Official Cert Guide

Practice tests

Flash Cards

Review Exercises

Study Planner

CCNP and CCIE Security Core

SCOR 350-701

2nd Edition

ciscopress.com

Omar Santos

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, a Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to **ciscopress.com/register**.
2. Enter the **print book ISBN:** 9780138221263.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated in your account under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log in to the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

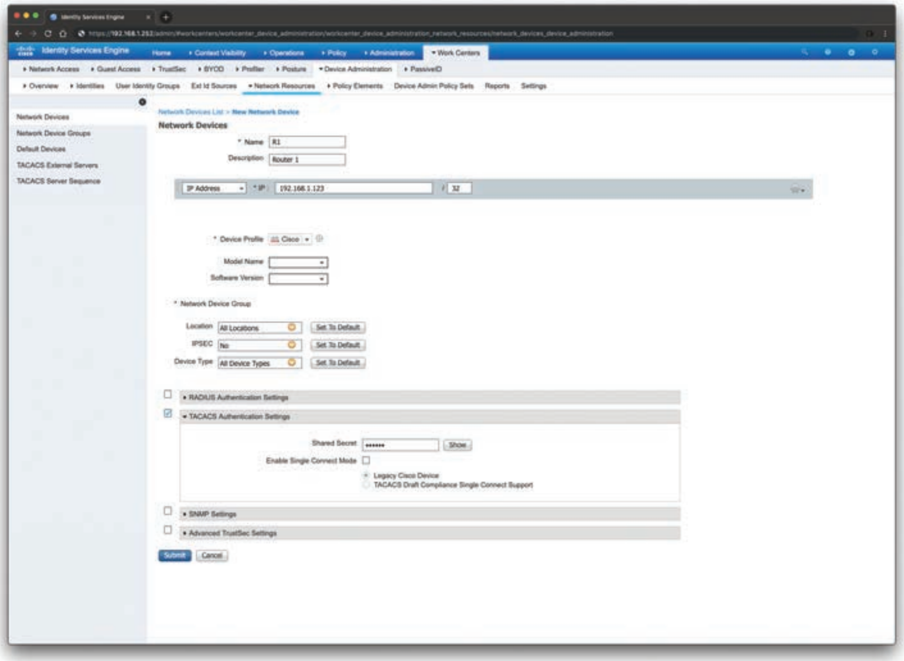
Example 4-2 *Debugging TACACS+ in the Router*

```
R1# debug tacacs
TACACS access control debugging is on
TPLUS: Queuing AAA Authentication request 102 for processing
TPLUS: processing authentication start request id 102
TPLUS: Authentication start packet created for 102()
TPLUS: Using server 192.168.1.252
TPLUS(00000066)/0/NB_WAIT/6812DC64: Started 5 sec timeout

User Access Verification

! Timing out on TACACS+ regarding authentication because no server is responding
TPLUS(00000066)/0/NB_WAIT/6812DC64: timed out
TPLUS(00000066)/0/NB_WAIT/6812DC64: timed out, clean up
TPLUS(00000066)/0/6812DC64: Processing the reply packet

! Now moving to the local database on the router
Username: admin
Password: supersecretpassword
! Timing out on TACACS+ regarding authorization due to no server responding.
TPLUS: Queuing AAA Authorization request 102 for processing
TPLUS: processing authorization request id 102
TPLUS: Protocol set to None .....Skipping
TPLUS: Sending AV service=shell
TPLUS: Sending AV cmd*
TPLUS: Authorization request created for 102(admin)
TPLUS: Using server 192.168.1.252
TPLUS(00000066)/0/NB_WAIT/6812DC64: Started 5 sec timeout
TPLUS(00000066)/0/NB_WAIT/6812DC64: timed out
TPLUS(00000066)/0/NB_WAIT/6812DC64: timed out, clean up
TPLUS(00000066)/0/6812DC64: Processing the reply packet
! After timing out, the router again uses its local database for
! authorization and appropriate privilege level for the user.

! If we exit, and change the debugs slightly, and do it again, it will give
! us yet another perspective.

R1# debug aaa authentication
AAA Authentication debugging is on
R1# debug aaa authorization
AAA Authorization debugging is on
AAA/BIND(00000067): Bind i/f
! Notice it shows using the authentication list we assigned to the vty
! lines
```

```
AAA/AUTHEN/LOGIN (00000067): Pick method list 'AUTHEN_via_TACACS'

! Not shown here, but indeed the ISE server is timing out, due to not yet
! being configured, which causes the second entry in the list "local" to
! be used.

User Access Verification
Username: admin
Password: supersecretpassword

! Now the authorization begins, using the method list we configured for
! the vty lines
AAA/AUTHOR (0x67): Pick method list 'Author-Exec_via_TACACS'
AAA/AUTHOR/EXEC(00000067): processing AV cmd=
AAA/AUTHOR/EXEC(00000067): processing AV priv-lvl=15
AAA/AUTHOR/EXEC(00000067): Authorization successful
R1#
```

