Notes.net

Iris Today

by Jane Marcus
and Cara Haagenson

Level: Beginner
Works with: Notes 6
Updated: 09/04/2001

Please note: This article discusses features that are still being planned and developed in the Notes 6 beta program. The final feature set and UI may differ from what you see in this article.

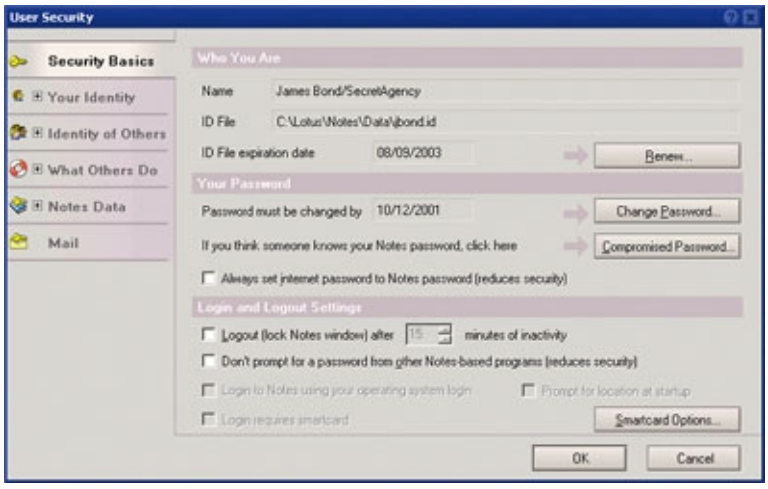
In a classic James Bond film, we find Agent 007 and Agent Saunders providing security for a defecting KGB general.

Bond: "What's your escape route?"
Saunders: "Sorry, old man. Section 26, paragraph 5—that information is on a need-to-know basis only. I'm sure you understand."

Have you ever had trouble figuring out your Notes security configuration, as if it was a top-secret plan that nobody was willing to share with you? Have you ever wanted to accomplish a security task, such as securing an outgoing e-mail message, but have not been able to figure out how all of the pieces work together?

It's a fact that Notes security components could sometimes be hard to find. Information was scattered throughout the product in places such as User Preferences, User ID, Location documents, Domino Directory documents, and so on, and may have only been discovered by the most security-conscious users.

We realized that we could do a better job of offering our "secret services." For this reason, Notes 6 includes the new User Security dialog box. It is an easy-to-use interface that brings together the most important aspects of security. In addition, User Security comes equipped with the latest security gadgets, such as smartcard login. You can find the User Security dialog box on the new Security submenu by choosing File - Security - User Security.



How did the User Security dialog box come to be?

Security is a very powerful component of Notes. Because of this, we created the User Security dialog box in hopes that it would give you a clearer picture of the many cool protections and options Notes security provides, allowing you to use this power to your advantage.

The User Security dialog box was developed with the following goals in mind:

- To reduce the complexity of security, making it easier to understand and use.
- To organize the user interface and consolidate security information so that important security functions can be easily found. This not only helps you perform everyday tasks, but it also helps you troubleshoot security related problems when they arise.
- To educate you about the many security options available in Notes that you may not know about.
- To group related security features in one area, so you can understand how the features work together in Notes.

New features for Notes 6 found in User Security

Along with supporting the existing security features, the new User Security dialog box includes the following new features:

- Configure Notes to automatically encrypt every new local database replica.
- Log in to Notes using a smartcard.
- Synchronize your Notes and Internet password, if allowed by your administrator.
- Change your password with greater convenience. The acceptance of your new password may be judged on its length or its quality, and you may be able to reuse old passwords sooner, if allowed by your administrator.
- Recover from identity theft when someone steals your user ID and guesses your password.
- Find out why you can send encrypted mail to some people but not to others, and use the tools to take corrective action.
- Request new Internet certificates with greater convenience.
- View expired or deleted keys that may still be useful in decrypting old mail messages.
- View advanced details of your certificates.

The User Security dialog box has six sections with each section dealing with a particular area of security. To get a better understanding of how the User Security dialog box works, let's take a look at each section..

Security Basics

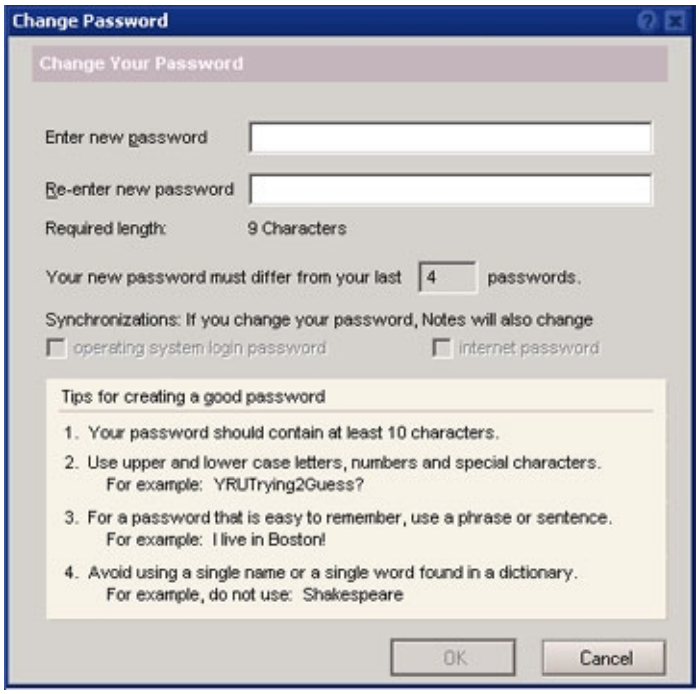
Security Basics is the section you see each time you open the User Security dialog box. It includes all of the security features that you need to access most frequently, and gives you the ability to complete those tasks quickly. This section caters to the end user who doesn't want to be bothered with anything more than basic security functions.

