



Cisco UCS Director Tech Module

Cisco Adaptive Security Appliance (ASA & ASAv)

Version: 1.0

September 2016

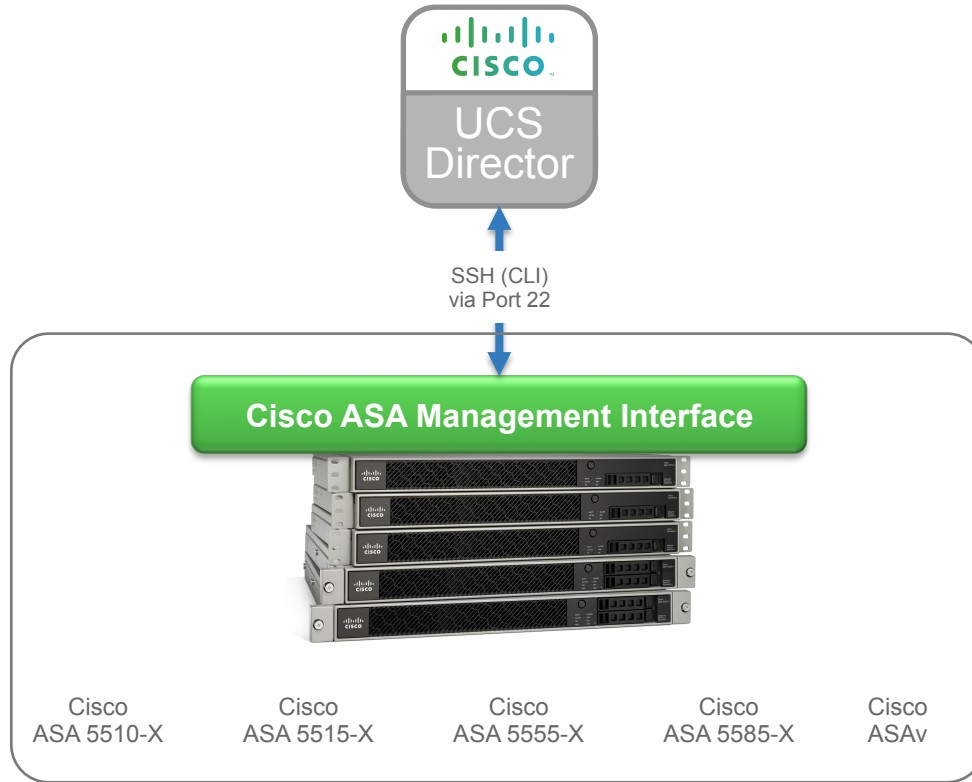
Agenda

- Overview & Architecture
- Hardware & Software Compatibility
- Licensing
- Orchestration Capabilities
- Reports
- Example Use-Cases



