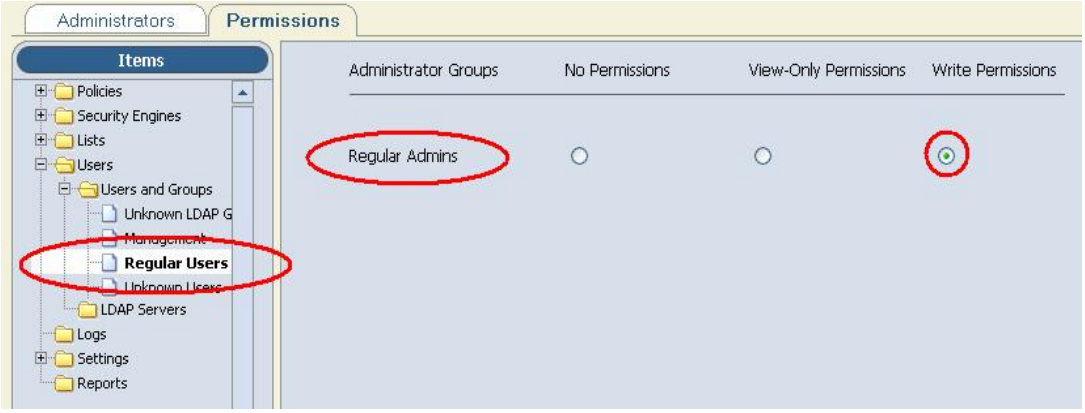
Roles

In this example, 2 additional administrators will be created: John who will be defined with the role of a "Security administrator" and Mary who will be defined with the role of a "Report administrator".

⇨ **To implement administrator roles:**

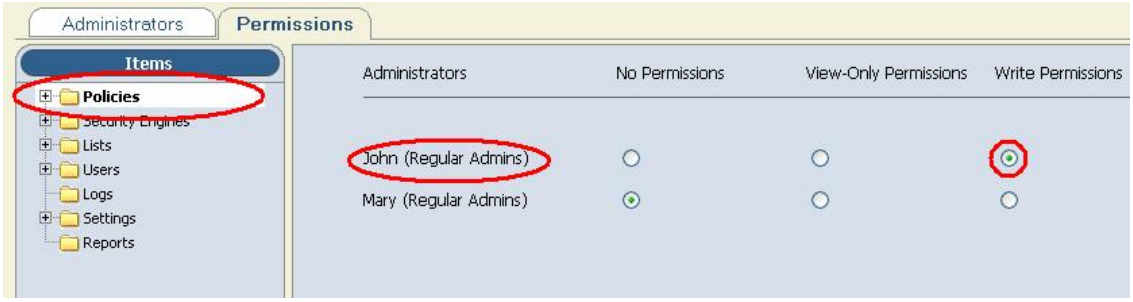
1. Create a new administrator group. For example, "Regular Admins".

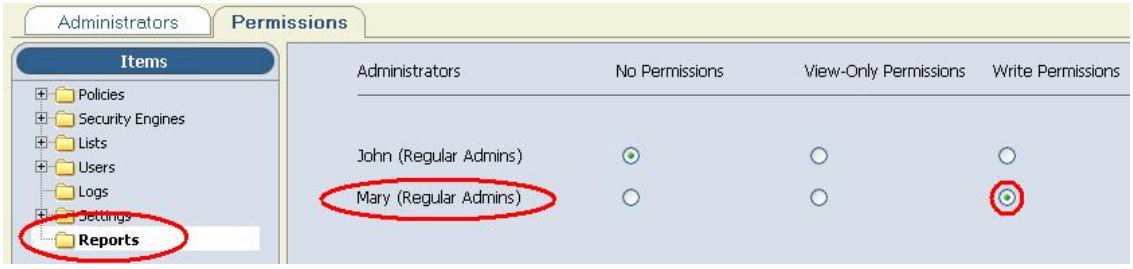
2. Provide the Regular Admins group with "Write" permissions for all users and user groups



3. Create multiple administrators (e.g. John and Mary) within the Regular Admins group.

4. Assign relevant permissions to each of the administrators with respect to the different functionalities, so as to define their roles. In this example, John has Write permissions for Policies and no permissions for Reports, and Mary has Write permissions for Reports and no permissions for Policies.





