

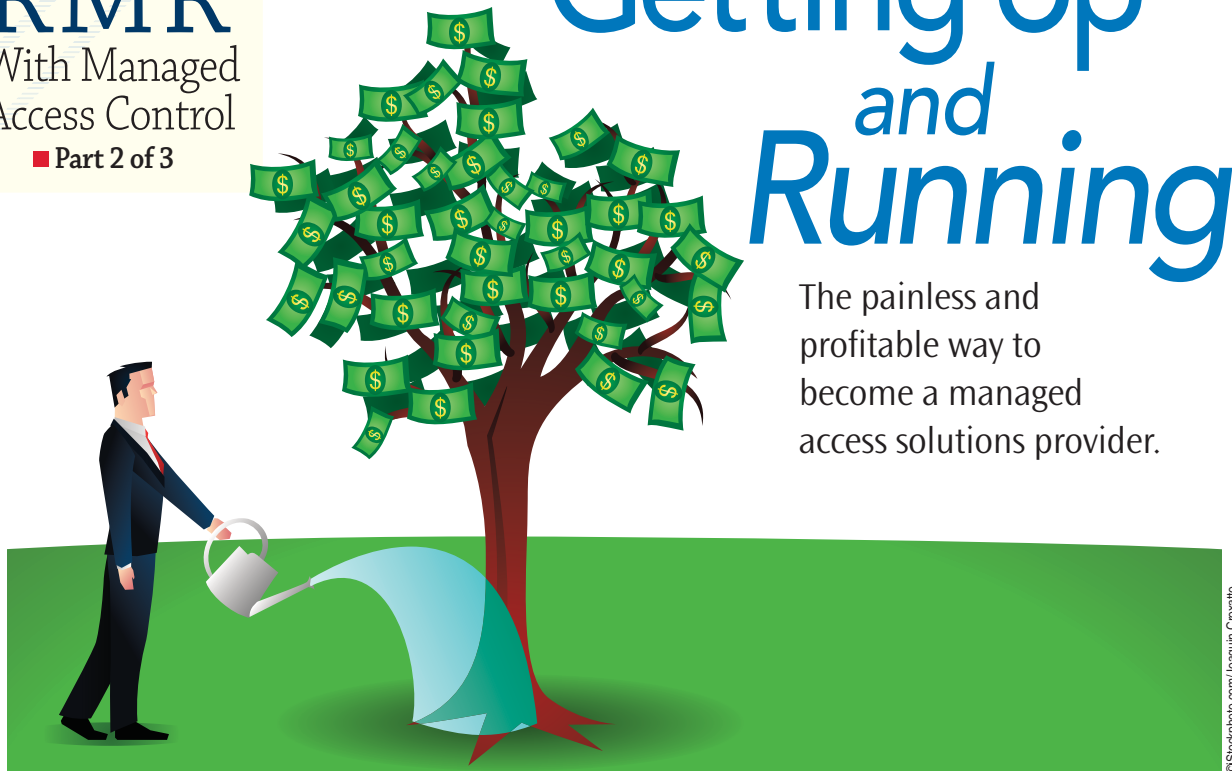
# How to Grow RMR

## With Managed Access Control

■ Part 2 of 3

# Getting Up and Running

The painless and profitable way to become a managed access solutions provider.



©Stockphoto.com/Isaquin Crovatto

BY STEVEN O. GIBBS

Welcome to Part 2 of *SECURITY SALES & INTEGRATION*'s three-part series, "How to Grow RMR With Managed Access Control." Brought to you by Honeywell Access Systems, this material has been designed to educate security dealers and systems integrators all about managed access control (MAC) technology and how to leverage it to build recurring monthly revenue (RMR).

Part 1 (see the February issue or visit [www.securitysales.com/managed-access](http://www.securitysales.com/managed-access)) served as an introduction to MAC and compared it to the more traditional site-managed access control model. It also explored the rationale for why both customer and dealer would consider MAC and reviewed potential applications.

Part 2 takes it all a step further by explaining the implementation of MAC in the form of infrastructure (both hardware and software). We'll also discuss Internet connectivity requirements, staffing needs and the roles required to support a MAC service.

### INITIAL INVESTMENT IS MINIMAL

First, a quick review of the benefits MAC offers the customer and what the security dealer or systems integrator needs to do, at a minimum, to ensure deliverability of these benefits.

While MAC promises to remove the overall operational burden of traditional, site-managed access control from the customer and the task of supporting multiple access control systems (ACS) from the dealer, these issues don't just disappear. Rather, they are "compressed" into a single point of operation. The customer no longer maintains the hardware, operating systems and ACS software. Instead, in exchange for a monthly service fee, the dealer takes on the responsibility.

