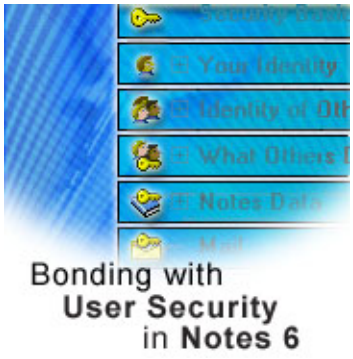
Lotus Developer Domain
The Technical Resource for Lotus software
LDD Today



Level: Beginner
Works with: Notes 6
Updated: 01-Oct-2002

by Jane Marcus
and Cara Haagenson

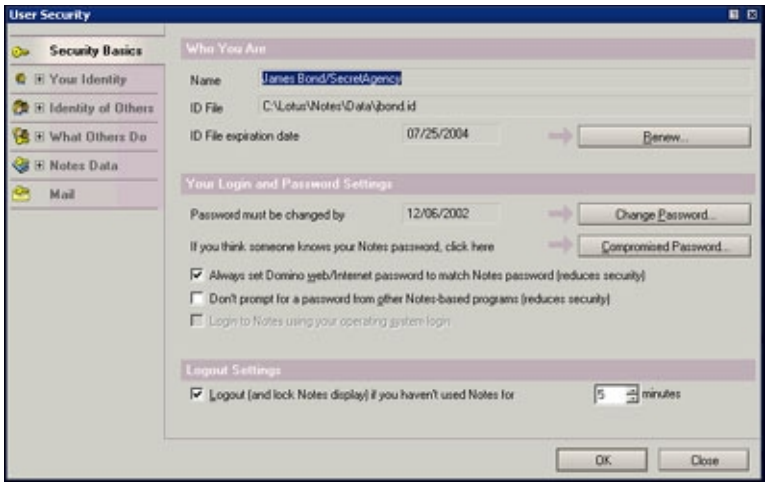
In a classic James Bond film, we find Agent 007 and Agent Saunders providing security for a defecting KGB general.

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 were 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 email message, but were unable to figure out how all of the pieces work together?

Before now, 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's 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.



In this article, we describe the new features available in the User Security dialog box.

How did User Security 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 that Notes security provides, allowing you to use this power to your advantage.

User Security 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 to 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, User Security 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 Domino Web/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. If you have trouble choosing a password that meets your password quality requirement, Notes can generate a password for you so that you don't have to make one up yourself.)
- 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
- View advanced details of your certificates and use new tools to manage certificates
- Request new Internet certificates with greater convenience
- View expired or deleted keys that may still be useful in decrypting old mail messages

If you become a frequent visitor to User Security, you may want to customize your Notes toolbar to include the User Security icon. User Security is only one click away and is playing now on desktops everywhere!

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

Security Basics

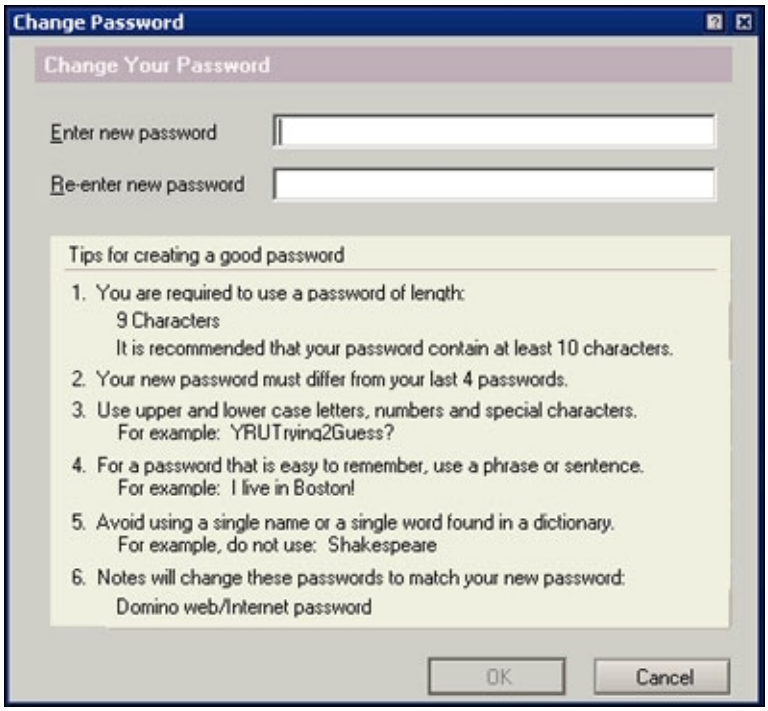
Security Basics is the section you see each time you open User Security. It includes all of the security features that you need to access most frequently and gives you the ability to complete those tasks quickly. This section caters to the end user who doesn't want to be bothered with anything more than 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 Domino Web/Internet and Notes passwords (if allowed by your administrator)
- Set a timer for automatic Notes logout
- Enable your Notes password for other Notes-based programs
- Enable/disable Windows single logon, if installed on your machine (Single logon allows you to share one password for Windows and Notes login. Once you are logged into Windows, you do not have to re-type your password when logging into Notes.)

