Cisco UCS Central Best Practices

Updated for Release 1.1(1a)

Revision 2.05 Aug 20, 2013

Contents

Forward for the UCS Central 1.1(1a) Release

The UCS Central 1.1(1a) release is the first release that supports a fully Globalized UCS environment, with Global ID's, Global Policies and Global Service Profiles. This release represents the most significant innovation in the server management space for Cisco, since the introduction of Cisco UCS Manager itself. With this 1.1(1a) release, UCS administrators are able to take advantage of global identity management, global policy consistency and global service profile mobility.

The UCS Central 1.0 release[1] introduced:

- Global Inventory, Faults, Logs
- Global ID Pools (UUID, MAC, WWNN, WWPN)
- Global Firmware Updates, Global Backups
- Global Administrative and Operational Policies

[1] UCS Central 1.0 Release Notes:
http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/UCS_28314.html

The signature features for this 1.1(1a)[2] release include:

- Global Policies, Global Service Profiles and Global Templates
- Statistics on External Database for historical reporting
- High-Availability for UCS Central Virtual Machine in Cluster-mode

In terms of scale, UCS Central can manage 10,000 servers, corresponding to roughly 70 – 125 UCS Management domains, depending on domain size.

Future releases will target greater scale, additional functionality enhancements, and cover any current caveats.

Introduction/Goals/Audience/Scope

Cisco UCS Central simplifies the management of multiple Cisco UCS domains through standardization, global policy enforcement and global ID consistency. While UCS Manager provides policy-driven management for a single UCS domain, UCS Central is aimed at the management and monitoring activities of UCS on a global basis, across multiple individual UCS Management domains worldwide, providing an even greater degree of administrative power, operational efficiency and policy-driven automation.

This document is intended for administrators of multiple UCS management domains, and to help those administrators understand the procedures/impacts/etc for adopting UCS Central. An experienced level of UCS Administration is assumed. This document is intended as an accompaniment, and not a replacement, for the UCS Central product reference guides and documentation[3].

Standard Abbreviations

The following standard abbreviations are used throughout this document

Abbreviation	Stands for
UCSM	UCS Manager
SP	Service Profile
LSP	Local Service Profile
GSP	Global Service Profile
DG	Domain Group

[2] UCS Central 1.1(1a) Release Notes:
http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/RN-CiscoUCSCentral_1-1.html
[3] All product downloads and documentation for UCS Central can be found here:
http://www.cisco.com/en/US/products/ps12502/tsd_products_support_series_home.html

Installation and Upgrade Pre-requisites

There are version compatibility requirements for UCS Central and the underlying UCS Manager releases:

- UCS Central 1.0(1a) supports communication with UCSM 2.1.1 and UCSM 2.1.2
- UCS Central 1.1(1a) supports communication **only** with UCSM 2.1.2

Therefore, prior to attempting an upgrade of UCS Central to 1.1(1a), all registered UCS domains must first be upgraded to UCSM 2.1.2

Any use of any UCS Central release requires a minimum UCSM release of 2.1.1.

UCS Central Virtual Machine (VM) system requirements

UCS Central concentrates monitoring, configuration and management across multiple UCS domains and across potentially thousands of servers. For this reason, minimum performance thresholds are required for the UCS Central VM (primarily around disk access) to ensure problem-free operations.

Administrators also need to make sure that the underlying VM storage is sized appropriately for the 80GB VM. Shared storage (if H/A cluster mode is enabled) needs to be at least 40GB. UCS Central serves as an image repository for all firmware bundles. For each UCSM release, plan for the size of entire release (infrastructure, blade and rack bundles) to be 1.5 GB if the full images are downloaded and stored locally.

Free space monitoring within the UCS Central VM can only be shown through the CLI. Login from the VM Console (not the GUI), and type "`scope monitoring; show storage`" to view the percentage of used disk space in the VM.

UCS Central should be deployed on a high speed datastore, preferably provisioned from high speed SAN.

Significant changes in the underlying VM structure between UCS Central 1.0 and 1.1(1a) include:

- 4 vCPU (cores)
- 12 GB Memory
- VM virtual hardware version format change from version 7 to 8 (relevant for VMware only)

Management Access for UCS Central to UCS domains (ports, firewalls etc.)

Typically, the IP addresses for all existing UCS Management domains exist on a common administrative subnet or VLAN. If this is not the case, UCS Central should still work, provided that routing access is assured from UCS Central to all subordinate management domains. For this reason, care must be taken to ensure that any firewalls/proxies/etc. are configured to permit read/write access on the following ports for continuous communications between UCS Central and all subordinate UCS domains:

LOCKD_TCPPORT=32803
MOUNTD_PORT=892
RQUOTAD_PORT=875
STATD_PORT=32805
NFS_PORT="nfs"(2049)
RPC_PORT="sunrpc"(111)

Also, any firewall session timeout limits for these ports should be reviewed with respect to sessions being dropped due to inactivity. For the full list of installation pre-requisites, please refer to the UCS Central Deployment Guide

UCS Central licensing

With UCS Central, the first 5 domains are licensed free of charge, excluding support. There is a 120-day "trial period" after the registration of the first domain.