Again, the advantage to the dealer is a cost savings from reducing the number of systems in the field to a single, robust MAC server. While the customer no longer worries about maintaining trained staff to perform daily system operation tasks and non-routine maintenance, the dealer must provide personnel to perform these functions. The advantage

lies in the dealer's ability to have staff perform these functions for multiple customers from a single point of control in a much more cost-effective manner, thus creating a profit center based on RMR (while reducing service calls as remote administration provides more immediate service for customers).

At first glance, the dealer may envision a large, sophisticated operation center, much like a UL-Listed central station, along with the business complexity and expense normally associated with such an operation. This is not the case. Remember how access control systems usually start out fairly small

Brought to you by

# Honeywell

Presented by

## SECURITY SALES & INTEGRATION

## Managed Access Control Staffing Requirements

Task	Description	Number of Accounts**	Time	MONTHLY TOTALS
Creating a new account	1 new account/month	1	1 hour/account	One time
Customer request*	1 request/account each week at 3 minutes/request	15	12-15 minutes/account	3 hours
Managing the system	Operating system, WPPC software, virus checking	15	4 minutes/account	1 hour
Initial photo-ID badging	50-100 badges (average)	15	3 hours/month or 1 batch/month	One time
Replacement cards/new employees	3 cards/month at 2 minutes/card	15	15 minutes/account	2 hours

\* Typical requests include: add user, remove user, open door and change time schedule.  
\*\* Based on 15 accounts per year.

**Total Time to Administer 7 Hours/Month**

with a limited number of access points and grow, over time, through additions and upgrades. This will also be true of MAC. Day One will not normally see the addition of 100 or more client systems.

For this reason, the dealer can usually begin a MAC service rollout with resources, such as onsite technicians and support staff, already in place. As the revenue grows in concert with the customer list, upgrades in computer hardware and Internet bandwidth along with increases in support staff will be financially supported by continued growth.

It is then very important to remember another basic rule of the ACS business: ACS hardware and software solutions chosen for a MAC service should be “scalable” in nature. This simply means that as the number of access points and credential holders grow, the ACS software should not require complete replacement. Instead, upsizing should simply be a matter of increasing capacity through license upgrades — and increased RMR.

### MAC SERVER AND SOFTWARE NEEDS

The core of a MAC center will be the computer head-end. This computer should have plenty of processing power and the ability to quickly upgrade hard drive storage capacity with minimal system downtime. Although not a strict requirement, a “server-class” machine will certainly meet almost any anticipated growth during the lifecycle of the typical computer platform. A professional or server-class operating system will also be a good investment.

As the customer base grows, it will eventually make sense to split the ACS software processing function, database management (DBMS) application, field device communications and Web-based interface portal access across two or more task-oriented computers. Having one or more backup computers ready to slip into place or set up for automatic failover in case of a primary failure will provide the reliability the customer will expect from their MAC service provider. However, most access control systems will still run independently of the remote management system.

This should not bring to mind a room filled with PCs, monitors and keyboards. With small footprint rack-mount servers and storage devices along with keyboard/video/mouse (KVM) switches, all of this can easily be installed in a remote and secure location within the dealer’s office.

Although the customer no longer worries about backing up essential data, this responsibility now lies squarely on the dealer’s shoulders. The dealer should take advantage of widely available and inexpensive backup solutions including redundant arrays of inexpensive/independent disks (RAID), disk imaging soft-

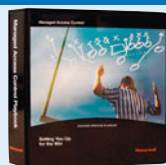
ware and/or automated offsite backups of critical data over the Internet.

Choosing an appropriate ACS software solution for the core of the MAC service is also critical. While several applications exist, it is important to select one that is strong in two important features: database partitioning and operator logon/activity tracking.

True database and device partitioning separates access points, security levels, time codes, and credential holders, as well as all the other logical and physical elements of a typical ACS into partitioned areas within a single ACS software database. Obviously, the customer accessing their own system through a Web portal should not even see, let alone have access to, the data and devices of another customer.

The dealer will be held accountable to the customer for the security integrity of their ACS. All access to customer data and device control (i.e. locking/unlocking doors, assigning security levels, etc.) should be managed through a reliable operator login process that also tracks activities of both the dealer’s personnel and the activities performed through the Web portal by the customer’s staff. Hand in hand

### ‘Playbook’ Gets You in the Managed Access Game



Those interested in pursuing the concepts presented in this series and maximizing their RMR are advised to reference the *Honeywell Access Control Playbook*. Find out how you can obtain this comprehensive guide by visiting [www.honeywellaccess.com](http://www.honeywellaccess.com).

with this feature should go the ability to flexibly control exactly which functions may be performed by specific operators (based on their role) once they have logged into the ACS software.