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

Changing your password
When you click the Change Password button, you 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 previous screen, the administrator has adopted a policy of a password length of nine characters. This means that when you create a new password, the Change Password operation checks that the new password is at least nine 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.

We can see above that James Bond's administrator lets him off easy by adopting a password length policy. However, we security geeks stick by our recommendation for password quality, and to encourage use of password quality rather than password length, we have added tips on the Change Password dialog box to help Bond create a high quality password. In fact, James Bond's password meets the standards for either password length of nine characters or password quality level of nine. His password is "Tomorrow never dies."

If your administrator requires password quality (rather than length) standards, the Change Password dialog box shows examples of passwords that meet your particular quality setting. If you have used all of the passwords you can think of that satisfy the password quality rules set by your administrator, you can click the Generate Password button repeatedly to select a randomly generated password as your new password.

Another convenience feature that administrators can implement for their users is to set a password re-use policy.

In the example pictured earlier, James Bond can re-use his "Tomorrow never dies" password after he changes his password four times.

In addition to password length and/or quality information, the Change Password dialog box also pulls together other 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 Logon user, in which case Notes will attempt to change your operating system login password to match your new Notes password. When creating a new password, a Single Logon user must be mindful of any rules put in place both by the Notes administrator and by the operating system for acceptable passwords. James Bond is reluctant to join forces with his operating system security; therefore, he has not installed the Single Logon feature.

While Bond is not a Single Logon user, he is currently synchronizing his Domino Web/Internet password with his Notes password. The Domino Web/Internet password is used to access Domino servers whenever Bond is connecting to Domino using a Web browser or other Internet application. Users who access Domino both through a Notes client and through the Web can have separate passwords for the two modes of access, or they can set their passwords to be the same. Prior to Notes/Domino 6, a user who chose to keep the two passwords in sync would have to make two separate password changes (one password change for the Notes client, and an edit to the Domino Directory Person document to change the Domino Web/Internet password).

In Notes/Domino 6, password synchronization can be automated so that whenever a user changes the Notes client password, the Notes client automatically changes the Domino Web/Internet password to match. In all cases, password synchronization must be initiated by the administrator through a security policy. A user, such as James Bond, can then allow the synchronization or can decline the synchronization and keep separate passwords. In Bond's case, he has approved the synchronization by selecting the option "Always set Domino web/Internet password to match Notes password" on the User Security Basics tab. The Change Password dialog box above reminds Bond that his Domino Web/Internet password will be changed to match his new Notes password.