After the 120 day trial period, an initial license ("L-UCS-CTR-INI=") can be purchased that is good for 5 domains through the standard ordering process. The INI= license is $0, but does not include support. Additional licenses – beyond the first 5 domains – can be purchased using "L-UCS-CTR-LIC=".

Failure to activate licenses results in failure to register addition domains, as well as faults being generated in UCSM, indicating that the domain has ended its trial period.

The 1.0(1a) release did not actively enforce licensing compliance. The 1.1(1a) release does enforce licensing compliance and restrictions.

Terminology

The Definitions table below should be followed for naming conventions and terminology:

Term	Description
UCS Manager	Embedded software that manages a UCS Domain
UCS Domain	A collection of resources managed by a UCS Manager – also the client for UCS Central
UCS Central	Product that Scales UCS Management Domains across global datacenters to provide global control and visibility
Domain Group	Name of the group that multiple domains are a part of. Operational policies can be defined at this level that pertain to all domains in the group
Sub Domain Group	A child of the domain group. Inherits its properties from the parent. Can have specific local policies for the domains in the sub domain group
Ungrouped	Domains that do not belong to any domain group

Domains	
Domain-wide	Properties/configurations that are common or pervasive across an entire UCS domain (sometimes historically **incorrectly** referred to inside UCSM as "global")
Local	Reference to an object that is owned and resident in a single UCS Manager domain, e.g. Local policies or Local pools .
Global	A reference to an object that is owned and resident in UCS Central, e.g. Global Service Profiles , Global Policies, and Global Pools
Localize	Move something from a global context to a local context, e.g. a Policy from UCS Central is instantiated on a UCS Domain
Globalize	Move something from a UCS Domain to UCS Central, e.g. a policy that was defined inside UCS Manager gets moved to UCS Central, e.g Importing Operational Policies.[4]
Register	Initial process through which a UCS Manager connects to UCS Central
Unregister	Intentional removal of UCS Domain from UCS Central management
Disconnect	Unintentional loss of connectivity between UCS Manager and UCS Central
Suspend	An action where management communications between UCS Central and UCS Manager is temporarily halted. Not an "Unregister" operation.
Suspended Mode	UCS Manager is registered with UCS Central but there is no management communication between the two
Resume	An action where management communications is re-established between UCS Central and UCS Manager

Use of the terms "Pod", "Clusters" or "Blocks" should be avoided, in favor of "Domain". Past usage of certain terminology in a single UCS Manager context may need revisiting in the truly global and multi-UCS context of UCS Central. For example, prior to UCSM 2.1, VLANs were referred to as "global" for scope within a single domain. Going forward, a common understanding of names/terms/contexts is essential.

"Best Practices"

The term "Best Practices" is intended more as a set of guidelines and suggestions --- not gospel. The only real "Best Practice" is whatever works best for your specific operating requirements.

Flexibility, adaptability and control are all hallmarks of UCS Manager, and continue as goals for UCS Central. The UCS Central management model differs significantly from the standalone, local management model. Administrative power is *highly* concentrated within UCS Central,

[4] Ability to Import Server/Network/Storage Policies is coming in a future release

and the scope of control and impact can be very broad. Unexpected service interruptions could be a consequence of not following recommended practices. Please understand this well, as you adopt and deploy UCS Central. You are strongly advised to:

- Model and Test as much as possible, in advance of deployment
- Be conservative with global configuration changes

UCS Central is not a replacement for UCS Manager. UCS Central is intended as the way to centralize policy definition and to create pools of global identifiers that can be consumed across multiple UCS domains. Over time, even as more functionality becomes available through UCS Central, UCS Manager will continue to be the interface for direct management of the UCS domain, as well as the vehicle for policy termination and resolution.

1. Domain Group (DG) Design

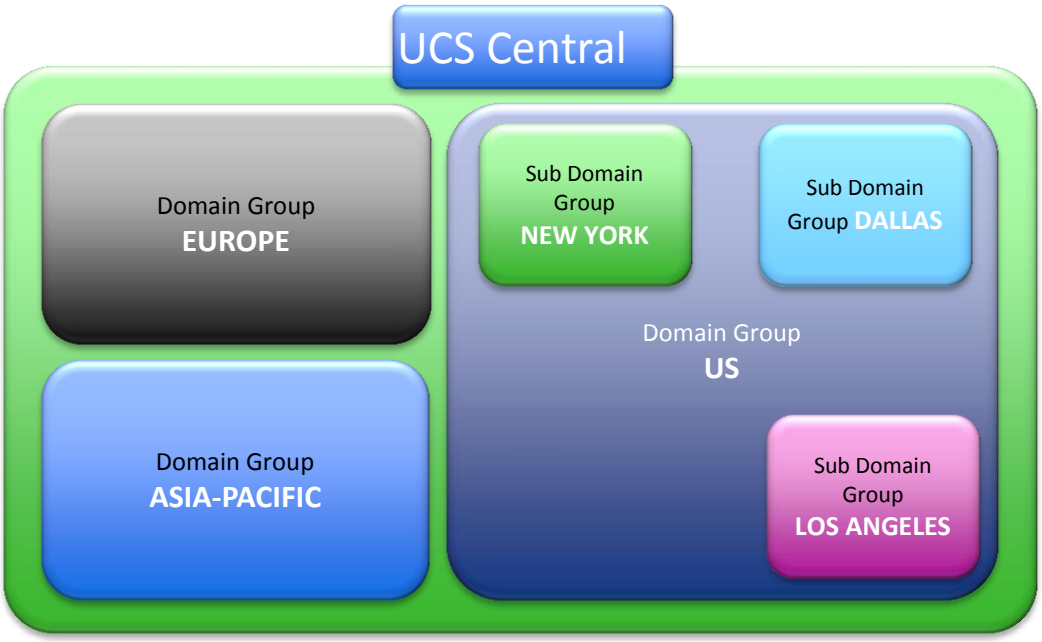
Domain Group (DG) hierarchy design is probably the most important design decision. There is no right/wrong way. The goal for this feature is to best reflect your specific environment and management design choices. The following attributes of (DG's) should be understood:

- A Domain Group (DG) is arbitrary grouping of individual UCS domains. Grouping design is left to the UCS Central Administrator. There is nothing within the context of an individual UCS domain that creates affinity for a particular Domain Group. In fact (and very important) --- within the context of an individual UCS domain, there is absolutely no concept/notion whatsoever regarding a "Domain Group". A DG is purely a UCS Central construct.
- UCS domains can be a part of only one DG at a time. Unlike blades and Server Pools, where one blade can be in multiple Server Pools, a given UCS domain can only be in one DG at a time.
- All UCS domains by default are placed in the "Ungrouped Domain Group" at registration. Domains in the Ungrouped DG will not resolve any global policies, even if the local UCS administrator has opted-in for global policy resolution.
- Policies are defined on a per DG basis, and are in effect for all domains in the DG. A DG is where Operational Global Policy is resolved (or applied).
- UCS domains can move between DGs. However, any DG to DG move for a domain can be disruptive depending on new policies. UCS Domains resolve their own policies from DG's. If a new domain joins, then the global policies will be applied --- and that might impact service.
- Newly registered domains can "auto-join" a DG based on qualification policies at registration time. Domain Group Policy Qualifications work in a similar manner to Pool Policy qualifiers. ("Equipment -> UCS Domains -> Policies")
- Global Policies can be defined anywhere in the DG hierarchy can then be overridden by policies defined at a subordinate DG policy.

- When moving a Domain to a new DG, the policies that are currently binding for the old DG are not necessarily removed (or reset). Instead, the old policies remain in place, unless the new policies overwrite the old policies. If the old policies are not over-written by new binding policies, then the old policies remain in place as 'non-binding' policies[5].
- Sub-domain Groups can be created and nested hierarchically for finer granularity of policy control. The degree with which sub-domains are employed should be weighed against the amount of additional administration/management required for managing the different sub-domains.

Some examples that might serve as the basis for DG partitioning include:

- Geography, Timezones, etc.
- Organizations, Business Units, etc.
- Production Criticality (Prod, Dev, Test/QA, etc.)
- Network Domains (Internal, External, etc.)



Domain Group hierarchy example

Domain Groups should be used to help simplify configuration and deployment of operational policy. Use of Domain Group hierarchy should only be used when it best fits the operational challenge.

[5] Policies which are resolved based on reference, like host packs, maintenance policy, schedules, firmware distribution bundles (Infra, B, C) will be removed if they are not present in the new domain group. Among the operational policies which are resolved based on policy controls (local, global knobs), named policies like roles, locales, trust points will be removed if they are not present under new domain groups.

2. UCS Central Authentication

UCS Central version 1.1(1a) supports either local[6] or LDAP based authentication. Native authentication for other types such as TACACs+ or RADIUS are not currently supported in UCS Central. UCS Central only supports one defined form of Native Authentication to be active at once (either local or LDAP). UCS Central currently does not support the ability to select the form of authentication during the login process like UCS Manager does.

UCS Central currently only supports LDAP Attribute-based authentication, requiring a LDAP schema change[7]. This does not support UCS role to LDAP group mappings, UCS authentication provider groups, nor multiple authentication schemes such as a combination of Local, RADIUS, TACACs+, and LDAP --- as is currently supported in UCSM. Deployment options currently include either using an existing attribute of the user class, as defined in your LDAP schema (ex. Description), or to extend your LDAP schema by creating a new attribute for populating the UCS role and Locale definitions for UCS Central users. Each user would need to be modified in LDAP to add the appropriate role and locale definitions needed. The following is an example of the syntax that needs to be added to LDAP attribute defined for each user:

```
shell:roles="<role-X>,<role-Y>" shell:locales="<locales-X>,<locales-Y>"
```

Parameters “role-X” and “role-Y” signifies the UCS Central role to be applied to the user being authenticated, and parameters “locale-X” and “locale-Y” are the locales in UCS Central to which you want the roles applied.

If you plan to globalize authentication or other operational policies across multiple UCS domains, then the best practice is to group those domains in Domain Groups other than the "root" DG. UCS Central resolves its own operation policies such as authentication / DNS / Time zone / etc. from the "root" DG. Because of this, you will need to create sub-domain groups that have different operational settings defined that differ from UCS Central. The operational settings defined in these sub-domain groups will then be applied locally to the UCS domains that are opting in to globalize these settings.

3. Use Hierarchy for Orgs and Domain Groups

The UCS Manager is hierarchical in nature, as reflected through the “org” structure. For UCS Central, the hierarchical “org” structure takes on a global scope.