NOTE The 300-715 SISE exam (Implementing and Configuring Cisco Identity Services Engine [SISE]) focuses on the configuration and troubleshooting of Cisco ISE. However, the following are a few examples of the Cisco ISE configuration for TACACS+ access.

To configure TACACS+ in Cisco ISE, navigate to **Work Centers > Device Administration > Network Resources** and add a network device. You will see the screen in Figure 4-40.



Network Devices

* Name: R1

Description: Router 1

IP Address * IP: 192.168.1.123 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations

IPSEC: No

Device Type: All Device Types

□ RADIUS Authentication Settings

☑ TACACS Authentication Settings

Shared Secret: ••••••

Enable Single Connect Mode □

● Legacy Cisco Device

○ TACACS Draft Compliance Single Connect Support

□ SNMP Settings

□ Advanced TrustSec Settings

Figure 4-40 *Adding a Network Device for TACACS+ Authentication in ISE*

In Figure 4-40, the Router (R1) details are entered. The **TACACS Authentication Settings** checkbox is selected, and a shared secret used to authenticate the TACACS+ session between the router and ISE is entered.

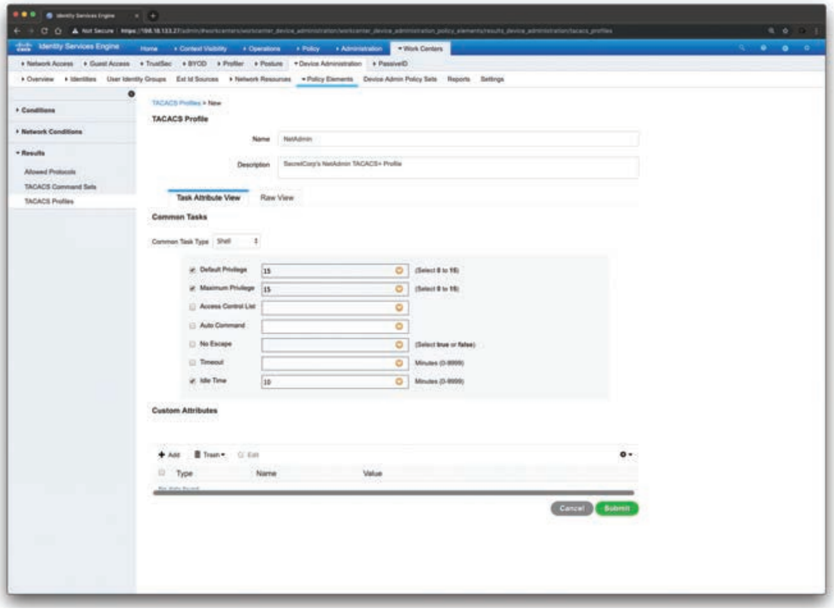
> **NOTE** The shared secret (password) must match the password entered in the router's configuration.

You can create different policies to support different groups of people who require access to the organization's infrastructure devices, as shown in Figure 4-41 (network administrators, network operators, security administrators, help desk support, and so on).

NetAdmin	NetOps	SecAdmin	Helpdesk
• Network admins who need full control of the network devices	• Network operators who receive full control of the network devices but are not permitted to erase the configuration	• Security admins who receive read-only access to view the configuration but not change anything	• Personnel who need to be able to see the status of certain commands, to aid in their assistance of employees and guests

Figure 4-41 *Different Groups of People Who Require Access to Infrastructure Devices*

To configure these groups and policies, navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles.** The screen in Figure 4-42 shows the TACACS+ profile of a NetAdmin.