Some thoughts on synchronizing your passwords

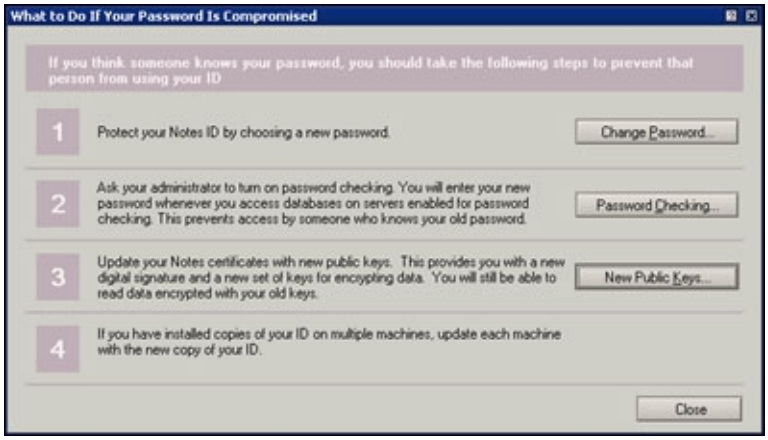
Users are often faced with having lots of passwords for different systems. You need a password to login to your machine, other passwords to login to applications, and still others to access unrelated systems like phone mail and your ATM card. It is common practice for users to set the same password for multiple systems just so that they have fewer passwords to remember. This is convenient, and may even provide better security than choosing different passwords but writing them all down on an insecure yellow sticky note. Having one password for multiple systems can be dangerous, however, because it means that someone who breaks into one system and steals your password can login as you on all of the other systems. A conservative strategy is to have a small number of passwords—some that are used on systems that may be less protected (for example, public Web sites) and other passwords to highly secure, critical systems (such as your ATM card).

Should Bond make use of the feature to synchronize his Notes password and his Domino Web/Internet password? The Notes password is generally well protected, never leaving the user's desktop. An attacker can't even begin to guess the Notes password without stealing the user's ID file. In contrast, the Domino Web/Internet password may be less protected, depending on how Domino has been deployed. In some installations, users may enter the Domino Web/Internet password over connections not protected by SSL, in which case someone eavesdropping on the network can read the password. This scenario scares the living daylights out of us security geeks! While a strong security configuration could be in place to prevent password exposure, the cautious user has good reason for setting a different password for his Notes client than for his Web access to Domino.

James Bond, who could not be classified as a cautious user, seldom worries about danger (and perhaps 007 need not worry given the fact that he has an excellent track record for surviving catastrophe and always lives to die another day). More to the point, Bond is one of the many users already in the habit of using the same password for the Notes client and for Domino access from the Web. Given Bond's decision to use one password, it makes sense for him to save time with automated synchronization. Password synchronization is not a feature for everyone, but is very convenient for those who use it.

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 can the thief 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 finish panicking, 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 provides the steps you need to follow if you have to recover from disaster.

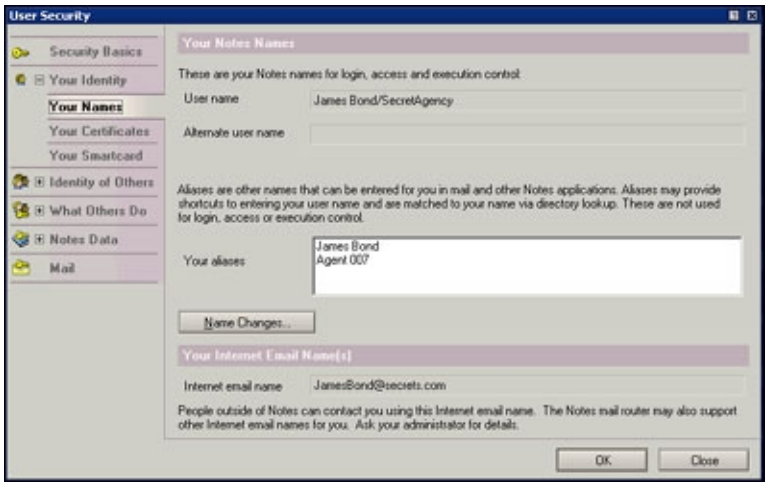


Your Identity

Your Identity is the second section of User Security, and it has three subsections: Your Names, Your Certificates, and Your Smartcard.

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).



Because James Bond is known worldwide 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.

