brivo onair

Tiered Administration

7/16/2015

brivo
simply better security

Table of Contents

About This Document 3
What is Tiered Administration? 4
What is Tiered Administration? (Continued) 5
Putting it together 5
Enterprise, Stationary Employee Base 6
Enterprise, Mobile Employee Base 7
Enterprise, Regional Structure 8
Enterprise, Security Department 9
Enterprise, Human Resources Department 10
Landlord/Multi-Tenant, Base-Building Only 11
Landlord/Multi-Tenant, Base-Building + Private Access 12
Guard Station/Central Station Read-Only 13
Guard Station/Central Station Read + Write 14
Receptionist, Visitor Management 15
Tiered Administration Worksheet 16

About This Document

This document introduces Tiered Administration, a framework for wide-area, distributed access control administration. It presents ten sample scenarios and a worksheet to help you design your organization's access control environment.

This document is a companion to the *Administrator's Manual* and is intended for Master Administrators and Senior Administrators only.

Document Scope

This document discusses business applications for Tiered Administration. It does not explain how to create, edit or delete Administrators or how to use the online interface.

Before reading this document, you should have a solid understanding of the following subjects (from the *Brivo OnAir Administrator's Manual*):

- *What is the Activity Log?*
- *What are Users and Groups?*
- *Editing Group Privileges.*
- *What is a Site?*
- *What are Administrators?*
- *Creating and Deleting Administrators.*
- *Editing Assistant Administrator Permissions.*

Document Status

This document is subject to change as features are added to the system. To download the latest version, please visit www.brivo.com.

What is Tiered Administration?

Overview

Tiered Administration is a framework for distributed access control administration.
Tiered Administration lets you control multiple facilities — and multiple, disparate user populations — via a single account interface by delegating routine tasks to many people throughout your organization. These tasks include adding and deleting cardholders, monitoring incident data, and controlling doors and devices.

Tiered Administration is ideal for "wide area" access control environments, including:

Retail Chains
where each store administers its own employee base.

Multi-Tenant Properties
where each tenant company administers its own employee base.

Distributed Enterprises
where each office administers its own employee base.

Central Stations
where a security officer reviews incident data for a particular group of doors.

Tiered Administration also supports traditional applications, including:

Guard Stations
where a security guard monitors incident data for a particular group of doors.

Visitor Management Systems
where a receptionist issues access cards to visitors only.

How it works

Take a moment to review the building blocks of an account:

- An account has **Sites**, which contain **Doors.**
  - A Site represents a building or part of a building.
  - A Site has **Activity** (or Events).
- An account has **Groups**, which contain **Users.**
  - A Group can have privileges to access any number of Doors.
  - A User can be in one or more Groups.
  - A User inherits access privileges from the Groups to which he or she belongs.
  - A User has a single set of credentials, such as a **Card** and/or **PIN.**
- An account has **Administrators.**
  - An account has one Master Administrator, who can administer *all* account data.
  - An account can have many Senior Administrators, who can administer *all* account data.
  - An account can have many Assistant Administrators, who can administer *some* account data.
- An account has **Schedules** and **Holidays.**
  - A Schedule can apply to many Groups via "Group Privileges".
  - A Holiday can apply to many Schedules.

(Continued on the next page)

What is Tiered Administration? (Continued)

Now, review the permissions that can be granted to Assistant Administrators on a per-Site and per-Group basis:

Site Permissions

"View" permission allows an Assistant Administrator to:
View Activity at the Site
View Doors and Devices in the Site

"Edit" permission allows an Assistant Administrator to:
Edit parameters of Doors and Devices in the Site

Group Permissions

"View" permission allows an Assistant Administrator to:
View Privileges of the Group
View Users who belong to the Group
View Cards that belong to Users who belong to the Group

"Edit" permission allows an Assistant Administrator to:
Edit credentials and properties of Users who belong to the Group
Delete Users who belong to the Group

"Append" permission allows an Assistant Administrator to:
View Privileges of the Group
Add Users to the Group
Remove Users from the Group

Putting it together

As you'll see in the following scenarios, you can combine "View," "Edit" and "Append" permissions in a variety of ways to produce a variety of results.

Study each scenario to see if it applies — in whole or in part — to your organization's access control needs. When you're done, use the worksheet on the back page to design your own wide-area access control system.