TACACS Profiles > New

TACACS Profile

Name: NetAdmin

Description: SecretCorp's NetAdmin TACACS+ Profile

Common Tasks

Common Task Type: Shell

☑ Default Privilege 15 (Select 0 to 15)

☑ Maximum Privilege 15 (Select 0 to 15)

☐ Access Control List

☐ Auto Command

☐ No Escape (Select true or false)

☐ Timeout Minutes (0-9999)

☑ Idle Time 10 Minutes (0-9999)

Custom Attributes

☐ Type Name Value

No data found

Figure 4-42 *NetAdmin Profile*

Configuring RADIUS Authentication

You can configure RADIUS authentication in multiple scenarios, including Remote Access VPN, Secure Network Access, 802.1X, and more. Chapter 8, "Virtual Private Networks (VPNs)," provides examples of remote access VPN configurations using RADIUS authentication. In the following section, you will learn how RADIUS can be configured in network switches and Cisco ISE for secure access with 802.1X authentication.

Cisco IOS 15.2.x and Cisco IOS-XE 3.6.x switches follow the Cisco Common Classification Policy Language (C3PL) style of configuration. C3PL is a structured replacement for the configuration commands of various features in Cisco IOS and Cisco IOS-XE. C3PL allows administrators to configure traffic policies based on events, conditions, and actions. This provides some intriguing and advanced authentication features, as well as a very different configuration style that has powerful options, but it can be confusing when learning how to use it. However, many administrators who start to use this configuration style end up loving it and rarely want to go back to the classic methods of configuration.

TIP The default behavior of 802.1X is to deny access to the network when an authentication fails. In many of the early 802.1X deployments, this was a problem because it does not allow for guest access and does not allow employees to remediate their computer systems and gain full network access. The next phase in handling 802.1X authentication failures was to provide an "Auth-Fail VLAN" to allow a device/user that failed authentication to be granted access to a VLAN that provided limited resources. This was a step in the right direction, but it was still missing some practicality, especially in environments that must use MAC Authentication Bypass (MAB) for all the printers and other non-authenticating devices. With the default behavior of 802.1X, an administrator has to configure ports for printers and other devices that do not have supplicants differently from the ports where they plan to do authentication. In response to these issues, Cisco created Flexible Authentication (Flex-Auth). Flex-Auth enables a network administrator to set an authentication order and priority on the switch port, thereby allowing the port to attempt, in order, 802.1X, MAB, and then WebAuth. All of these functions are provided while maintaining the same configuration on all access ports, thereby providing a much simpler operational model for customers than is provided by traditional 802.1X deployments.

There are multiple methods of authentication on a switch port:

- 802.1X (dot1x)
- MAB
- WebAuth

With 802.1X authentication, the switch sends an identity request (EAP-Identity-Request) periodically after the link state has changed to up. Additionally, the endpoint supplicant should send a periodic EAP over LAN Start (EAPoL-Start) message into the switch port to speed up authentication. If a device is not able to authenticate, it merely waits until the dot1x timeout occurs, and then MAB occurs. Assuming the device MAC address is in the correct database, it is then authorized to access the network.

The default behavior of an 802.1X-enabled port is to authorize only a single MAC address per port. There are other options, most notably Multi-Domain Authentication (MDA) and Multiple Authentication (Multi-Auth) modes. During the initial phases of any Cisco TrustSec deployment, it is best practice to use Multi-Auth mode to ensure that there is no denial of service while deploying 802.1X.

TIP Port Security is not compatible with 802.1X, because 802.1X handles this function natively. You will learn more about Port Security in Chapter 6, "Infrastructure Security."

Multi-Auth mode allows virtually unlimited MAC addresses per switch port, and requires an authenticated session for every MAC address. When the deployment moves into the late stages of the authenticated phase, or into the enforcement phase, it is then recommended that you use MDA mode, which allows a single MAC address in the Data domain and a single MAC address in the Voice domain per port.