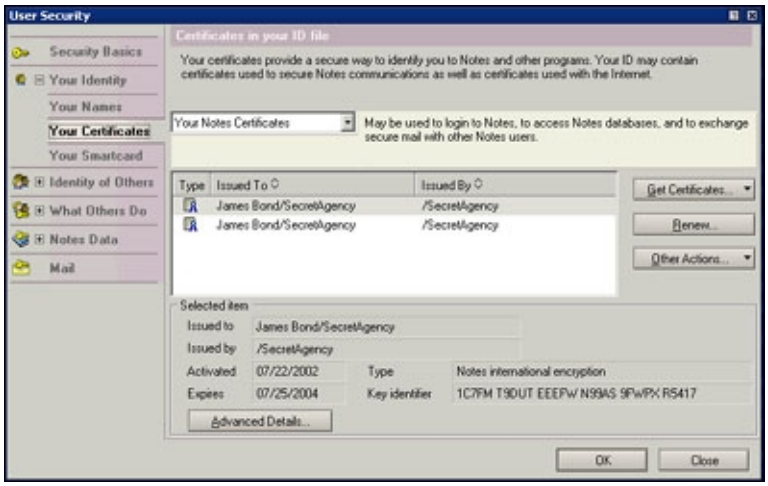
If Bond meets a beautiful woman (doesn't he always?) and wants to tell this woman how to contact him by email, he can visit the Your Names subsection to find out what his Internet email name is. Bond's Internet email name is also a unique identifier for him.

If Bond is off on assignment and is running Notes as a disconnected user, he cannot see the information on his aliases or his Internet email 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 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 use the Notes client to connect to servers or to 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 counterfeits 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 User Security 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 containing your public key.

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).

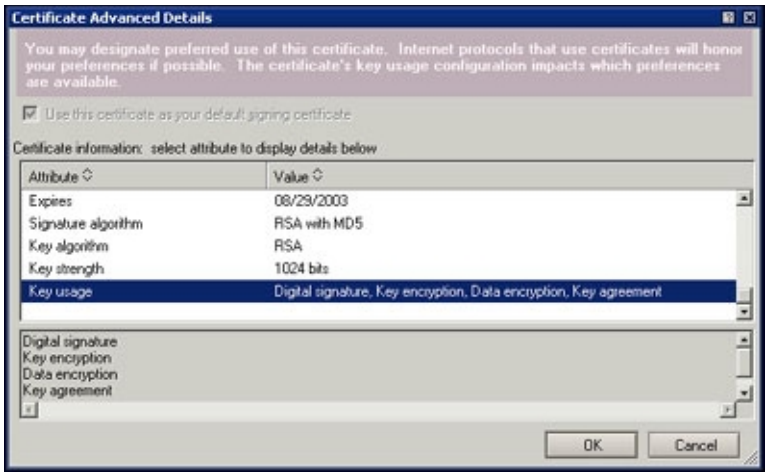
From the Your Certificates subsection, you can view the following items:

- 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:

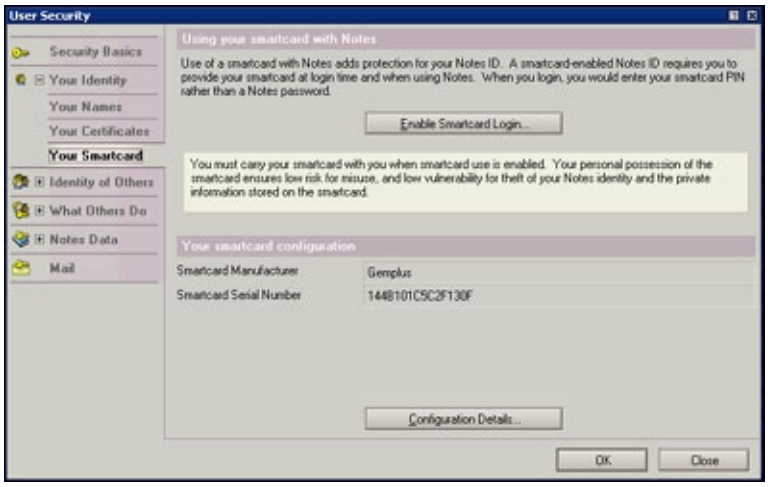
- Greater convenience to request new Internet certificates from an Internet certificate authority
- Additional formats supported for the import of Internet certificates
- Additional formats supported for the export of your Internet certificates
- An option to store private keys associated with your Internet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

