# Introducing Role-Based Administration in System Center 2012 Configuration Manager

September 23, 2011

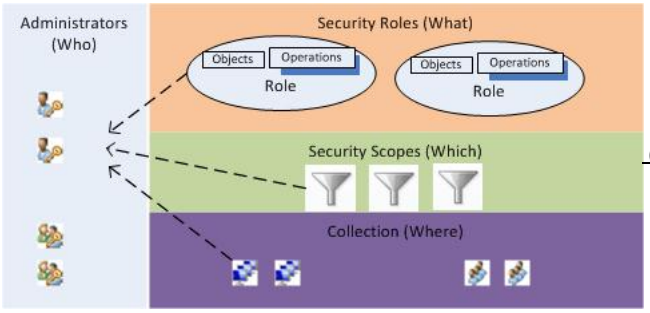
YVETTE O'MEALLY (HTTPS://CLOUDBLOGS.MICROSOFT.COM/ENTERPRISEMOBILITY/AUTHOR/YVETTE-OMEALLY/)

in System Center Configuration Manager (/enterprisemobility/?product=system-center-configuration-manager)

*[Today's post contributor is Lin Tang (http://blogs.technet.com/b/configmgrteam/archive/2011/09/30/lin-tang-s-bio.aspx)]*

## Overview

Role-based administration (RBA) is a new feature introduced in Configuration Manager 2012. RBA provides Configuration Manager administrators with an easy way to implement the security model that allows them to assign and manage administrative permissions by assigning which actions they are able to perform using security roles, which users and systems they can manage through collections, and which objects they can access using security scopes. Based on their administrative permissions, the Configuration Manager console has been significantly enhanced to provide administrators with a streamlined view that is customized to their specific role—showing only what they need to do their job.




(https://cloudblogs.microsoft.com/enterprisemobility/wp-content/uploads/sites/2/2017/10/2260.RBA1_.jpg)

## Key Concepts

Security Role

Each security role combines objects with permitted operations that collectively allow a Configuration Manager administrative users to perform a job function such as "Application Administrator". Objects are the items in Configuration Manager that you want to protect, such as applications. Operations are what you can do with the objects, like read, modify, and delete. Administrators who are familiar with Configuration Manager 2007, could view security roles as a set of "Class Permissions". (reference http://technet.microsoft.com/en-us/library/bb632332.aspx)

Security roles are created for different job functions. Instead of granting granular permissions to a Configuration Manager administrative user, you assign a particular security role to them. Configuration Manager provides several built-in roles which can meet some popular functions, like Software Update Manager for managing software updates. You also can define customized security roles by copying an existing role and making some modifications, or importing security roles that you have obtained.

### Security Scope

Use security scopes to limit an administrative users access to specific secured objects. Security roles grant the class level permission to the user such as "Read Applications". Security scopes grant instance level permission for *which* applications they can read. Administrators who are familiar with Configuration Manager 2007, could view security scopes as a way of grouping "Instance Permissions". (reference http://technet.microsoft.com/en-us/library/bb632332.aspx)

Let's look at an example: You have two collections: "All Desktops" and "All Servers", and you have different asset managers to manage these collections. According to the security role definition, both of them have the permission to create and modify software metering rules. However, you really don't want the "All Desktops" administrator to modify the metering rules for the "All Servers" collection. You can use security scopes to assign the "All Desktops" metering rules to the "Desktop Content" security scope, and server metering rules to the "Server Content" security scope. You then assign the correct security scope to each administrator. Once you configure the security assignments in this way, the "All Desktops" administrator cannot create a rule targeting "All Servers", nor can they modify a metering rule that the "All Servers" administrator created. Other examples are where you want to protect other object types such as applications, packages, boundaries, sites, task sequences, etc. You can just assign them to a security scope which is only assigned to the administrative users that need to access them.

When discussing security scopes, we should also discuss the "Default Scope". The "Default Scope" is a concept that might be confusing at first. When the Configuration Manager site is installed, there are many secured objects already in the system, e.g. site and query. Because all securable object types must have a security scope assigned to them, their default scope is the built-in "Default Scope". The "Default Scope" is not a security scope to which new objects are automatically associated. When you create a new object, the security scopes associated with the object depend on the security assignments of the administrative user who creates the object.

