

# *Sending Secure and Encrypted Messages with GroupWise 6.5: User's Guide*

## Feature Article

NOVELL APPNOTES

### Tay Kratzer

Primary Support Engineer  
Novell, Inc.  
[tkratzer@novell.com](mailto:tkratzer@novell.com)

This AppNote explains how to send secure and encrypted e-mail messages, which can only be received and read by the stated recipient.

**Note:** This is the User's Guide portion of the AppNote entitled "Sending Secure and Encrypted Messages with GroupWise 6.5." For the full version that includes the preparatory steps that must be taken by the GroupWise administrator, see <http://developer.novell.com/research/appnotes/2003/may/02/a030502.htm>.

### Contents:

- Introduction
- Step 1: Export Your Encryption Key/Certificate
- Step 2: Import the Encryption Key/Certificate into GroupWise
- Step 3: Exchange Encryption Keys
- Step 4: Test Sending an Encrypted Message
- Conclusion

Topics	GroupWise, e-mail, security, encryption, digital certificates
Products	GroupWise 6.5, NetWare 5.1 and 6, Novell Certificate Server 2.0, Novell eDirectory 8.6 or later
Audience	network users
Level	beginning
Prerequisite Skills	familiarity with GroupWise
Operating System	NetWare 5.1, NetWare 6
Tools	none
Sample Code	no

## Introduction

The following are step-by-step instructions for sending secure and encrypted messages that will comply with the security and encryption standards your organization has adopted.

When you send messages normally within GroupWise, they are encrypted. However, the recipient can forward your messages to other people with ease. Also, when you send messages across the Internet, they are often not secure or encrypted. The procedures outlined in this AppNote are designed to fill in these gaps in information security.

By sending secure and encrypted e-mails, you can ensure that only the stated recipient is able to read the messages you send. Examples of e-mails that you'd want to send secure and encrypted are messages that contain:

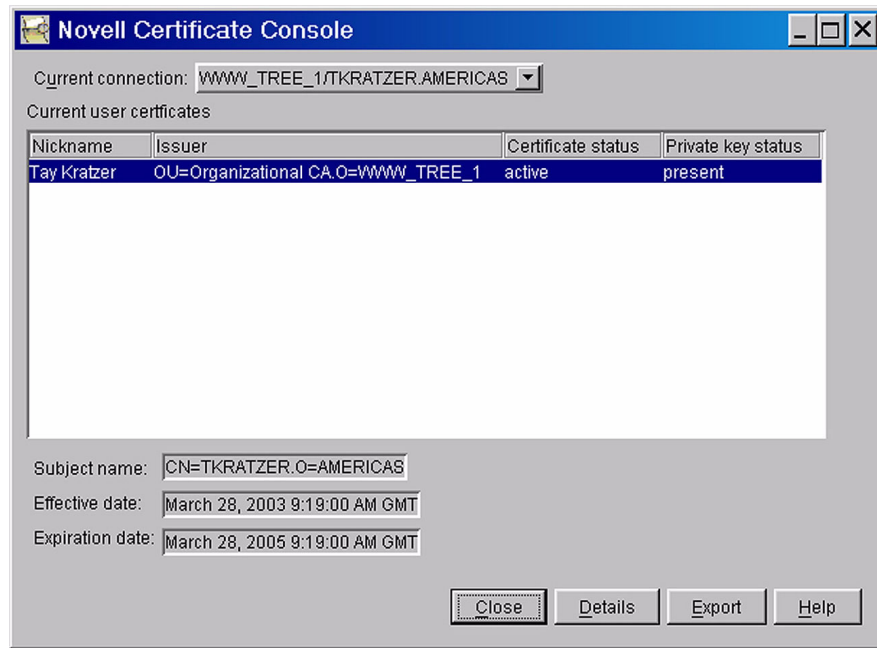
- Contract information
- Trade secrets
- Purchase requisitions
- SEC-restricted information
- HIPAA-restricted information

While the process described here may seem foreign and arcane, you will need to perform most of these steps only once. You must execute the technical steps personally, because that is the only way to assure recipients that messages you compose and send encrypted are done with your authorization.

### Step 1: Export Your Encryption Key/Certificate

You only need to perform this procedure once.