Enterprise, Stationary Employee Base

Synopsis

This is an enterprise with multiple sites and a predominantly stationary employee base (i.e. employees do not require access to multiple sites).

Scenario

Acme Corp has three stores, Store A, Store B and Store C, which are administered by Admin A, Admin B and Admin C, respectively.

At each store, there are two Groups: "Store X Staff" and "Store X Managers." For example, at Store A, "Store A Staff" can access "Front Door," while "Store A Managers" can access "Front Door" and "Stock Room."

Employees do not travel from store to store.

Each Administrator can manage Users and monitor Activity at his or her store. For example, Admin A can create, edit and delete Users in "Store A Staff" and "Store A Managers," as well as review Activity data and receive E-mail Notifications that correspond to events at Store A.

Site Permissions

			Admin A			Admin B			Admin C		
Site Name	*Doors in Site*		VIEW	EDIT		VIEW	EDIT		VIEW	EDIT	
Store A	*D1. Front Door*	*D2. Stock Room*	X								
Store B	*D3. Front Door*	*D4. Stock Room*				X					
Store C	*D5. Front Door*	*D6. Stock Room*							X		

Group Permissions

		Admin A			Admin B			Admin C		
Group Name	*Has access to*	VIEW	EDIT	APPEND	VIEW	EDIT	APPEND	VIEW	EDIT	APPEND
Store A Staff	*D1*	X	X	X						
Store A Managers	*D1, D2*	X	X	X						
Store B Staff	*D3*				X	X	X			
Store B Managers	*D3, D4*				X	X	X			
Store C Staff	*D5*							X	X	X
Store C Managers	*D5, D6*							X	X	X
Executives	*All Doors*									

Enterprise, Mobile Employee Base

Synopsis

This is an enterprise with multiple sites and a mobile employee base (i.e. some employees require access to multiple sites).

Scenario

Acme Corp has three offices, Office A, Office B and Office C, which are administered by Admin A, Admin B and Admin C, respectively.

At each office, there are three Groups: "Office X Staff," "Office X Managers" and "Office X Visitors." For example, at Office A, "Office A Staff" can access "Front Door," "Office A Managers" can access "Front Door" and "Server Room," and "Office A Visitors" can access "Front Door."

Some employees travel from office to office. For example, "User A," who belongs to "Office A Staff" and whose home base is Office A, sometimes visits Office B. He uses one card to access both facilities.

Each Administrator can manage Users and monitor Activity at his or her office. For example, Admin A can create, edit and delete Users in "Office A Staff" and "Office A Managers," as well as review Activity data and receive E-mail Notifications that correspond to events at Office A.

In addition, each Administrator can look up employees from other offices and grant them access to his or her own office, without being able to change their credentials or personal information. For example, Admin A can look up "User B," who belongs to "Office B Staff," and add the User to "Office A Visitors."

Site Permissions

			Admin A			Admin B			Admin C		
Site Name	*Doors in Site*		VIEW	EDIT		VIEW	EDIT		VIEW	EDIT	
Office A	*D1. Front Door*	*D2. Server Room*	X								
Office B	*D3. Front Door*	*D4. Server Room*				X					
Office C	*D5. Front Door*	*D6. Server Room*							X		

Group Permissions

		Admin A			Admin B			Admin C		
Group Name	*Has access to*	VIEW	EDIT	APPEND	VIEW	EDIT	APPEND	VIEW	EDIT	APPEND
Office A Staff	*D1*	X	X	X	X			X		
Office A Managers	*D1, D2*	X	X	X	X			X		
Office A Visitors	*D1*	X		X	X			X		
Office B Staff	*D3*	X			X	X	X	X		
Office B Managers	*D3, D4*	X			X	X	X	X		
Office B Visitors	*D3*	X			X		X	X		
Office C Staff	*D5*	X			X			X	X	X
Office C Managers	*D5, D6*	X			X			X	X	X
Office C Visitors	*D5*	X			X			X		X
Executives	*All Doors*									

Enterprise, Regional Structure

Synopsis

This is an enterprise with a regional structure and many sites per region.

Scenario

Acme Corp has six offices, Office A through Office F, which are administered by Admin A through Admin F, respectively. In addition, there are two regional Administrators, Admin ABC and Admin DEF, who administer three sites each.