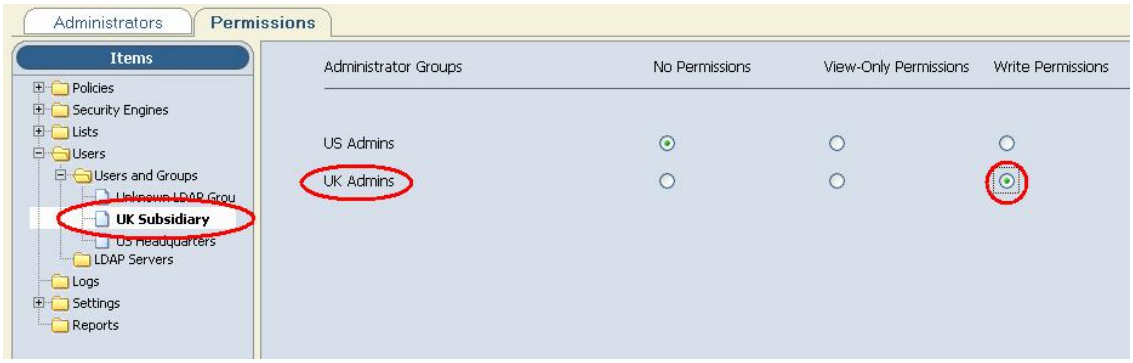
Managing Separate Departments

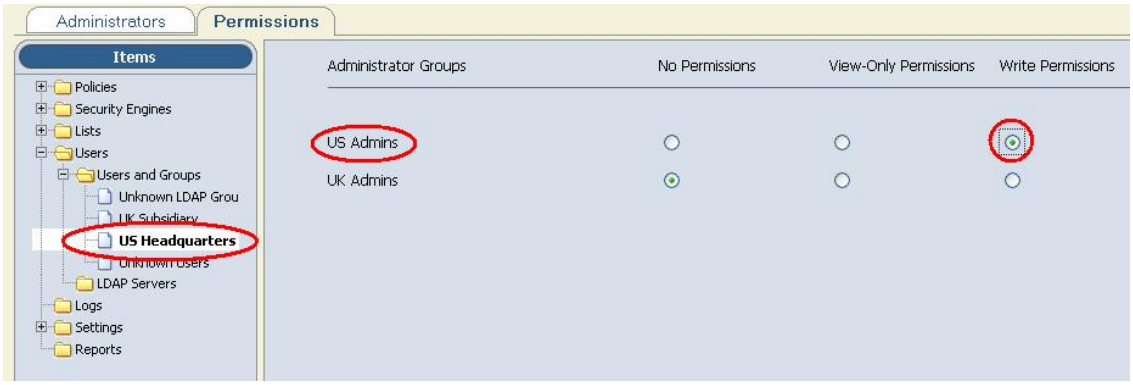
In this example, an administration scenario will be created for a company with US headquarters and a UK subsidiary. Each of the branches will be managed by its own administrators using its own data.