The DG structure in UCS Central is also hierarchical. One important distinction is that DG is purely a UCS Central construct --- Local UCS domains have no visibility in to DGs.

[6] The ‘$’ should not be used as a password character when using local authentication.
[7] Similar what was required with UCS Manager version 1.3 and before

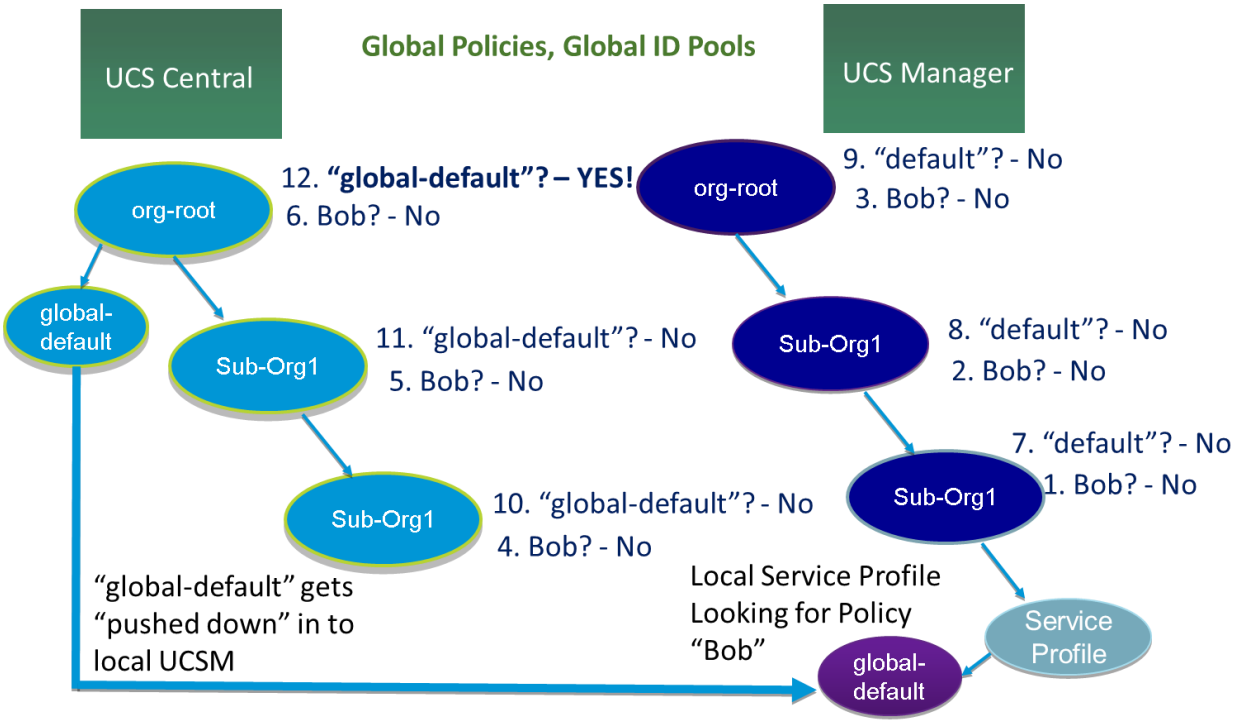
Best Practice

The best practice for both "orgs" and DG's is to take advantage of the hierarchy to best reflect the logical (org) and physical (DG) segmentation of the enterprise. Ensure that any pools, policies or service-profiles that are placed in "org-root" or the "root" DG are truly intended to have global applicability and visibility for all domains. Be aware that creating policies (local or global) in "root" can have unexpectedly broad (and possibly unpleasant) consequences.