### Collection

A Collection is the group of devices or users the administrative user can manage. Unlike security roles and security scopes, collections support a hierarchy relationship by using the collection limiting functionality that is new in Configuration Manager 2012. The Configuration Manager collection features, which include Collection Limiting and the "Exclude" and "Include" membership rules, are very powerful administration tools. If you define a query based collection called "All Desktops", it can be limited to (a subset of) of the "All Systems" collection. If you want to ensure that "All Desktops" never contains servers, you can create a membership rule that excludes the "All Servers" collection. Even if you accidentally add a server as a direct member to "All Desktops", that server would not be evaluated as "All Desktops" member because the exclude rule takes precedence.

When you add a new Configuration Manager administrative user that has collection creation permissions and they are assigned the "All Desktops" collection, you are ensuring that they cannot manage the servers since any collections they create will always be limited to (a subset of) the "All Desktops" collection. When you assign the "All Desktops" collection to an administrative user, they will automatically have permissions on all collections which are limited to "All Desktops", and they are restricted from modifying the collection definition for "All Desktops".

**Collection Based Security Partitions**

In Configuration Manager 2007, you may have used Configuration Manager sites as administrative boundaries. If you wanted to assign one administrator exclusive permissions for Europe, and different administrator permissions for North America, you may have set up two different sites that enforced these security limitations. With Configuration Manager 2012, sites are no longer administrative boundaries and administrative permissions are achieved by assigning collections to administrative users. This has a few important implications:

1) If you have multiple Configuration Manager 2007 sites only to serve as administration boundaries, you can now reduce your infrastructure cost by using fewer servers and sites through the use of collections!

2) When an administrator is assigned to the "All Windows 7" collection, that collection is evaluated across the entire hierarchy, not just within the local site. This means that if you have a global "Assets and Compliance Manager", they can manage all systems from one Configuration Manager console. With Configuration Manager 2007 they would need to sign into each site and repetitively perform their duties. Now, they can do this once, from one console, from wherever they are located.

3) If you would like to keep your previous administrative boundaries (e.g. Europe and North America), you will need to define a collection for each of these groups and assign them to your administrative users.