### ASSESSING INTERNET CONNECTIVITY

Internet access with adequate bandwidth is another important element required for MAC. Internet connectivity will be the primary communication path between the customer's ACS field devices and the dealer's MAC server. Most dealers will already have some form of Internet access with enough bandwidth to support MAC operations during initial rollout. However, as the MAC account list grows, so will demands on the Internet connection.

DSL is the most popular connectivity used by small businesses for Internet access providing the bandwidth necessary for most applications needing access to outside networks. Most DSL service is actually ADSL, or asymmetric DSL, which provides a larger pipe from the service provider to the subscriber than is available back the other way. This works fine when the subscriber is the one doing most of the "downloading" or receiving text and images from a remote server.

However, as the MAC account list grows and more data must be uploaded to various customer sites, this imbalance of service will eventually start to cause a bottleneck. How soon this occurs will depend on how many of the MAC clients utilize the option to connect to their system through the Web portal option. During this activity the dealer's MAC server essentially becomes a Web site and data traffic being downloaded by multiple customers becomes data that must be uploaded through the dealer's single Internet connection.

The first basic upgrade step for a dealer, without increasing bandwidth, is symmetric DSL (SDSL) where the total bandwidth is equal for download and upload. Further steps would include subscribing to additional T-1 channels (DSL is essentially one of the 64 channels in full T-1 service) in order to obtain

needed bandwidth. Again, these are scalable options as the MAC service grows.

### DESIGNATING PERSONNEL AND TASKS

Although it should not be necessary to hire new personnel in order to prepare for initial rollout of a MAC service, it will require identifying current staff abilities and assigning responsibility for various MAC functions to them.

The dealer's current installation force will continue to install the ACS field devices as with any traditional, site-managed system. When adding a MAC account, someone tasked with the system administrator role at the dealer's MAC center will be responsible for working with the new client and programming ACS devices, security levels, time schedules, and the other system parameters necessary to initiate the new account.

Once the new MAC account is commissioned, a dealer staff member with the assigned role of system operator will enter the initial credential holders and, if part of the MAC service offering, will create access cards/credentials for the customer.

To assist with the flow of information between the new customer and dealer staff, a basic set of procedures and data entry forms should be developed. Consideration should be given to making these forms electronic in nature allowing the customer to E-mail both initial data and ongoing changes directly to the system operator.

While developing various service levels and monthly charges for a MAC, the dealer should also consider the issue of 24/7 availability and response to data changes and access requests versus a



A dealer can usually use existing staff to roll out MAC services. More customers bringing in more revenue then makes it easy to adjust hardware, bandwidth and personnel.

9-5 business model. Remember, with Web portal functionality built into the MAC server, the dealer staff could respond to after-hours requests for service from just about anywhere. Obviously, for the customer that requires 24/7 service, an increase in the basic monthly service fee is justified and likely acceptable to meet their needs.

Another optional service that many customers, especially those with a small number of users and limited turnover, would benefit from is photo ID badge creation as part of the MAC service. This alone greatly reduces the initial customer investment by eliminating an expensive badge printer, software, and badging card stock and ribbons.

The customer simply captures the credential holder's image with an inexpensive digital camera and E-mails that image, as an attachment, to the dealer's system operator. The system operator creates the finished credential, enters it into the ACS, and mails it out to the customer's point of contact. RMR for this service should include a basic fee plus a per badge production fee. In the MAC setup, *all* the RMR comes back to the dealer. Thus the potential revenues are unlimited, as opposed to other alternatives where the RMR may be shared.

### CONTINUING THE PROGRESSION

In summary, as participating dealers' lists of MAC clients expand so too will their ever-increasing profit margins. Offering these services allow providers to tap into potentially unlimited sources of RMR since 100 percent of the revenues go directly to the dealers and are not shared. That business growth will make it easy to incrementally increase MAC server capacity, network bandwidth and staff as needed. ■

### Next Up: MAC Sales, Marketing & Pricing

Be sure to check out Part 3 of this series in SSI's April issue for details on developing a MAC marketing and sales compensation program, as well as establishing a menu of customer pricing options. All parts of this series will also be available at [www.securitysales.com/managedaccess](http://www.securitysales.com/managedaccess).

# grow your business



## Plant the seed for RMR growth.

Now there's a way to offer an efficiently managed access control system—and earn RMR at the same time. Honeywell's managed access control helps you cultivate more business and maximize the value of each sale. Managed access control lets your end user hand over chores like badging, reporting, and daily task automation—allowing you to create solutions that secure their facility and streamline

their operations. Let Honeywell's managed access control solution help you grow your business. Plant the seed now and begin to see the green that grows with RMR.

## Honeywell

Start growing your business today! Call us at **1-800-323-4576** to find out more about the Managed Access Control Playbook – your step-by-step guide to selling managed access control.

© 2010 Honeywell International Inc. All rights reserved.

[www.securitysales.com/freeinfo/13143](http://www.securitysales.com/freeinfo/13143)