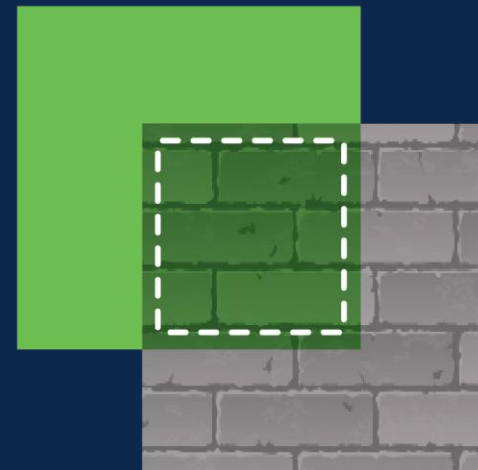


Firewall Ignite

Hands-on SE Pre-Sales Training



Agenda



- ▶ Training Overview
- ▶ Event Logistics and Requirements
- ▶ Licensing Steps
- ▶ Q & A

Training Agenda



Audience

- Presales SE training

Pre-event (you are here)

- Purpose of training – Hands on to build a home/office lab for learning, testing and demoing
- Requirements for hands-on training (SCC tenant)

Training Agenda

(Full day,
lunch included)

Hands-on setup and provisioning of new Firewall
Vision and Strategy

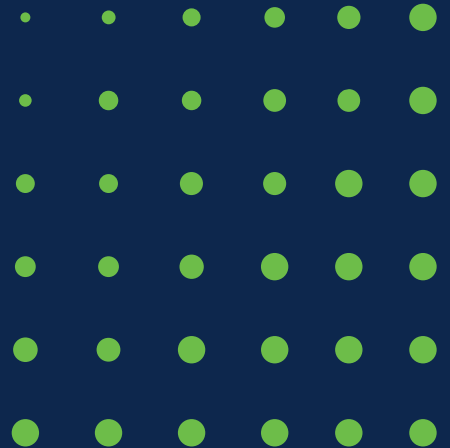
Focus on the primary firewall use case

1. Provision for branch direct Internet access
2. SDWAN Overview
3. Threat
4. Remote Access VPN

Post Event

- Additional use cases shared to expand knowledge

Training Event Logistics



Cisco Account

The training labs are in Cisco's dCloud environment, which requires a Cisco Account (CCO) to access.

Sign up at <https://id.cisco.com>



Log in

Email

Next

[Unlock account?](#)

[Forgot email address?](#)

[Help](#)

Don't have an account? [Sign up](#)

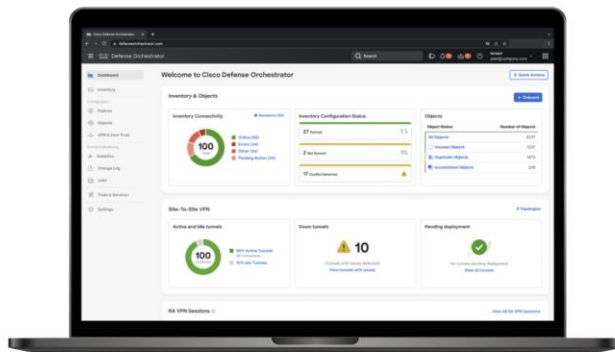
Security Cloud Control (SCC)

Part of the training will involve using your own personal SCC account.

Sign up at <https://getcdo.com>*



Security Cloud Control



Staying on top of security is easier than ever. Security Cloud Control helps you consistently manage policies across your Cisco security products. It is a cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.

Security Cloud Control is also home to Cisco Multicloud Defense, which connects, protects, and unifies security across environments at cloud speed and scale.

Begin your experience of managing:

- Secure Firewall Threat Defense (FTD)
- Cisco Multicloud Defense
- Secure Firewall ASA
- and more

Let's get started!

1

Select your region

2

Log in to your existing Cisco account or create a Cisco account

3

Get started with Security Cloud Control

Select Your Region 1

India

Sign Up



Defenses Orchestrator

Search

awesome-cisco-ignite-partner
adam@symposi.com

Hide Menu

Dashboard

Multicloud Defense

Inventory

Configuration

Policies

Objects

VPN

Events & Monitoring

Analytics

Change Log

Jobs

Tools & Services

You are in a free trial of CDO with 30 days left.

