

Technical Brief

Multiple Administrators





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

© Copyright 1996 - 2006. Finjan Software Inc. and its affiliates and subsidiaries ("Finjan"). All rights reserved.

All text and figures included in this publication are the exclusive property of Finjan and are for your personal and non-commercial use. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, use or sell any part of its content in any way without the express permission in writing from Finjan. Information in this document is subject to change without notice and does not present a commitment or representation on the part of Finjan. The Finjan technology and/or products and/or software described and/or referenced to in this material are protected by registered and/or pending patents including U.S. Patents No. 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892, 6804780, 6922693, 6944822, 6993662, 6965968 and 7058822 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Anti.dote and Window-of-Vulnerability are trademarks or registered trademarks of Finjan. Sophos is a registered trademark of Sophos plc. McAfee is a registered trademark of McAfee Inc. Kaspersky is a registered trademark of Kaspersky Lab. SurfControl is a registered trademark of SurfControl plc. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation. All other trademarks are the trademarks of their respective owners. Q3 2006.

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: <u>salesapac@finjan.com</u>

Catalog number: VSNG_TB2 Email: <u>support@finjan.com</u> Internet: www.finjan.com United Kingdom Tel: +44 (0)1252 511118 Email: <u>salesuk@finjan.com</u>

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

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



CONTENTS

Introduction	4
The basics of multiple administrator support	4
Super Administrators	
Multiple Administrator Scenarios	6
Conclusion 1	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 multidepartment 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.

Administrators	Name:	Mary
🔓 🌆		
Default	Email:	mary@company.com
Super Administrators	Notes:	IT Manager
admin	notest	
	New password:	
Mary	Confirm password:	



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

Administrators Pe	ermissions			
Items	Administrator Groups	No Permissions	View-Only Permissions	Write Permissions
E Policies				
Gecurity Engines Gecurity Engines Gecurity Engines				~
	Regular Admins	0	0	()
🗄 🔂 Users and Groups				
Unknown LDAP G				
Regular Users	-			
	+			
LDAP Servers				
E Settings				
Reports				

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



Administrators	Name:	John
🔓 🏭	Name.	J0000
Default	Email:	john@company.com
Super Administrators	Notes:	Security Administrator
support	New password:	
John Mary	Confirm password:	

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.

Administrators Permiss	ions			
Items Policies	Administrators 	No Permissions	View-Only Permissions	Write Permissions
 	John (Regular Admins)	0	0	0
← Logs	Mary (Regular Admins)	۲	0	0
Administrators Permiss	ions			
Items	Administrators	No Permissions	View-Only Permissions	Write Permissions
Gecurity Engines Lists Users	John (Regular Admins)	۲	0	0
Elegents	Mary (Regular Admins)	0	0	0

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.



Administrators		LIC Adaptions
8 12 122	Name:	US Admins
Default	Notes:	US administrators
Super Administrators		
admin		
B sapport		
🚽 🔐 US Admins 💦 🔨		

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

Administrators Permissi	ons			
Items	Administrator Groups	No Permissions	View-Only Permissions	Write Permissions
Security Engines Lists Users Users and Groups Users and Groups Ut Subsidiary Us neadquarters LOAP Servers Logs Settings Reports	US Admins UK Admins	⊙	0	õ
Administrators Permissi	Administrator Groups	No Permissions	View-Only Permissions	Write Permissions
Gecurity Engines Gecurity Engines Gecurity Engines	US Admins	0	0	(
Users and Groups Unknown LDAP Grou UK Subsidiary US Headquarters Unknown osers LDAP Servers Logs B Settings Reports	UK Admins	⊘	0	0

3. Create an administrator within each new administrator group.



Administrators	Name:	John
12 122		John
Sefault	Email:	john@hq.com
Super Administrators	Notes:	US administrator
admin		[
E 23US Admins	New password:	
John	Confirm password:	

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

Administrators Perm	issions			
E- Policies	Administrators	No Permissions	View-Only Permissions	Write Permissions
Security Engines Lists Output Users	John (US Admins)	0	0	0
	Mary (UK Admins)	0	0	0

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.

Administrators Permissi	ons			
Items	Administrator Groups	No Permissions	View-Only Permissions	Write Permissions
Policies Default Basic Securit Default Emergency P Default Security Polic	US Admins	0	0	0
UEFault X-Ray Policy	UK Admins	0	0	0

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.