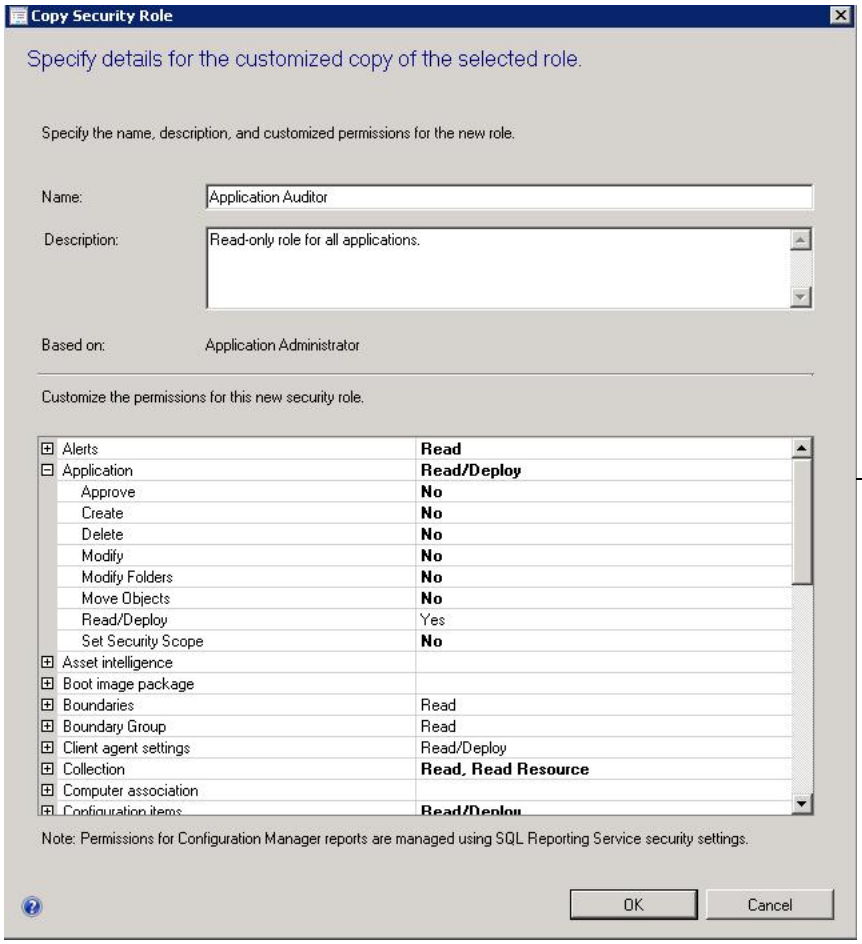
# Example Scenario

1. Background

Let's go through a full user scenario to understand these concepts. Kevin is granted the "Full Administrator" security role with access to all objects and all collections during the installation of the Configuration Manager site. Kevin's company has two primary locations, North America and Europe. Kevin wants to grant Meg the responsibility of managing applications for the North America desktops. Also, Kevin prefers that Meg can see all of the applications in the Configuration Manager, including those for the Europe desktops.

2. Create Security Role

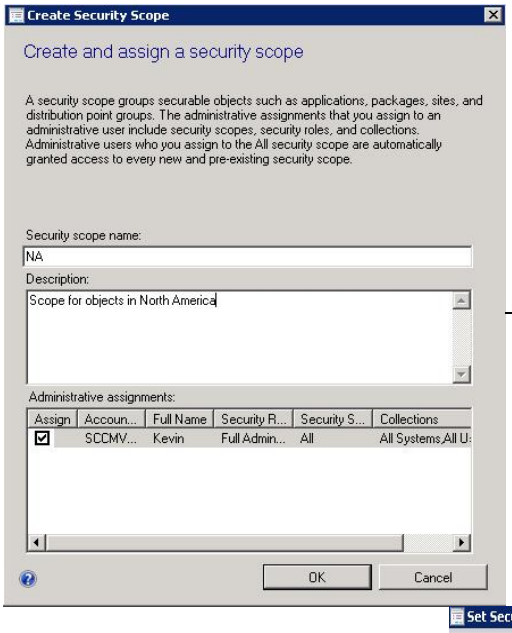
Kevin checks all the security roles in system, and the built-in role "Application Administrator" can meet his requirement for Meg to manage applications. He also notices there is no security role he can use for only reading all the applications in Configuration Manager. Therefore, kevin will make a custom security role named Application Auditor that is based on the Application Administrator security role. On the Copy Security Role page, Kevin removes all permissions for modify/delete/create, and keeps onlythe read permissions.



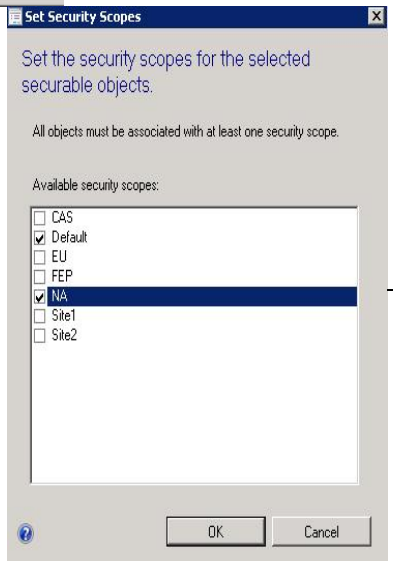
(https://cloudblogs.microsoft.com/enterprisemobility/wp-content/uploads/sites/2/2017/10/2514.RBA2_.jpg)

3. Create Security Scope

Kevin then goes to the Security Scope node of the Configuration Manager console, and adds two new security scopes. He names them as NA and EU. Now he needs to assign related objects to the right security scope based on the objects locations. To make the application deployment scenario work correctly, Kevin not only assigns some applications to the security scopes, but also associates the proper distribution points and distribution point groups into the security scope he created. To do this, Kevin has to go to the Application the Distribution Points node or the Distribution Point Groups node in the Configuration Manager Console, select the objects, and set the security scopes for these objects. There are already two existing collections which include desktops in North American and Europe. Kevin can use them to limit the devices Meg can manage.



