



RUNAS RADIO



<http://www.runasradio.com>



Richard  
Campbell

RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.



Greg  
Hughes

*Text Transcript of Show #032*  
(Transcription services provided by [PWOP Productions](#))



**Jeremy Moskowitz Sets Our Group Policy!**  
**November 14, 2007**



## Jeremy Moskowitz Sets Our Group Policy!

November 14, 2007

[Music]

**Carl Franklin:** From [runasradio.com](http://runasradio.com), you're listening to RunAs Radio, the weekly Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Carl Franklin, introducing show #32, with guest Jeremy Moskowitz, recorded Thursday, October 18, 2007. RunAs Radio is produced each week by PWOP Productions, offering professional media and podcasting services online at [pwop.com](http://pwop.com).

**Richard Campbell:** Hi. This is Richard Campbell and you're listening to RunAs Radio. With me as always, my co-host, Greg Hughes.

**Greg Hughes:** Hi there, guys.

**Richard Campbell:** Doing more of our amazing radio tricks; now we're in Barcelona.

**Greg Hughes:** Barcelona, Spain. Yes, we are here and we are attending the IT Forum Week of TechEd Europe.

**Richard Campbell:** And if you're listening to this on a Wednesday while in Barcelona, what do you do doing?!? We'll keep! Listen on the airplane. Come and see us in person.

**Greg Hughes:** Yeah, but if you're there, then definitely stop by and say hi.

**Richard Campbell:** I'm sure we're having a good time, but now we're sort of done. When this Barcelona trip is over, we're actually done through the end of the New Year.

**Greg Hughes:** Yeah, then we'll be sort of sitting at home and occasionally doing the weekly show and keeping those going, but it would probably nice to slow down for a little bit, especially for you. I know you've been across the pond as they say several times even just in the last few months.

**Richard Campbell:** Yeah, it's been a very frantic fall and winter for me. So, I'm looking forward to staying home for a little while. I'm betting we are getting a stack of shows while we're in Barcelona, so we'll be free for a bit.

**Greg Hughes:** Well, there's an awful lot of really cool stuff coming up. We have obviously this year's release of Vista. We have the upcoming release of Windows Server 2008, a lot of really cool stuff up and coming and an awful lot to talk about.

**Richard Campbell:** If we're not covering the topics you care about, send us an email,

[info@runasradio.com](mailto:info@runasradio.com). We'd love to hear from you. Tell us what you'd like to see.

**Greg Hughes:** Yes. Your ideas and your suggestions and your thoughts are a big part of what drive the things that we talk about and the people that we ask to come and inform you.

**Richard Campbell:** All right, Greg. Let me introduce to you Jeremy Moskowitz. Jeremy Moskowitz is a Group Policy MVP who runs Moskowitz, Inc., a company specializing in Microsoft consulting and education. Since becoming one of the world's first MCSEs in Windows NT and Windows 2000, Jeremy has performed Active Directory, Group Policy and Windows management planning and implementation for some of the world's largest organizations. He has also been seen at some of the world's largest conferences including Microsoft TechEd, Microsoft MMS, MCP Magazine's TechMentor, and Windows Connections. He is a noted author of multiple books on Windows. His most popular book is Group Policy: Management, Troubleshooting and Security and it is the flagship title in the "Mark Minasi Windows Administration Series." He also has a book about Windows & Linux integration and that's entitled "Windows & Linux Integration: Hands-On Solutions for a Mixed Environment." Jeremy runs GPanswers.com and WinLinAnswers.com, two websites to help people get their tough Group Policy and Windows/Linux questions answered. Welcome Jeremy.

**Jeremy Moskowitz:** Hey. Thanks for having me.

**Richard Campbell:** So, I have not breeched the topic of group policy on RunAs Radio yet. It's a huge topic and I think it's one that's often not well known. So, I want to start at the beginning and I figured you're the guy to get us started on this topic.

