Export or Back Up Your MIT Personal Certificates

Export or Back Up Your MIT Personal Certificates

On this page:

Firefox on Macintosh, Windows, Athena, Linux
Internet Explorer on Windows
Micrsoft Edge on Windows
Mac OS X Using Keychain Access
Getting Help
Related Links

There are a couple of reasons to export or back up your personal certificates:

- If you send or receive email which has been signed or encrypted with your personal certificate (S/MIME), you will need to keep that certificate on your system even after it expires, in order to validate and read the email.
    - Not sure if you're using S/MIME? Learn more
    - If you experience any difficulty accessing certificate-protected MIT websites, you can export your certificates from your browser to a backup file, then delete them from your browser, before you get new certificates

Firefox on Macintosh, Windows, Athena, Linux

1. Launch Firefox.
2. Do the following, according to your platform:
    - Macintosh: **Firefox > Preferences > Privacy and Security > Certificates > View Certificates > Your Certificates**
    - Windows: **Tools > Options > Advanced > Encryption > View Certificates > Your Certificates**
    - Athena, Linux: **Edit > Preferences > Privacy and Security > Certificates > View Certificates > Your Certificates Tab**
3. Select the certificate to back up.
4. Click **Backup** (or **Backup All** to select all certificates).
5. When prompted, enter a filename and specify a location for the backed up certificates.
6. Click **Save**.
7. When prompted, enter the master password used to protect your certificates.
8. Click **OK**.
9. When prompted, create and enter a Certificate backup password. Enter it again to confirm.
10. Click **OK**.
    Note: Backed up certificates contain personal information and should be protected with a password. It should be different from your Kerberos password. The password quality meter will indicate the strength of the password entered; the higher the strength, the more secure the password.
11. In the Alert showing successful back up, click **OK.**
12. You can now delete the expired certificates

Internet Explorer on Windows

1. Launch **IE**
2. Go to **Tools > Internet Options > Content**
3. Click the **Certificates** button and then the **Personal** tab.
4. Select the certificate to export.
5. Click **Export**
6. In the *Certificate Export Wizard*, click **Next**.
7. In the *Export Private Key* dialog, click **Next**.
8. In the *Export File Format* dialog, accept the default, "DER encoded binary".
9. Click **Next**.

Micrsoft Edge on Windows

1. Launch **Edge Browser**
2. Go to **Three Dots in the top right corner > Settings > Privacy and Servies**
3. Under the privacy heading, click on **Manage Certificates**
4. Select the certificate to export.
5. Click **Export**

6. In the *Certificate Export Wizard*, click **Next**.
7. In the *Export Private Key* dialog, click **Next**.
8. In the *Export File Format* dialog, accept the default, "DER encoded binary".
9. Click **Next**.

Note: For details on exporting a private key, if that option is available, and on certificate file formats, see "Export a certificate" in Windows Help and Support.

1. In the *File to Export* dialog, click **Browse**.
2. In the *Save As* dialog, specify a location for the exported file and enter a file name.
3. Click **Save**, then **Next**, then **Finish**.
   Result: A message appears confirming that export was successful.
4. You can now delete the expired certificates

Mac OS X Using Keychain Access

1. Launch Keychain Access: **Macintosh HD / Applications / Utilities / Keychain Acess.app**
2. Under Category (left-hand panel), click **My Certificates**.
   Result: Your personal certificates are listed.
3. Select the certificate to export.
4. From the **File** menu select **Export Items**
5. In "Save As", enter a filename and specify a location for the exported certificates.
6. Click **Save**.
7. When prompted, enter and verify a password for exporting, then click **OK**. (If your Keychain is locked, you will be prompted to unlock it by entering your Mac account password.)
   Note: Exported certificates contain personal information and should be protected with a password. It should be different from your Kerberos password. The password quality meter will indicate the strength of the password entered; the higher the strength, the more secure the password.
8. In the dailog box *Keychain Access wants to export...* enter your Macintosh account password (or keychain login password, if different), then click **Allow**.
   Result: The certificates you selected are exported from your Keychain into a file that is protected with the password entered in step 6. If this password is forgotten, you will not be able to open the exported certificates, or read email signed or encrypted under those certificates.
9. You can now delete the expired certificates

Getting Help

- Help Desk

Related Links

Certificates at MIT