From this section you can:

- Renew your user ID when you are prompted to do so.
- Change your password.
- Recover if someone has stolen your user ID and guessed your password.
- Synchronize your Internet and Notes passwords (if allowed by your administrator).
- Set a timer for automatic Notes logout.
- Set your Notes password to be enabled for other Notes-based programs.
- Enable smartcard login.

Let's take a closer look at the new features you can expect to find in Security Basics.

Changing your password
When you click the Change Password button, you will find a number of additions and changes in the Change Password dialog box.



The appearance of the Change Password dialog box may vary slightly, depending on what administrator policies are in place. In the screen above, the administrator has adopted a policy of password length 9. This means that when you create a new password, the Change Password operation checks that the new password is at least 9 characters long. A password length-checking policy may be implemented by administrators for the convenience of their users who have difficulty understanding the more complex and rigorous password quality checking rules. Unfortunately, password length policies may permit users to supply fairly bad (that is, easy to guess) passwords. If the administrator does not put a specific length policy in place, the Change Password dialog box shows the required password quality, rather than the required length. To encourage use of password quality rather than password length, we have added tips on the Change Password dialog box to help you create a high quality password. For example, James Bond's password meets the standards for either password length of 9 or password quality level of 9. His password is "Tomorrow never dies."

Another convenience feature that administrators can implement for their users is to set a password re-use policy. In the example pictured above, James Bond could re-use his "Tomorrow never dies" password after he changes his password four times.

The Change Password dialog box pulls together some critical pieces of information that you need to create an acceptable password. For instance, the dialog box tells you if you are a Windows Single Login user, in which case Notes attempts to change your operating system login password to match your new Notes password. When creating a new password, a Single Login user must be mindful of any rules put in place both by the Notes

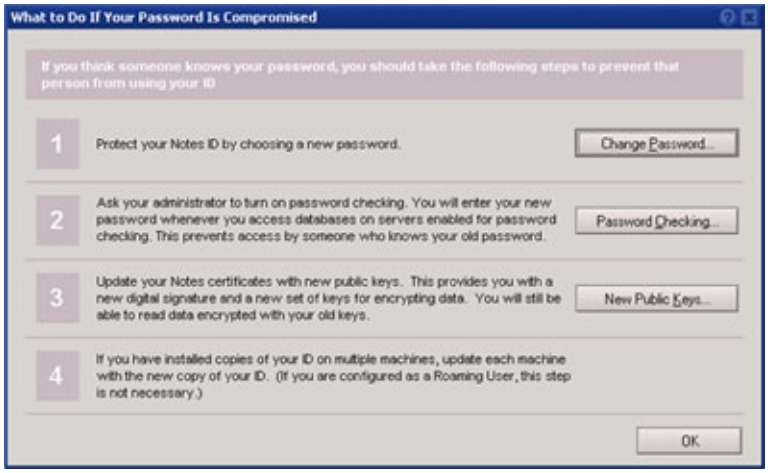
administrator and by the operating system for acceptable passwords. The dialog box also informs you of any synchronization that will be done of your Internet password for use with Domino Web access.

Some thoughts on synchronizing your passwords

Users often complain that they can't remember more than one password and might feel forced to write multiple passwords down on an insecure yellow sticky note. For such users, we have introduced the ability to automatically set your Internet password (for use with Domino Web access) to be the same as your Notes password. This option is only available if your administrator has specifically allowed such synchronization. If you are tempted to adopt this feature, we offer one bit of advice—*don't do it!* This feature scares the living daylights out of us security geeks! When you synchronize your Notes and Internet passwords, you are vulnerable to a number of security attacks. We hope you have more willpower to resist temptation than Agent 007 does, and that you'll steer clear of this convenience item.

Recovering from a compromised password

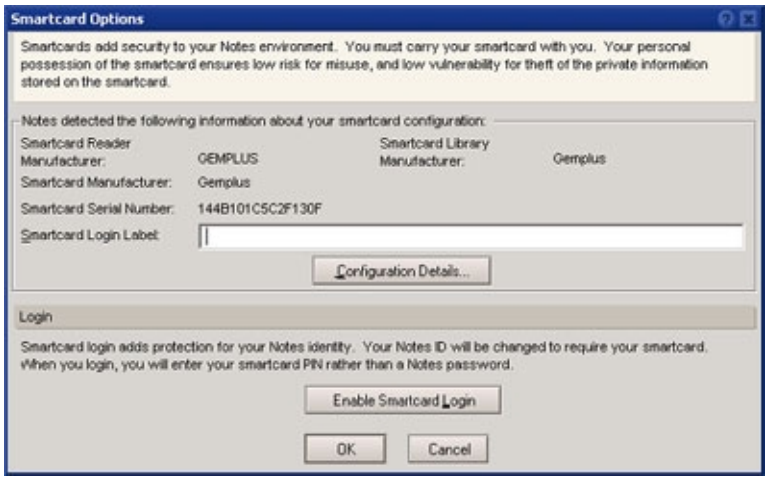
What can happen if someone steals your user ID and guesses your password? To put it mildly, this is a disaster! Not only would the thief be able to impersonate and misrepresent you, but the thief may also access your encrypted secrets. If this happens, you should do what we would do—panic! Then, when you've finished panicking, you should click the Compromised Password button in the Security Basics section. Luckily, identity theft happens infrequently, so it's unlikely you'll ever need to use this button. But, in the security business, we must be prepared for the unexpected. Even James Bond sometimes finds himself in a compromising situation. The What to Do If Your Password Is Compromised dialog box, shown below, provides the steps you need to follow if you have to recover from disaster.