Upgrade to full version

Welcome to Cisco Defense Orchestrator

Quick Actions

Multicloud Defense

Connect a cloud account

Gain visibility and control of what's happening in your cloud environment while ensuring they are managed securely.

[Learn more](#)

CDO Full Version

Thank you for choosing Cisco Defense Orchestrator! Please enter your sales order number to begin using the full version of CDO.

Sales Order Number

IGNITE2024

Cancel Save

Secure Account

Setup a Service VPC and Multi-Cloud gateway to secure your account

[Get started](#)

[+ Onboard](#)

PARTNERS ONLY

Select **Upgrade to Full Version** within the trial banner enter **IGNITE2024** within the prompt.

☰ Hide Menu

 Dashboard

 Multicloud Defense

 Inventory


Configuration


 Policies >

 Objects

 VPN >

Events & Monitoring

 Analytics >

 Change Log

 Jobs

 Tools & Services >

 Settings >

 You are in a free trial of CDO with **30 days left**.

[Request an extension](#)

[Upgrade to full version](#)

Welcome to Cisco Defense Orchestrator

[Quick Actions](#)

Multicloud Defense

[Get started](#) 

Connect a cloud account

Gain visibility and control of what's happening in your cloud environments while ensuring they are managed securely.
[Learn more](#)



Connect Cloud Accounts

Connect a cloud account with the Multi-Cloud Controller



Enable Traffic Visibility

Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account



Secure Account

Setup a Service VPC and Multi-Cloud gateway to secure your account

Inventory & Objects

[+ Onboard](#)



No Active Jobs

Cloud-Delivered Firewall Management Center (cdFMC)

Within SCC we utilize cdFMC, which must be provisioned in advance.

<https://defenseorchestrator.com>

From within SCC:

1. *Administration > Integrations > Firewall Management Center*
2. *Enable Cloud-Delivered FMC*

- General Settings
- User Management
- Notification Settings

Integrations

Secure Connectors

Firewall Management Center

Multicloud Defense Management

Home

Monitor

Events & Logs

Manage


Objects

Security Devices


Secure Connections

Administration


Follow the steps below




Firewall Management Center
Cisco Secure Firewall Management Center




Enable Cloud-Delivered FMC
Add a Cloud-Delivered FMC to your tenant





Use Credentials
Onboarding a device using an IP address or host name and a username and password (Version 6.4+)




 Home


Monitor


 Insights & Reports >


 Events & Logs >


Manage

 Objects

 Security Devices



 Secure Connections >

 Administration >



Use the cloud-delivered Firewall Management Center (cdFMC) in Security Cloud Control (SCC) to configure security policies, establish virtual private networks, and monitor network traffic in your Cisco Secure Firewall Threat Defense devices. See [Introduction to cdFMC](#) for details about the features available in cdFMC. Click **Enable cdFMC** to add cdFMC to this tenant.


Enable cdFMC



FMC

Secure Connectors

Multicloud Defense


<input type="checkbox"/>	Name	Version	Devices	Type	Status	Last Heartbeat
<div></div> <div>No results found</div>						


Training Registration

When you attend the training workshop, you will provide us your SCC Tenant Name


<https://defenseorchestrator.com>


Go to Administration > *General Settings* to find it.




 Home


Monitor


 Insights & Reports >


 Events & Logs >


Manage


 Policies >


 Objects

 Security Devices

 Secure Connections >

 **Administration**

Administration 

General Settings 

User Management

Notification Settings

Log Settings

Integrations

Secure Connectors

Firewall Management Center

Multicloud Defense Management


Dynamic Attributes Connector

Migration


Firewall Migration Tool

Migrate FTD to cdFMC


General Settings

Enable the option to schedule automatic deployments 

☐

Web Analytics 

☒

Default Recurring Backup Schedule 

Frequency

Time (UTC +00:00) :

Su ☒ Mo ☐ Tu ☐ We ☐ Th ☐ Fr ☐ Sa

Auto onboard On-Prem FMCs from Cisco Security Cloud

☒

Tenant ID

c05fe3d9-5827-46ad-97c4-e4dd96bbbf47

Secure Services Exchange Tenant ID

c05fe3d9-5827-46ad-97c4-e4dd96bbbf47

Tenant Name

CDO_cisco-esherwoo-roadshow

AttackIQ

Breach and Attack Simulation Tool

- Part of the workshop uses a tool called Attack IQ for efficacy testing.
- This is a breach and attack simulation tool that you can continue to use for demo, lab, and POV purposes.
- AttackIQ is a third party, the Flex package is an EXE for Windows workstations.