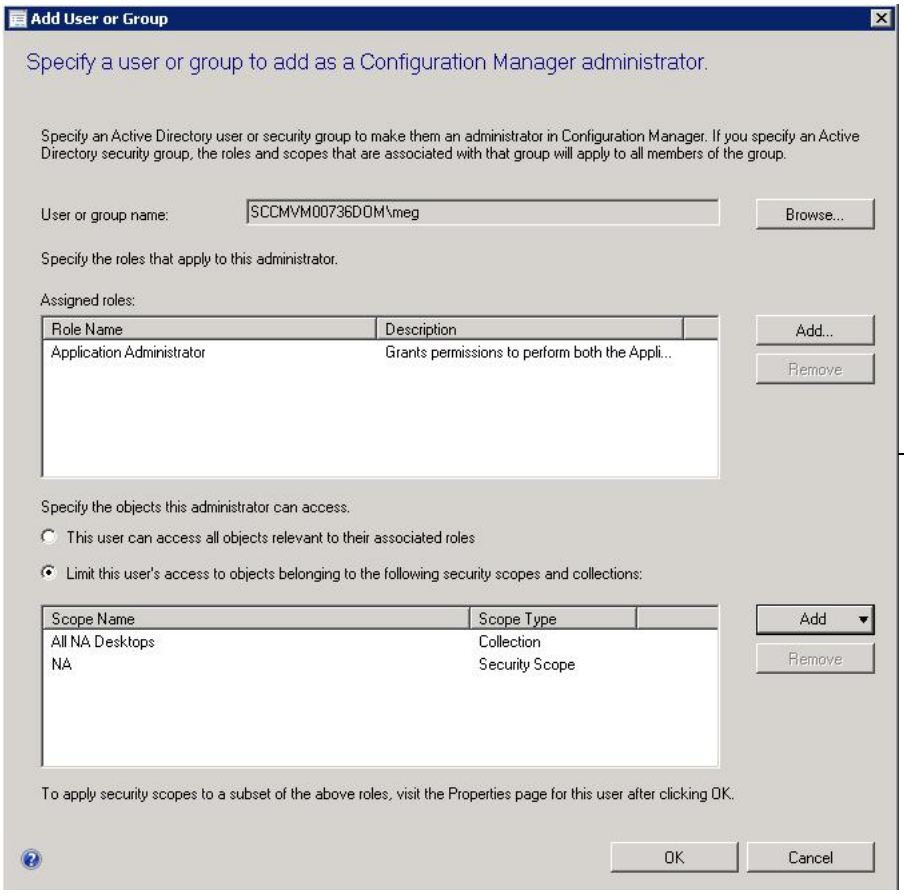

(https://cloudblogs.microsoft.com/enterprisemobility/wp-content/uploads/sites/2/2017/10/8508.RBA3_.jpg)




(https://cloudblogs.microsoft.com/enterprisemobility/wp-content/uploads/sites/2/2017/10/1207.RBA4_.jpg)