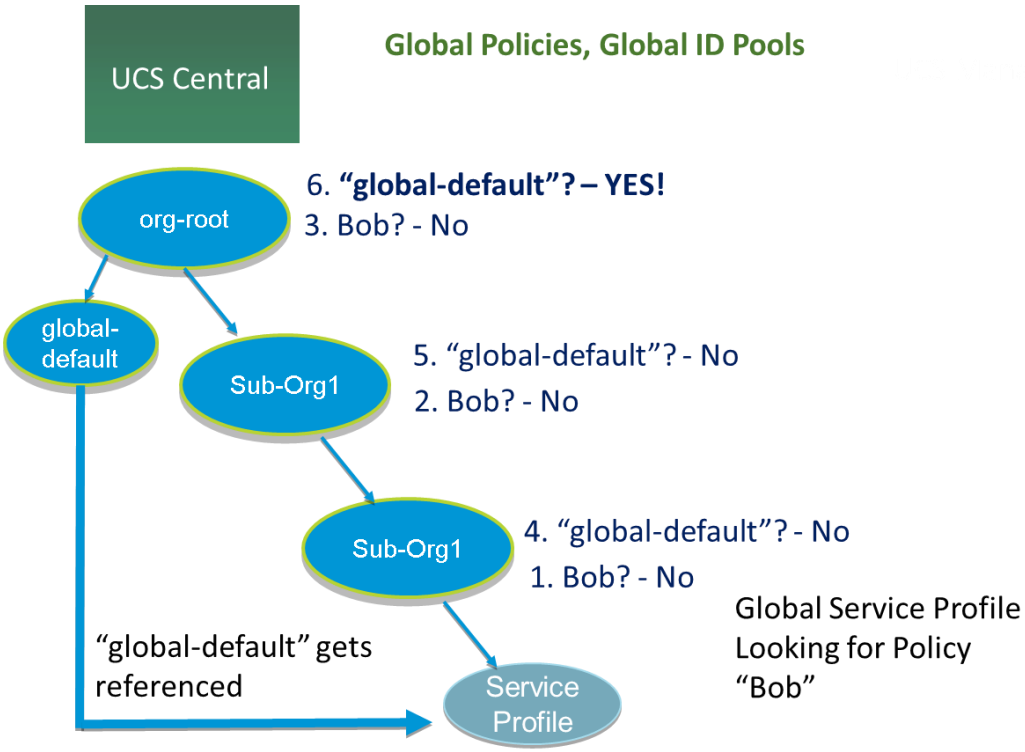
4. Name Ambiguity and Resolution

Few restrictions are placed on object naming within both UCSM and UCS Central, which in turn could lead to ambiguity. As pools and policies are bound to managed objects in UCSM, there is nothing (except best practices) that prevents the same object "name" from having both a local and a global scope. When any policy or pool name is specified in a Service Profile , VNIC or VHBA, a well-defined "name resolution process" is followed in UCSM. Preference is given to local names over global names, for both pools and policies. Resolution for locally managed objects happens in the following order for a given "name":

1. Use the object name if found and defined in the local org --- else…
2. Use the object name if found and defined in subsequently higher parent orgs, up through the local "org-root" --- else …
3. Use the object name if found and defined in the global org --- else …
4. Use the object name as defined in subsequently higher global parent orgs up through the global "org-root".
5. Use the values corresponding to the "default" object in the local org, and up through "org-root"
6. Use the values corresponding to the "global-default" object in the global org, and up through "org-root".



Example of Hierarchical Name Resolution Order for Policy "Bob" by Local Service Profile



Example of Hierarchical Name Resolution Order for Policy "Bob" by Global Service Profile

Best Practice

As a best practice for avoiding ambiguity, administrators should not create nor use the same "name" in both local and global contexts. To avoid ambiguity, global policy and pool names should have unique prefixes (Ex: "G-MAC-A" or "Global-MAC-A" for all VNICs bound to the A-side fabric). Another best practice is to always make use of explicitly defined pools and policies, and to avoid use of the "default" or "global-default" names altogether.

Class of Object	Local "default" object	Global "default" object
MAC Pools , WWPN Pools, and most Policies	default	global-default
Out-of-band IP Addr Pool	ext-mgmt	global-ext-mgmt
iSCSI Initiator Pool	default	global-iscsi-initiator-pool
WWNN ID's	node-default	global-node-default

5. Registration and Certificates

Registration is the process by which UCS domains and UCS Central establish a trusted communication path. Communication between UCSM and UCS Central uses HTTPS and signed certificates. Therefore, the system time must be the same between UCSM and UCS Central.

Ensure that UCS Central and all local UCS domains point to common NTP servers and have their clocks all in sync, prior to registration.

Please see Appendix I and II for detail on troubleshooting registration and certificates issues.

6. Identifier Management

Global identifier management addresses one of the biggest challenges around multi-domain management : unique address management for system identifiers (MAC's, WWxN's, UUID's, etc.). Previously, UCSM best practices recommend embedding a "domain ID" within the high-order bytes of the ID pool ranges. However, this still involved manual intervention and could be error prone.

With UCS Central, all the ID pools can be defined and accessed globally across all UCS domains. Service Profile assignment can be guaranteed unique and non-overlapping with respect to ID's across all UCS domains.

Global ID Pools belong to the "org" structure. Global pools do not terminate on DGs, as the UCS Central "Operational Policies" do. Instead, the range of Global ID Pools extends across all UCS domains in the scope of the org structure within UCS Central, regardless of any DG partitioning.