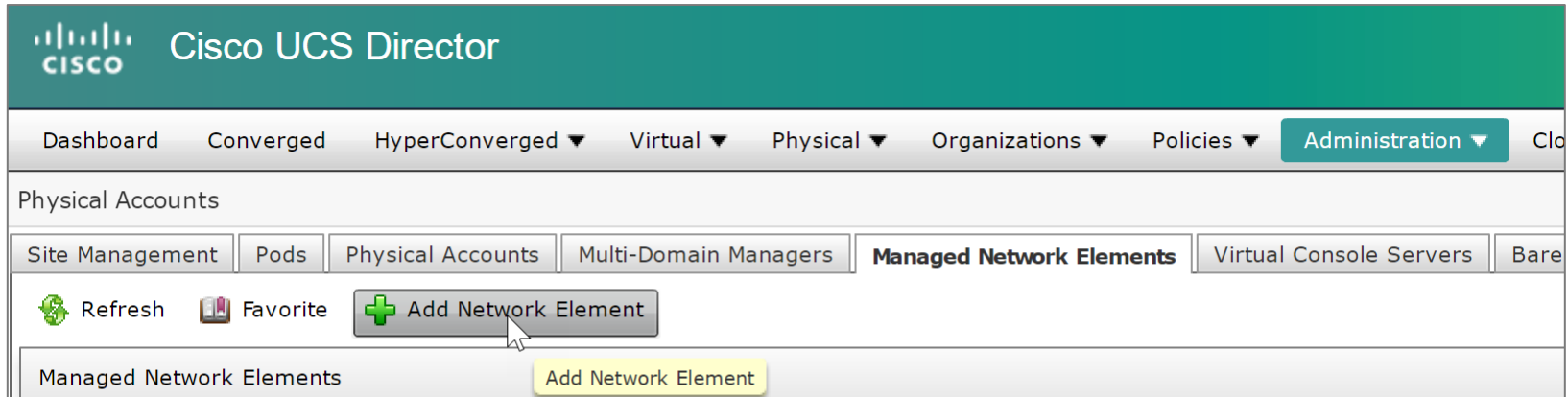
Architecture & Overview

UCS Director – ASA Integration Architecture



Adding an ASA Account

- Navigate to **Administration** → **Physical Accounts**, choose the **Managed Network Elements** tab and click **Add Network Element**



The screenshot displays the Cisco UCS Director web interface. At the top, the Cisco logo and 'Cisco UCS Director' are visible. Below this is a navigation bar with tabs for Dashboard, Converged, HyperConverged, Virtual, Physical, Organizations, Policies, Administration, and Close. The 'Administration' tab is selected. Underneath, the 'Physical Accounts' section is active, with sub-tabs for Site Management, Pods, Physical Accounts, Multi-Domain Managers, Managed Network Elements, Virtual Console Servers, and Bare. The 'Managed Network Elements' sub-tab is selected and highlighted. In this sub-tab, there are three buttons: Refresh, Favorite, and Add Network Element. The 'Add Network Element' button is highlighted with a yellow background, and a mouse cursor is pointing at it.

Adding a ASA Account

- Enter the information about the ASA device to add the account

Add Network Element

Pod *

Device Category

Device IP *

Use Credential Policy

Protocol

Port

Login *

Password *

Enable Password



Hardware & Software Compatibility

IMPORTANT!!

- The following slide featuring support information may be out of date
- **ALWAYS** check the most up to date version of the UCS Director Compatibility Matrix
- The latest Compatibility Matrix and other supporting UCS Director documentation can be found at the following location:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html