Notes

This scenario demonstrates how to achieve "hierarchical" administration. At the bottom of the hierarchy are the local Administrators; in the middle are the regional Administrators; at the top is the Master Administrator.

Site Permissions

Site Name	*Doors in Site*	Admin A VIEW	Admin A EDIT		Admin ABC VIEW	Admin ABC EDIT		Admin DEF VIEW	Admin DEF EDIT	
Office A	*D1. Front Door*	X			X					
Office B	*D2. Front Door*				X					
Office C	*D3. Front Door*				X					
Office D	*D4. Front Door*							X		
Office E	*D5. Front Door*							X		
Office F	*D6. Front Door*							X		

Group Permissions

Group Name	*Has access to*	Admin A VIEW	Admin A EDIT	Admin A APPEND	Admin ABC VIEW	Admin ABC EDIT	Admin ABC APPEND	Admin DEF VIEW	Admin DEF EDIT	Admin DEF APPEND
Office A Staff	*D1*	X	X	X	X	X	X			
Office B Staff	*D2*				X	X	X			
Office C Staff	*D3*				X	X	X			
Office D Staff	*D4*							X	X	X
Office E Staff	*D5*							X	X	X
Office F Staff	*D6*							X	X	X
Executives	*All Doors*									

Enterprise, Security Department

Synopsis

This is an enterprise with multiple sites. Access is administered centrally by a security department, but a local Administrator at each site can view data relevant to his or her site.

Scenario

Acme Corp has three offices, Office A, Office B and Office C, which are administered by Admin A, Admin B and Admin C, respectively.

All company employees are added to (and deleted from) the User database by the security department at Acme headquarters. However, Admin A, Admin B and Admin C can monitor Activity at their respective offices and have visibility of their respective employees.

Site Permissions

			Admin A			Admin B			Admin C		
Site Name	*Doors in Site*		VIEW	EDIT		VIEW	EDIT		VIEW	EDIT	
Office A	*D1. Front Door*	*D2. Server Room*	X								
Office B	*D3. Front Door*	*D4. Server Room*				X					
Office C	*D5. Front Door*	*D6. Server Room*							X		

Group Permissions

		Admin A			Admin B			Admin C		
Group Name	*Has access to*	VIEW	EDIT	APPEND	VIEW	EDIT	APPEND	VIEW	EDIT	APPEND
Office A Junior Staff	*D1*	X								
Office A Senior Staff	*D1, D2*	X								
Office B Junior Staff	*D3*				X					
Office B Senior Staff	*D3, D4*				X					
Office C Junior Staff	*D5*							X		
Office C Senior Staff	*D5, D6*							X		
Executives	*All Doors*									

Enterprise, Human Resources Department

Synopsis

This is an enterprise with multiple sites. Users are added to the system by a human resources department, but a local Administrator at each site can view data relevant to his or her sites *and move Users in and out of specific Groups*.

Scenario

Acme Corp has three offices, Office A, Office B and Office C, which are administered by Admin A, Admin B and Admin C, respectively.

All company employees are added to (and deleted from) the User database by the human resources department at Acme headquarters. However, Admin A, Admin B and Admin C can monitor Activity at their respective offices and have visibility of their respective employees. *In addition, each Administrator can move employees in and out of specific Groups as they see fit, but cannot edit employees' credentials or personal information.*

Notes

In this scenario, the Group "All Employees" is a holding Group; its only purpose is to create a "public directory" of Users. Each Administrator can view the Users in "All Employees" and append the Users in their own Group(s) as they see fit.

Site Permissions

Site Name	Doors in Site		Admin A VIEW	Admin A EDIT	Admin B VIEW	Admin B EDIT	Admin C VIEW	Admin C EDIT
Office A	*D1. Front Door*	*D2. Server Room*	X					
Office B	*D3. Front Door*	*D4. Server Room*			X			
Office C	*D5. Front Door*	*D6. Server Room*					X	

Group Permissions

Group Name	Has access to	Admin A VIEW	Admin A EDIT	Admin A APPEND	Admin B VIEW	Admin B EDIT	Admin B APPEND	Admin C VIEW	Admin C EDIT	Admin C APPEND
All Employees	*No Doors*	X			X			X		
Office A Junior Staff	*D1*	X		X						
Office A Senior Staff	*D1, D2*	X		X						
Office B Junior Staff	*D3*				X		X			
Office B Senior Staff	*D3, D4*				X		X			
Office C Junior Staff	*D5*							X		X
Office C Senior Staff	*D5, D6*							X		X
Executives	*All Doors*									

Landlord/Multi-Tenant, Base-Building Only

Synopsis

This is a multi-tenant commercial property with shared building entry. Each tenant administers its own employee base.