4. Create Administrative User

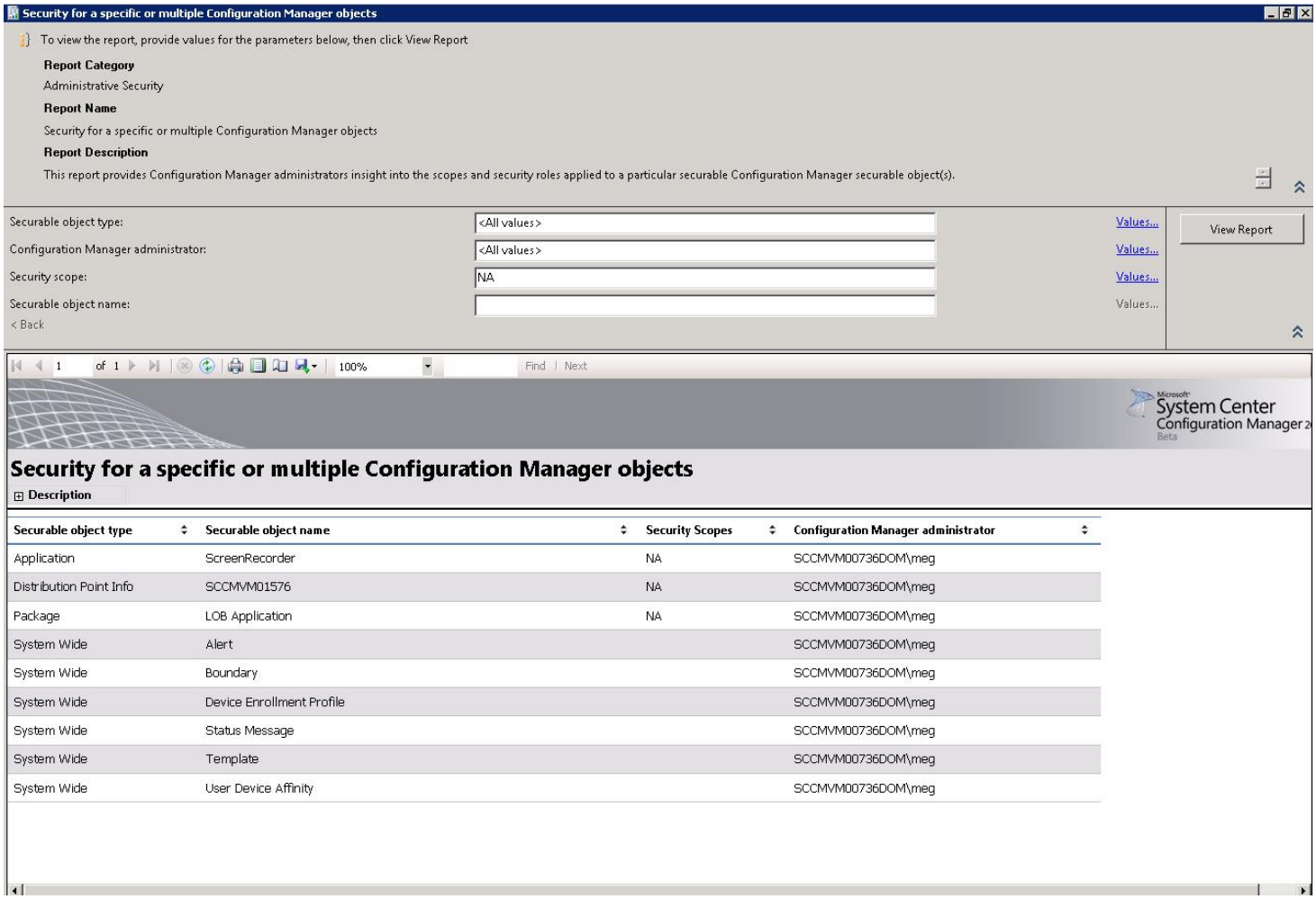
Kevin now goes to Administrative Users node to add Meg's account to the system. He assigns the Application Administrator security role to Meg and limits Meg's access only to objects in the NA security scope. Also he assigns the All NA Desktops collection to Meg, which means Meg can manage only the devices in this collection. Instead of granting Meg another security role, Kevin wants to create an Active Directory security group, Application Auditors, which contains the users he wants to grant the read permission to for all the applications. He follows the same steps as he creates Meg's account to add the security group to the system but with different security role and security scope. He also adds Meg's account to the new Active Directory security group he created that was named Application Auditors.