1. Start up the Novell Certificate Console utility. Your network administrator will tell you where this utility is located.
2. You will see a screen similar to the one shown in Figure 1; however, the username and other information displayed will be specific to you.



**Figure 1:** Initial screen of the Novell Certificate Console utility.

3. Click the **Export** button.
4. In the next dialog (see Figure 2), you are asked if you want to export the private (encryption) key with the certificate. Answer “Yes” to this prompt and then click the **Next** button.



**Figure 2:** The “Export A User Certificate” prompt.

5. In the next screen (shown in Figure 3), do the following:



Figure 3: The "Export A User Certificate" dialog.

- Make sure the checkbox for "Include available certificates in certification path" is checked.
- Keep the default filename and path specified. Note the name of the \*.PFX file that is being created.
- Enter and re-enter a password of 6 characters or longer. This does not have to be the same as your login password. In fact, you won't have to remember this password beyond the initial setup period explained in this AppNote. You will need to provide this password later on in these procedures, but that's it—you will not need it beyond that.

When you are ready, click **Next** to continue.

6. The last screen (see Figure 4) shows a summary of your selections.

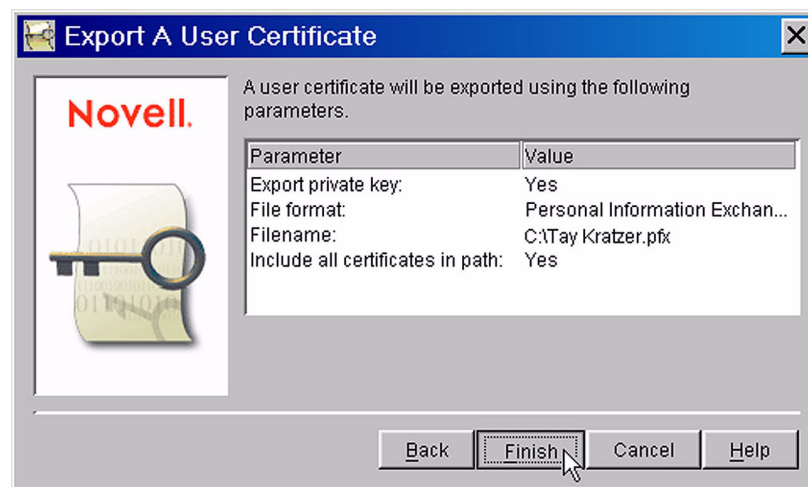


Figure 4: The "Export A User Certificate" summary screen.

Review the information and then click the **Finish** button. You will not see a screen confirming the success of the operation, but it's generally safe to assume the export went just fine. You can now close the Novell Certificate Console utility.

## Step 2: Import the Encryption Key/Certificate into GroupWise

You will only need to perform this procedure once.

1. From the GroupWise 6.5 32-bit Windows client (not the GroupWise WebAccess browser-based client), access your GroupWise Mailbox.
2. Select Tools > Options > Certificates. You will see the screen shown in Figure 5.

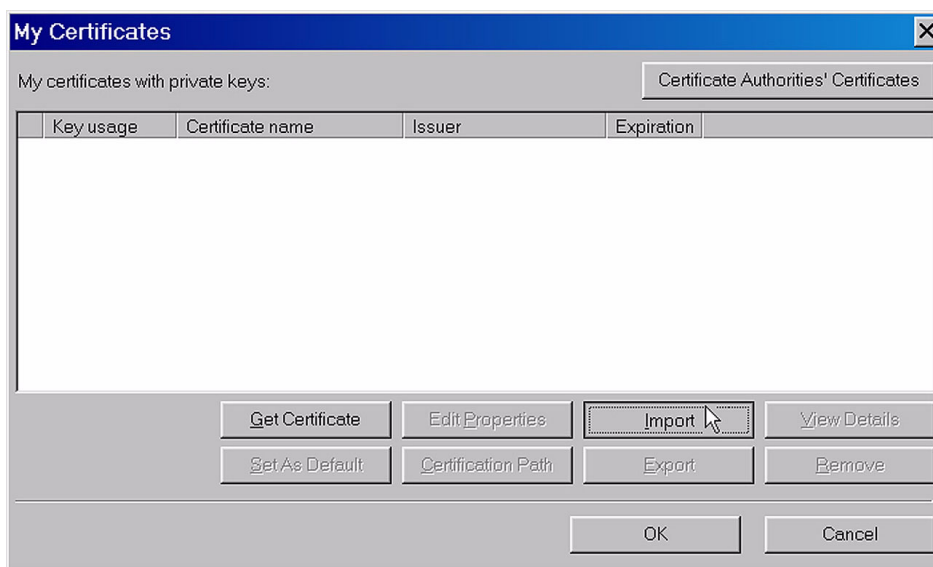


Figure 5: The "My Certificates" screen in GroupWise 6.5.

