

Microsoft Root Update Utility may have caused some of your problems:

The Navy help desk has seen a distinct rise in the number of users that can't access their websites due to recent updates by the Microsoft Root update utility. Appendix B in this [attachment](#) shows the intermediate certificates that cause the CAC-based logon systems to properly read the primary CAC certs. Some other good information can be found here: <https://www.us.army.mil/suite/page/474113>

Removal of the following intermediate root certificates has allowed them to clear up issues with many of the new CACs

Issued to: Entrust

Issued by: Common Policy

Serial nm: 3BAE7B920EE6616755BE4FA287777EEF2F6B33F6

Issued to: DoD Interoperability Root CA1 Issued by: Entrust Serial nm:
DC92F91BAB283472023B32178504E19BF7D9A94C

Issued to: DoD Root CA 2

Issued by: DoD Interoperability Root CA 1 Serial nm:
EEA68FC8701E41E6429A341AE4162BBDA634F7F4

Here's how:

1. **Open IE. Go to Tools->Internet Options->Content tab**
2. **Click on Certificates and go to the Intermediate Certification Authorities tab**
3. **Remove any of the following certs that are found.**

Common Policy → Entrust (FBCA) cross-certificate
Common Policy → Entrust (FBCA) cross-certificate (Revoked)
Entrust (FBCA)→IRCA cross-certificate
IRCA→DoD Root CA 2 cross-certificate
Entrust (FBCA) self-signed certificate

4. Click OK twice to return to the main IE window. User should now be able to visit CAC enabled sites.

Our basic way of knowing this is the issue is when doing this

1. **Open IE. Go to Tools->Internet Options->Content tab**
2. **Click on Certificates and double click on your main CAC certificate (lastname.firstname.edipi, friendly name ID certificate)**
3. **Click on Certification Path. If you see entrust in the path, the certificates are corrupt and certificates need to be reviewed. A good path looks like this:**

DoD Root CA 2
DOD CA-XX
ID certificate