(https://cloudblogs.microsoft.com/enterprisemobility/wp-content/uploads/sites/2/2017/10/2677.RBA5_.jpg)

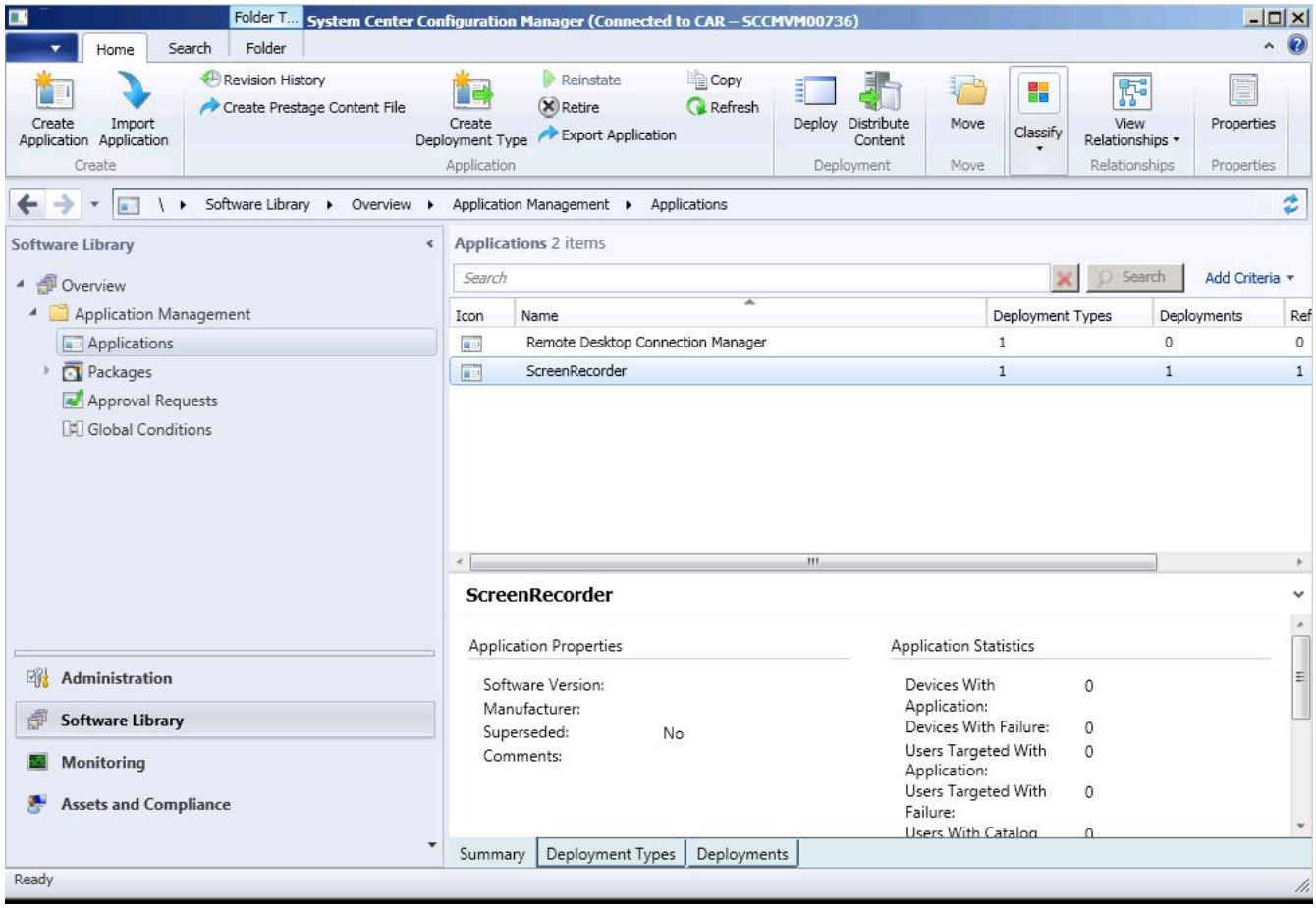
5. Review Security Configuration

Kevin can go to the Reports node to check the security configuration of Configuration Manager. He runs the report “Security for a specific or multiple Configuration Manager objects” to see what objects he has assigned to the NA security scope. Also, he can run the report “Audit log of Role-Based Access Control objects” to check all the security activities that have occured in the site to see whether there are violations configured by other administrators. There are several other reports under Administrative Security which Configuration Manager provides to help the administrator.