⇨ **To manage separate departments and/or companies, each having its own data**

1. Create multiple new administrator groups, one per department or company.

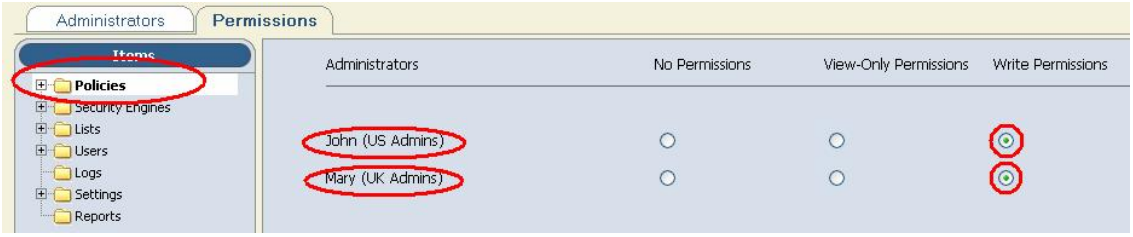
2. Provide each new group with "Write" permissions on all users and user groups of the relevant departments.



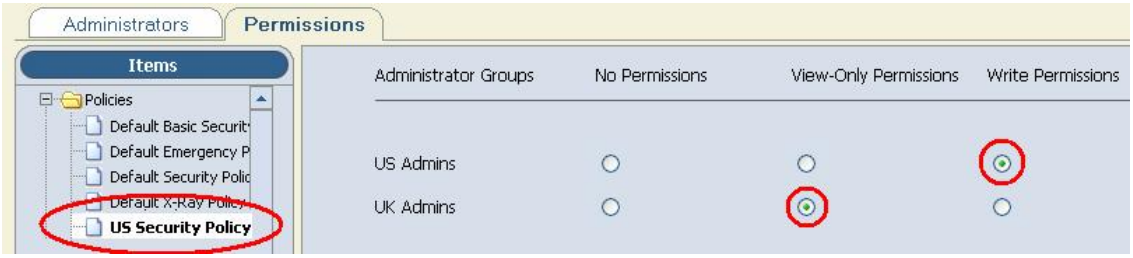


3. Create an administrator within each new administrator group.

4. Assign the administrator "Write" permissions on all functionalities.



5. Assign the appropriate permissions for the private data. In this example, "US Admins" have "Write" permissions for the "US Security Policy", while "UK Admins" have "View-Only" permissions on the same policy, so that they can use it but not change it.



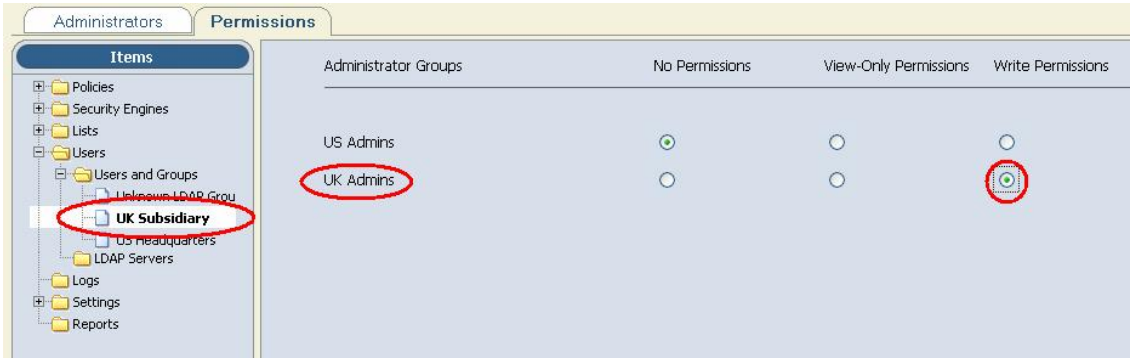
Managing Separate Departments with role-based administration - Alternative One