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



Your Smartcard
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, imagine a credit card or ATM card with a small computer chip on it. Information can be stored on your Smartcard, and your Smartcard becomes part of your Notes identity because its presence is required for any use of your Notes User ID. 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. Note that to use a Smartcard with Notes you must have a Smartcard, a Smartcard reader, and Smartcard software from a third-party vendor. For a list of Smartcards that Notes supports, refer to the **Notes/Domino 6 Release Notes**.

The Smartcard subsection, shown below, allows you to use your Smartcard with Notes.

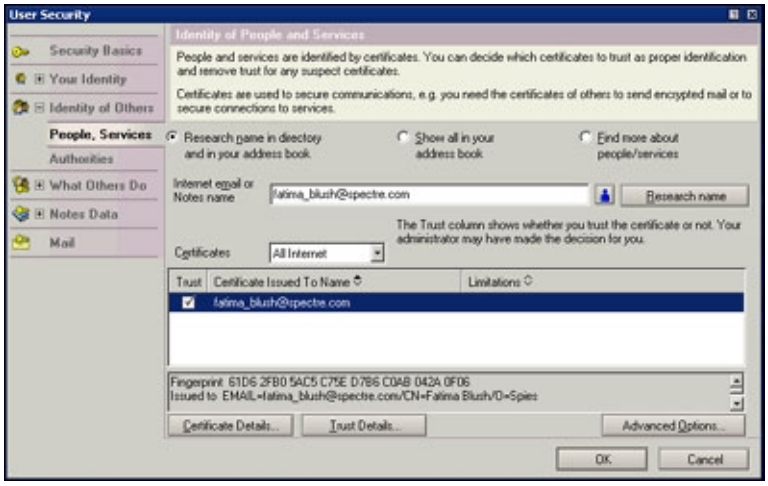


Identity of Others
Identity of Others is the third section of User Security, and it has two subsections: People, Services and Authorities.

People, Services
The People, Services subsection allows you to find other people's certificates (and to 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 to complete the encryption operation. In many cases, Notes mail can 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 or not you can send a particular person encrypted mail, you can research a name in

the Domino Directory and in your personal address book. Enter that person's name in the "Internet email or Notes name" field, and then click the Research Name button. You will 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. (See the *LDD Today* article, "**Be the authority on the Domino 6 certificate authority**" for more about certificates.)



Suppose that James Bond encounters a beautiful woman, Fatima Blush, and later wants to contact her by email. Bond may wish to protect his love letter so 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. Bond's haste to proceed is typical of the vast majority of users, and Bond has little understanding of how his security configuration has just been changed.

Sooner or later, Bond will be ready to move on to his next lady friend. He may wisely wish to review his past decisions and indiscretions, including his recent security alert encounter. Rather than being used proactively to approve certificates for security use, the People, Services subsection may likely be used as a morning-after thought. Bond can use the People, Services subsection to assess the situation with Fatima Blush. Bond enters Fatima's email address and clicks the Research 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.

Bond can click the Trust Details button to get more information on the trust that resulted from clicking OK to the security alert. 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.