Administrators		
	Name:	US Admins
l 🔓 🚘		New York Control of Co
Sefault	Notes:	US administrators
🖻 🔐 Super Administrators		
admin 🛁		
- dioddor -		
BUS Admins		

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

Items	Administrator Groups	No Permissions	View-Only Permissions	Write Permission
Security Engines				
🔁 Lists 😋 Users	US Admins	۲	0	0
🗄 🚖 Users and Groups	UK Admins	0	0	\bigcirc
Unknown LDAP Grou				
LDAP Servers				
C Settings				

Items	Administrator Groups	No Permissions	View-Only Permissions	Write Permission
Policies				
C Security Engines	\frown			0
🔁 Users	US Admins	0	0	\odot
🗄 😋 Users and Groups	UK Admins	۲	0	0
Unknown LDAP Grou				
UK Subsidiary				
Unknown osers				
DAP Servers				
C Logs				
🚞 Settings				

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



Administrators	Name:	US Super admin
5 t <u>28</u> t228		
2 Default	Email:	admin@us-hq.com
Super Administrators	Notes:	US administrator
admin		
	New password:	
🔤 🕹 US Super admin	Confirm password:	- 51

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

Ttoms	Administrators	No Permissions	View-Only Permissions	Write Permissions
Geconity Engines Lists Users	US Super admin (US Admins)	0	0	0
E Cogs	UK Super admin (UK Admins)	0	0	Ō

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

Administrators Perm	nissions	
Administrators	Name: Email:	John john@us-hq.com
Super Administrators	Notes: New password:	US Report Administrator
Den BLUS Admins John Mary	Confirm password:	
US Super admin UK Admins Jack		
UK Super Admin		

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.



Items	Administrators	No Permissions	View-Only Permissions	Write Permissions
Security Engines Lists Users	John (US Admins)	0	0	۲
Logs	Mary (US Admins)	0	۲	0
E Contraction C	Jack (UK Admins)	۲	0	0
	Jill (UK Admins)	0	0	۲
	UK Super Admin (UK Admins)	0	0	۲
	US Super admin (US Admins)	0	0	۲
Administrators Perm Items	nissions Administrators	No Permissions	View-Only Permissions	Write Permission
Policies Security Engines Lists	John (US Admins)	()		0
🗄 🦳 Users				

Gettings				
Reports	Jack (UK Admins)	۲	0	0
	Jill (UK Admins)	0	0	\odot
	UK Super Admin (UK Admins)	0	0	۲
	US Super admin (US Admins)	0	0	•

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.



Administrators	News	LIC. A during
l 🔓 🚘	Name:	US Admins
and the second	Notes:	US administrators
- 🕵 Default 🗇 - 🎎 Super Administrators		
BUS Admins		

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

Items	Administrator Groups	No Permissions	View-Only Permissions	Write Permissions
Gecurity Engines Gecurity Engines	US Admins	0	0	0
	a second s	۲	0	
Guers and Groups Groups Guers and Groups Guers LDAP Grou UK Subsidiary Os readquarters GubAP Servers Gues Settings Reports	UK Admins	0	0	
Administrators Permiss	Administrator Groups	No Permissions	View-Only Permissions	Write Permissions
Items		No Permissions	View-Only Permissions	Write Permissions

3. Create multiple administrators within each new group.



Administrators	Name:	John
Default	Email:	john@us-hq.com
- Super Administrators	Notes:	US Report Administrator
support	New password:	
John Mary	Confirm password:	
E - 22 UK Admins		

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

Items	Administrators	No Permissions	View-Only Permissions	Write Permission:
Security Engines Security Engines Security Engines Security Engines	John (US Admins)	۲	0	0
Logs	Jack (UK Admins)	0	0	\odot
Reports	Mary (US Admins)	0	0	۲
	Jill (UK Admins)	۲	0	0

Items	Administrators	No Permissions	View-Only Permissions	Write Permission
⊢ Policies ⊢ 🔁 Security Engines			<u></u>	
C Lists	John (US Admins)	0	۲	0
Concerning	Jack (UK Admins)	۲	0	0
Reports	Mary (US Admins)	۲	0	0
	Jill (UK Admins)	0	۲	0



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.