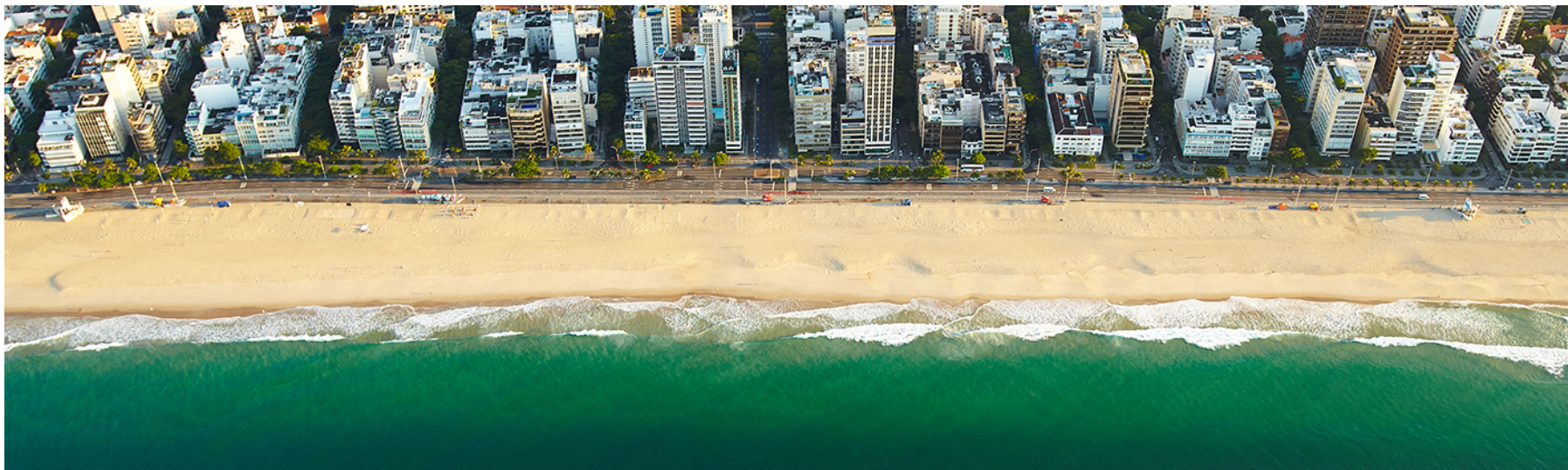
UCS Director Cisco Physical ASA Support

(as of UCS Director 6.0)

Supported Models	Supported Software (NX-OS)
ASA 5510-X	8.4(5) 9.1(5)
ASA 5515-X	9.1(1) 9.1(2) 9.3(1)
ASA 5555-X	9.5(2)
ASA 5585-X	9.1(2) 9.3(1) 9.4(1) 9.4(2) 9.5(2)

UCS Director Cisco Virtual ASA (ASA v) Support (as of UCS Director 6.0)

Supported Models	Supported Software (NX-OS)
ASA v	9.1(2) 9.2(0) 9.3(1) 9.3(2) 9.4(2) 9.5(2)



Licensing

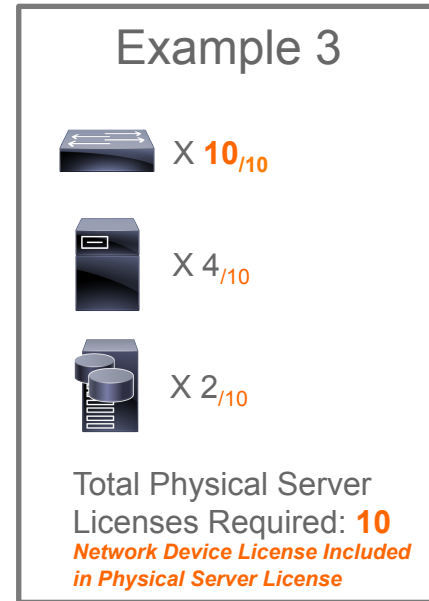
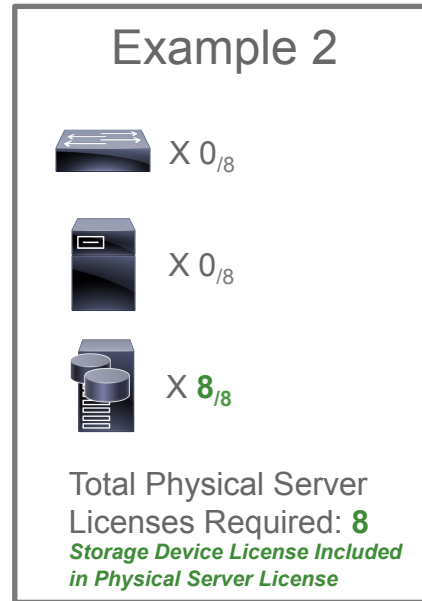
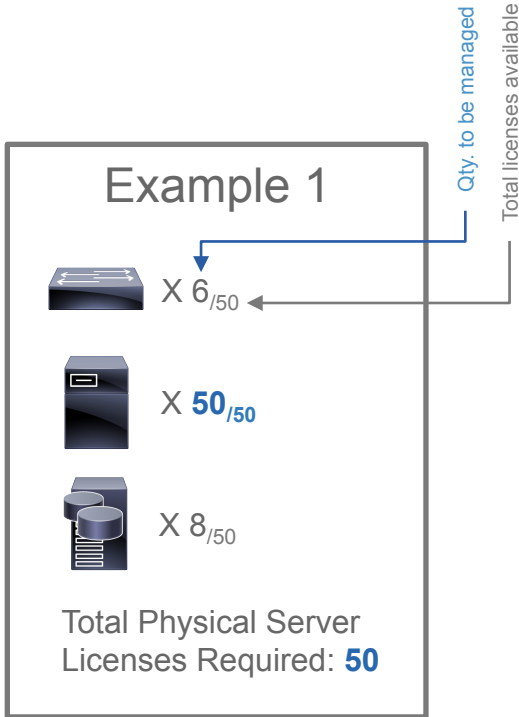
Licensing Information