(https://cloudblogs.microsoft.com/enterprisemobility/wp-content/uploads/sites/2/2017/10/3124.RBA6_.jpg)

Finally, Kevin notifies Meg that she has access to the Configuration Manager system. Meg installs the Configuration Manager console and now logs in to do her job. Meg opens the Configuration Manager console and finds she has all the permissions to manage applications for NA desktops. She can also see some applications in the EU security scope but cannot modify them.




(https://cloudblogs.microsoft.com/enterprisemobility/wp-content/uploads/sites/2/2017/10/1732.RBA7_.jpg)

# Summary

With RBA feature introduced in Configuration Manager 2012, managing your Configuration Manager administrative permissions becomes more efficient and flexible. Administrators can delegate tasks by assigning the roles, scopes, and collections faster, easier, and with greater confidence.

—Lin Tang (http://blogs.technet.com/b/configmgrteam/archive/2011/09/30/lin-tang-s-bio.aspx)

*This posting is provided "AS IS" with no warranties, and confers no rights.*

‹ Older Post (https://cloudblogs.microsoft.com/enterprisemobility/2011/09/21/remote-desktop-services-coverage-at-build-2011/) Newer Post (ht

**RELATED BLOG POSTS**

Update 1712 for Configuration Manager Technical Preview Branch – Available Now! (https://cloudblogs.microsoft.com/enterprisemobility/2017/12/16/update-1712-for-configuration-manager-technical-preview-branch-available-now/) Hello everyone! We are happy to let you know that update 1712 for the Technical...
Read more (https://cloudblogs.microsoft.com/enterprisemobility/2017/12/16/update-1712-for-configuration-manager-technical-preview-branch-available-now/)

Microsoft Intune and Jamf Pro: Better Together to Manage and Secure Macs (https://cloudblogs.microsoft.com/enterprisemobility/2017/12/14/microsoft-intune-and-jamf-pro-better-together-to-manage-and-secure-macs/) This post is co-authored by Brad Anderson, Corporate Vice President, Microsoft and Dean Hager, CEO,...
Read more (https://cloudblogs.microsoft.com/enterprisemobility/2017/12/14/microsoft-intune-and-jamf-pro-better-together-to-manage-and-secure-macs/)

RDP and PCoIP graphics accelerated virtualization solutions (https://cloudblogs.microsoft.com/enterprisemobility/2017/12/07/rdp-and-pcoip-graphics-accelerated-virtualization-solutions/) This blog post is authored by Ivan Mladenov, Senior Program Manager, RDS/WDG. Once upon a...
Read more (https://cloudblogs.microsoft.com/enterprisemobility/2017/12/07/rdp-and-pcoip-graphics-accelerated-virtualization-solutions/)

## Join the conversation

Add comment

edgard — 2 years ago

is there any updates coming to the current RBA Viewer tool for compatibility with SCCM 2012 R2 SP1?

Anthony — 4 years ago

Good article Lin. Question… So how do you handle making changes to an existing application. Lets say you need to add a deployment type for app-v or add a condition or something similar. Do you move the application back into the packaging container by
changing the security scope? This would also stop the current deployment, right? what if you did not want to take the app out of production availability? Would you create another application and when ready for production just retire the existing production
application? This would be a bit problematic if the application has dependencies or is dependent on other apps right? How did you guys go about dealing with those scenarios??

Kim Oppalfens — 4 years ago

Enforce security allows you to trigger the endpoint protection actions

James — 5 years ago

Yes, there is a table here:

blogs.technet.com/…/role-based-administration-in-system-center-2012-configuration-manager.aspx (http://blogs.technet.com/b/hhoy/archive/2012/03/07/role-based-administration-in-system-center-2012-configuration-manager.aspx)

Chicago — 5 years ago

I agree with Adam a table would help. A book on the subject would also be nice.