Scenario

Acme Corp has one building, Acme Tower. Acme Tower has three tenants, Company A, Company B, and Company C, which are administered by Admin A, Admin B, and Admin C respectively.

All tenants are permitted to access Lobby Door and Garage Door. (The individual suites are not access-controlled).

Each Administrator can grant and revoke access to the shared doors. For example, Admin A can create "User A" in Group "Tenant A Staff," which has no access privileges. At the same time, Admin A can put User A into the Group "All Tenants," which can access the shared doors at all times.

Notes

An alternate (but less efficient) approach is to apply "Lobby Door" and "Garage Door" privileges to every Group and not have a single "All Tenants" Group.

Site Permissions

Site Name	*Doors in Site*	Admin A VIEW	Admin A EDIT	Admin B VIEW	Admin B EDIT	Admin C VIEW	Admin C EDIT
Acme Tower	*D1.Lobby Door D2. Garage Door*						

Group Permissions

Group Name	*Has access to*	Admin A VIEW	Admin A EDIT	Admin A APPEND	Admin B VIEW	Admin B EDIT	Admin B APPEND	Admin C VIEW	Admin C EDIT	Admin C APPEND
All Tenants	*D1, D2*			X			X			X
Tenant A Staff	*No Doors*	X	X	X						
Tenant B Staff	*No Doors*				X	X	X			
Tenant C Staff	*No Doors*							X	X	X
Management	*All Doors*									
Alternate Version										
Tenant A Staff	*No Doors*	X	X	X						
Tenant B Staff	*No Doors*				X	X	X			
Tenant C Staff	*No Doors*							X	X	X
Management	*All Doors*									

Landlord/Multi-Tenant, Base-Building + Private Access

Synopsis

This is a multi-tenant commercial property with shared building entry *plus individual site entry.* Each tenant administers its own employee base.

Scenario

Acme Corp has one building, Tower 1. Tower 1 has three tenants, Company A, Company B, and Company C, which are administered by Admin A, Admin B, and Admin C respectively.

All tenants are permitted to access Lobby Door and Garage Door. In addition, Company A tenants are permitted Front Door access at Suite A, Company B tenants are permitted Front Door access at Suite B, and Company C tenants are permitted Front Door access at Suite C.

Each Administrator can grant and revoke access to the shared doors *and to his or her private door*. For example, Admin A can create "User A" in Group "Tenant A Staff," which has can access Suite A door; at the same time, Admin A can put User A into the Group "All Tenants," which can access the shared doors.

In addition, each Administrator can monitor Activity at his or her own suite. For example, Admin A can review Activity data and receive E-mail Notifications that correspond to events at Suite A.

Notes

An alternate (but less efficient) approach is to apply "Lobby Door" and "Garage Door" privileges to every Group and not have a single "All Tenants" Group.

Also note, each physical area is considered to be a separate Site, even though they are part of the same structure.

		Admin A			Admin B			Admin C		
Site Permissions		VIEW	EDIT		VIEW	EDIT		VIEW	EDIT	
Site Name	*Doors in Site*									
Tower 1 Base	*D1.Lobby Door D2. Garage Door*									
Tower 1 Suite A	*D3 Front Door*	X								
Tower 1 Suite B	*D4 Front Door*				X					
Tower 1 Suite C	*D5 Front Door*							X		
		VIEW	EDIT	APPEND	VIEW	EDIT	APPEND	VIEW	EDIT	APPEND
Group Permissions										
Group Name	*Has access to*									
All Tenants	*D1, D2*			X			X			X
Tenant A Staff	*No Doors*	X	X	X						
Tenant B Staff	*No Doors*				X	X	X			
Tenant C Staff	*No Doors*							X	X	X
Management	*All Doors*									
Alternate Version										
Tenant A Staff	*No Doors*	X	X	X						
Tenant B Staff	*No Doors*				X	X	X			
Tenant C Staff	*No Doors*							X	X	X
Management	*All Doors*									

Guard Station/Central Station Read-Only

Synopsis

This is a “guard station” or “central station” application for monitoring incident data.

