Net Admin Weekly
56,000 Subscribers Worldwide
September 25, 2002
Issue #10

Feature

Q & A

Security Advisories

News Headlines & Resources

Download of the Week

Feature

A Second Look at EFS

to top

You're probably already familiar with EFS – Microsoft's Encrypting File System – if you've been using Windows 2000. The introduction of built-in file encryption that could be easily implemented by users (by simply setting the attribute in a file's or folder's Properties sheet) was one of the many welcome new features when Win2K was released. But that was more than two years ago, and EFS is old news. Or is it? In this week's feature article, we'll take a second look at EFS, including the enhancements that have been added in Windows XP/.NET, and some troubleshooting tips for when EFS doesn't seem to be working.

On the surface, EFS seems simple. To encrypt your data so that unauthorized persons won't be able to read it if they manage to get past Windows' access permissions, all you have to do is navigate to the file or folder in Explorer, right click, select Properties, click the Advanced button, and check the box labeled "Encrypt contents to secure data". (Microsoft recommends that you encrypt folders instead of individual files – then all you have to do is place a file into the encrypted folder to encrypt it).

If you're slightly more of a geek and prefer the command line interface, you can accomplish the same thing using the cipher command with the /e switch and folder name to encrypt the folder.

This hasn't changed in Windows XP/.NET; encryption still works the same way – but there's a new twist. One of the slightly annoying things about Win2K's EFS is the fact that only the user who encrypts the file/folder can decrypt it. This means that you can't share encrypted files with someone you want to authorize to access them, at least not without first decrypting them.

Windows XP, however, supports multiple users for encrypted files (as will Windows .NET, 2003, or whatever Microsoft is calling its next generation server product this week). After you've encrypted the file, in the same Advanced Properties dialog box where you checked the encryption attribute, click the Details button, then the Add button. You can select one or more users with whom you want to share access to the encrypted file. When you're finished adding users, click OK to exit out of each of the dialog boxes.

The ability to share encrypted files adds a lot of functionality to EFS. However, there are a few caveats to be aware of. A user who's been granted access to an encrypted file won't be able to edit it unless he/she also has the Write or (for Word documents) Modify permission assigned (NTFS permissions, set on the Security tab of the file's Properties sheet). Even if the user has been added for EFS access and does have the proper permissions, he/she won't be able to access any encrypted files from a Macintosh client computer.

What else can go wrong with EFS? There are several instances where encryption just doesn't seem to work. If you right click a file or folder and discover that it doesn't have an Advanced button on the General tab of its Properties sheet, you'll probably find that the partition on which it's located is formatted in FAT16 or FAT32. EFS encryption is an NTFS

attribute, so only files and folders stored on NTFS-formatted partitions can be encrypted. The solution is simple enough: move the file/folder to an NTFS partition.

Some problems aren't quite so easily solved. If you're unable to encrypt files or folders even though they're on NTFS partitions, one thing to check is the applicable group policy. If your computer is part of a domain, you'll need to check the domain's group policies (through the Active Directory Users and Computers admin tool). If not, check the Local Security Policy (on XP Pro, via Control Panel | Administrative Tools | Local Security Policy). Either way, in the Security Settings node of the MMC, expand Public Key Policies and right click the folder labeled Encrypting File System. Select Properties and ensure that on the General tab, the box that says Allow users to encrypt files using Encrypting File System (EFS) is checked. If you change this setting, you may need to wait until group policy has been refreshed before it takes effect (or refresh it yourself using the gpupdate command line utility that replaced the secedit command that was used to refresh group policies in Win2K).

Other problems you may run into are related to the underlying technology that EFS uses to identify users who encrypt or decrypt files: certificate services. A user needs a valid EFS certificate to encrypt or decrypt files. To view your certificates, create a custom MMC by typing mmc in the Run box. In the new, empty MMC, click File | Add/Remove snap-in. Click Add on the Standalone tab and select Certificates from the list. Choose to manage certificates for your user account. Expand the Certificates node in the left pane of the MMC and you can view certificates that have been installed for your user account. You can request a certificate if there is a certification authority (a Windows 2000 or .NET server running certificate services) on the network, using the certificate services web page (in the browser, type \\<servername>>\certsrv).