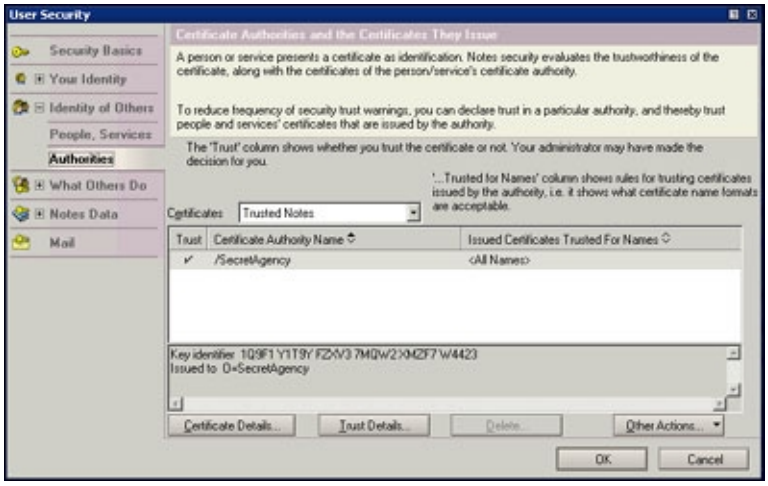
Comments for advanced users

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 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. Click the radio button "Find more about people/services" to see the button "Retrieve Internet service certificate;" this button is a replacement for the Notes 5 menu item Add Internet Cross Certificate. This is another instance in which security options have been consolidated from various places in the product.

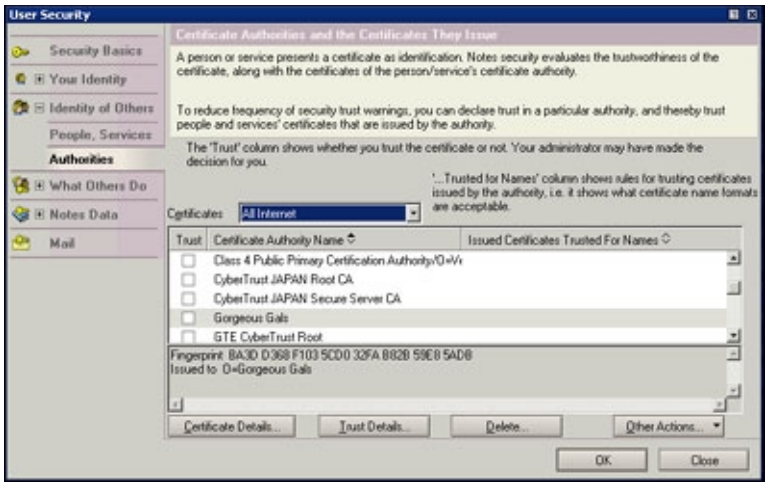
Authorities
The Authorities subsection allows you to view the list of certificate authorities that are known within your Notes client, as well as to find others that might be of interest. In general, the Authorities subsection presents information for advanced users only.



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 recognizes certificates issued by that authority as legitimate forms of identification.

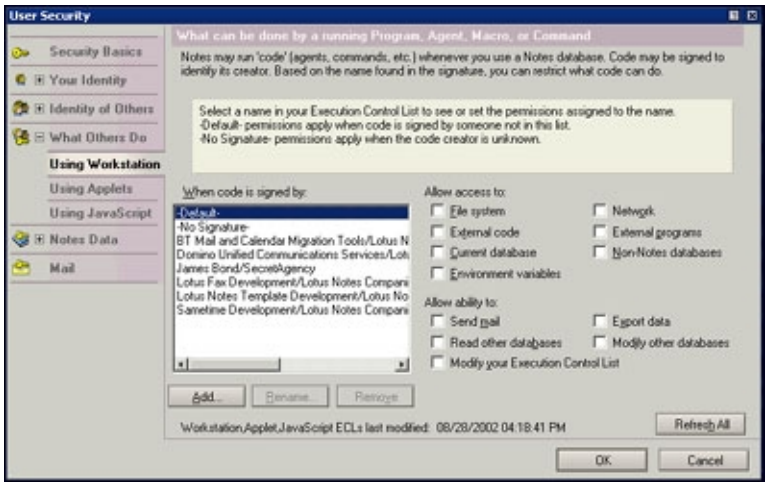
For example, suppose there is an organization for beauty pageant contestants. An Internet certificate authority called Gorgeous Gals may issue certificates for each one of the ladies. Currently, the Gorgeous Gals certificate authority is untrusted, which means that James Bond will encounter errors if 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 because 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 User Security, and it has three subsections: Using Workstation, Using Applets, and Using JavaScript. This section allows you to manage your Execution Control List. In Notes 5, 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 User Security and contain few content changes when compared to Notes 5.



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 or not 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.