ATTACKIQ

Real-time Cybersecurity Readiness.

Get your cybersecurity program tested against real-world threats, optimized for effectiveness, and ready for future attacks.

AttackIQ Flex

Instant testing and remediation recommendations on a pay-as-you-go model.

Agentless test-as-a-service. Run full security control assessments with the click of a button.

AttackIQ Ready!

A fully managed weekly and monthly baseline of testing and remediation recommendations.

AttackIQ Ready! is a fully managed breach and attack simulation as a service. It provides continuous and on-demand security control validation with clear results and remediation guidance.

AttackIQ Enterprise

Customers manage the AttackIQ BAS Platform with AttackIQ as your co-pilot.

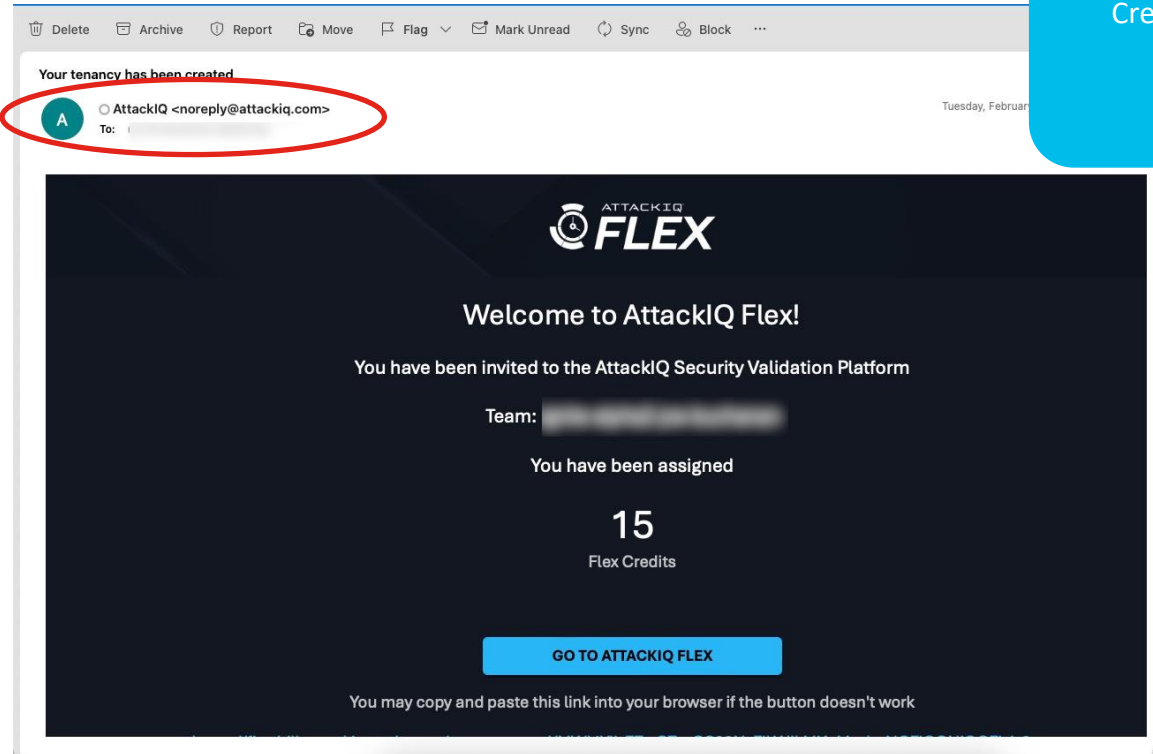
The full AttackIQ Breach and Attack Simulation Platform. Customers gain full access to the AttackIQ library of content, giving you comprehensive testing and remediation data along with the constant support of our team of experts.

Great value using a commercial solution!!