Smartcard options

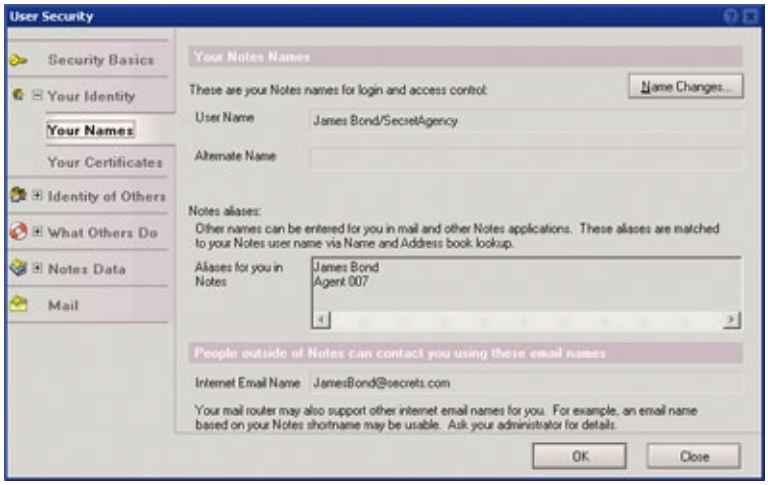
It's clear that there are some vulnerabilities when using passwords, especially if you adopt a weak password that is easy to guess. For the security-minded user, Notes 6 supports the use of smartcards with your Notes user ID. If you're not familiar with smartcards, you can imagine a credit card or ATM card with a small computer chip on it. Similar to an ATM card, you protect your smartcard and user ID by carrying the smartcard with you, making it very difficult for someone to steal. Of course, if you are James Bond, you'd better be careful with your smartcard when you jump out of a hot air balloon.

The Smartcard Options dialog box, shown below, allows you to start using your smartcard with Notes.



Your Identity

Your Identity is the second section of the User Security dialog box, and it has two subsections: Your Names and Your Certificates.



Your Names

Who are you? If you don't know, this subsection will tell you. Your Names displays your Notes user name and alternate name. Your alternate name is another name that you are known by, and is most often your name in a language other than English (usually using some alternate character set). Since James Bond is known world wide as "Bond. James Bond," he does not have an alternate name. Your user name and your alternate name are a critical part of your Notes identity. These names uniquely identify you in the Notes world, and may appear in security contexts such as Access Control Lists and Execution Control Lists.

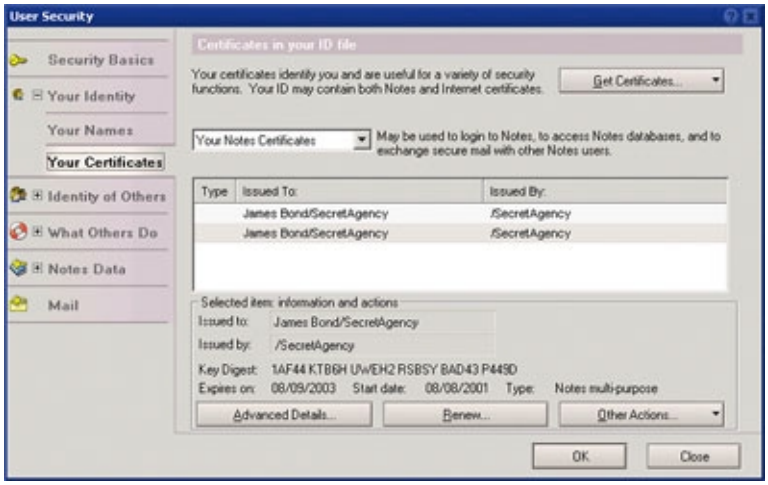
James Bond's Notes user name is "James Bond/SecretAgency," however, when you send Notes mail to him, you may use any of his aliases instead of his user name. Aliases often provide useful shortcuts to entering a person's name. In this case, Notes recognizes aliases of "James Bond" and "Agent 007." Unlike the Notes user name and alternate name, aliases cannot appear in Access Control Lists and Execution Control Lists.

If Bond meets a beautiful woman (doesn't he always?) and wants to tell this woman how to contact him by e-mail, he can visit the Your Names

subsection to find out what his Internet e-mail address is. Bond's Internet e-mail address is also a unique identifier for him.

If Bond is off on assignment and is running Notes as a disconnected user, he will not be able to see the information on his aliases or his Internet e-mail name. This is because the information is retrieved from the Domino directory, which is not available when disconnected.

Your Certificates
The answer to who are you also lies in your certificates. As far as Notes security is concerned, you are represented by your names and by your certificates. In fact, your Notes name and alternate name are stored in your Notes certificates.



The Your Certificates subsection contains everything you would want to know about your certificates. Many Notes users do not know that they have certificates. What are these things? You can think of certificates as being similar to other types of IDs, such as a driver's licence or passport. Certificates are the cornerstone of your security. Without them, you cannot connect to servers or send Notes mail. Your certificates provide a proof of identity, and even the greatest criminal brains in the world will find it virtually impossible to produce a counterfeit of your certificates. In addition to being your identification, your certificates, and their corresponding keys, are used for security operations such as encryption.

Typical users will never need to visit the Your Certificates subsection in User Security (although we should never say never again). The Your Certificates subsection is intended for advanced users only. Those of you who are Notes old-timers should note that a number of operations previously found in the User ID dialog box (which the User Security dialog box now replaces) can now be found in the Your Certificates subsection. This includes operations such as exporting your Notes user ID by making a safe copy, and copying or mailing your Notes certificate.