What Others Do subsections manage the various types of permissions that you can assign to guests. The What Others Do - Using Workstation subsection encompasses permissions for the general operation of the Notes client workstation. You can grant Notes workstation guests access to the local machine—for example, its file system—or guests may be allowed permissions for the Notes environment—for example the ability to send Notes mail. James Bond's workstation ECL is set to allow few guest permissions. This means that Bond may often see various workstation security alerts, especially because he can't resist the temptation to push any button labelled "For a good time, click here."

The What Others Do - Using Applets subsection handles the special subset of permissions that apply when a Java applet is running within Notes. This subsection specifies whose applets may access certain Notes resources—for example, Notes Java classes—or access the local system—for example, to submit print jobs. James Bond sometimes may see applet security alerts regarding printing permissions because his favorite database welcome page is running an applet for displaying and printing the latest Spy of the Month slide show.

The What Others Do - Using JavaScript subsection covers permissions for JavaScript executing in the Notes client—for example, when a Notes form contains JavaScript or when the Notes browser renders a Web page containing JavaScript code. Permissions include, for example, allowing guest JavaScript code to open a different Notes document or a new Web page. If Bond were a Notes browser user, it's likely that Bond's adventurous spirit would lead to a variety of security alerts intended to keep him out of trouble. However, Bond has configured Netscape as his browser, and therefore, he seldom sees JavaScript security alerts. It's important to note that the Execution Control List does not impact the operation of any third-party browser, even if the browser is being displayed in a Notes window.

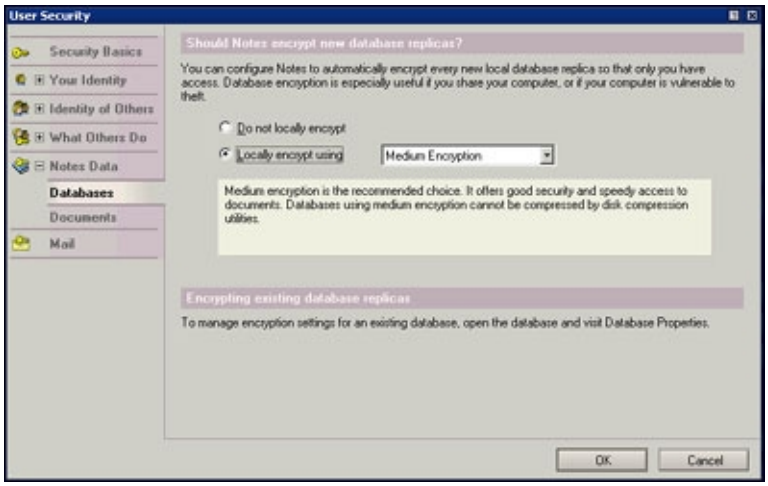
The Execution Control List (ECL) is fairly complex and often is poorly managed by users. New in Notes 6, administrators have greater control over a user's Execution Control List, which removes from the user some of the responsibility associated with managing it and may also reduce the number of security 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 have been unwisely given. To find out more about the ECL, read the *LDD Today* article, "**Staying alert with Execution Control Lists**."

Notes Data

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

Databases

The Databases subsection allows you to determine whether or not 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.)

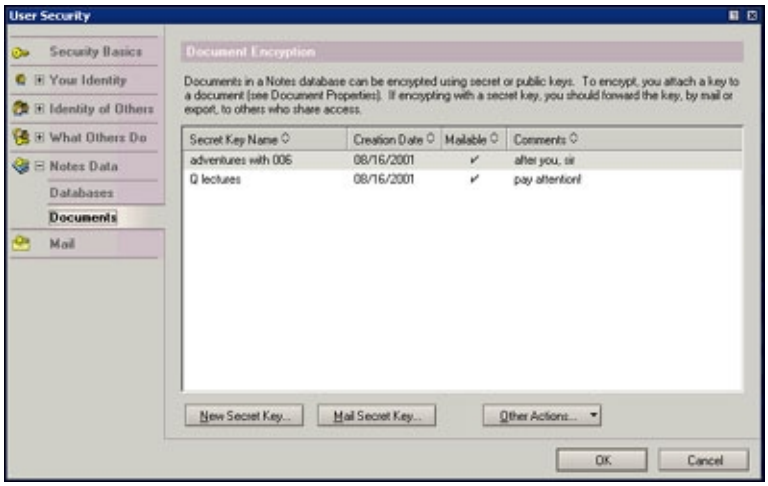


When a database is encrypted, it is for your eyes only; that is, it is readable only by you. James Bond might store the schematics for his spy gadgetry in a database on his laptop. If Bond does not encrypt the database, a laptop

