


http://<ibmi_name_or_ip>:2002/Navigator

 **Warning: NAV_200001:** The GUI is leveraging encryption to secure passwords. The encryption keys and the key to Web trust store are being protected by IBM Cryptographic Services for i. The GUI is using Master key 1 and this must be loaded and set. Currently, Master key 1 is not available on the GUI node. Users with *ALLOBJ and *SECADM special authorities are allowed to load and set Master key 1 within IBM Cryptographic Services for i. If the password and CA certificates in the trust store have previously been encrypted the Master Key 1 will need to be loaded and set again. You will need to re-input passwords and re-accept the CA certificates when prompted. To load and set the Master key, click on Serviceability then the Cryptographic Services tab to load and set master key 1.


IBM Navigator for i qsecofr

Connection Properties

- General
- Thresholds
- Authentication
- TLS Connection
- Cryptographic Services**

IBM i Cryptographic services is used for encryption key management in Navigator for i GUI. Master key 1 is used to secure keys and must be loaded and set correctly.

Master Key Status

Master Key 1:  **Load**

Note: If Master key 1 is cleared or reset twice without translating keystores encrypted by this master key outside Navigator GUI, all encrypted data and CA certificates in web trust store are lost. This is because the configuration could not be decrypted. Master key 1 might be used for other products and monitored by some exit programs, so the load and set operations might fail, check master key exit points if issues occur.

Load and Set Cryptographic Services Master Key 1

Passphrase:

<passphrase goes here>

IBM Cryptographic Services for i is used to protect the encryption keys in Navigator. Master key 1 must be loaded and set. Currently, it is not available on the GUI node. Without the support, the passwords and accepted CA certificates will not be stored and you need to input passwords and accept CA certificates for TLS enabled nodes again for every sign in until master key 1 is set and the passwords and the Web trust store can be properly encrypted and stored for future access.

The load master key operation takes a passphrase as input. It is hashed and then loaded into the new version. To activate the new master key value, the set operation is required. The user must have *ALLOBJ and *SECADM special authorities to load and set a master key. Note, you should write down the passphrase for the master key and store them securely. Load and Set a master key impacts all products using this master key.

Load and Set

Close