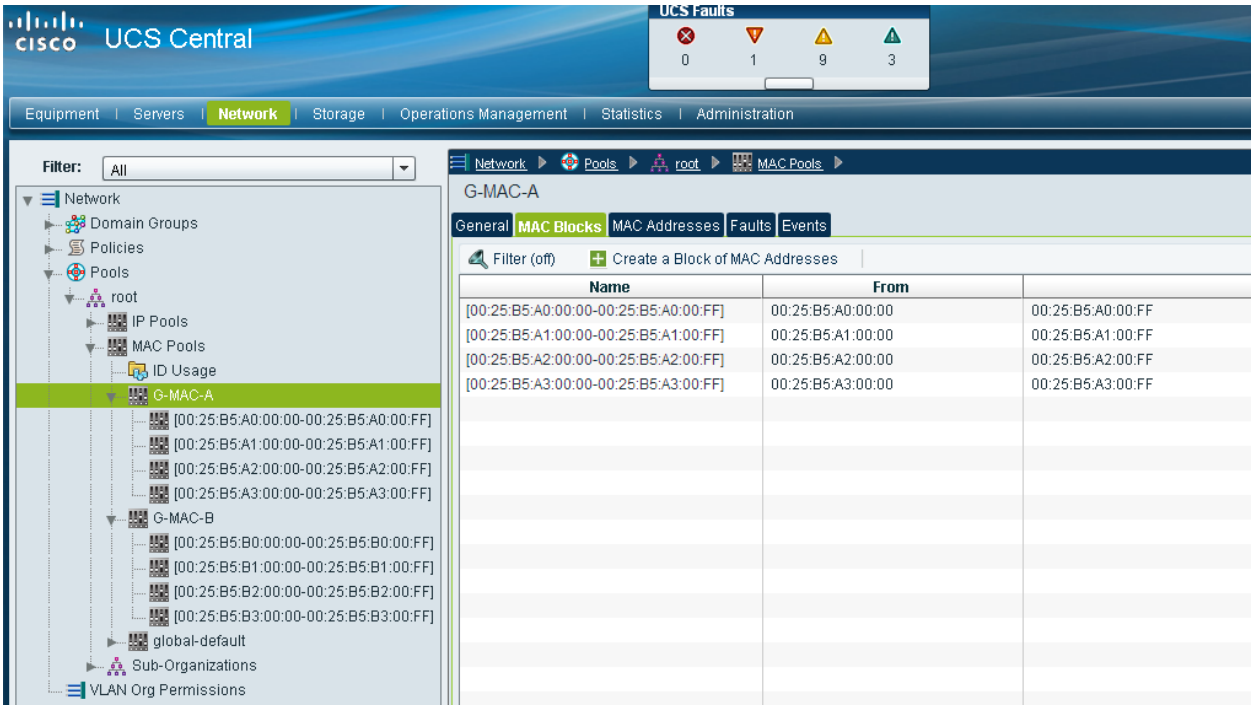
Best Practice

When deploying UCS Central, a Best Practice is to adopt Global IDs along with Global Service Profiles for deployment of new UCS domains.

a) Pool sizing

As a way of minimizing the number of managed objects, one best practice would be to create a smaller number of pools with a larger number of blocks, as opposed to creating a larger number of individual pools themselves.

A common existing UCS best practice involves drawing from corresponding A-side/B-side pool names, with an "A" or "B" embedded in the high-order byte of the MAC/WWPN address range, as a way of distinguishing A-side versus B-side traffic. Extending this model towards UCS Central would involve creating multiple blocks under such a pool structure. The best sizing for each block is with 256 addresses (0xFF)[8].



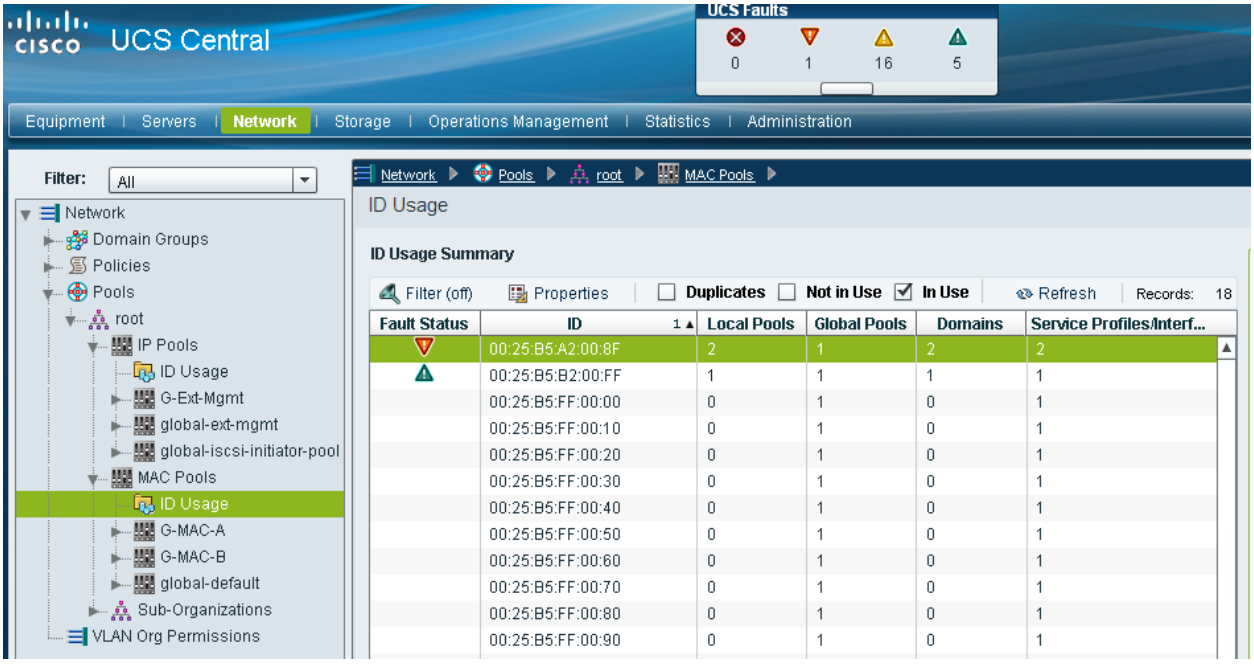
Example of Global Mac Pools (A-side, B-side) with multiple blocks

b) Checking for Duplicates

UCS Central provides visibility in to possible duplicate ID usage.
All of the pool types (UUID, MAC, WWxN) offer the ability to display duplicate IDs that may exist across UCS domains, through the "ID Usage Summary". Duplicate ID