In some cases, EFS may not work because there is no recovery agent specified in the the EFS policy. A recovery agent is a user who has a special recovery agent certificate allowing him/her to decrypt files/folders that were encrypted by someone else (without being added to the file's properties by that user). The purpose of this is to have a way to recover encrypted files if the original user leaves the company or is otherwise unavailable. To add a recovery agent, we go back to the Public Key Policies node of Security Settings as discussed earlier. Right click the folder labeled Encrypting File System, and this time select Add Data Recovery Agent. This will start a wizard that walks you through the process. Another option is to select, in the context menu, All Tasks and then Do Not Require Data Recovery Agents.

Certificate services is a complex topic, especially in an Active Directory domain. We've noticed problems with EFS on Windows XP computers when the domain controllers/certificate servers are running Windows 2000. The above are only a few tips for troubleshooting certificate-related problems with EFS. Luckily, most of the time, EFS just works transparently, giving you another good tool for protecting your data in a multi-layered security plan.

This week's feature article by
Deb Shinder
Net Admin Weekly Author

Q & A

Why Assign a VPN Gateway a Virtual IP Address?

to top

Question:

Hey Dr. Tom,
I set up two Windows 2000 servers to test a router-to-router VPN connection. I found when one router called the other router, both will assign an IP address to the counterpart, but I think that this is unnecessary. Why did Microsoft design it this way? –Brave Heart

Answer:

Hey Brave Heart, you ask a good question. What you're wondering is why the gateways need to assign an IP address to themselves that represent endpoints of the VPN tunnel. The reason for this is that you're creating a "virtual network" that runs on top of the actual network connection that connects the two VPN gateways to one another over the Internet. If you were to use the actual IP addresses on the gateways, you wouldn't be able to create the virtual network's point-to-point link. You need to assign IP addresses that are valid on the virtual point-to-point link in order to create the virtual network connection between the gateways.

The data moving through the tunnel moves through the virtual network connection. The virtual network connection is made private via the encryption protocol you're using. If you have a PPTP virtual network, you're using PPTP (Point to Point Tunneling Protocol) as the virtual networking protocol and MPPE (Microsoft Point to Point Encryption) as the encryption protocol. If you're using L2TP/IPSec, you're using Layer 2 Tunneling Protocol as the virtual networking protocol and IPSec as the encryption protocol. All VPN gateways need to assign themselves a virtual network address in order to create the link, so it's not a Microsoft specific implementation.

Configuring an ISA Server Test Lab for Exam 70-227

to top

Question:

Hey Dr. Tom,
I have decided to take the ISA Server exam (70-227) for my MCSA and towards the MCSE. I have a 640K up and download DSL with an 8 IP address stack, two P3 systems (one dual 550 MHz and one 1.3 GHz) and two older systems. I am going to put together a low-end system from some parts I have. I want to reinstall everything from scratch. I was thinking of installing the 2000 server then IIS and then ISA. What steps should I take and where can I find reading material to help with my designing plans? When I set up my labs for the other exams I just set them up as the books outlined to do so. This time I want to do it as if I were setting up a small network for a client if that makes any sense. --

HHarvey

Answer:

Dear labattsblue,
Yo H! Sounds like you have enough computers to put together a fine lab network. When setting up your ISA Server, you should use the DSL modem as your external interface. You might run into some problems if you use PPPoE, so make sure to check out Microsoft KB article Q259783. The ISA Server also needs an internal interface which connects the server to the LAN. To optimize your testing, you should make one client on the internal network a SecureNAT client, one a Web Proxy client, one a Firewall client, and one that's all three ISA Server client types. This will allow you to investigate the different features and capabilities of each ISA Server client type, and see how the client types interact with one another. Regarding your interface configuration, keep in mind that your DSL connection is most likely going to be considered a dial-up link, so you'll have to configure the Dial-up Entry in the ISA Management console. For more info on ISA Server configuration and more advanced firewall scenarios, check out **Configuring ISA Server 2000** and **ISA Server and Beyond**.

Security Advisories

Cryptographic Flaw in RDP Protocol can Lead to Information Disclosure

to top

There are two security vulnerabilities associated with the RDP protocol. The first involves how session encryption is implemented, and the second involves how RDP in Windows XP handles RDP packets that have been corrupted by an intruder. Check out the site for details and a fix.

