

802.1X for RingCentral Phones

Support of 802.1x relies on three components, the endpoint (phone), the network switch, and the Network Policy Server (RADIUS server, Windows Network Policy Server, or Cisco ISE). All three components must share common root CA certificate(s). Configuration of the network switch and the Network Policy Server are not within the scope of this document. There are complex interactions which are best dealt with by vendor experts.

The included code examples show EAP-PEAPv0-MSCHAPv2 authentication.

The yellow highlighted terms in the following configuration scripts are the phone's login credentials. Multiple phones can use the same login credentials so long as the authentication server allows it.

The RingCentral provisioning system provides hooks for Custom Code files to inject non-standard settings into a phone as it provisions.

Polycom IP Phone Configuration

Polycom phones use XML files stored in the RingCentral provisioning system to establish customized functionality. Be very careful to maintain full XML syntax compliance.

Method	Comments
EAP-None	No authentication
EAP-MD5	No certificates required
EAP-PEAPv0-MSCHAPv2	Requires CA certificate
EAP-PEAPv0-GTC	Requires CA certificate
EAP-TTLS-MSCHAPv2	Requires CA certificate
EAP-TTLS-GTC	Requires CA certificate
EAP-TLS	Requires device and CA certificates
EAP-FAST	Complex (see Polycom documentation)

This is an example of the file used when there is a single root CA certificate.

```
<PHONE_CONFIG>
  <device.sec.TLS device.set="1"
    device.sec.TLS.customCaCert1="-----BEGIN CERTIFICATE-----
    MIIIFhzCCA2+gAwIBAgIQTt6q9X+d9KdC6KJgchZJjTANBgkqhkiG9w0BAQ0FADBJ
    ...[certificate contents go here]...
    pOz1HfW0KUV9TuV53t3EOP/U/eDWOCxj+BsL
    -----END CERTIFICATE-----"
  />
```

```

<device.sec.TLS.customCaCert1
    device.sec.TLS.customCaCert1.set="1">
</device.sec.TLS.customCaCert1>

<device.net.dot1x device.net.dot1x.enabled="1"
    device.net.dot1x.enabled.set="1"
    device.net.dot1x.identity="phone-802-1x"
    device.net.dot1x.identity.set="1"
    device.net.dot1x.password="phonepassword"
    device.net.dot1x.password.set="1"
    device.net.dot1x.method="EAP-PEAPv0-MSCHAPv2"
    device.net.dot1x.method.set="1"
/>

<sec.dot1x sec.dot1x.eapollogoff.enabled="1"
    sec.dot1x.eapollogoff.lanlinkreset="1"
/>

</PHONE_CONFIG>

```

And this is an example of the file used when there are both a root CA certificate and a subordinate CA certificate.

```

<PHONE_CONFIG>
<device.sec.TLS device.set="1"
    device.sec.TLS.customCaCert1="-----BEGIN CERTIFICATE-----
    MIIIFhzCCA2+gAwIBAgIQTt6q9X+d9KdC6KJgchZJjTANBgkqhkiG9w0BAQ0FADBJ
    ...[certificate contents go here]...
    pOzlHfW0KUV9TuV53t3EOP/U/eDWOCxj+Bsl
    -----END CERTIFICATE-----"
/>
<device.sec.TLS.customCaCert1
    device.sec.TLS.customCaCert1.set="1">
</device.sec.TLS.customCaCert1>

<device.sec.TLS device.set="1"
    device.sec.TLS.customCaCert2="-----BEGIN CERTIFICATE-----
    MIIIFYDCCBEigAwIBAgITMQAAAAAXV3rQ6/7JaswAAAAAABTANBgkqhkiG9w0BAQsF
    ...[certificate contents go here]...
    pOzlHfW0KUV9TuV53t3EOP/U/eDWOCxj+Bsl
    -----END CERTIFICATE-----"
/>
<device.sec.TLS.customCaCert2
    device.sec.TLS.customCaCert2.set="1">
</device.sec.TLS.customCaCert2>

<device.net.dot1x device.net.dot1x.enabled="1"
    device.net.dot1x.enabled.set="1"
    device.net.dot1x.identity="phone-802-1x"
    device.net.dot1x.identity.set="1"
    device.net.dot1x.password="phonepassword"
    device.net.dot1x.password.set="1"
    device.net.dot1x.method="EAP-PEAPv0-MSCHAPv2"
    device.net.dot1x.method.set="1"
/>

<sec.dot1x sec.dot1x.eapollogoff.enabled="1"
    sec.dot1x.eapollogoff.lanlinkreset="1"
/>