No cost to you

Credits subject to change. Current allocations:

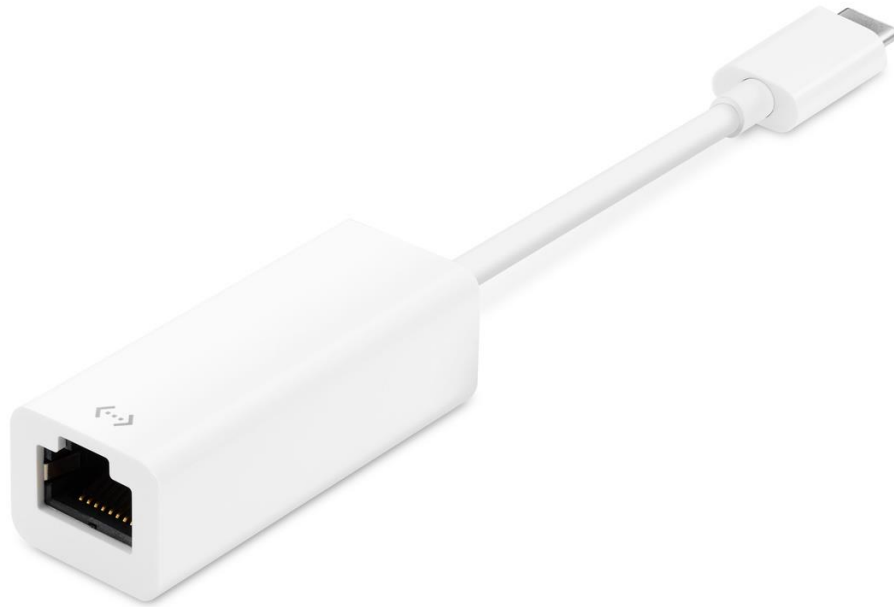
- 10 for attending class
- 10 for completing Certificate process
- 10 for registering an opportunity



- You will receive an email from AttackIQ inviting you to create an account with only 7 days to activate!
- Keep your custom AttackIQ URL from your email that will be used during class.

On the day of training

- Bring your **laptop**
- **Ethernet** is required so bring a USB to Ethernet adapter if your laptop needs an **adapter**, along with a **short ethernet cable**.
- **Tablet** or portable display is optional but recommended
- **Lab guides** will be shared at the event



Licensing

You will need a Smart Virtual Account and request the below license PIDS be deposited in your account prior to class

- L-AC-APX-LIC-SMART
= (Remote Access VPN)
- L-FPR1010T-TMC
= (Threat/Malware/URL Features)

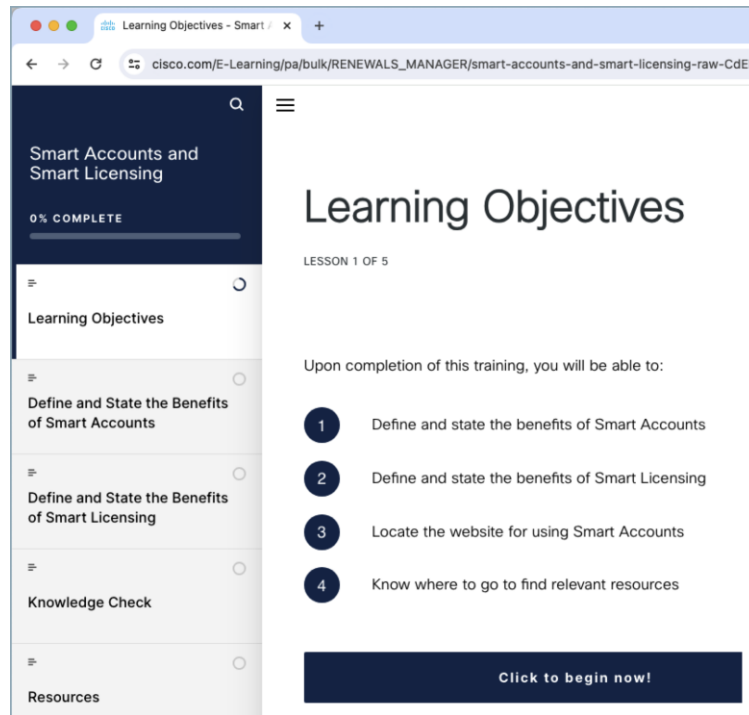
What is Smart Licensing?



https://www.cisco.com/E-Learning/pa/bulk/RENEWALS_MANAGER/smart-accounts-and-smart-licensing-raw-CdEI-zDg/content/index.html#/

Also, Cisco Licensing 101 Training
<https://community.cisco.com/t5/smart-licensing-enterprise-agreements-saas-knowledge-base/cisco-licensing-101-training-january-2024/ta-p/4685602>

(Optional) If you are unfamiliar with Smart Licensing, scan the QR Code to find a training module on the topic.