**Jeremy Moskowitz:** Well, you know, that's the thing. I get this from a lot of people. They're like, "You know, I think I need to start using group policy." What they may not know is that they're already using group policy. That's right.

**Richard Campbell:** It does permeate everything, right?

**Jeremy Moskowitz:** Well, not only does it permeate everything, but some people think that "I'll hold off using it until later." You're already using it. That's the thing is that every Windows administrator who has an Active Directory is already using it. There are two default group policy objects out there already working for you to best utilize the system you've already invested in. That's what group policy is all about. In fact, sometimes I get the question of "Moskowitz, why do you care so much about group policy? Why is this



your forte?" The answer for me is like, a hundred years ago when people were getting started dealing with Active Directory and they were trying to migrate from NT 4.0 to, say, Windows 2000 at the time, people on the whiteboard drawing circles and arrows and figuring out migration and "How are we gonna get there?" and "What's our path?" and "What's our roadmap?" and I was thinking, "Well, what's our destination?" like what happens after we're here. Group policy is what you do with Active Directory once you have it.

**Greg Hughes:** Once it's already in place.

**Richard Campbell:** So, really, once you've gone through the pain of an Active Directory migration, you're really not getting the reward unless you take advantage of group policy.

**Jeremy Moskowitz:** Well said. That's the thing. Most people have in fact gotten it -- you ask people to raise their hand in an audience of how many people have Active Directory, 99% of the hands go up, one guy still has Novell Netware and one guy actually still has Banyan VINES. We're happy with that guy, but the point of the story is that most people still have Active Directory and maybe some NT 4.0 laying around, that's totally fine and they're at the point now where there's no reason at all not to take advantage of this Active Directory they paid for. They've invested, let's make use of the Ferrari they now have.

**Greg Hughes:** Right. You've set up a Windows domain for logins and stuff. You have an Active Directory and by the virtue of that, you have group policy in place whether you know it or not. So, maybe using group policy really means taking advantage of the tools of group policy and the controls that group policy allows me to exert. So, why should people be leveraging the capabilities of group policy?

**Jeremy Moskowitz:** Well, for me, the reason I love group policy is that it's got so much power and it's in the box and it's free. In other words, you've already paid for it. There are lots of other opportunities for third party tools and add-on tools that have great power too, that's not a debate; but the stuff that group policy gives you in the box for free is a humongous array of control. So, group policy deals with -- there are actually 13 categories of group policy. We're not going to go into all of them. Don't worry. I'm not going to bore anybody to death. The kinds of things that people get really excited about are, you know, I can walk up to 100 people and say, "Did you know that in the box you can use group policy in Active Directory to deploy your application to your target machine?"

**Greg Hughes:** Right.

**Jeremy Moskowitz:** They're like, "Let me get this straight. I have a way to actually push ostensibly application to my users and computers?" Absolutely and it's been in the box since the dawn of time. Now, it's not super crazy easy to use, but did I mention it's free? And because it's in the box, you now have this incredible ability to push applications and dictate the CTRL-ALT-DEL settings and control panel settings and all those touchy-feely settings you like and the real big one, the real reason that I try to get people jazzed up about group policy is here's a truism. If you don't know group policy, you don't know security.

**Greg Hughes:** Absolutely.

**Jeremy Moskowitz:** Let me say that again. If you don't know group policy, you don't know security. Here's why. You may know like every RFC and you may be a super compiler head and you might know bit level stuff, but if you don't know when that thing is supposed to apply, who it applies to, how it's filtered, and how to configure it, and of course you're going to be doing that using group policy because you don't want to run around to every single machine, group policy knowledge is the fundamental gateway toward being a good security administrator.

**Greg Hughes:** I think that's a great point. It's an important point to make is using and leveraging group policy, workable powerful tools in order to put security controls in place is if for no other reason, that is the number one reason to really leverage group policy on a Windows environment.