- UCS Director licensing is purchased solely in the form of physical server licenses
- Each physical server license includes a storage device license and a network device license as well.
- UCS Director tracks the number of physical servers, storage and network devices being managed against the number of installed licenses.
- If additional storage and/or network device licenses are required, you can purchase additional physical server licenses

Licensing Information

- Each managed/added ASA account, whether physical or virtual, is counted as a network device license in UCS Director
- **NOTE!:** network device licenses are included in and solely available by purchasing additional physical server licenses for UCS Director

Licensing Examples





Orchestration Capabilities

Orchestration Capabilities

- UCS Director provides Orchestration tasks to automate ASA configurations to provision and de-provision the below objects. (as applicable to the platform)
 - Security Context
 - Sub-Interfaces
 - Context Interface
 - Context ACL
 - Context NAT
 - NAT
 - Licensing
 - Firewall Mode
 - ASA v OVF deployment

Orchestration Capabilities

Security Context

- Create Security Context
- Remove Security Context

NAT

- Configure Context NAT
- Configure NAT

ACL

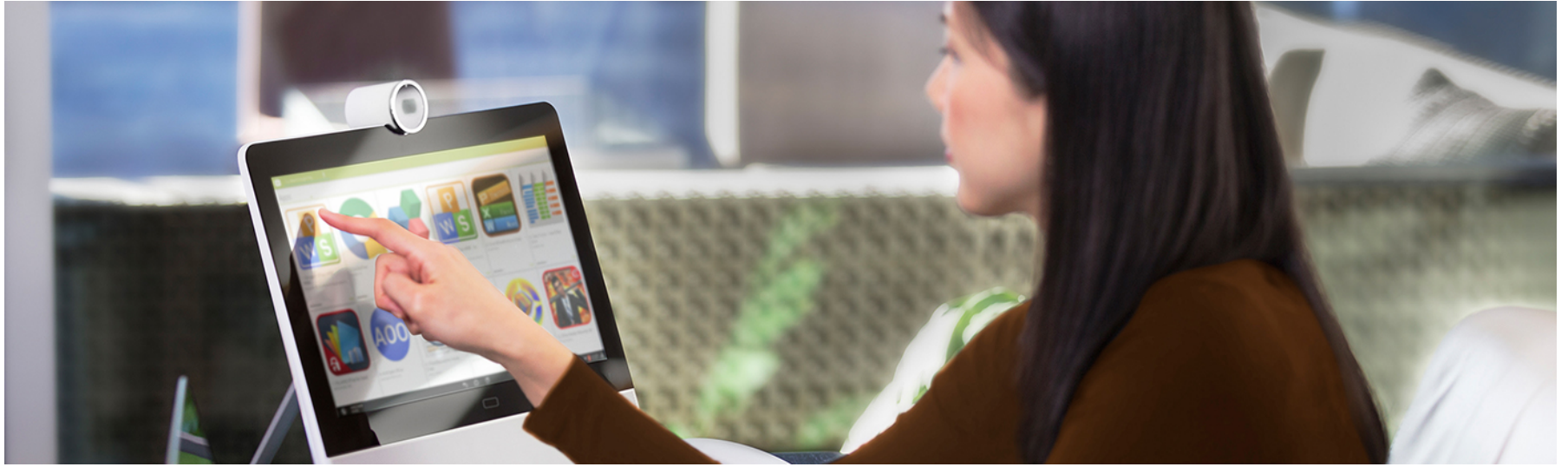
- Configure Context ACL

Interfaces

- Configure Sub Interface
- Configure Context Interface

Other

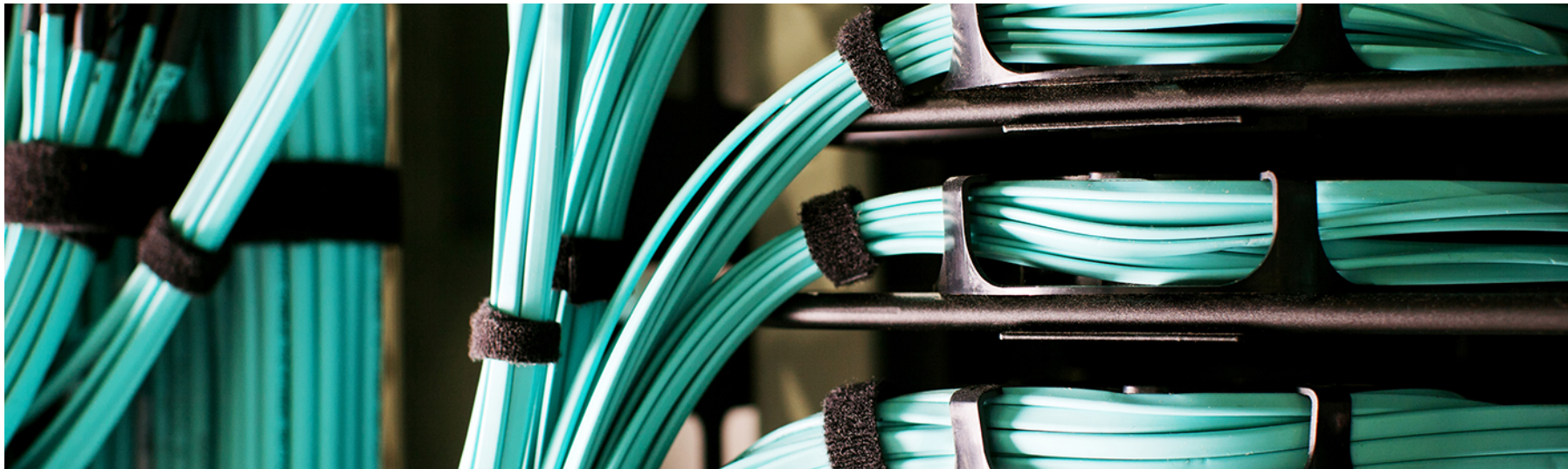
- Deploy ASA v OVF
- TrustSec Refresh
- Configure License
- Configure Cisco ASA Firewall Mode



Reports

Tabular Reports and Information

- Configurations
- Modules
- Interfaces
- Licenses
- ASA Contexts
- ACL
- SXP Connection Peers
- SGT
- Service Request Details



Example Use-Cases

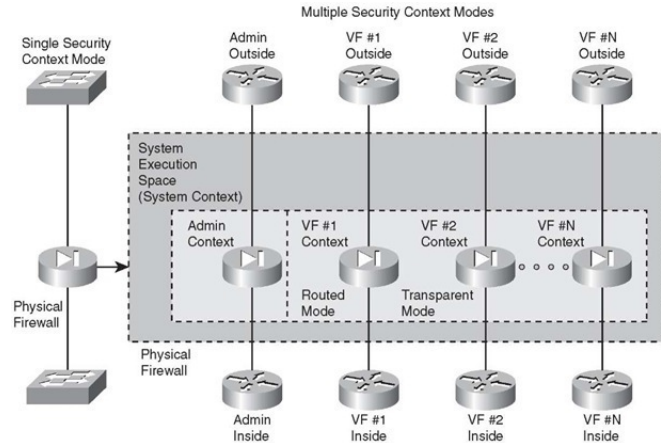
Example Use-Cases

Use-Case #1: Create Security Context on Physical ASA

Use-Case #2: Configure any ASA commands unsupported by UCSD

Use Case # 1

- Physical ASAs can be logically divided into multiple firewall instances (security contexts), with each context operating independently and has separate configuration, interfaces and policies