How do I find or create a Smart Account?

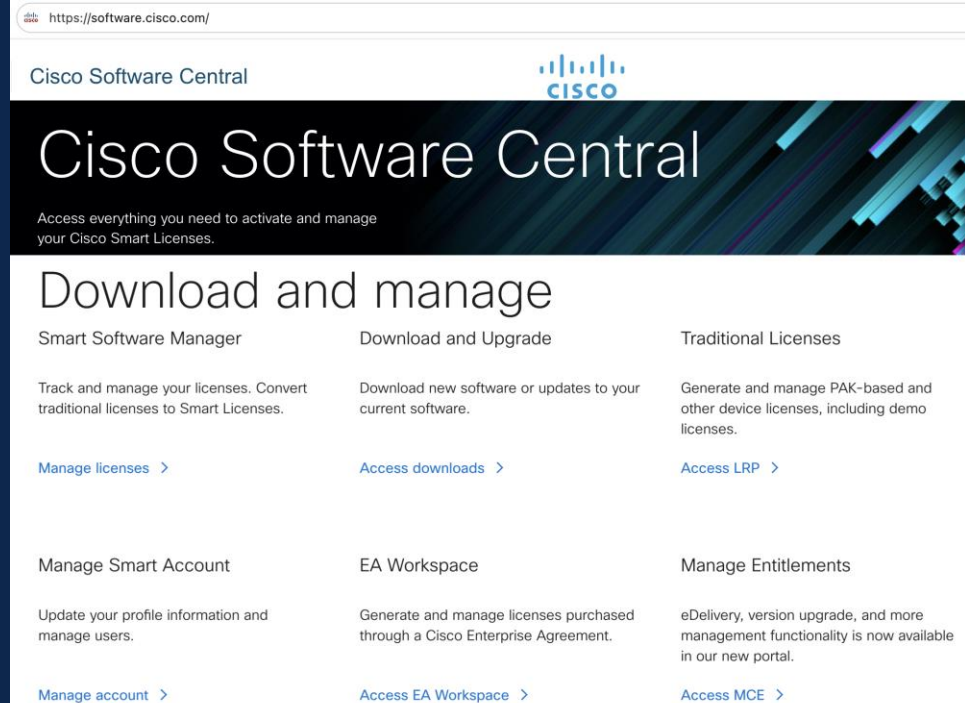
From software.cisco.com

You can:

- Manage Account
- Manage Licenses

Scroll down on page

- Create a new account
- Open a TAC case



The screenshot shows the Cisco Software Central website. The header includes the Cisco logo and the text "Cisco Software Central". Below the header, the main heading "Cisco Software Central" is displayed, followed by the subtext "Access everything you need to activate and manage your Cisco Smart Licenses." The main content area is titled "Download and manage" and contains six sections arranged in a 2x3 grid:

Smart Software Manager	Download and Upgrade	Traditional Licenses
Track and manage your licenses. Convert traditional licenses to Smart Licenses.	Download new software or updates to your current software.	Generate and manage PAK-based and other device licenses, including demo licenses.
Manage licenses >	Access downloads >	Access LRP >
Manage Smart Account	EA Workspace	Manage Entitlements
Update your profile information and manage users.	Generate and manage licenses purchased through a Cisco Enterprise Agreement.	eDelivery, version upgrade, and more management functionality is now available in our new portal.
Manage account >	Access EA Workspace >	Access MCE >

Cisco Employees ONLY

Cisco Employees follow the process on this site if you don't have a Smart Account
<https://cs.co/FWIgnite-internal>

software.cisco.com/software/cs/smartaccount/internalAccess

Cisco Software Central

Scheduled Downtime Notification - License Registration Portal (LRP), Manage Smart Account & Account Administration, Plug-N-Play (PNP), Smart Software Manager (SSM), Cisco Device Activation(CDA) and Enterprise Agreement

Cisco Software Central > Internal Access

Request Access to an Existing Smart Account

Welcome to the site for requesting Smart Accounts for internal use. This page is maintained by the Smart Accounts Operation Team.
New Smart Accounts are not provided for Internal Cisco users. However, you can leverage existing Smart Accounts for demos or test order purchases.