3. Click on the **Import** button. Follow the instructions below while referring to Figure 6.



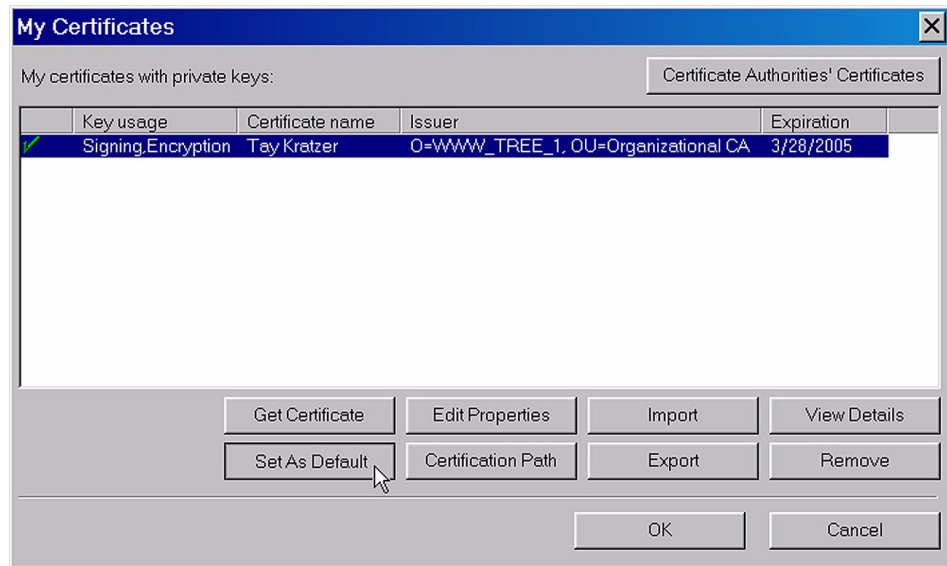
Figure 6: The "Import My Certificate" dialog.

- To fill in the “Certificate file to import” field, click the **Browse** button and navigate to the \*.PFX file you exported in the previous procedure.
- Type the password that you were prompted to enter earlier when exporting your certificate and private key.
- Make sure the checkbox for “Allow export of private key in the future” is checked.
- Do not check the checkbox for “Set strong private key protection” (unless your network administrator tells you otherwise).

Click the **OK** button to continue.

**Note:** If you are prompted to add the “Root Store Certificate,” answer “Yes”.

4. Highlight the certificate you just created and click the **Set As Default** button. You should then see a green checkmark next to the certificate, as shown in Figure 7.