A drop-down list allows you to select the type of certificate to display. Because this area of security has some complexity, the User Security dialog box provides you with help text explaining how the different types of certificates can be used. For example, when you select Your Internet Certificates from the drop-down list, the dialog box explains that your Internet certificates can be used to exchange secure mail with users outside of Notes, to access secure Web pages with the Notes browser, or to secure connections to Internet services (using SSL).

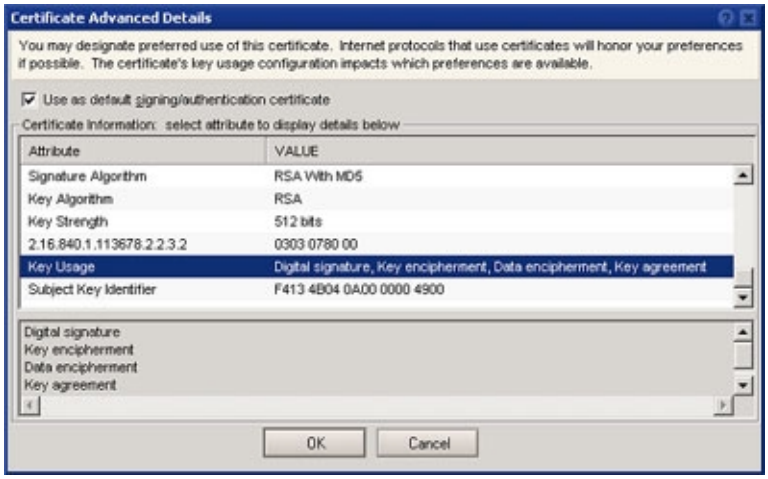
From the Your Certificates subsection, you can view the following items:

- Your Notes certificates
- Your Internet certificates
- Certificates belonging to the certificate authorities that issued your certificates (both Notes and Internet)
- Saved keys extracted from old certificates that might decrypt old mail messages (both Notes and Internet)
- Notes pending keys, which have been proposed as new certificate keys (if you are requesting a change to your Notes keys)

You might visit the Your Certificates subsection to request new Internet certificates or to import and export certificates for use with other software products. There are a number of new features supported for Internet certificates, including:

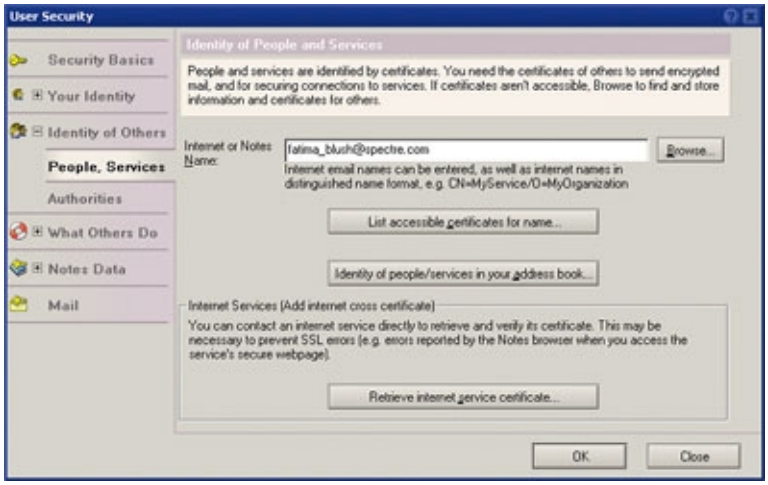
- Greater convenience to request new Internet certificates from an Internet certificate authority
- Additional formats supported for the import of Internet certificates
- Additional formats supported for the export of your Internet certificates
- Option to store private keys associated with your Internet certificates onto a smartcard for greater security
- Advanced details of Internet certificate information, including certificate extensions

Advanced details of Internet certificates, shown below, are intended for security experts only.



Identity of Others

Identity of Others is the third section of the User Security dialog box, and it has two subsections: People, Services and Authorities.



People, Services
The People, Services subsection allows you to find other people's certificates (and have a closer look at them if you wish). There are a variety of reasons why you need another person's certificate, but the best example is when you want to send encrypted mail. Have you ever wondered why you can send encrypted mail to some people, but not to others? When you send encrypted mail, Notes must have access to the recipient's certificate in order to complete the encryption operation. In many cases, Notes mail is able to find other people's certificates for you. But, occasionally Notes may report errors when attempting to send encrypted mail.

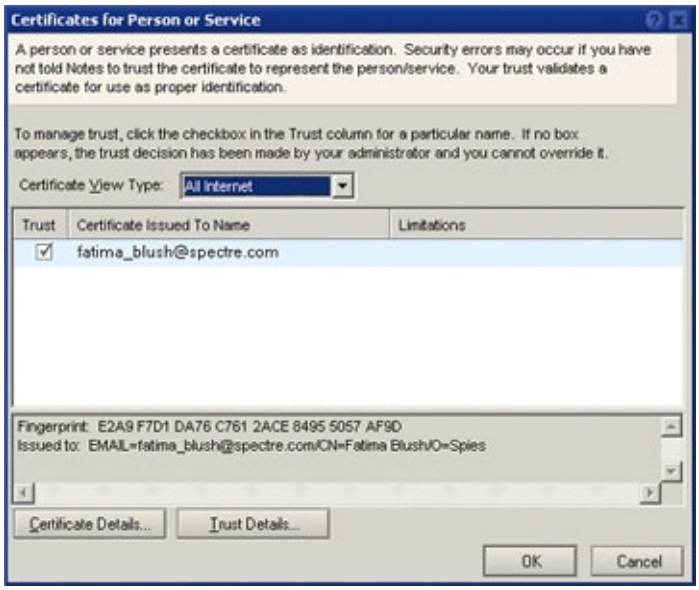
If you want to know whether you can send a particular person encrypted mail, you can enter that person's name in the Internet or Notes Name field and then click the "List accessible certificates for name" button. You would then see a list of Notes and Internet certificates found for that name. If no certificates are found, you can browse various address books to continue searching for an acceptable certificate. If a certificate is found, you can usually succeed at sending encrypted mail, although a special mail configuration may be required if you are using Internet certificates for encrypting mail (which is discussed in the Mail section later in this article). But, finding a certificate may not be the final step in being able to send encrypted mail to another person. The certificate must be trusted for use as well. We mentioned that certificates are a form of identification. A fake ID will not do—the certificate must come from a recognized and reliable source that is trusted.