Scenario

Acme Corp has three buildings, Tower A, Tower B, and Tower C, which are administered by Admin A, Admin B, and Admin C respectively.

Each Administrator can monitor Activity at his or her building and view details of Users who have access to the building.

Site Permissions

Site Name	*Doors in Site*	Admin A VIEW	Admin A EDIT	Admin A	Admin B VIEW	Admin B EDIT	Admin B	Admin C VIEW	Admin C EDIT	Admin C
Tower A	*D1. Lobby Door*	X								
Tower B	*D2. Lobby Door*				X					
Tower C	*D3. Lobby Door*							X		

Group Permissions

Group Name	*Has access to*	VIEW	EDIT	APPEND	VIEW	EDIT	APPEND	VIEW	EDIT	APPEND
Tower A Tenants	*D1*	X								
Tower B Tenants	*D2*				X					
Tower C Tenants	*D3*							X		
Management	*All Doors*	X			X			X		

Guard Station/Central Station Read + Write

Synopsis

This is a “guard station” or “central station” application for monitoring incident data, managing Users, and editing Door and Device parameters.

Scenario

Acme Corp has three buildings, Tower A, Tower B, and Tower C, which are administered by Admin A, Admin B, and Admin C respectively.

Each Administrator can monitor Activity at his or her building; view details of Users who have access to the building, create, edit, and delete Users with access to the building; and control doors at the building.

Site Permissions

		Admin A			Admin B			Admin C		
Site Name	*Doors in Site*	VIEW	EDIT		VIEW	EDIT		VIEW	EDIT	
Tower A	*D1. Lobby Door*	X	X							
Tower B	*D2. Lobby Door*				X	X				
Tower C	*D3. Lobby Door*							X	X	

Group Permissions

		Admin A			Admin B			Admin C		
Group Name	*Has access to*	VIEW	EDIT	APPEND	VIEW	EDIT	APPEND	VIEW	EDIT	APPEND
Tower A Tenants	*D1*	X	X	X						
Tower B Tenants	*D2*				X	X	X			
Tower C Tenants	*D3*							X	X	X
Management	*All Doors*	X			X			X		

Receptionist, Visitor Management

Synopsis

This is an implantation of a visitor management system, in which a receptionist or front desk worker is permitted to issue access cards to visitors.

Scenario

Acme Corp has one office, Office A. The office has many visitors who stay for days or weeks.

Admin A can create, edit, and delete Users in the Group "Visitors."

Site Permissions

Site Name	*Doors in Site*	Admin A VIEW	Admin A EDIT	Admin A	Admin B VIEW	Admin B EDIT	Admin B	Admin C VIEW	Admin C EDIT	Admin C
Office A	*D1. Front Door D2. Server Room*									

Group Permissions

Group Name	*Has access to*	Admin A VIEW	Admin A EDIT	Admin A APPEND	Admin B VIEW	Admin B EDIT	Admin B APPEND	Admin C VIEW	Admin C EDIT	Admin C APPEND
Office A Regular Staff	*D1*									
Office A Weekend Staff	*D1*									
Office A Managers	*All Doors*									
Office A Visitors	*D1*	X	X	X						

Tiered Administration Worksheet

Before implementing a wide-area access control system, consider: How many Administrators will there be? How many distinct Sites and Groups should each Administrator be able to view or edit? Refer to the scenarios in this document for guidance – you can mix and match them or design your own.

Sites

Site Name	*Doors in Site*	VIEW	EDIT			VIEW	EDIT			VIEW	EDIT	
Site: _____	*D1* .____ __. ____ __. ____											
Site: _____	__. ____ __. ____ __. ____											
Site: _____	__. ____ __. ____ __. ____											
Site: _____	__. ____ __. ____ __. ____											
Site: _____	__. ____ __. ____ __. ____											

Groups

Group Name	*Has access to*	VIEW	EDIT	APPEND		VIEW	EDIT	APPEND		VIEW	EDIT	APPEND
Group: _____												
Group: _____												
Group: _____												
Group: _____												
Group: _____												
Group: _____												
Group: _____												
Group: _____												
Group: _____												
Group: _____												
Group: _____												
Group: _____												
Group: _____												
Group: _____												
Group: _____												