[8] UCS Central imposes a maximum block size of 999 addresses (0x3E7) for all pools (UUID, MAC, WWxN)

severity will be flagged as either “Major”, for IDs that appear in multiple Service Profiles, or flagged as “Warning” for IDs that appear in multiple local pools. Note that the only way to view Local ID Pool consumption is to select an individual ID, and view the corresponding drill-down details to the right (Local Pool and Local Service Profile)



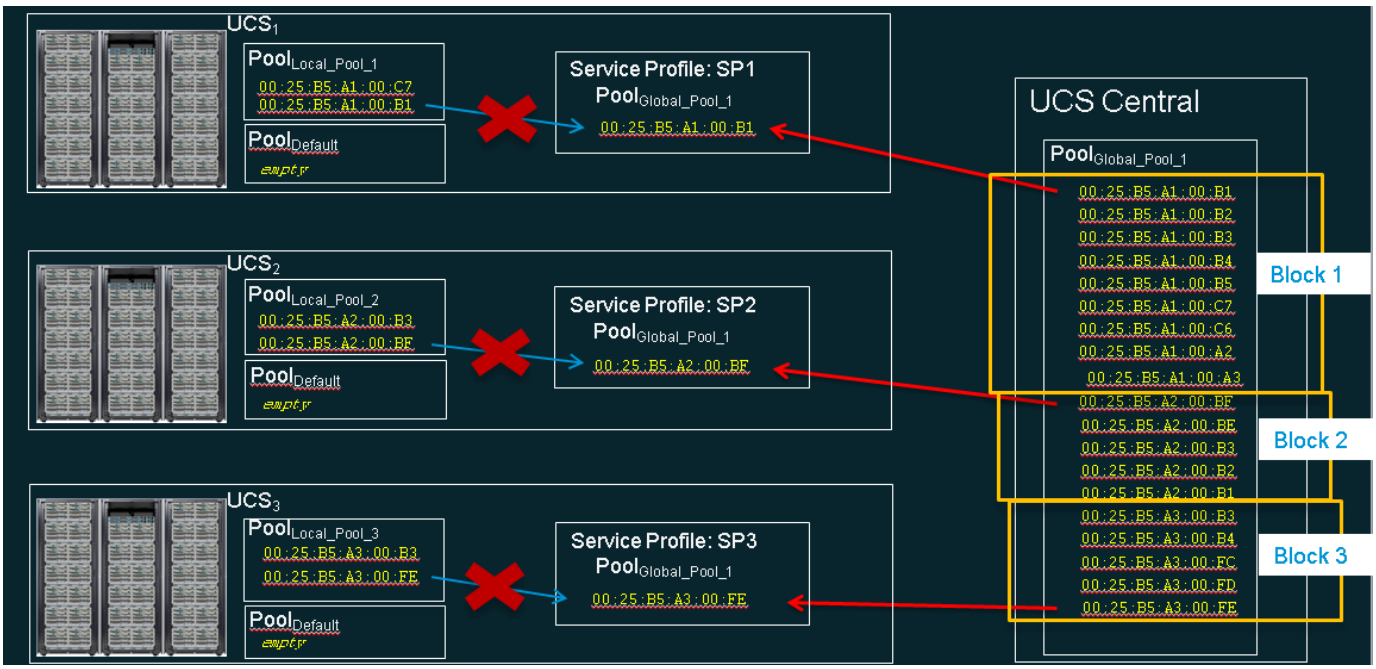
Example of detecting presence of duplicate ID’s

c) Transitioning to Global Pools

Local Service Profiles (LSPs) that currently reference local ID pools can be reconfigured to use Global ID pools. Changing any ID for an associated Service Profile would typically cause a service interruption. However, UCS Central was designed to ease this migration to Global ID pools and not cause a service interruption if the transition results in assignment of the same identifiers.[9]

LSPs that use Global ID’s will be guaranteed ID uniqueness, but will not be able to take advantage of Global Service Profile (GSP) mobility. LSPs that use Global ID’s will still reside in the local domain. Upcoming versions of UCS Central will provide features to migrate LSPs to GSPs.

[9] Check the “Caveats” section for known issues with UCS 2.1(2a) and UCS Central 1.1(1a) in this regard. Due to bug CSCud44377, a service interruption is unfortunately incurred. Until this bug is fixed, the recommendation is to NOT transition Local Service Profiles to Global Pools.



Local to Global ID Pool Migration

d) Creating New Global ID Pools

Existing UCS customers with multiple domains will have ideally addressed multi-domain ID challenges through best practices, such as embedding a "domain ID" within the high-order bytes of ID pool ranges[10]. Transitioning to Global Pools was highlighted in the previous section. But some admins might wish to completely segregate global ID's in a way that is completely distinct from previous local ID consumption. One way to accomplish this is to reverse the orientation for how "domain ID" was previously embedded. For example, if the Local ID method for MAC IDs was "00:25:B5:**3A**:FE:ED" (where **3** corresponded to the domain ID, and **A** corresponded to the Fabric Interconnect), then the Global ID method might be "00:25:B5:**A0**:AB:BA", which would provide an ID signature that is distinct from the Local ID convention.

