Wireless Certificate Information

Wireless Network Certificates

When you join the **UCCS-Wireless** or **eduroam** network for the first time, depending on your operating system or device type you may be asked to accept and trust a server security certificate.

When you are prompted to trust the server security certificate, you should verify its details before trusting it. Make sure the issuer and at least one of the fingerprints match the information outlined below. If the displayed certificate information on your device doesn't match the information above, DO NOT trust the certificate.

The security certificate helps you know that you are connecting to legitimate UCCS OIT wireless access points, and not rogues or impostors. Our wireless server security certificates are issued by *COMODO*, and it has a very specific fingerprint associated with it. Most devices allow you to preview the security certificate before accepting so that you know you are connecting to a legitimate UCCS OIT wireless access point. The certificate displayed on your device - the certificate you are being asked to trust before your connection is finalized - should have an issuer and a fingerprint that matches the information below.

Server Information

ⓘ ***Wireless authentication server (VM) name:*** ClearPass

Wireless authentication server hostname: cppm.uccs.edu

***Wireless certificate* issuer:** COMODO RSA Organization Validation Secure Server CA

Certificate in PEM format: cppm.pem

Certificate in CER format: cppm.crt

Certificate Fingerprints

Below are the fingerprints an end user can use to validate the certificate when connecting to *UCCS_Wireless* or *eduroam*:

ⓘ **CPPM Certificate Fingerprints (SHA-256 and SHA-1)**

SHA-256: 24 96 3E 77 CA 8C 98 AA 36 4B 07 C0 D6 63 16 7B 40 3A 68 BC 72 C2 7F 57 0C A1 E2 85 BB 8F E1 F3

SHA-1: 7F EF D3 17 14 12 50 59 1B B9 C0 CA D7 D6 C6 CC FB D6 03 45

If the fingerprints do not match, DO NOT trust the certificate! Click CANCEL and contact the OIT Helpdesk.

Advanced Information

Root CA and Intermediate CAs used to sign the certificate for UCCS's wireless environments can be download below:

Root Comodo RSA CA: comodorsacertificationauthority.crt

https://support.comodo.com/index.php?/Knowledgebase/Article/View/969/108/root-comodo-rsa-certification-authority-sha-2

Intermediate Comodo RSA Organization Validation Secure Server CA: comodorsaorganizationvalidationsecureserverca.crt

https://support.comodo.com/index.php?/Knowledgebase/Article/View/968/108/intermediate-ca-2-comodo-rsa-organization-validation-secure-server-ca-sha-2