thief could gain easy access to the instructions for ejecting passengers from the back seat of Bond's plane. Because Bond prefers to surprise any back-seat drivers, he encrypts his database replica. The encrypted database presents a major problem to the laptop thief—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 because 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.

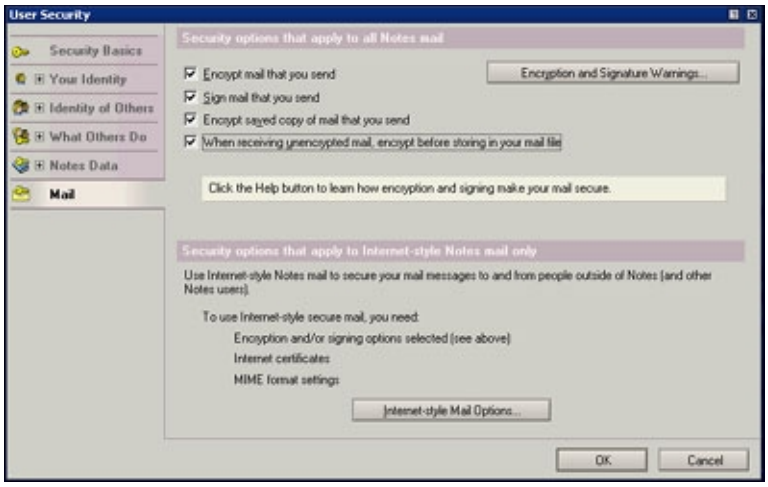


You might encrypt a document so that it can be read only by yourself and by selected others. An encrypted document can be accessed by those who have the required secret encryption key.

The concept of a shared secret encryption key can be compared to a situation in which 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 can read the encrypted document.

There are few changes from Notes 5 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 User Security.



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 to use Internet-style Notes mail (S/MIME) so that you can send to and receive secure mail from people using a different mail program, such as Netscape mail
- Configuring mail security defaults so that you receive Internet-style Notes mail (S/MIME) from Notes mail users

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 email 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 email bid that has a digital signature, which would verify the identity of the bidder.

Securing mail to people outside of Notes (using Internet-style 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 email with the maniacal Dr. No (who likely subscribes to mail services from the Evil Empire), Bond will have to configure Internet-style Notes mail that uses secure MIME (S/MIME) protocols. User Security offers assistance to set up secure mail using Internet certificates and secure MIME format. Users begin by clicking the Internet-style Mail Options button. This section is largely for advanced security users.

For sending secure mail to people outside of Notes, the configuration of Internet-style Notes 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 Internet-style Notes mail, you must have an Internet certificate residing in your Notes User ID file. The Your Certificates subsection in User Security 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. User Security assists you in choosing which Internet certificate you would like to set as your default signing certificate. The "Internet-style Notes mail Certificate Configuration" dialog box 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 Internet-style Notes mail. The Incoming Mail dialog box assists you with this configuration.

Epilogue

We hope that 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 User Security 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 head start 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 JANE MARCUS
Jane Marcus is a Senior Software Engineer at IBM and has been working in the Notes security group for the past three 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.

ABOUT CARA HAAGENSON
Cara Haagenson is a Senior User Assistance (UA) Writer and has been working in the GPD UA group for four years. Her projects include the Notes client, sample Domino JSP Tag Library applications posted in the LDD Sandbox, and iNotes Web Access. She is also a volunteer on the Customer Contact Team, which is responsible for collecting documentation feedback for Lotus products, and on the GPD UA Web Team, which is responsible for maintaining the Documentation Library on LDD.

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