Suppose that James Bond encounters a beautiful woman, Fatima Blush, and later wants to contact her by e-mail. Bond may wish to protect his love letter so that only she can read it, even if the message is intercepted or stolen. When Bond attempts to send encrypted mail, he receives an error saying that Fatima's certificate is not trusted. He may see a confusing dialog box that asks if he wants to make a cross certificate. Bond feels passionately about sending this mail, so he does not read the dialog box and instead just clicks OK to continue. But what has Bond just done to his security configuration by clicking OK?

Rather than being used proactively to research certificates, the People, Services subsection may likely be used as a morning-after thought. Sooner or later, Bond is ready to move on to his next lady friend. He may wisely wish to review his past decisions and indiscretions. He can use the People, Services subsection to assess the situation with Fatima Blush. Bond enters Fatima's e-mail address and clicks the "List accessible certificates for name" button. The display shows that a certificate is found for Fatima, and the trust column shows that Bond is currently trusting this certificate as

proper identification. What may alarm Bond on careful inspection is that Fatima's certificate has been issued by a foreign and untrusted Internet certificate authority named "Spies." Bond can make an exception to the rule that certificates from "Spies" are untrusted and continue to trust Fatima's certificate. Or he can remove his trust in Fatima's certificate by clicking the checkbox next to her certificate in the Trust column to remove the trust checkmark.

By trusting Fatima's certificate, Bond is not in too much hot water. But if things had gone badly for him when he wasn't paying attention and responded to the mail security alert, he could have inadvertently declared trust not only in Fatima's certificate, but also in the certificate of the "Spies" certificate authority. Declaring trust in an untrustworthy certificate authority is a much bigger mistake with a broader scope of impact. What can happen when you trust a certificate authority is discussed in more detail in the Authorities section below.

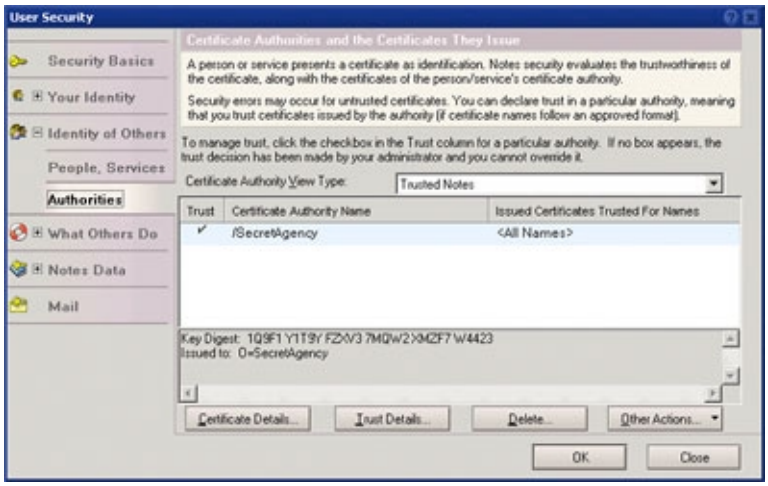


Comments for advanced users
Bond's decision to remove trust for Fatima's certificate would result in the removal of a cross certificate from Bond's personal address book (cross certificates are only visible in the address book Certificates view). If you don't know what cross certificates are, you are in good company. The concept of a certificate accompanied by a cross certificate is complicated to explain. If the cross certificate is removed, this means Fatima's certificate is no longer trusted, and Bond will encounter errors when attempting to send Fatima Internet-style encrypted (S/MIME) mail. In User Security, the idea of cross certificates need not be understood in order to accomplish the task of marking a certificate as trusted (thereby creating a cross certificate) or untrusted (removing the cross certificate). We've done our best to hide cross certificates to reduce complexity.

In addition to managing trust for other people's certificates, you can also find and establish trust in the certificates of services, which you may need to access specific Web sites that use SSL connections. The "Retrieve Internet service certificate" button is a replacement for the R5 menu item Add Internet Cross Certificate. This is another instance in which security options have been consolidated from various places in the product.