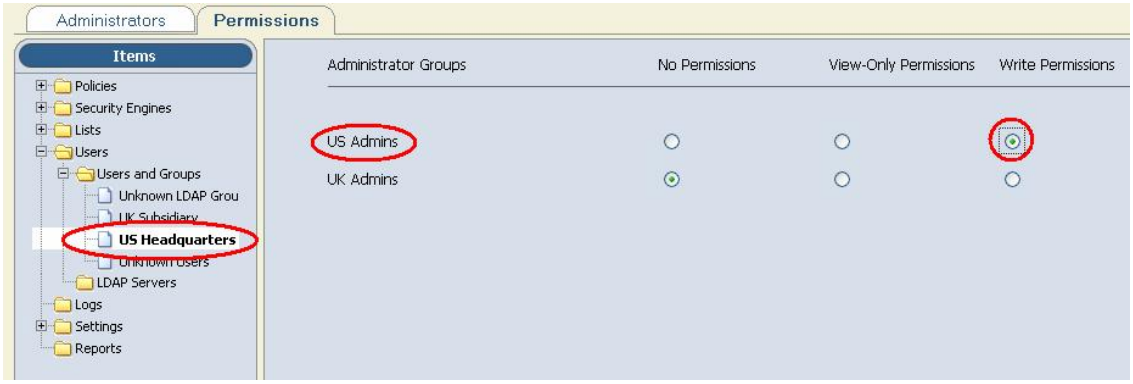
In this example, an administration scenario will be created for a company with US headquarters and a UK subsidiary. Each of the branches will be managed by its own administrators where one is a super administrator (managing its own administrators), one a security administrator and one a report administrator.

⇨ **To manage separate departments with role-based administration:**

1. Create multiple new administrator groups, one per department or company.

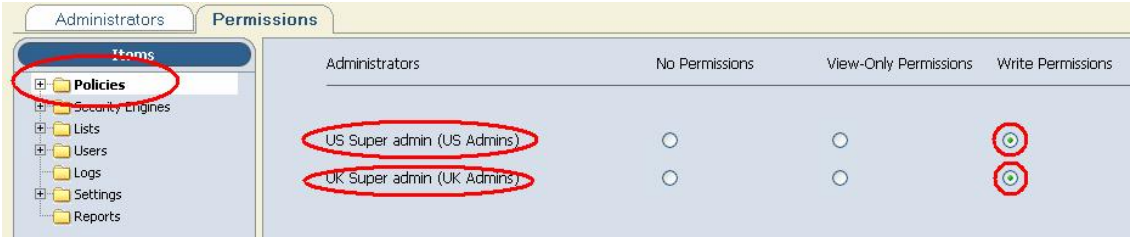
2. Provide each new group with "Write" permissions on all users of the relevant department.





3. Create an administrator within each new group – he/she will act as the group's super administrator.

4. Assign the administrator "Write" permissions on all functionalities.



5. The group's super administrator will create additional administrators all "managing" the same users, i.e. sharing the same rights on these users.

6. The group's super administrator will assign permissions to each administrator he/she created with respect to the different functionalities, so as to define their roles.

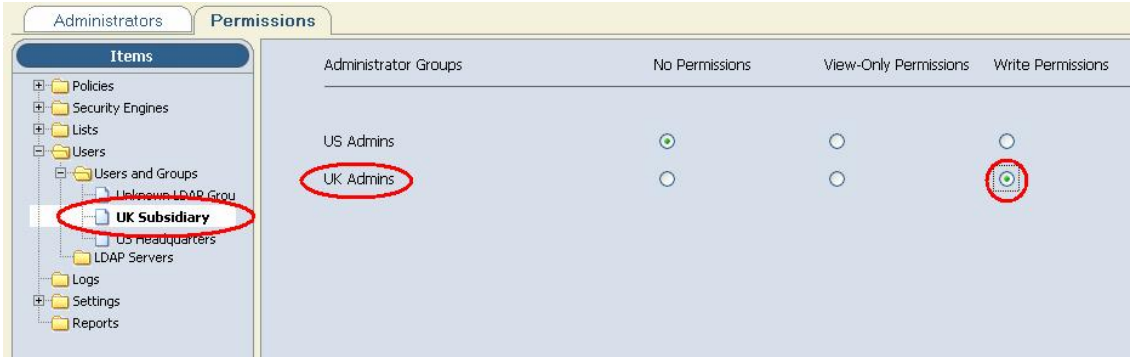
Managing Separate Departments with role-based administration - Alternative Two

In this example, an administration scenario will be created for a company with US headquarters and a UK subsidiary. Each of the branches will be managed by its own administrators where one is a security administrator and another is a report administrator. The overall administration will be managed by the system's super administrators.