**Richard Campbell:** All right, Jeremy. What is group policy really? Now that we know it's great, what is it?

**Jeremy Moskowitz:** Well, so I meet a lot of people at parties and I happen to tell them I'm a group policy guy and I have to try to explain it like I ask them, "What do you do?" and they say, "Oh, I'm an accountant." That's easy. You kind of know what an accountant is. When people ask me, "What does a group policy guy do?" It gets a little fuzzier. So, without getting too technical, let's sort of take the un-technical approach first then we'll go technical second. The un-technical approach is that group policy enables you to, get this, make a wish on your servers and your other servers, users, and computers embrace that wish. So, group policy is really two halves. Something you do on your management station, it's something that's stored in Active Directory, and then the client, the target machine, picks up that wish and does the dirty work for you. So, the idea is that let's say you wanted to kill the control panel for all of, say, the sales guys. Well, that's great. You want to run around to every single sales computer and make that change happen? Of course not. That



## Jeremy Moskowitz Sets Our Group Policy!

November 14, 2007

would take you 900 years and there's your whole weekend. What you want to do is create a group policy, get it over to where the sales guys are in Active Directory, the phrase that we use in group policy land is called linking that group policy. As soon as that thing is linked, the next time those users check in, and they do that every so often, they check in to see if there's any new instruction, they will automatically embrace your changes. So, instead of you working for the network, the network is now working for you.

**Richard Campbell:** So, this is not just at login, but periodically even if you are logged in, it will actually go pick those real changes up.

**Jeremy Moskowitz:** That's right. There are some exceptions, but by and large the idea is that every 90 minutes or so, the client says, "Hey, buddy. You got anything new for me?" If the answer is yes, they will automatically download and embrace those changes. That actually brings up an interesting technical point is that group policy is never pushed. Group policy is always pulled from the client, which is actually an interesting technical bit.

**Richard Campbell:** So, even though we're just talking about pushing applications out, it's not really pushed. The machine does ask for it.

**Jeremy Moskowitz:** That's right, the machine does that. In fact, that is one of those exceptions. The machine will only ask for it at either computer startup time or the next time the user logs on depending on how the app is configured.

**Richard Campbell:** Where is group policy?

**Jeremy Moskowitz:** Well, it's interesting. Like I said, group policy is sort of a multi-headed beast. Group policy is in multiple places depending on how you look at it. The answer for that could be it's a moving part inside Active Directory and also a part on every single client that you have out there from Windows 2000 and above. Like I said, group policy is sort of two things. It's storage of your wishes and then the implementation of your wishes.

**Richard Campbell:** Right.

**Jeremy Moskowitz:** So, the storage happens inside Active Directory and the implementation happens on your client machine. Now, the other half of the equation is how do I actually get to the group policy editor stuff, right? That's a longer answer. The medium-sized version is that there's a wonderful free downloadable tool for Microsoft called the GPMC or the Group Policy Management Console. You can get that at [microsoft.com/grouppolicy](http://microsoft.com/grouppolicy), that's all one word, and download the GPMC. Once you have that tool,

you'll be able to create, link and edit group policy objects for certain areas of your Active Directory.

**Richard Campbell:** It's interesting that Microsoft didn't ship this group policy editor with Windows. Why do we have to download it separately? Shouldn't it just be in the box?

**Jeremy Moskowitz:** Well, it's funny you should mention that. It actually has a long and sorted history of which I had a personal role. I was asked by Microsoft if that is something that they should potentially do. There are multiple philosophies on this. Philosophy number one is if it ships in the box and then there's an upgrade that might mean we'd would have to wait for a Service Pack or a whole operating system revision to get that upgrade.

**Richard Campbell:** Right.

**Greg Hughes:** Right.

**Jeremy Moskowitz:** And that might not be that good because the group policy team is a bunch of really smart people and if they come up with something new, should we have to wait for that update? That's problem number one. The other half of the equation is the GPMC feels so much like the operating system that boy how do you feel, like it *SHOULD* be part of the operating system.