Authorities
The Authorities subsection allows you to view the list of certificate

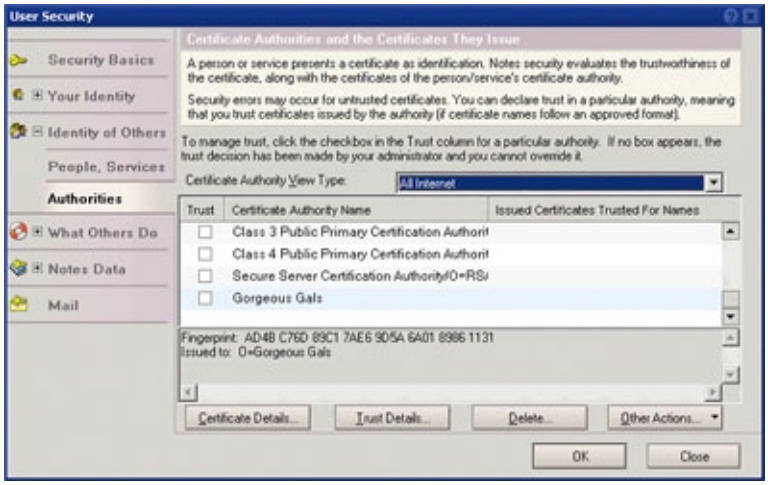
authorities that are known within your Notes client, as well as find others that might be of interest. In general, the Authorities subsection presents information for advanced users only.



We mentioned earlier that certificates are used for identification. James Bond implicitly trusts, as proper identification, all certificates issued by his Notes certificate authority "/SecretAgency." Therefore, he should not encounter many errors when he exchanges secure mail with other users in his Notes domain.

Problems are more likely to arise when he exchanges secure mail with users in foreign Notes domains and users outside of Notes. If Notes encounters certificates issued by untrusted authorities, security errors and warnings may result. To prevent these problems, the Authorities subsection allows you to declare trust in a particular authority (including Notes authorities and Internet authorities). When you decide to trust a particular authority, Notes will recognize certificates issued by that authority as legitimate forms of identification.

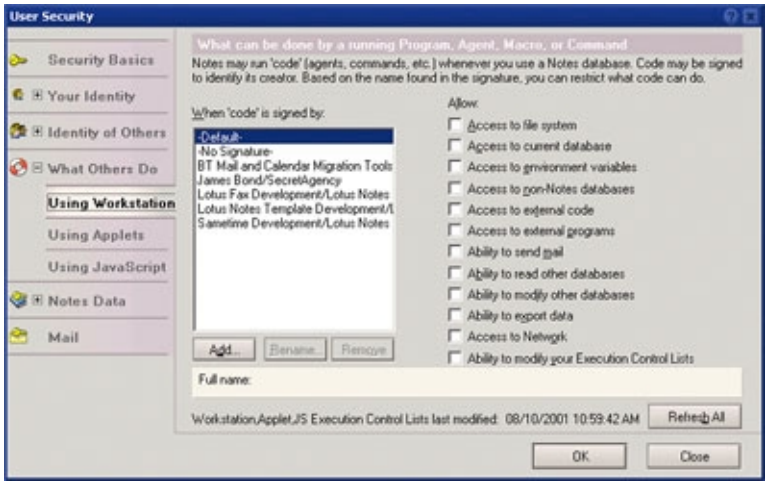
For example, suppose there is an organization for beauty pageant contestants. An Internet certificate authority called "Gorgeous Gals" may issue certificates for each one of the ladies. Currently the "Gorgeous Gals" certificate authority is untrusted, which means that James Bond will encounter errors if he wants to send encrypted mail to any of the ladies. James Bond could decide which of these beauty contestants he would like to proposition by encrypted mail, and then he could declare trust in each of their certificates individually. But, most likely it would save Bond a huge amount of time if he just declared trust in the "Gorgeous Gals" certificate authority itself. After declaring trust in the certificate authority, Bond could send encrypted mail to arrange rendezvous with all the beauty pageant contestants with a minimum amount of overhead.



While trusting the "Gorgeous Gals" certificate authority may provide Bond with some convenience, he should think carefully before doing this. The trust placed in the certificate authority casts a very wide net. Bond has little way to determine the full impact of this trust, as it extends beyond personal correspondence to any security operation involving Internet certificates issued by the trusted authority.

What Others Do

What Others Do is the fourth section of the User Security dialog box, and it has three subsections: Using Workstation, Using Applets, and Using JavaScript. This section allows you to manage your Execution Control List. In R5, the management of your Execution Control List was previously available from the Security Options button in User Preferences. These management dialog boxes are now included in the User Security dialog box, and contain few content changes compared to R5.



The What Others Do section allows you to manage "guest" programs, agents, applets, and other items that we loosely refer to as "code" that may operate in your Notes environment. When you access a Notes database, you may not be aware of the guest code that may execute, for example, an applet that executes when you open a document in the database. Consider that guest code has been created by someone other than you. For your protection, Notes allows you to maintain an Execution Control List that specifies which guests you are willing to accommodate and what your guests may do. Your Execution Control List, if carefully managed, provides

your best defense against the spread of viruses and other damage that could be inflicted by malicious guest code.

Code may be signed to identify its creator. If your Execution Control List does not contain an entry for the code creator, the Default permissions apply. Current defaults are set by your system administrator and should be set so that you are protected from executing guest code from an unknown creator. If code from an unauthorized guest is encountered, a security alert is produced. The security alert forces you to decide whether to allow the code to execute or not. James Bond effectively avoids code signed by would-be assassins, though in a weak moment he may foolishly decide to allow code signed by a gorgeous female assassin. Bond may make active use of this area in User Security to undo his bad decisions after the fact.