802.1X is designed to clearly differentiate a successful authentication from an unsuccessful authentication. Successful authentication means the user is authorized to access the network. Unsuccessful authentication means the user has no access to the network. This is problematic in a lot of environments. Most modern environments need to do workstation imaging with Preboot Execution Environments (PXEs), or they don't have any way to run a supplicant because they may have some thin clients that do not support it. When early adopters of 802.1X deployed authentication companywide, there were repercussions. Many issues arose. For instance, supplicants were misconfigured; there were unknown devices that could not authenticate because of a lack of supplicant, and other reasons.

TIP Cisco created Open Authentication to aid with deployments. Open Authentication allows all traffic to flow through the switch port, even without the port being authorized. This feature permits authentication to be configured across the entire organization, but does not deny access to any device.

Key Topic

Several devices that support the Cisco Common Classification Policy Language (C3PL) style of configuration still accept the old style of commands. The legacy style of commands is the default in most of those platforms, and you must enable the C3PL style of commands with the global configuration command **authentication display new-style**. Even if the name of the command includes the word "display," the command changes much more than just the display of the commands. It also changes the way the network administrator interacts with the switch and configures the device. You can change back to the classic model using the **authentication display legacy** command.

TIP After you start configuring the C3PL policies, you cannot revert to the legacy mode. You can only switch back if you haven't configured C3PL yet, that is, unless you erase the switch configuration and reload or restore an older backup configuration.

The C3PL syntax offers many benefits, most of which are transparent to the end user. For instance, C3PL allows the network device configuration to exist in memory once and be invoked multiple times. This is a resource efficient enhancement.

There are several additional benefits from the C3PL model. For example, 802.1X and MAB can run simultaneously without having to sequence the two distinctive authentication processes, whereas 802.1X authentication has to be failed for MAB to start when not using the C3PL model. You can also use service templates to control preconfigured access control lists on given interfaces in the event of RADIUS not being available.

In legacy devices, the sequencing of 802.1X and MAB can result in certain MAB endpoints not being able to obtain IP addresses via DHCP in a timely manner. Newer devices can process 802.1X and MAB simultaneously, allowing endpoints to obtain a DHCP-assigned IP address in a timely manner. Additionally, legacy devices require a static ACL often applied to interfaces in order to restrict network access for devices that have not yet authenticated. Consequently the ACL remains applied to devices attempting to connect while the RADIUS server is unavailable. This condition results in a denial of service until the RADIUS server is reachable. This may seem desirable in theory, but it is not recommended. This behavior actually makes life more difficult for the policy server administrator.

The ability to create service templates is a good enhancement of C3PL. A separate ACL that would permit network access can be applied to the interface using service templates. These rules can be configured to perform an action under a certain condition, such as when the RADIUS server is not reachable. This feature is known as the "Critical ACL functionality."

In addition, C3PL provides differentiated authentication. The differentiated authentication feature enables you to authenticate different methods with different servers. For instance, you can send MAB to one server and 802.1X authentications to another. Another interesting feature in C3PL is Critical MAB. Critical MAB allows the switch to use a locally defined list of MAC addresses when the centralized RADIUS server is unavailable.

Configuring 802.1X Authentication

Let's take a look at the topology shown in Figure 4-43. You are being hired to configure 802.1X in SecretCorp. The goal is to deploy 802.1X authentication in all of SecretCorp's switches and use ISE. SecretCorp's switch 1 (sc-sw1) is used in this example.

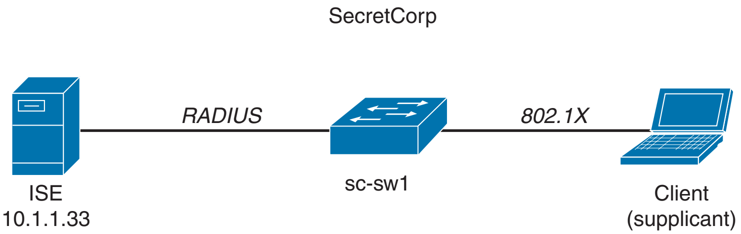


Figure 4-43 *SecretCorp 802.1X Deployment*

First, you need to configure certificates for URL redirection. To configure certificates for URL redirection, perform the following steps from global configuration mode on the switch (sc-sw1):

Step 1. Configure the DNS domain name on the switch. The domain name is **secretcorp.org.**

```
sc-sw1(config)# ip domain-name secretcorp.org
```