**Richard Campbell:** Right.

**Jeremy Moskowitz:** So, it's interesting you should say that, but the longer version of the story is it's not built in to any operating system except for, get this, it is built in to Vista and the new Server 2008 machine, but wait, there's more. Remember that whole idea that what if they come up with an update, how are we going to handle that? This is very interesting. Vista Service Pack 1 will uninstall the built in GPMC that comes in Vista.

**Richard Campbell:** Oh I love that.

**Jeremy Moskowitz:** But think about it. That way, they went back to the original philosophy.

**Richard Campbell:** Right.

**Jeremy Moskowitz:** It was the "we wanted to make sure that anybody could get an update if an update was available" and that's exactly what they're doing.

**Richard Campbell:** But you suddenly realize that Microsoft doesn't agree with itself sometimes. I mean obviously, somebody managed to push to put that into Vista and somebody else has now managed to push to take it back out.



## Jeremy Moskowitz Sets Our Group Policy!

November 14, 2007

**Jeremy Moskowitz:** That's right. So, I have a whole blog entry about this at [gpanswers.com/blog](http://gpanswers.com/blog) for anybody who wants to get more about my philosophy about this.

**Greg Hughes:** For the IT worker, the guys and gals that are running the networks, running the Active Directory domains, what's the term I seem to use repeatedly is low hanging fruit? What are the problems that they can solve by really leveraging group policy? Maybe we can be specific. What's the carrot that we can hang out there for the IT pro that will really tempt them into using group policy?

**Jeremy Moskowitz:** As soon as you said that, like 9 or 10 things came to mind. It's going to be hard for me to sort of put my hat on just one. My humblest suggestion for the people who are just getting started with group policy would be for the love of Pete, don't go bananas. There are 2400 policy settings available to you in Vista. What that means is that you're going to feel like a kid in a candy store when you really get started with this thing. So, don't feel like you should start turning everything on. That's not the right approach. The right approach, what I tell people in my training class is, is look to the wish. Try to figure out precisely what the business case is. For instance, and this is something very generic that we could hang our hats on, like let's say you have different divisions, doctors, nurses, sales, research, whatever and you wanted to get each one of those people their own custom desktop background, so that way whenever they're logged on to any machine, they kind of knew that they were authenticated and that they had the group policy and that they had the background. That's pretty neat. That's like a neat little trick just to say if I'm logged on, then I have my particular desktop background that shows I'm in research or something. Now, that is not particularly hard to do, but it's a really good sort of like flexing their muscles case or group policy. The next thing I might consider that people might want to do is to sort of start locking down some of the user interface attributes some people aren't using. Not everybody is qualified to go into control panels if you know what I mean, so maybe we can lock those things out. Finally, there are also lots of additional ways to configure, for instance, Office. Office is one of those big deals that don't get a lot of airtime in terms of the configuration using group policy. I go over this in the book and in lots of other areas on [gpanswers.com](http://gpanswers.com), but the idea is that you can download and integrate these things called ADM or ADMX files for Office 2000, 2003, and 2007 that says wherever Sally goes, and Sally's a nurse, she'll always get the following configuration for Office 2003. That's incredibly powerful to say wherever a user goes, they're guaranteed specific application settings. That's really, really neat and that's what group policy is all about.

**Greg Hughes:** Yeah. So, if I don't want to be in what they call *reader mode* every time that I open up Microsoft Word, there's a group policy that if I decide to cross our organization that we just don't want that, I can set that policy, for example.

**Jeremy Moskowitz:** Right, or set the spelling color or always force a grammar check or whatever. There's plenty of opportunity to make that application work the way your users need it to work. There are plenty of opportunities to get started. I also love demonstrating that group policy software installation stuff. When I show that off to people, really, their jaws drop open and that's very exciting for me.

**Richard Campbell:** Well, I always think about group policy around Windows Security and Network Security. I don't think about it in terms of its impact on applications.

**Jeremy Moskowitz:** Indeed, yeah, and that's the thing. Just the numbers of categories that group policy can do for controlling the most major application of all, which of course is Explorer. That is an application...