**Figure 7:** The imported certificate set as default.

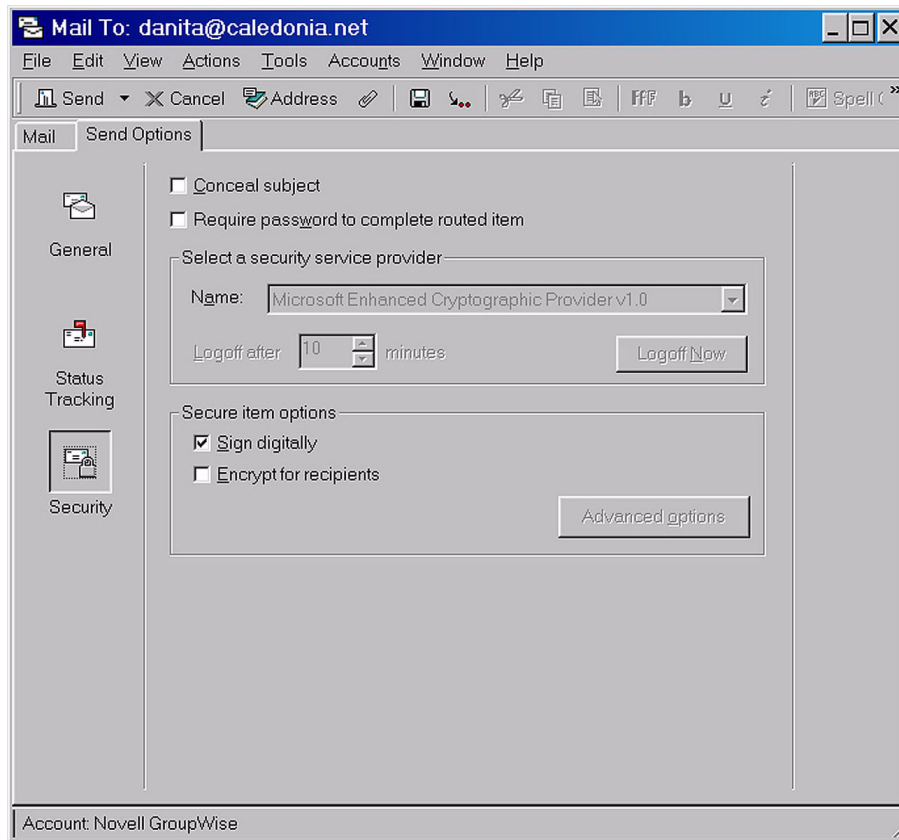
5. Click **OK** and then **Close** to return to the GroupWise 6.5 mailbox.

You have now configured GroupWise 6.5 so that, when you choose to do so, you can send secure and encrypted e-mail. However, you must first exchange your encryption key/certificate with those users who you intend to communicate with in a secure and encrypted manner. The following are step-by-step instructions that both you and another user must follow in order to send and receive your encryption keys.

### Step 3: Exchange Encryption Keys

**Sending the Encryption Key.** Both users must complete the following steps to exchange their encryption keys:

1. From the GroupWise Windows client (not a browser), select File > New > Mail.
2. Address the e-mail to the desired recipient.
3. Click the Send Options tab, and then click on the Security icon in the left-hand side of the window.
4. Under “Secure item options,” place a check in the checkbox for “Sign digitally”, as shown in Figure 8.

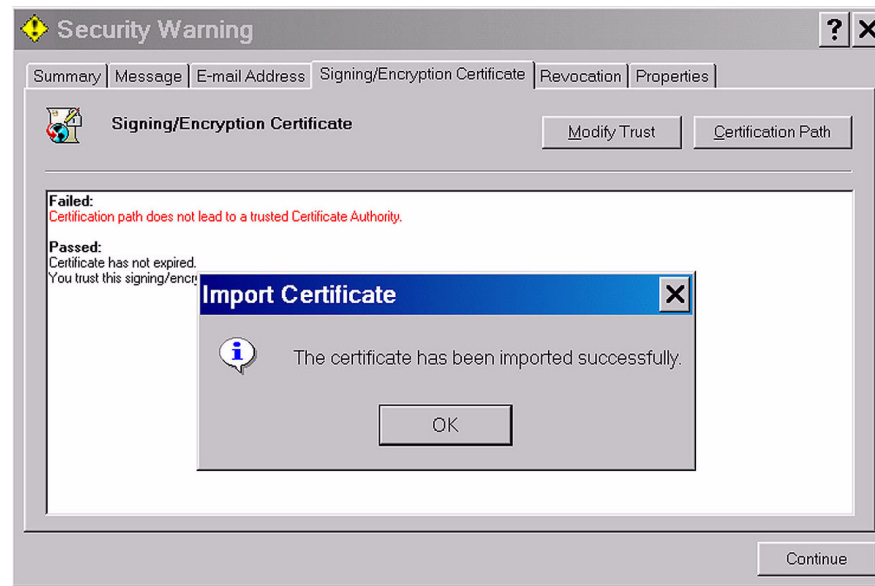


**Figure 8:** Selecting the option to “Sign digitally”.

5. Send the message to the recipient.

**Receiving the Encryption Keys.** Both users must perform these steps to accept and import the sender’s certificate/ private key that was just sent.