Use Case # 1

- UCSD has in-built task for workflows as well as 1-click button to create security context

The screenshot displays the Cisco UCS Director web interface. The top navigation bar includes 'Dashboard', 'Converged', 'HyperConverged', 'Virtual', 'Physical', 'Organizations', 'Policies', 'Administration', 'CloudSense™', and 'Favorites'. The main content area is titled 'Network for ASA5585X-1-R16-P' and features a sub-navigation menu with 'Summary', 'Configurations', 'Modules', 'Interfaces', 'Licenses', 'ASA Contexts', 'ACL', 'SXP Connection Peers', 'SGT', and 'Service Request Details'. The 'ASA Contexts' tab is active, showing a table with columns for 'Device IP', 'Context Name', and 'Allocated Interfaces'. A 'Create Asa Context' button is highlighted with a yellow tooltip. The table contains two entries:

Device IP	Context Name	Allocated Interfaces	
172.31.242.136	admin	Management0/0	disk0:/admin.cfg
172.31.242.136	Context1	GigabitEthernet0/2, GigabitEthernet0/3	disk0:/context1.cfg


Use Case # 1

Click on 'Create ASA Context' (from location shown in previous task) and provide below inputs.

The screenshot shows the 'Create Asa Context' configuration window with the following fields and callouts:

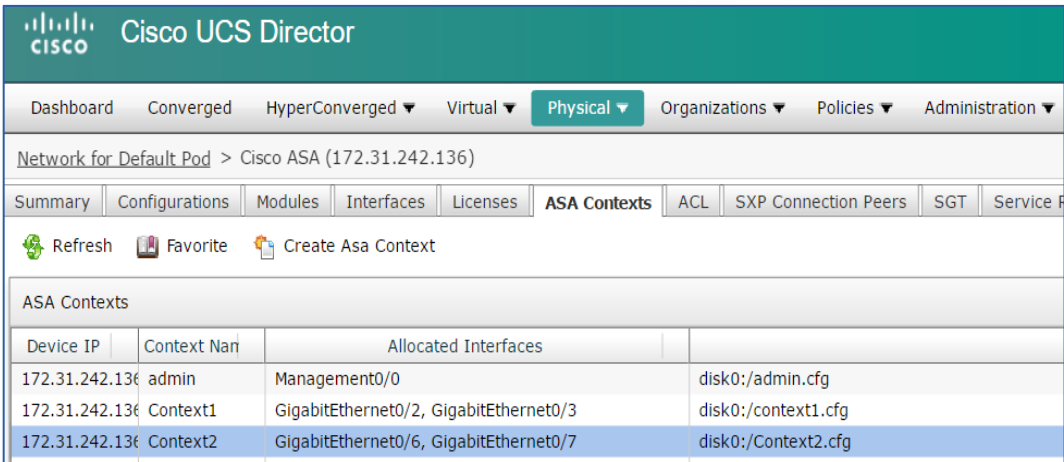
- Context Name:** context2 (Callout: Context Name)
- Context Description:** Created by UCSD (Callout: Context Description)
- File Name:** Context2.cfg (Callout: Disk0 Config File)
- OutSide Interface Name:** GigabitEthernet0/6 (Callout: Allocate Outside Interface)
- Inside Interfaces:** Select... GigabitEthernet0/7 (Callout: Allocate Inside Interface)
- Mode:** Routed (Callout: Context Mode – Transparent or Routed (default))
- Copy Running configuration to Startup configuration