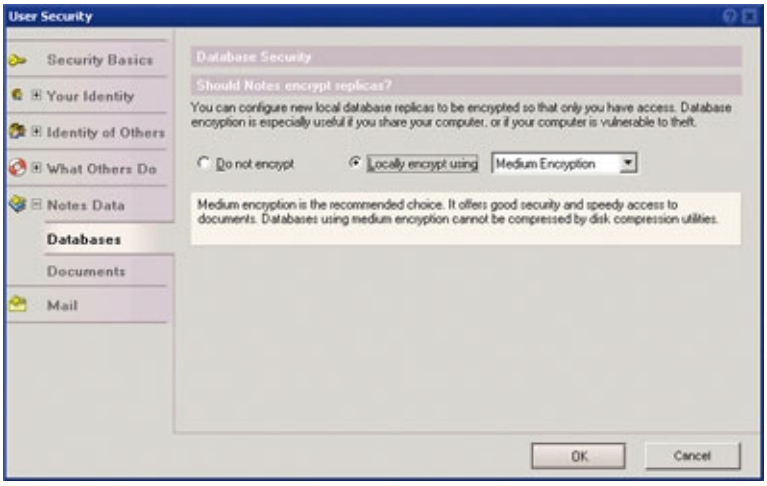
New in Notes 6, administrators have greater control over a user's Execution Control List, which removes from the user some of the responsibility associated with managing the Execution Control List and should also reduce the number of security alerts the user sees. The administrator can set a policy that automatically downloads a standard Execution Control List on a daily basis. If James Bond's administrator was Tracy di Vicenzo (whom Bond married in *On Her Majesty's Secret Service*), it's likely she might choose to replace Bond's Execution Control List on a daily basis, just in case permissions had been unwisely given. To find out more about the ECL, read the *Iris Today* article, "**Staying alert with Execution Control Lists**."

Notes Data

Notes Data is the fifth section of the User Security dialog box and it has two subsections: Databases and Documents.

Databases

The Databases subsection allows you to configure whether new, locally-stored databases are encrypted by default. (If you don't set this option, you can still encrypt databases using Database Properties, as offered in past releases.)

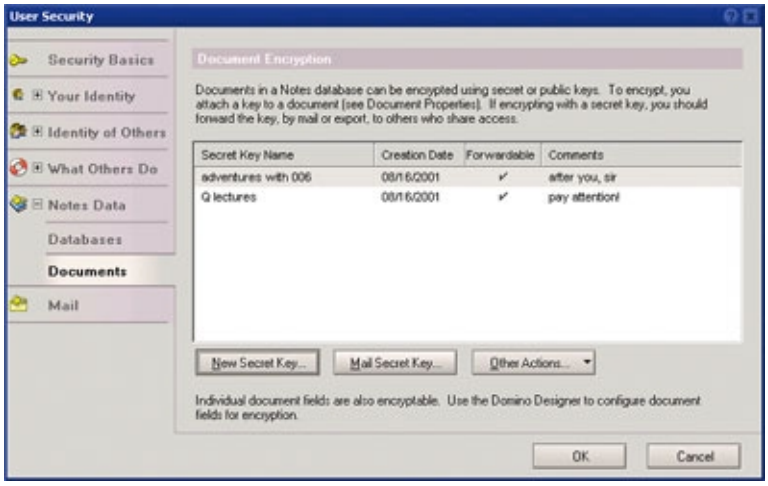


When a database is encrypted, it is for your eyes only, that is, it is readable only by you. James Bond might store the schematics for his spy gadgetry in a database on his laptop. If Bond does not encrypt the database, a laptop thief could gain easy access to the instructions for ejecting passengers from the back seat of Bond's jet. Since Bond prefers to surprise any back-seat drivers, he encrypts his database replica. The encrypted database presents a major problem to the laptop thief—in order to gain access to the encrypted database, the thief also has to steal Bond's user ID

file and guess Bond's difficult password.

Encryption is a powerful option that has become more important in Notes 6 because Notes 6 allows machines to be shared by multiple users. When many users share one computer, database encryption may be necessary to ensure privacy since unencrypted databases can be opened by anyone with physical access to the computer.

Documents
The Documents subsection allows you to create and manage secret encryption keys, which are useful for encrypting documents.

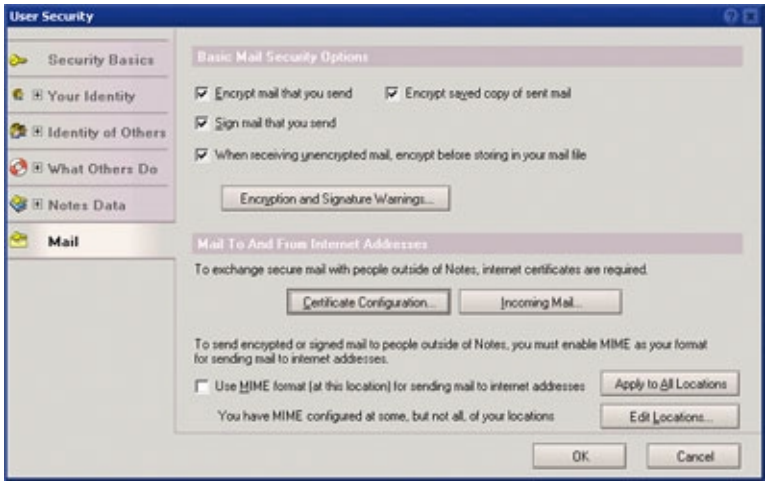


You might encrypt a document so that it can be read only by yourself and by selected others. An encrypted document can be accessed by those who have the required secret encryption key.

The concept of a shared secret encryption key can be compared to a situation where James Bond and his colleague agree on a secret greeting, such as "In London, April's a spring month." Information will be exchanged only if both parties know the secret greeting. The idea of secret encryption keys is similar, though of course much more rigorous and secure. Only those who have the secret encryption key in their Notes ID file will be able to read the encrypted document.

There are few changes from R5 in the area of secret encryption keys; however, User Security does inform users on the change in export regulations impacting encryption keys. In the large majority of cases, there is no longer a need to differentiate between domestic and international versions of encryption keys.