1. In the GroupWise Windows client, open the e-mail message that was signed digitally.
2. When the “Security Warning” dialog appears, select the Signing/Encryption Certificate tab.
3. Click on the **Modify Trust** button and select the choice “I trust this certificate.” A message box should appear confirming the successful import, as shown in Figure 9.



**Figure 9:** Message indicating successful import of the certificate.

Click on **OK** and then **Continue**.

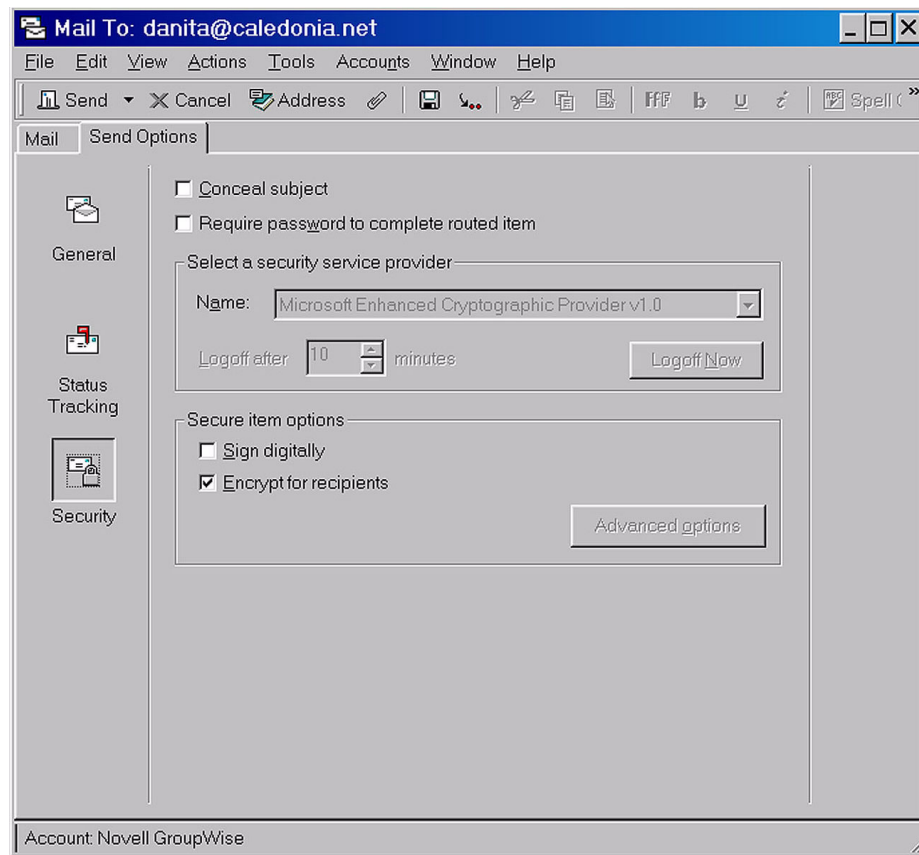
#### Step 4: Test Sending an Encrypted Message

Once the above procedures have been successfully completed, you are ready to test the sending of an encrypted message.

**Note:** Both users must have performed all of the steps outlined above before proceeding with the test.

1. From the GroupWise Windows client (not a browser), select File > New > Mail.
2. Click the Send Options tab, and then click on the Security icon at the left-hand side of the window.
3. Place a check in the checkbox next to “Encrypt for recipients”, as shown in Figure 10.





**Figure 10:** Selecting the option to “Encrypt for recipients”.

4. Compose a test message and send it to the recipient with whom you previously exchanged encryption keys.
5. Verify that the intended recipient, who has received your encryption key, is the only one able to read the encrypted message. You may want to send the e-mail to other recipients to verify that they *cannot* read the message.

From this time forward, you will be able to send secure/encrypted messages to the user with whom you exchanged encryption keys.

## Conclusion

This AppNote has shown how to send secure and encrypted e-mail message in GroupWise 6.5. For more information about Novell GroupWise 6.5, visit the product Web page at <http://www.novell.com/products/groupwise>.

Copyright © 2003 by Novell, Inc. All rights reserved.  
No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of Novell.

All product names mentioned are trademarks of their respective companies or distributors.