**Richard Campbell:** Right.

**Jeremy Moskowitz:** That's the way to think about it is that group policy out of the box ships with about 1800 settings, most of which affect Explorer. It's the biggest application of them all. It's security based, it's application deployment, it's management of all your Windows facets.

**Greg Hughes:** Yeah, really, just general IT policies and controls around a wide variety of different applications. From a security standpoint, I remember one organization beginning to leverage group policy deeper and deeper and like some of the obvious things are how long do the passwords have to be, how often do they expire, complexity and things like that and user group policy to set those types of things, but we change from the default (don't remember what it was) number of days that group policy specified and changed it to 42 and the reason being that's an even number of weeks, so if I change my password on a Wednesday, then six weeks from now, it's going to be a Wednesday when my password expires, so there's an example of a Helpdesk seeing a benefit not getting after hours and weekend calls because people's passwords are expiring on Sunday afternoon. So, there are a lot of little things and a lot of granular control that can be exercised and there's a lot of value that can be obtained.

**Jeremy Moskowitz:** Yeah. You're hitting right on the head. In all honesty, I think you could probably agree that some of the security ones have their own nuances. In other words, for instance, even things --



there's a security function called Restrictive Groups and Restrictive Groups, its main goal is to say that Fred, Sally and Joan, those people can be a member of, say, the backup operators group or, say, the local administrators group, but anybody who's currently in there is not, is going to be kicked out and replaced. Now, it's a very powerful function, but it doesn't quite work the way some of the other ones do. What I'm driving at is that group policy generally works the way you expect, but sometimes you need a little extra guidance.

**Greg Hughes:** Especially if you have policies that you are setting that may be competing with each other.

**Jeremy Moskowitz:** Yes. In that case, I always say, "Look to the test lab."

**Greg Hughes:** That's right. Yeah, I think there's a lot of value in having -- whether it's on virtual machines, real machines or what have you -- a test environment to really try these things out before you start pushing them out on your live network.

**Richard Campbell:** So, what does a test lab look like? Are we talking about needing to run a domain controller that's isolated from the rest of the network and then some workstations?

**Jeremy Moskowitz:** You bring up another good point! I do have a whole advanced lecture on test lab best practices. I'll jump to the end of the story and say no, it does not need to be a super powerful giant lab. There are in fact advanced techniques to -- get this, this is kind of neat. I teach in the advanced class how to basically do what equates to a WinZip of your Active Directory in production and bring it into your test lab. So, the idea is that once you have a photocopy of your real world test lab, you can then start testing out each of the group policy settings that you want to check out and then once you have a GPO -- again, this will blow your mind -- you don't have to recreate the wheel. You can actually take it on a USB stick or a CD-ROM and then get it back into the real world without actually having to recreate it. So, there are some advanced kind of manipulations to really take incredible use of a test lab to make sure you're not going to shoot yourself in the foot in the real world. You don't want to have a GPO out there that will affect a whole gaggle of users and then just anybody can use it. You want to make sure that it does exactly what you want in the test lab; and then get into the real world when you're ready.

**Greg Hughes:** Now, let's just be really clear. Why don't you go ahead and define GPO since we're getting into acronym world here so that everybody is really clear?

**Jeremy Moskowitz:** Sure. Well, the two phrases that I definitely want to clear up are GPO, which stands for group policy object, and another thing called a policy setting. The idea behind a group policy object is sort of like a new Word document, right? When you click New in Word, you haven't done very much. You just have a new blank page, a whole lot of nothing set, you haven't done anything really. The thing that's actually doing the work for you is the policy setting like kill the control panel, don't show the last logged in user, that sort of stuff. Each one of those line items is called a policy setting. So, a group policy object contains policy settings.

**Greg Hughes:** So, the object is the file that you can export and import and stick on that USB key and take to your lab and the settings are all the values that are contained within the object?