Read more...

Flaws Found Within the Dynamic Host Configuration Protocol

to top

Here's a nice change of pace: a security alert focused on a protocol, rather than a vendor's implementation of a protocol. This article reviews the DHCP protocol and describes a way to steal a DHCP client machine's identity. The man-in-the-middle attack can be accomplished against a DHCP client.

Read more...

Directory Traversal Exploit in Dino's Web Server

to top

There is a directory traversal exploit in Dino's Web Server that allows the intruder to access any folder on the same drive as the web application. Dino took his own site down, but you can still get the server from other download sites. He doesn't have time to fix it, so if you're using it, time to switch to another tiny Web server.

Read more...

News Headlines and Resources

A Week of Knowledge: Inside the Certified Wireless Security Professional class

to top

Ever hear of the Certified Wireless Network Administrator certification? Me neither. But it might be time to learn something about it. Wireless networking is the wave of the present and future, so the more you know about it, the better. Will Schmied shares his experiences with a class aimed at this exam in this article.

Read more...

Microsoft Outsources Development of MCP Exam

to top

This is an interesting piece of news. Why would Microsoft outsource development of the MCP exams? Is Microsoft trying to offload liability issues? It's possible, but I think they need some help with the design exams. The Windows 2000 Design Exams were indicative of nothing other than reading skills. Maybe ACT will help Microsoft build some valid design exams for Windows 2003?

Read more...

Lindows Version 2.0 Now Available

to top

If you or your company are trying to get out of the nightmare of paying zillions of dollars for software, you might want to check out the latest version of Lindows. The GUI is slicker than ever, has improved printer driver support, better laptop support, improved networking control interface, and a lot more!

Read more...

IPv6: Seven Killer Capabilities

to top

Is IPv6 right around the corner? Maybe, but only if there's a compelling reason to roll it out. Our industry learned that implementing costly and labor intensive stuff is not the smart way to go. Implementing IPv6 "just for fun" probably won't fly. Check out this article on seven killer capabilities of IPv6 to see if it's worth the effort.

Read more...

Secure Your Servers Using Security Templates

to top

Windows 2000 Security Templates make applying security configuration changes to a server quick and easy. They're also the hands-down most effective way to render useless many common and important networking, server, and 3rd-party services. Check out this article by Roberta Bragg, and get up to speed on how to use security templates to save time and money.

Read more...

You Need to Create a Split DNS!

to top

Do you host your Web and Mail servers? Do you use the same domain

name for internally and externally accessible resources? If so, you need to create a split DNS! The split DNS infrastructure will save you a lot of time and prevent many hours of lost troubleshooting time.

Read more...

Support Webcast: Windows 2003 -- Upgrading, Migrating, and Restructuring Windows Domains

to top

This WebCast covers strategies you can use to upgrade Microsoft Windows NT 4.0–based and Windows 2000–based domains to Windows 2003 Active Directory. This WebCast presents migration and restructuring options that will help simplify domain structure and management when/if you upgrade to Windows 2003.

Read more...

Download of the Week

Net2phone Call Center

to top

First of all, I don't own any stock in Net2phone so it doesn't matter to me if you like it or not. If you have just a dial-up connection, you can pass on it too. But if you have an ISDN or better connection, then you should check out Net2phone. I used it from behind ISA Server 2000 and it works a treat. What's even better is that I never pay more than two cents a minute for a phone call within the continental USA. That price beats the heck out of a POTS-to-POTS connection. The call quality is crystal clear and the call center software has built-in echo cancellation, just like the Windows XP Messenger's call IP to POTS calling feature (when it works, which isn't often).

Read more...

Free Cramsession IT Newsletters - Choose Your Topics!

H = HTML Format **T** = Text Format

H	T		H	T		H	T	
☐	☐	A+ Weekly	•	☐	Exam Tips 'N Tricks	☐	•	.NET Insider
☐	•	ByteBack!	☐	•	IT Career Tips	•	☐	Script Shots
☐	☐	Cisco Insider	•	☐	Linux News	☐	☐	Security Insider
☐	☐	Developers Digest	☐	•	Must Know News	•	☐	Trainers News

Enter your Email

Subscribe Now!

CramSession
Prepare for Success!