⇨ **To manage separate departments with role-based administration:**

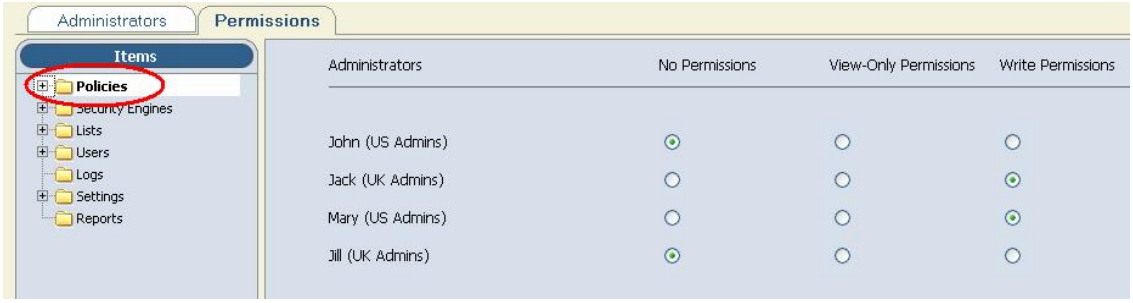
1. Create multiple new administrator groups, one per department or company.

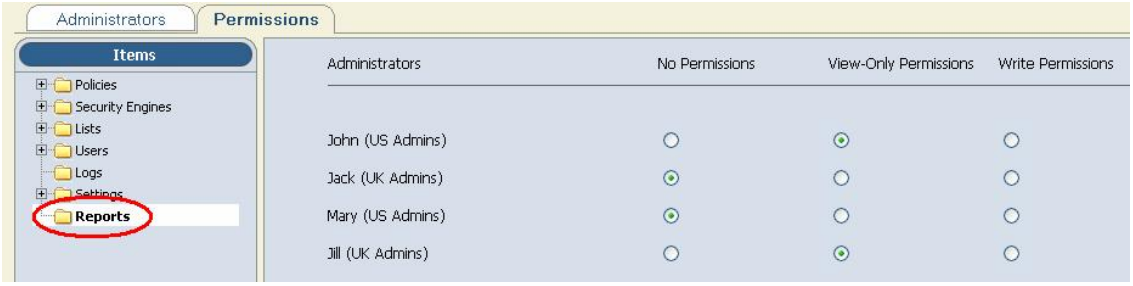
2. Provide each new group with "Write" permissions on all users of the relevant department.



3. Create multiple administrators within each new group.

4. Assign permissions to each new administrator with respect to the different functionalities, so as to define their roles.





Known Issues

- As most changes in settings of multiple administrators affect only the Policy Server, there is no need to commit those changes to the Scanning Servers. An exception, is the "Write" permission for Users which effect the ability to view log and report entries, which should be commited. In version 8.3.5, these changes do not flag a database change; hence the "Commit" functionality is not enabled. In order to force a commit, you should perform another change through the Policy Server and commit all changes together. In version 8.4.0 this has been fixed.
- Due to log viewing optimization, each log entry stores the administrator group associated with the user, i.e. the group which has view permission for this log entry. The consequence of this is that any change performed related to this, for example changing the permissions of an administrator group for a user group, or moving a user to a different group, will only affect log entries later than the time of the permission change.

Conclusion

Vital Security supports various scenarios for the multiple administrators feature within the Management Console. Privacy and security is maintained while allowing for enhanced and streamlined management of the system's users.

This flexibility allows you to define system administration and maintenance according to your company's needs.