Mail
Mail is the sixth and final section of the User Security dialog box.



At the beginning of this article, we said that security information has always been scattered across the Notes client, and there is no better example than your mail security configuration. The new User Security Mail section includes information gathered from:

- User ID
- User Preferences
- Location documents
- Domino Directory documents
- Your NOTES.INI file

The Mail section brings together everything that has to do with mail security, including:

- Setting mail encryption options.
- Setting a digital signature for outgoing mail.
- Configuring whether or not you would like to see mail encryption and signing warnings generated by Notes. (If you do not care about security, you may configure Notes to omit mail security warnings.)
- Configuring mail security defaults so that you receive mail that is secured using Internet protocols (S/MIME) from Notes mail users.
- Configuring mail security to use S/MIME so that you can send to and receive secure mail from people using a different mail program, such as Netscape mail.

For the novice security consumer, the basic mail security options to configure are encryption and signing.

Encrypting mail

Encrypting mail is how you protect your messages from eavesdroppers and thieves. The encryption process transforms a message into an unreadable format that can only be transformed back to the original state using a particular mathematical key. The owner of the key is the only person who can read the message. In more detail, if you send someone an encrypted message, the message is transformed using the recipient's public key (the recipient's certificate is needed because it contains the public key to use). The message can only be read by the person for whom it is intended, because the recipient is the only person who has the corresponding decryption key to transform the message back to readable form.

Encrypted mail is one secure way in which M could send James Bond his briefings. Mail encrypted for James Bond can only be read by James Bond. Encrypted mail intercepted by an enemy cannot be read, because the enemy doesn't have Bond's decryption key.

If mail is sent to Bond and the sender has not bothered to encrypt it, the

message is vulnerable to attack as it travels to Bond's mail file. But once it arrives, the mail can be stored in an encrypted form in Bond's mail file. The option to encrypt stored mail in the mail file limits the exposure for secrets traveling in an unencrypted message. In the same respect, when Bond sends mail he may keep an encrypted copy for future reference, so only he can read it.

Digitally signing mail
A digital signature is a message integrity check that can be used alone, or in conjunction with encryption, to secure your mail. When you choose to sign your mail, it means that a digital signature (and your certificate) is added to the outgoing mail message before it is sent. A digital signature provides proof that the message has been generated by you, the owner of the accompanying certificate. Furthermore, the digital signature is used to verify that the message is not tampered with as it travels to its destination.

If James Bond wants to conduct an electronic auction for a (fake) Faberge egg, he may want to only accept an e-mail bid that has a digital signature, which would verify the identity of the bidder.

Securing mail to people outside of Notes (using S/MIME mail)
Encryption and signing options require certificates. Each Notes user is issued a Notes certificate that can be used for exchanging secure mail with other Notes users; however, Notes certificates cannot be used to secure mail exchanges with people outside of Notes. If you want to exchange secure mail with someone using another mail program, such as Netscape mail, Internet certificates must be used as the basis for security. When Internet certificates are used for signing and encryption operations, the public key found in the user's Internet certificate is used rather than the Notes public key from the Notes certificate.

If 007 wants to correspond by secure e-mail with the maniacal Dr. No (who likely subscribes to mail services from the Evil Empire), Bond will have to configure secure MIME mail (S/MIME). User Security offers assistance to set up secure mail using Internet certificates and secure MIME format. This topic is largely for advanced security users.

For sending secure mail to people outside of Notes, the configuration of S/MIME mail includes your Location document. MIME must be selected as the format for sending mail to Internet addresses. User Security helps you accomplish this configuration across all of your Location documents or a subset of them.

To use S/MIME mail, you must have an Internet certificate residing in your Notes user ID file. The User Security dialog box's Your Certificates subsection helps you request new Internet certificates if you do not already have one. You can also import Internet certificates that you are already using with a third-party product, such as Netscape.

You are allowed to have more than one Internet certificate. The User Security dialog box's Mail section assists you in choosing which Internet certificate you would like to set as your default signing certificate. The Certificate Configuration dialog box from the Mail section summarizes items in your Location document that must be coordinated with your default signing certificate.

If you wish to standardize all of your mail to be secured with Internet certificates, you can encourage other Notes users to send you S/MIME mail. The Incoming Mail button assists you with this configuration.

Epilogue

We hope you've enjoyed this look at the new User Security dialog box and that you are on your way to "bonding" with this new tool. It's likely that User

Security will grow and evolve over time to include other functions so that it rapidly becomes the center of your security world. We hope it is also clear how the User Security dialog box is accomplishing its goals to make your security options more accessible and understandable. We've divulged a number of "secrets" in this article to give you a headstart in learning about your security options. The only secret that we do not disclose is our choice for which actor is the most handsome Agent 007!

ABOUT THE AUTHORS

Jane Marcus is a Software Architect at Iris, and has been working in the Notes security group for the past 2 years. In her previous lives, Jane tried her hand at being a starving artist and rising opera star. She was also a professional student for more than a decade, studying music, German literature, and ultimately computer science. If you were to meet her today, you would agree that she no longer appears to be starving. Instead she more or less fits the description of computer geek, wife, and mother of two wonderful kids.

Cara Haagenson is a Senior User Assistance (UA) Writer for Lotus, and has been working in the Notes UA group for three years. She writes documentation for the Notes client and Domino Designer. She is also a volunteer on the Customer Contact Team, responsible for collecting documentation feedback, and on the Notes UA Web Team, maintaining the Documentation Library on Notes.net.

ACKNOWLEDGMENT

Special thanks to **Charlie Kaufman** for helping to review this article.

