RSA KNOWLEDGE RSA SecurCare® Online

How to decrypt SSL or TLS sessions with RSA NetWitness Investigator

New KB Sear

Rate This Article	(Average Rating: No Rating)	Show Properties

Article Content

Article Number 000026270

Product Details
RSA NetWitness NextGen
RSA NetWitness Decoder
RSA NetWitness Investigator

Issue How to decrypt SSL or TLS sessions with RSA NetWitness Investigator.

Resolution

Decrypting SSL or TLS sessions with RSA NetWitness Investigator

If you have the unencrypted .pem private keys of SSL transactions, Investigator can decrypt these sessions.

- In Investigator go to **Edit --> Options --> Display**
- At the very bottom should be an option to **Automatically Decrypt Sessions**.
- Checking this option will allow you to select a folder where the .pem private keys are contained.
- Once the keys are selected you will either need to start a new collection or delete the content cache of the current collection.
- If you are deleting the content cache, select the collection and go to **Collections --> Delete Content Cache**
- When reconstructing sessions the text and web views decrypt the sessions.
- Due to the fact SSL has the ability to resume sessions, if you view a part of a resumed session before you view the beginning of the session where the key exchange was performed, you will not be able to decrypt the session with the private key at this point.
- If you find the place where the key exchange took place and view that first you will be able to view any resumed sessions afterward.
- If you locate the key exchange location after you have already viewed a part of the resumed sessions - you can delete the content cache of the collection, view the key exchange session and then view the decrypted resumed session.

Decrypting SSL with NetWitness Investigator FAQ

Q1: What encryption protocol types are supported?

A1: SSL v3.0 and TLS v1 (protocol values on the wire of "3 0" and "3 1", respectively)
Q2: What PEM certificate/private key files are supported?
A2: PEM certificate/private key files need to be in an unprotected (passphrase removed) PEM format. The file extension needs to be lower case (.pem). If you view the private key .pem file using a text editor, you should see something like this:

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAs1s7VQqzHThwXHzrqOHZgJBefuZo9Ntli21ZJNkAHWK1FZhd
.....

uxBxFLIN7UK9MykmyJlaLqMwi4FGwVdzl/GeukCfF6fELzA72lei
-----END RSA PRIVATE KEY-----

Q3: What SSL keys are supported?

A3: The following SSL keys are supported

rsa-with-null-0-md5
rsa-with-null-0-sha
rsa-with-rc4-128-md5
rsa-with-rc4-128-sha
rsa-with-rc2-128-sha
rsa-with-idea-128-sha
rsa-with-des-64-sha
rsa-with-des-64-sha
rsa-with-3des-192-sha
rsa-with-rc4-128-md5
rsa-with-rc2-128-md5
rsa-with-des-64-sha
rsa-with-rc4-128-sha

*** The following keys support are added in release 9.6.5.11 & 9.7.5.10:

RSA-with-AES-128-SHA

RSA-with-AES-128-SHA

Note: Any keys generated with Diffie-Hellman are not supported, SSLv2 is not supported. Clients useing Elliptic Crypto Curves extension to negotiate the keys are not supported.

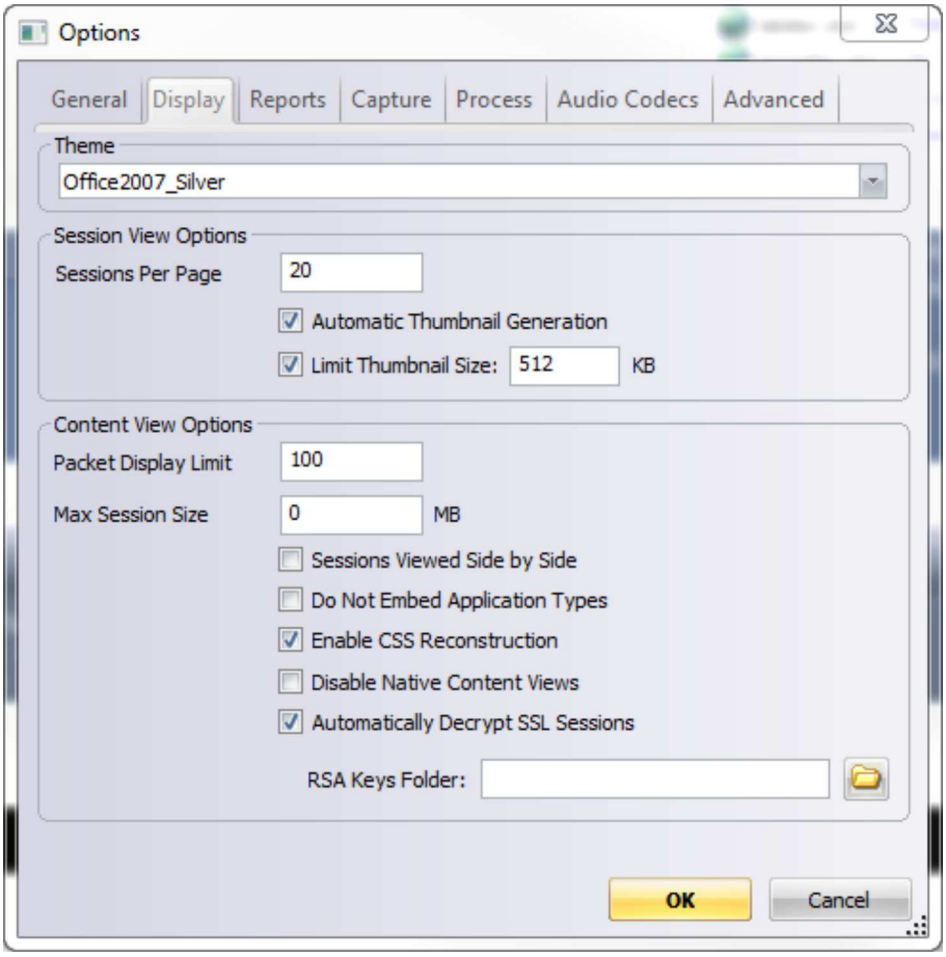
Q4: Can I decrypt and any portion of an SSL session by drilling directly into it?
A4: No. When working with a set of tcp sessions that represent a continuing ssl session, the initial session must be viewed first. Decrypting the initial tcp session is the key to viewing the entire ssl session.

Q5: Can a Decoder be made to perform SSL decryption rather than Investigator

A5: This is not possible and also not desirable as it would have serious negative performance impact on a Decoder

Notes

The screenshot below shows the Display tab in the RSA NetWitness Investigator Options.



Legacy Article ID a58556

Feedback

Did This Article Solve Your Problem?

Feedback