**Jeremy Moskowitz:** More or less, yes.

**Richard Campbell:** So, would you ever have more than one group policy object?

**Jeremy Moskowitz:** Sure. In fact, let's say you had different gaggles of users. You had sales, marketing and research. Well, they're not going to act the same as each other, right? Sales is going to act one way, marketing another way, and research quite another way. So, your goal as an administrator, an Active Directory administrator, is to learn how those guys do their job and then craft your corporate policy into group policy. For instance, your corporate policy says no one in the world can get the control panel except for researchers. Well, great. You can do that using group policy. That's exactly what it's meant for. It's meant to enforce your corporate edicts based on who people are.

**Greg Hughes:** Now, you can apply policies to people or to computers or classifications thereof. Maybe you can describe how that works.

**Jeremy Moskowitz:** Sure. In fact, the big misnomer out there is why the heck is it called group policy at all. Because as you very specifically described, group policy only affects two categories of things in the whole world, users or computers, and those users or computers can only be in one of three locations. That's sites, domains or OUs. Notice how I didn't say the word group there, which gets nice and confusing because our thing here is called group policy.

**Richard Campbell:** Right.

**Greg Hughes:** Right.

**Jeremy Moskowitz:** You don't round up an NT style group or an Active Directory style group of nurses and then somehow force feed them to kill the control



panel. It just doesn't work that way. What you need to do is round up those nurses, put them in an OU, create the GPO, and the phrase that pays is "link them." You link that GPO over to the nurses' OU that contains that user account.

**Greg Hughes:** So, I have an organization unit or an OU with the nurses and now on that OU, think of it as a container that maybe contains different machines and/or people accounts, now I can set group policy at that organization unit or OU level?

**Jeremy Moskowitz:** That's right. The way I like to explain it is that group policy objects, they don't live at the level that they're being used at. Group policy objects live at what I like to call the group policy object swimming pool. The idea is that they're all sitting in the swimming pool waiting to be used. If you want to use it, let's say you had an edict called "kill the control panel," great. Its whole life, it lived in the swimming pool. To utilize it over sales and marketing, you're going to link that GPO from the swimming pool over to both sales and to marketing.

**Richard Campbell:** But when you say sales and marketing, you're not meaning sales and marketing groups, but sales and marketing organizational units.

**Jeremy Moskowitz:** That's right. Organizational units are meant, or an Active Directory administrator, to craft the experience for their users. It's exactly what they're meant for. They're meant to organize their user and computer population.

**Richard Campbell:** Right.

**Greg Hughes:** Now, it sounds like you could really build up an awful lot of policies, OUs, files. We end up with some performance problems eventually if we really go crazy with this stuff. What about that?

**Jeremy Moskowitz:** Well, you know, there's some debate on that. I have done some performance testing of group policy and I can pretty much tell you that under most circumstances, it's really hard to bog down a group policy engine. Without getting too geeky and technical into it, group policy used to get a bad rap. It's sort of like somebody who is bad as a kid and then when they grow up, people sort of still eyeball them wrong. So, during beta of Windows 2000, group policy was kind of to blame for slowdown, but what people weren't realizing was it wasn't group policy that was causing the slowdown, no, no, no, it was the thing that group policy was doing that was causing the slowdown.

**Richard Campbell:** Right, of course.

**Greg Hughes:** Right.

**Jeremy Moskowitz:** So, here's the deal, right? By the way, logon, log off, startup, and shutdown scripts are all available using group policies, one of the 13 categories of group policy. So, let's say you had a logon script that, I don't know, let's go crazy, it REACLS every single file on the hard drive. Clearly, you'd never want to do that with a logon script, but you could also do that by hand. You could have some kind of batch file that would do the same thing. Now, the point of the story is that how long would each one of these things take? Well, they would take exactly the same amount of time, but who gets the bad rap? Well, group policy gets the bad rap because it's executing these 13 things that you are asking it to do. In this particular case I asked you to, don't blame the messenger, blame the message.