Please follow the steps below to get started:

- a. Search if a test account is already setup for your BU or Product by
 - a. Business Unit Name or the Product Name
 - b. CCO ID of known colleagues from your BU or Product Name
- b. If you find that a test account is already setup for your need, you can view the information of the current users
- c. If no test account is setup for your need, create a new Virtual Account

Search for **Internal** Accounts By:

☒ BU Name or Product Name

☐ CCO ID of a known colleague

- OR -

Search for **Customer** Smart Accounts By:

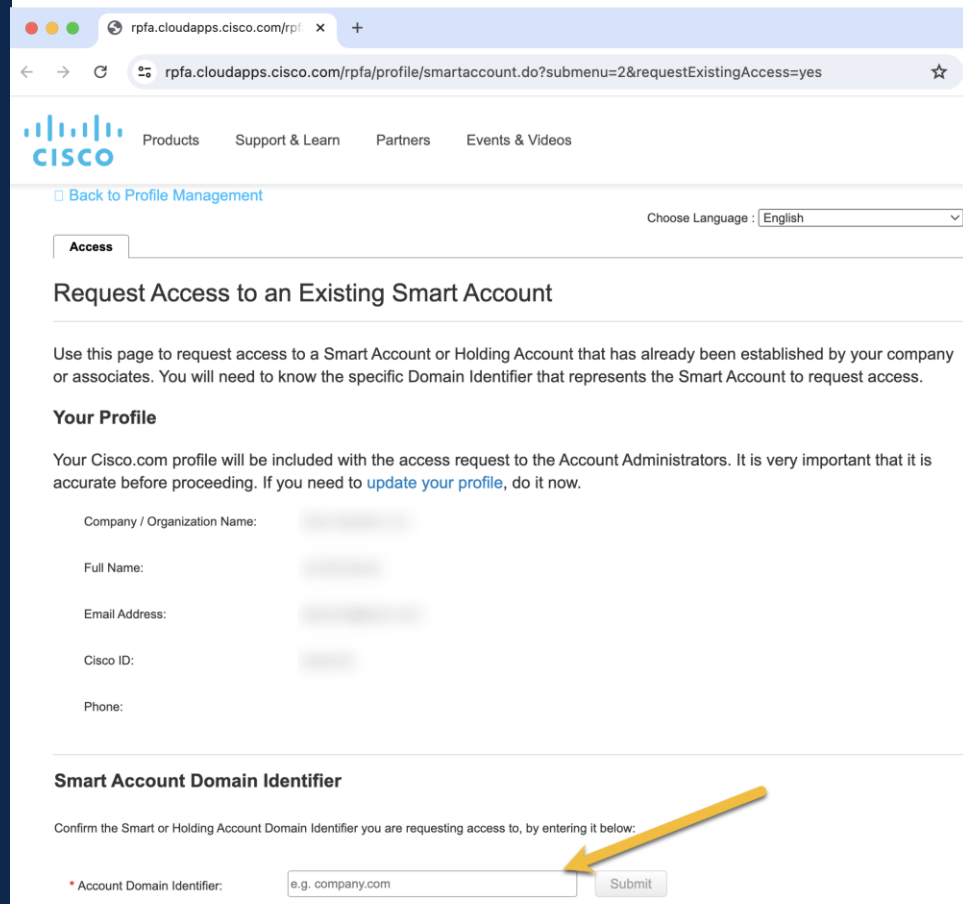
☐ Account Name or Domain



For Partners Request Access to an Existing Smart Account

Reference:

<https://rpfa.cloudapps.cisco.com/rpfa/profile/smartaccount.do?submenu=2&requestExistingAccess=yes>