Buttons: Submit, Close



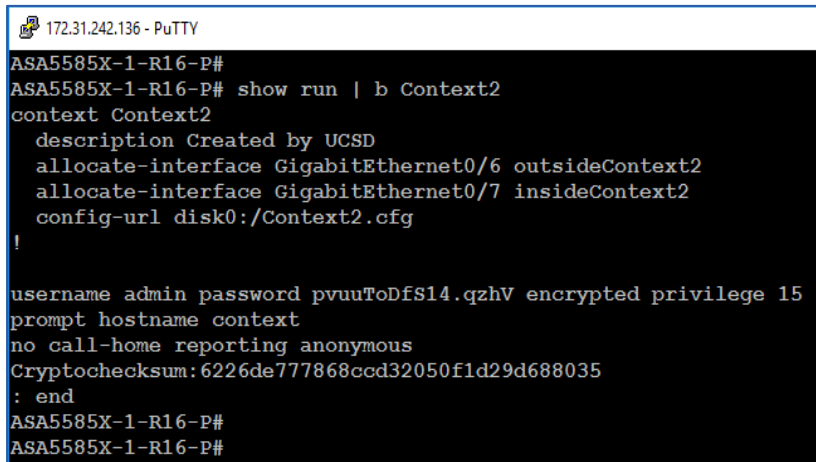
Use Case # 1

UCSD and ASA Verification...



The screenshot shows the Cisco UCS Director web interface. The top navigation bar includes 'Dashboard', 'Converged', 'HyperConverged', 'Virtual', 'Physical', 'Organizations', 'Policies', and 'Administration'. The main content area is titled 'Network for Default Pod > Cisco ASA (172.31.242.136)'. Below this, there are tabs for 'Summary', 'Configurations', 'Modules', 'Interfaces', 'Licenses', 'ASA Contexts', 'ACL', 'SXP Connection Peers', 'SGT', and 'Service'. The 'ASA Contexts' tab is active, showing a table of configurations. The table has columns for 'Device IP', 'Context Name', 'Allocated Interfaces', and 'Config File'. Three contexts are listed: 'admin', 'Context1', and 'Context2'. The 'Context2' row is highlighted in blue.

Device IP	Context Name	Allocated Interfaces	Config File
172.31.242.136	admin	Management0/0	disk0:/admin.cfg
172.31.242.136	Context1	GigabitEthernet0/2, GigabitEthernet0/3	disk0:/context1.cfg
172.31.242.136	Context2	GigabitEthernet0/6, GigabitEthernet0/7	disk0:/Context2.cfg

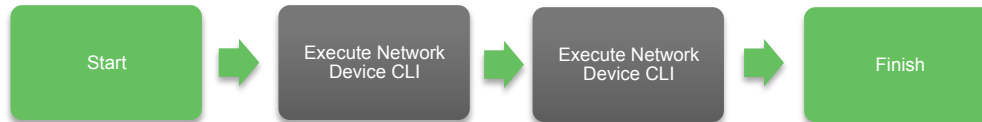


The screenshot shows a PuTTY terminal window connected to the device 172.31.242.136. The user has entered the command 'show run | b Context2'. The output shows the configuration for context 'Context2', including a description, interface allocations, and configuration file paths. The terminal also shows the user's login prompt and the end of the command output.

```
172.31.242.136 - PuTTY
ASA5585X-1-R16-P#
ASA5585X-1-R16-P# show run | b Context2
context Context2
  description Created by UCSD
  allocate-interface GigabitEthernet0/6 outsideContext2
  allocate-interface GigabitEthernet0/7 insideContext2
  config-url disk0:/Context2.cfg
!
username admin password pvuUtoDfs14.qzhV encrypted privilege 15
prompt hostname context
no call-home reporting anonymous
Cryptochecksum: 6226de777868ccd32050f1d29d688035
: end
ASA5585X-1-R16-P#
ASA5585X-1-R16-P#
```

Use Case # 2

- Leverage 'Execute Network Device CLI' task to configure specific command/feature which is currently not supported by UCSD (this task is executed on existing accounts and so you don't have to provide IP and credentials)
- Below workflow has Failover commands executed on pair of ASA (primary/secondary) Currently UCSD doesn't have any built-in tasks for Failover configurations but using task 'Execute Network Device CLI', UCSD can SSH into ASA device and configure any supported commands



- Workflow can be downloaded from the UCS Director community site <https://communities.cisco.com/docs/DOC-69484>

Use Case # 2

'Execute Network Device CLI' task has input for rollback commands which should be listed as shown (in case there is need for workflow rollback)

The dialog box titled "Executing Workflow: ASA Failover" contains a "Workflow Version:" dropdown menu set to "0 (default version)". Below it are two "Select..." buttons for "ASA Primary" and "ASA Secondary". At the bottom are "Submit" and "Close" buttons. Blue callout boxes on the left point to the "ASA Primary" and "ASA Secondary" labels.