**Greg Hughes:** I know the one area that I've heard and I've actually heard Microsoft recommend that you're just careful about how much policy -- it really comes down to replication across the network and how often you're pushing how much data across and how often it needs to be updated on the machines. Maybe that's the one area where performance at the domain level could potentially be impacted, so thinking carefully about that could easily medicate that type of problem as well.

**Jeremy Moskowitz:** Well, you're right. In the largest of environments, there can be a situation. Let's say you are a large airplane manufacturing company that shall remain nameless. Let's say you are that company, okay? You had 80 gazillion GPOs because you're huge and you got 80 million sites. Okay, well, think about that. Every time you create a GPO, it's got to be replicated all over the universe. Well, that can potentially be a problem. It turns out Microsoft knows about this problem and they've mitigated it using the new technology that's built into Vista and Server 2008. The idea is that instead of having big fat GPOs that contain editable content, what they do is they have these thinner, leaner GPOs that have the editable content stored centrally in one place. They've thought that through, so new GPOs if created properly will be thinner and trimmer and won't have to go through -- and even though you have to replicate them everywhere, they're going to be a lot thinner.

**Greg Hughes:** Right. So, you're replicating the delta as opposed to the whole thing over and over again.

**Jeremy Moskowitz:** It's not precisely a delta; it's a matter of that the actual editable contents, which are these files called ADM files...

**Greg Hughes:** Gotcha.



**Jeremy Moskowitz:** That stuff is not stored inside the group policy object anymore inside of Active Directory at the file level. That stuff is only stored if you want to centrally in one place or on the local machine. So, basically, they've taken away it used to be where every single GPO that was created that took 4MB of *goo*, so every time you created your GPO, you basically burned 4MB of *goo* on every domain controller. Let's say you had 100 domain controllers, you just burned 400MB out there. So, the idea is that they've come up with this interesting way called the central store to sort of reduce that overhead of what's actually inside the file-based portion of group policy out object.

**Greg Hughes:** That sounds pretty cool.

**Jeremy Moskowitz:** Yeah.

**Richard Campbell:** So, Microsoft on TechNet has a whole group policy site and they talked about all of these templates. What exactly is in the templates?

**Jeremy Moskowitz:** Right. That's the editable content of what I was describing. So, the idea is that a template, an ADM or an ADMX template is simply a definition of what's possible to manipulate in group policy land. Think about it. Let's take it back to the 50-yard line. So, we have a wish and the wish is to kill the control panel. Well, let's take it back even further. What's the program that needs to embrace that wish? Well, like I said, the biggest program out there is Explorer. That means we need to have a definition for Explorer in how to kill the control panel. So, how do we do that? Well, we got to know what registry punch that is. Okay, great. Now, we know what the registry punch is, we need to then put that registry punch in a file for us to then edit to then say, "Go do it." That is the ADM file. The newer technology is called ADMX, which isn't incredibly "different" in what it's capable of except for the fact that it's XML. That's basically an apples to apples of what it can do.

**Richard Campbell:** Okay. That's why we have ADMXs for Office 2007, for example, besides really just telling you what you can do with Office 2007.

**Jeremy Moskowitz:** That's right. Office 2007 has 8 zillion entries you can possibly manipulate. Somebody really smart in Microsoft said, "Great! How do I make the spelling color orange?" Well, that means that if I change this registry value, I guarantee the spelling color is going to be orange. Fine. So, then they coded that into a definition filed called an ADM or an ADMX file and make it available for you.

**Richard Campbell:** All right. We're coming up on the end of a half-hour here and I think we've sort of gone around in a circle on group policy. What have

we missed? What are the guys starting out with group policy need to know?

**Jeremy Moskowitz:** Well, when most people ask me what kinds of resources are there for my assistance, because it's like learning to ride a motorcycle -- actually, better analogy than that is have you ever walked into a casino and you're seeing everybody having fun at the craps table?

**Richard Campbell:** Right.

**Jeremy Moskowitz:** Right, and you really want to learn craps, but you don't have time to sort of like, you know, you could stand there and watch people play, it's still really hard to pick up the game that way.