Adam — 5 years ago

Is there any documentation describing the different rights and what they allow a user to do? Some of the rights are fairly self-explanatory, like "modify resource," but others aren't ("enforce security?"). A table with a break-down of what they all do would be REALLY helpful.

Anonymous — 2019 years ago

James – that table just lists the object, but not the permission. Still no explanation of what exactly "modify resource" and "Enforce security" do. In practice, none of these items are self explanitory when it comes to exactly what UI controls you'll be able to view or modify.

Comments are closed for this post.

## Recent Posts from EMS Leaders

**BRAD ANDERSON**

Corporate Vice President, Enterprise Mobility + Security

### Microsoft Intune and Jamf Pro: Better Together to Manage and Secure Macs (https://cloudblogs.microsoft.com/enterprisemobility/2017/12/14/microsoft-intune-and-jamf-pro-better-together-to-manage-and-secure-macs/)

This post is co-authored by Brad Anderson, Corporate Vice President, Microsoft and Dean Hager, CEO, Jamf. At the Jamf Nation User Conference (JNUC) in October, we talked about how our partnership would provide an automated compliance-based solution for secure access to corporate data from Mac devices. This solution uses Microsoft Enterprise Mobility + Security… Read more (https://cloudblogs.microsoft.com/enterprisemobility/2017/12/14/microsoft-intune-and-jamf-pro-better-together-to-manage-and-secure-macs/)…

**ALEX SIMONS**

Director of Program Management, Microsoft Identity Division

### Improving the app launcher user experience in Azure AD (https://cloudblogs.microsoft.com/enterprisemobility/2017/12/04/improving-the-app-launcher-user-experience-in-azure-ad/)

Howdy folks, Imagine a user visiting your company's Azure AD app launcher for the first time and finding exactly the apps they need to be productive and effective. No confusion or clutter. A dream scenario, right? You've sent us more and more requests for features that allow you to better manage third-party apps as you're... Read more (https://cloudblogs.microsoft.com/enterprisemobility/2017/12/04/improving-the-app-launcher-user-experience-in-azure-ad/)...

**ANDREW CONWAY**

General Manager, Product Marketing, Enterprise Mobility + Security

### Enterprise Mobility + Security @ Ignite 2017 – Wrap Up (https://cloudblogs.microsoft.com/enterprisemobility/2017/10/03/enterprise-mobility-security-ignite-2017-wrap-up/)

Last week at Microsoft Ignite, more than 25,000 IT professionals converged in Orlando Florida to learn about Microsoft's technology advancements, skill up across new products, and meet with Microsoft experts. For EMS we unveiled a wave of new capabilities, presented more than 45 sessions, and met with thousands of customers. I wanted to take a... Read more (https://cloudblogs.microsoft.com/enterprisemobility/2017/10/03/enterprise-mobility-security-ignite-2017-wrap-up/)...

LOAD MORE

## Related Sites

Enterprise Mobility (https://www.microsoft.com/en-us/server-cloud/enterprise-mobility/overview.aspx)

Cloud Platform (https://www.microsoft.com/en-us/server-cloud/)

Azure (http://azure.microsoft.com)

Brad Anderson's Lunch Break (https://www.youtube.com/watch?v=O_ewV_a5WOQ&list=PL8nfc9haGeb4h0xDswkkS0I0b3KFxWsuO)

Enterprise Mobility overview videos (https://www.youtube.com/watch?v=Y0K8CEfcn7o&list=PL8nfc9haGeb6qSm1kLU8n3Zqg398764h5)

Microsoft Mechanics Enterprise Mobility + Security videos (https://www.youtube.com/watch?v=3FXbSgRBTKg&list=PLXtHYVsvn_b-0X3R9QCJ4T-Y27DK376NR)

Security + Identity documentation (https://docs.microsoft.com/en-us/azure/#pivot=products&panel=security)

Security (https://www.microsoft.com/en-us/security/default.aspx)

SQL Server (https://www.microsoft.com/en-us/sql-server/sql-server-2017)