```

</PHONE_CONFIG>

Yealink IP Phone Configuration

Yealink phones use files stored in the RingCentral provisioning system to establish customized functionality.

Yealink IP phones support 802.1X authentication based on EAP-MD5, EAP-TLS, EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-PEAP/GTC, EAP-TTLS/EAP-GTC and EAP-FAST protocols. The table below lists the protocols supported by Yealink SIP IP phones with different versions.

Authentication Protocol	IP Phone Models	Firmware Version
EAP-MD5	All IP Phones	All Versions
EAP-TLS	T46G, T42G, T41P, CP860	71 and later
	T48G	72 and later
	T58V/A, T56A, T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP960 and W56P	80 and later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P	81 and later
	T46G, T42G, T41P, CP860	71 and later
	T48G	72 or later
	T58V/A, T56A, T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP960 and W56P	80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60P and CP920	81 or later
	W53P	83 or later
EAP-TTLS/EAP-MSCHAPv2	T46G, T42G, T41P, CP860	71 or later
	T48G	72 or later
	T58V/A, T56A, T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP960 and W56P	80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60P and CP920	81 or later
	W53P	83 or later

Authentication Protocol	IP Phone Models	Firmware Version
EAP-PEAP/GTC	T48G, T46G, T42G, T41P	73 or later
	T58V/A, T56A, T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP860, CP960 and W56P	80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60P and CP920	81 or later
	W53P	83 or later
EAP-TTLS/EAP-GTC	T48G, T46G, T42G, T41P	81 or later
	T58V/A, T56A, T49G, T40P, T29G, T23P/G, T21(P) E2, T19(P) E2, CP860, CP960 and W56P	80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60P and CP920	81 or later
	W53P	83 or later
EAP-FAST	T58V/A, T56A, T29G, T23P/G, T21(P) E2, T19(P) E2, T49G, T48G, T46G, T42G, T41P, T40P, CP860, CP960 and W56P	80 or later
	T54S, T52S, T48S, T46S, T42S, T41S, T40G, T27G, W52P, W60P and CP920	81 or later
	W53P	83 or later

Code elements are listed in the following:

```

#!version:1.0.0.1
#
#
static.network.802_1x.mode = 0 thru 7
# Settings are:
#   0 - EAP-None
#   1 - EAP-MD5
#   2 - EAP-TLS
#   3 - EAP-PEAP/MSCHAPv2
#   4 - EAP-TTLS/EAP-MSCHAPv2
#   5 - EAP-PEAP/GTC
#   6 - EAP-TTLS/PEAP-GTC
#   7 - EAP-FAST
#

```

```
static.network.802_1x.eap_fast_provision_mode = 0 or 1
# Settings are:
#   0 - Unauthenticated Provisioning
#   1 - Authenticated Provisioning
# Note: only used if 802_1x.mode is set to 7 (EAP_FAST)
#
static.network.802_1x.anonymous_identity = id string
#
static.network.802_1x.identity = id string
#
static.network.802_1x.md5_password = password string
#
# Certificates must be in DER / Base64 format, usual filename extensions
# are .pem, .crt, .cer, or .der)
#
static.network.802_1x.root_cert_url = url string
#
static.network.802_1x.client_cert_url = url string
```

Other Phones to Follow as Requested