The "Edit Task (Execute Network Device CLI)" window shows configuration options for "Task Information", "User Input Mapping", "Task Inputs", and "User Output Mapping". The "CLI Commands" section contains a list of commands for configuring an ASA failover. A blue callout box labeled "Config Commands" points to this list. The "Undo CLI Commands" section contains a list of corresponding rollback commands. A blue callout box labeled "Rollback Steps" points to this list. At the bottom are "Back", "Next", and "Close" buttons.

```
CLI Commands
1 changeto system
2 configure t
3 !
4 interface GigabitEthernet0/0
5 description LAN Failover Interface
6 no shut
7 !
8 interface GigabitEthernet0/1
9 description STATE Failover Interface
10 no shut
11 !
12 failover lan unit primary
13 failover lan interface failover-lan GigabitEthernet0/0
14 failover link failover-link GigabitEthernet0/1
15 failover interface ip failover-lan 10.1.1.1 255.255.255.0 standby 10.1.1.2
16 failover interface ip failover-link 10.1.2.1 255.255.255.0 standby 10.1.2.2
17 failover group 1
18 primary

Undo CLI Commands
1 changeto system
2 configure t
3 !
4 no failover
5 !
6 interface GigabitEthernet0/0
7 no description LAN Failover Interface
8 shut
9 !
10 interface GigabitEthernet0/1
11 no description STATE Failover Interface
12 shut
13 !
```

Use Case # 2

Service Request completion and ASA Verification...

Workflow Status		Log	Objects Created and Modified	Input/Output
Service Request				
Status Refresh				
▼ Overview Current status for the service request.				
Request ID	237	1	Initiated by admin	09/06/2016 13:57:40
Request Type	Admin Workflow	2	Execute Network Device CLI	09/06/2016 13:59:21
Workflow Name	ASA Failover	3	Execute Network Device CLI Completed action	09/06/2016 14:00:57
Workflow Version Label	0	4	Complete Completed successfully.	09/06/2016 14:00:58
Request Time	09/06/2016 13:57:38 GMT-0700			
Request Status	Complete			
Comments				
▼ Ownership				
Initiating User	admin			

```
ASA5585X-1-R16-P#
ASA5585X-1-R16-P# show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover-lan GigabitEthernet0/0 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1049 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.5(2), Mate 9.5(2)
Group 1 last failover at: 14:27:15 UTC Sep 6 2016
Group 2 last failover at: 14:27:15 UTC Sep 6 2016

This host:      Primary
Group 1        State:          Active
                Active time:    5452 (sec)
Group 2        State:          Active
                Active time:    5452 (sec)

slot 0: ASA5585-SSP-20 hw/sw rev (2.2/9.5(2)) status (Up Sys)
admin Interface management (172.31.242.136): Normal (Monitored)
```

```
ASA5585X-1-R16-P# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: failover-lan GigabitEthernet0/0 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1049 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.5(2), Mate 9.5(2)
Group 1 last failover at: 14:28:18 UTC Sep 6 2016
Group 2 last failover at: 14:28:18 UTC Sep 6 2016

This host:      Secondary
Group 1        State:          Standby Ready
                Active time:    1217 (sec)
Group 2        State:          Standby Ready
                Active time:    1217 (sec)

slot 0: ASA5585-SSP-20 hw/sw rev (2.0/9.5(2)) status (Up Sys)
admin Interface management (172.31.242.137): Normal (Monitored)
```





CISCO

TOMORROW starts here.