

Re: Configuring RSA Securid on ISA 2004 server

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa.configuration/2004-10/0010.html>

From: Vin McLellan (vin_at_theworld.com)

Date: 10/02/04

Date: 1 Oct 2004 17:27:10 -0700

Michael Green <michael.green@twcable.com> queried the newsgroup:

- > *What is the best way to configure RSA secureId on a*
- > *Microsoft ISA 2004 & Windows 2003? I need to make users*
- > *authenticate to website using the RSA Securid.*

Hi Michael,

No problem. Microsoft's ISA Server 2004 supports the native SecurID APIs for strong authentication to hosted web content, one notable benefit from the increasingly close collaboration between RSA and Microsoft.

Your query is timely. Just a few days ago, RSA published its "SecurID-Ready" Implementation Guide for ISA 2004. See RSA's PDF file at: <<http://tinyurl.com/59hq3>>.

The setup seems relatively straightforward for what you want. If you choose to add SecurID support for the ISA VPN (which now offers stateful inspection and filtering of all VPN traffic), you'll need to also install RSA's ACE/Agent for Windows.

While you could doubtless set this up with no assistance, you might consider giving your RSA Sales Support Engineer a call. This is a particularly good time to get reacquainted with in your RSA SSE. I do consulting for RSA, and there is a palpable air of expectation among many RSA customers about the imminent release of RSA's new "SecurID for Microsoft Windows" (SID4Win) infrastructure, which will be made available at no extra charge to RSA customers with the latest ACE/Server.

This is a major advance in the integration of RSA's authentication technology and Microsoft Windows. SID4Win — to use the RSA engineers' unofficial acronym — not only simplifies the user experience by replacing the traditional Window's logon password with a SecurID, it also finally brings RSA's AAA controls to critical resources *inside* the corporate perimeter. (See RSA's data sheet, white paper, and webcast on SID4Win at: <<http://www.rsasecurity.com/node.asp?id=1173>>.)

This is a big deal. With a batch of new Authentication Agents that RSA is about to release, SID4Win will allow you to install discrete auditable SecurID access controls on not only your ISA firewall, webserver, and VPN — but also on your Microsoft network domains, *and* your individual XP desktops and laptops, even when they are temporarily off-line.

A neat trick, particularly since all this leaves the Windows security model intact and unchanged. (SID4Win also doesn't require any changes in current corporate security policies that enforce regular changes in a user's Windows password.)

As you know, in the installation you have planned — or in any installation which grafts two-factor strong authentication on top of Windows — the RSA Authentication Agent sets up a second line of defense, an additional layer of user authentication. The user *first* fills in his regular Windows username and password. Only after those credentials has been validated by the OS does the RSA Authentication Agent challenge the user for his SecurID "passcode": a memorized PIN and his SecurID's 60-second token-code.

This scheme offers real security, but at the price of some <sigh> inconvenience for the user.

By contrast, with RSA's new SID4Win infrastructure in place, the traditional Windows login screen gets replaced with a SecurID login screen. The user, bless his heart, gets challenged only once: for his username, memorized PIN, and SecurID token-code.

A little magic happens in the background. The user's traditional Windows password is still used; only now it will be remembered and managed by the RSA Authentication Manager. This means the password can be long and complex, and subject to draconian rules. The user will even be prompted to change it, as necessary, to conform to the requirements of a company's password security policy.

After the RSA Authentication Manager — what RSA has traditionally called the ACE/Server — validates the SecurID logon, the RAM will automatically forward the user's Windows username and Windows password to the OS. The Windows security model doesn't change; the corporate security policy doesn't change. Windows still uses its own password system to validate user access to system or network resources. The task of managing the complexity has just been shifted from the user to the computers, where it belongs.

>From a network administrator's point of view, the big changes are elsewhere. With SID4Win, RSA and Microsoft have extended the SecurID strong authentication mechanism — buttressed by the RSA Authentication Manager's centralized audit logs — from the perimeter (LAN, Internet, dialup or wireless) to the network domains, and even down to the desktop PCs and mobile laptops.

Although there has been a growing pressure from corporate security officers and auditors, both internal and external, to better control and log access to all repositories of corporate data, it was probably the new IT security requirements associated with various external regulatory regimes (Basel II, Sarbanes–Oxley, HIPAA, GLBA, etc.) that finally made these internal controls inevitable.

With the increasingly robust Windows security model, Microsoft apparently decided that this burgeoning demand, RSA's dominance in strong authentication, and RSA's notable expertise in crypto, all combined to make SecurID access controls on both network domains and networked PCs an attractive enhancement for the enterprise Windows market.

With RSA's SDI4Win infrastructure, PC users temporarily disconnected from the network can still use their SecurIDs for local access, and laptop users remain free to roam. An RSA Authentication Agent securely stores the user's Windows password locally on the user's PC, although it is locked down and centrally managed over the network by the RSA Authentication Manager.

A corporate laptop user can use his SecurID (and memorized PIN) to access his mobile machine in a plane at 35,000 feet, even without a network connection, because the RSA Authentication Manager also stores a secure cache of future SecurID token–codes — for a variable number of days (pre–set, per user or group, by the network admin) — on the laptop.

When the PC or laptop again connects with the enterprise network and the RSA Authentication Manager, the laptop's Authentication Agent forwards an audit log to the Authentication Manager about what has happened in the interim... and replenishes its stored cache of SecurID token–codes for future off–line access.

(Whew, I think I got that all right;–)

For all the smoke and mirrors, of course, SID4Win is still only an AAA infrastructure. Authentication, authorization, and audit are necessary, but not necessarily sufficient for security in the face of an evolving threat model. Corporate data on a PC's disk drive, just like data traffic on the network, still requires encryption to provide full security in the face of direct attack — and that is something that not even this enhanced SecurID infrastructure provides.

In your case, Michael, the SSL/TLS channel for your ISA webserver handles the communications security issues quite well, of course. I hope you find this digression helpful (or at least entertaining;–) It took a little longer than I expected to unwrap SID4Win, and I beg the indulgence of the the newsgroup for my burden on the bandwidth.

microsoft.public.isa.configuration: Re: Configuring RSA Securid on ISA 2004 server

As I said at the top, there **is** a simple answer to your question. If, however, you are planning an extension to an existing RSA SecurID installation, this seems like a particularly good time to check in with your RSA SSE to see what additional strong authentication options might be available to you, perhaps at no extra cost, in the immediate future.

It never hurts to be a little ahead of the curve.

Suerte,

_Vin