The screenshot shows a web browser window with the URL `rpfa.cloudapps.cisco.com/rpfa/profile/smartaccount.do?submenu=2&requestExistingAccess=yes`. The page features the Cisco logo and navigation links for Products, Support & Learn, Partners, and Events & Videos. A 'Back to Profile Management' link is present. A language dropdown menu is set to 'English'. The 'Access' tab is selected, leading to the 'Request Access to an Existing Smart Account' section. This section includes a paragraph explaining the purpose of the page and a 'Your Profile' section with input fields for Company / Organization Name, Full Name, Email Address, Cisco ID, and Phone. Below this is the 'Smart Account Domain Identifier' section, which instructs the user to confirm the domain identifier and provides a text input field with the placeholder 'e.g. company.com' and a 'Submit' button. A yellow arrow points to the 'Submit' button.

rpfa.cloudapps.cisco.com/rpfa/profile/smartaccount.do?submenu=2&requestExistingAccess=yes

Products Support & Learn Partners Events & Videos

[Back to Profile Management](#) Choose Language : English

Access

Request Access to an Existing Smart Account

Use this page to request access to a Smart Account or Holding Account that has already been established by your company or associates. You will need to know the specific Domain Identifier that represents the Smart Account to request access.

Your Profile

Your Cisco.com profile will be included with the access request to the Account Administrators. It is very important that it is accurate before proceeding. If you need to [update your profile](#), do it now.

Company / Organization Name:

Full Name:

Email Address:

Cisco ID:

Phone:

Smart Account Domain Identifier

Confirm the Smart or Holding Account Domain Identifier you are requesting access to, by entering it below:

* Account Domain Identifier:

For Partner ONLY

If you are unable to connect to your company's Smart Account, you can set up a personal Smart Account using your own email address (e.g., @gmail.com or @icloud.com).

To do this, you will need to open a case with the TAC team to add a prefix to your public domain email.

You can submit the TAC request through the software.cisco.com page.

Pro Tip: When setting up a personal Smart Account, make sure to configure your CCO profile with two separate addresses: one for your personal use and one for your organization. This means you will need to add a new address twice.

Perform these steps to have licensing applied to your Smart Account prior to training.

1. Create 1 case using the text to the right:
<https://cep.cloudapps.cisco.com/#/pov>
2. Use request type and description as shown
3. Edit and paste in the description to include **your Smart Account information** and submit.



Request type:

- Primary Technology = Network Security
- Title = Licensing for Firewall Ignite Training

Description:

Lab licenses for Firewall Ignite training program.

Please deposit the below lab licenses for the Firewall Ignite training program into my smart account.

Product type [FTD & AnyConnect]

PIDs:

- L-AC-APX-LIC-SMART= (Remote Access VPN) - Quantity 1
- L-FPR1010T-TMC= (Threat/Malware/URL Features) Quantity 1
- Sensor type: [Cisco Firepower Threat Defense Hardware 1010 Appliance]
- Smart Account Domain ID [----- .com]
- Smart Account [-----]
- Smart Virtual Account [-----]
- Duration: 365 Days

Yours after training...

- FTD 1010 for demo/lab use
- Personal SCC tenant with cdFMC provisioned
- Certificate of Completion*
- AttackIQ Credits (great value!)
 - *Credits subject to change. Current allocations:*
 - 10 for attending class*
 - 10 for completing Certificate process*
 - 10 for registering an opportunity*
- Memories to cherish

Prerequisite Summary

1. You must have a Cisco Account. If needed, sign up at <https://id.cisco.com>.
2. You must have a Security Cloud Control tenant. If needed, request one at <https://getcdo.com>.
3. Once provisioned, enable Cloud-Delivered FMC. Login to SCC at <https://defenseorchestrator.com> then:
 - a) Administration > Integrations > *Firewall Management Center*.
 - b) Click *Enable Cloud-Delivered FMC*.
4. Be on the lookout for an email from noreply@attackiq.com to activate your AttackIQ account!
5. Capture your custom URL provided within the above AttackIQ email so you have for the day of training.
 - Use <https://firedrill.attackiqready.com> to find your custom URL if you loose.
6. Request license PIDS as outlined in the above licensing section.
7. Bring laptop, **ethernet adapter and short ethernet cable**, tablet/screen (optional) to training event.



Q & A



The bridge to possible