**Richard Campbell:** Yes.

**Jeremy Moskowitz:** But then after somebody explains, "Well, these numbers are important because of this. The puck does this thing. The chips are very important because that's how you get paid and this is how you know you'll get paid because the dealer is putting those chips in a very specific way." Once somebody explains to you the ins and outs of how group policy works, you're going to be more confident in wanting to do more group policy in the first place. It's a very self-fulfilling thing. You need to get more confident in group policy to be able to do group policy because, again, if we think about it, the group policy editor in and of itself is like the biggest registry editor on the planet.

**Richard Campbell:** Right.

**Jeremy Moskowitz:** You make one false step, bam! Everybody in the entire domain is now affected by that. That, my friend, would be a CLM or career-limiting move. So, you have to be particularly careful with this. It's not to say that you shouldn't use it. Obviously, I encourage everybody to experiment and learn and grow with it. On the other hand though, you really need a friend and that's where my site GPanswers is all about. We have newsletters, community forums. I do intensive group policy training or workshop classes and we do advanced classes and we do XP to Vista catch up classes. Basically, when you're ready for group policy, I'm ready for you.

**Richard Campbell:** Cool. All right; one last question and then we'll wrap it up. At the beginning of the show, you said, "Everybody's using two policies whether they know it or not." What are those two policies?

**Jeremy Moskowitz:** Sure. One policy is called the default domain policy. In Windows 2003, this is a truism, in Windows 2003, if you want five-character



## Jeremy Moskowitz Sets Our Group Policy!

November 14, 2007

passwords for your domain and I want seven-character passwords for my domain, we have a problem because in that particular case for Windows 2003 domains, you can only have what's called one-password policy per domain. With that in mind, if you can only have one-password policy per domain and that, my friend, is stored in one of those defaults, if that's the case, well, we're going to have to have two domains in order to make our business case happen. Now, good news, let's jump to the end of the story, that is no longer a requirement in Server 2008, but that's another topic for another day. The other one is the default domain controller's policy. Let's think about this for a second. You want to make sure that whenever Sally authenticates to your domain, she gets an event log logged on every domain controller. Okay, that's cool. That makes sense. You don't want her to authenticate to domain controller 3 and get an event log, but she doesn't get an entry when she logs on to domain controller 4. Oh, that makes sense. So, the default domain controller's policy is all about making sure all the domain controllers act the same way and it works for you too, the administrator. You don't want to be able to walk up to the console on 3 and be able to log on but not be able to log on to the console on 4.

**Greg Hughes:** Right.

**Jeremy Moskowitz:** So, it works for you in that capacity as well. So, those are the two defaults. You're already using them. If you've ever set domain-based password policies, you, my friend, are a group policy administrator.

**Richard Campbell:** Whether you knew it or not.

**Jeremy Moskowitz:** Yeah, whether you knew it or not.

**Richard Campbell:** All right, Jeremy. That was a lot of fun. I didn't think group policy was that interesting.

**Jeremy Moskowitz:** Well, people ask me this all the time, "Why did you get into it?" because it's a rich technology and it's only getting richer. Really, we're going to need another session to go over all the new stuff that's coming out.

**Greg Hughes:** In 2008.

**Jeremy Moskowitz:** I know we just sort of touched the introduction. There's so much great new stuff around the bend including new stuff that's already out with Vista, new stuff that's going to be out by the time Windows Server 2008 ships and I will have even more stuff to talk about right around the bend. So, I definitely hope we can set up another session as well.

**Richard Campbell:** You bet. We'll revisit this topic some time soon. There are lots more to talk about.

**Jeremy Moskowitz:** Great.

**Greg Hughes:** We'll look forward to doing that. It's probably one of the most underutilized and important capabilities in Windows. I'd definitely be interested to find out what 2008 has to offer.

**Jeremy Moskowitz:** I'm here for you guys.

**Richard Campbell:** All right. Thanks Jeremy. And we'll talk to you next week on RunAs Radio.