Understand Certificate and Trustpoint Types on the 9800 WLC

Contents

Introduction

This document describes the different types of certificates and trustpoints that can be used on the 9800 WLC.

Prerequisites

Requirements

Cisco recommends you have basic knowledge of:

- Cisco Wireless LAN Controller (WLC) 9800 series
- Digital Certificates, Certificate Authorities (CAs) as well as the Public Key Infrastructure (PKI)

Components Used

This document is not restricted to specific hardware or software versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Certificates

What is a Certificate?

A certificate is a unique document which identifies a device, for example, to ensure that it is legitimate. A certificate must be verified by a CA to validate said identity.

Types of Certificates on the 9800

Access Points (APs) and the WLC need some sort of way to validate each other's identity. Whenever a new AP joins the WLC the AP validates the WLC's certificate to ensure that it is not only legitimate but that it is still valid. This way, APs can trust the appliance they are joining for the first time ever.

Manufacturer Installed Certificate (MIC)

This certificate is by default installed on the physical appliances—such as the 9800-80, 9800-40, and the 9800-L. As it names implies, it is factory installed and cannot be modified. This certificate is used for when the AP joins for the first time to the WLC.

To check if a MIC certificate is indeed installed on the 9800, you can enter the command **show wireless management trustpoint.**

```
<#root>

9800#show wireless management trustpoint
Trustpoint Name  : CISCO_IDEVID_SUDI
Certificate Info : Available

Certificate Type : MIC <--

Private key Info : Available
FIPS suitability : Not Applicable
```

Self-Signed Certificate (SSC)

For the virtual instance of the controller, the 9800-CL, there is no factory-installed certificate. But rather, it uses a self-signed certificate that can be generated automatically through the Day 0 wizard, or through a script in which the certificate is manually created. In virtual instances of the 9800, the SSC is used mainly for AP join but also for all HTTP(s), SSH and NETCONF services. Physical appliances also contain a SSC, but as stated before, it is not used for AP join, but for the services instead.

Again, to check the SSC certificate on the 9800, enter the command **show wireless management trustpoint.**

```
<#root>

9800#show wireless management trustpoint
Trustpoint Name  : 9800-CL-TRUSTPOINT
Certificate Info : Available

Certificate Type : SSC <--

Certificate Hash : e55e61b683181ff0999ef317bb5ec7950ab86c9e
Private key Info : Available
FIPS suitability : Not Applicable
```

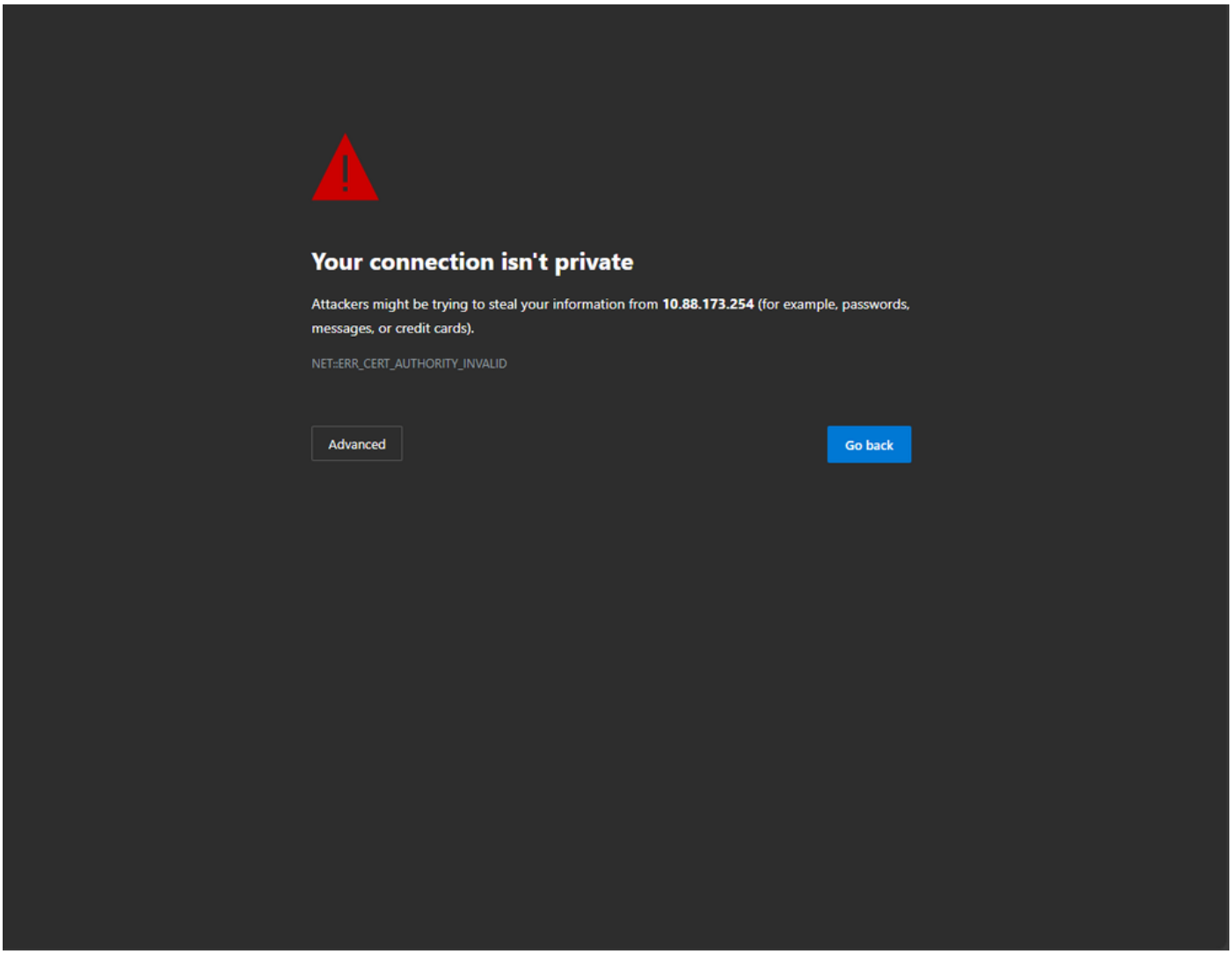
Locally Significant Certificate (LSC)

These certificates are solely used by APs that need to prove their identity to the WLC. They do not exist by default on neither the WLC nor the APs. The LSC certificates need to be signed by a CA and later installed on both the WLC and the APs to mutually validate each other. For more information on how to configure LSCs on the 9800 refer to Locally Significant Certificates.

Trustpoints

What is a Trustpoint?

A trustpoint is what links a certificate to a specific service. There are two main types of trustpoints: web administration and web authentication. By default, the WLC uses the self-signed certificate for both services, but this causes a warning message to pop-up stating that the site is not secure. This is because the self-signed certificate has not been validated by any CA.



CA Invalid Warning Message on Web Page

In order to avoid this, a third-party certificate can be used making sure that it has been validated already by a CA. For more information on how to generate and upload to the WLC a certificate, please refer to Generate and Download CSR Certificate on Catalyst 9800 WLCs.

Web Administration

The trustpoint for the web administration links the certificate to the user graphical user interface (GUI). The

controller selects one of its available certificates, and, if there is no custom certificate uploaded to the WLC, then the self-signed certificate is used. If the default certificate is not something you want to use, you can use a custom certificate for the trustpoint.

Once the certificate has been uploaded to the 9800, as per the document above, the next step is to link the trustpoint to the web administration, the next commands need to be entered:

```
configure terminal
ip http secure-trustpoint <custom-cert>.pfx
!Restart HTTP services
no ip http secure services
ip http secure services
end
write
```

One way to validate the newly installed certificate is now being used as a trustpoint for HTTP services, for example, enter the command **show ip http server status | include trustpoint**

<#root>

```
9800#show ip http server status | include trustpoint
```

HTTP secure server trustpoint: <trustpoint>.pfx <-- trustpoint configured for HTTP services

```
HTTP secure server peer validation trustpoint:
```

Web Authentication

Similar to web administration, layer 3 authentication can also be used on the 9800. This trustpoint links a certificate to a web portal that is shown to a user as it attempts to authenticate to a WLAN through a guest portal that is automatically presented to the user. Using a trustpoint for web authentication helps protect the user credentials between the WLC and the client that is connecting to.

By default, the WLC uses the self-signed certificate. Again, this causes a warning message to pop up for the client stating that the web page is not trusted. To avoid this, a 3rd party certificate can be used just as with the web administration.

Similar to web administration, once the custom certificate has been uploaded to the WLC, it must be linked to the web paramater map as trustpoint.

```
configure terminal
parameter-map type webauth global
trustpoint <custom-cert>
!Restart HTTP services
no ip http secure services
ip http secure services
end
write
```

To validate the trustpoint used for web authentication, enter the next command

<#root>

```
show run | section parameter-map type webauth global
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
```

trustpoint <custom-trustpoint> <-- trustpoint configured for web authentication

Related Information

- Locally Significant Certificates
- Generate and Download CSR Certificate on Catalyst 9800 WLCs