[10] Sites with existing overlapping IDs will need to address these issues, as well as others surrounding global server management. Addressing existing overlapping ID's is beyond the scope of this document.

e) Migrating from Existing ID Pools

To maintain the same ID for LSPs while migrating to Global ID Pools, construct the Global ID pools so that they are "supersets" of the corresponding Local ID pools (i.e., the Global ID pool should contain all of the identifier blocks that are currently within the Local ID pools). A best practice would be to adopt an "A/B" naming orientation for MAC and WWPN pools with respect to the fabric, such as "G-MAC-A" or "G-WWPN-B". Once the Global ID pools have been created, the Administrator can change the Service Profile to reference the Global ID pools. If not already assigned, UCS Central will automatically assign the same identifier that was previously used in the local ID pool, thus eliminating the need for a service interruption[11].

When the ID space is already partitioned and completely non-overlapping, the adoption sequence could be as follows:

1. Create new ID Pool in UCS Central with unambiguous name and a "Global" or "G" in the pool name prefix. For MAC and WWPN pools, add a "-A" or "-B" suffix to the pool name.
2. For each local ID block in the local pool, recreate a corresponding ID block in the global pool
3. Change any existing templates (Service Profiles, VNICs, VHBAs) to refer to the corresponding global ID pool name.
4. Verify the corresponding local ID block has no assignments
5. Delete the corresponding local ID block for each local ID block in the local pool

For VNICs/VHBAs based on "initial templates", once the ID's reference global ID pools, then all subsequently created managed objects should reference the new global ID pools. This is by nature of "initial templates".

For VNICs/VHBAs that are bound to "updating templates", once the ID's reference global ID pools, then all existing managed objects bound to the template should reference the new global ID pools. If the existing managed object's ID is present and unassigned in the global pool, then this transition will not cause a reconfiguration, reboot or service impact.

For VNICs/VHBAs that are not bound to a template, if service-profile's pool name is modified to point to global pool, and the existing ID is already consumed in the global pool, then the service-profile will get a new ID, causing a reconfiguration, reboot and service impact. If the ID is not already consumed, then the ID will be

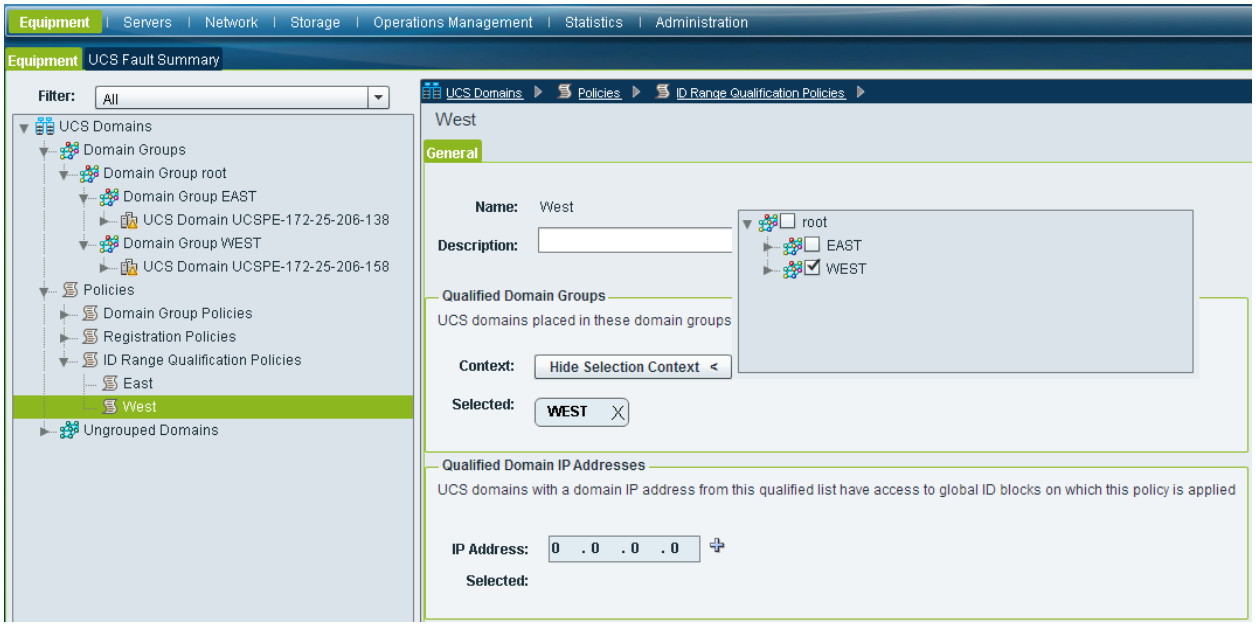
[11] The 1.0(1a) and 1.1(1a) releases unfortunately cause service interruptions when migrating to Global Pools in this manner. This has been identified as bug CSCud44377 and will be fixed in UCSM release 2.1(3)

retained and will point to the global pool, without incurring a reconfiguration or service impact.

Note that IP addresses for “ext-mgmt” and “iscsi-initiators” can also be managed through global pools. Similarly, the current allocations for existing domains can be viewed from Network->Pools->[Org]->IP Pools->ID Usage

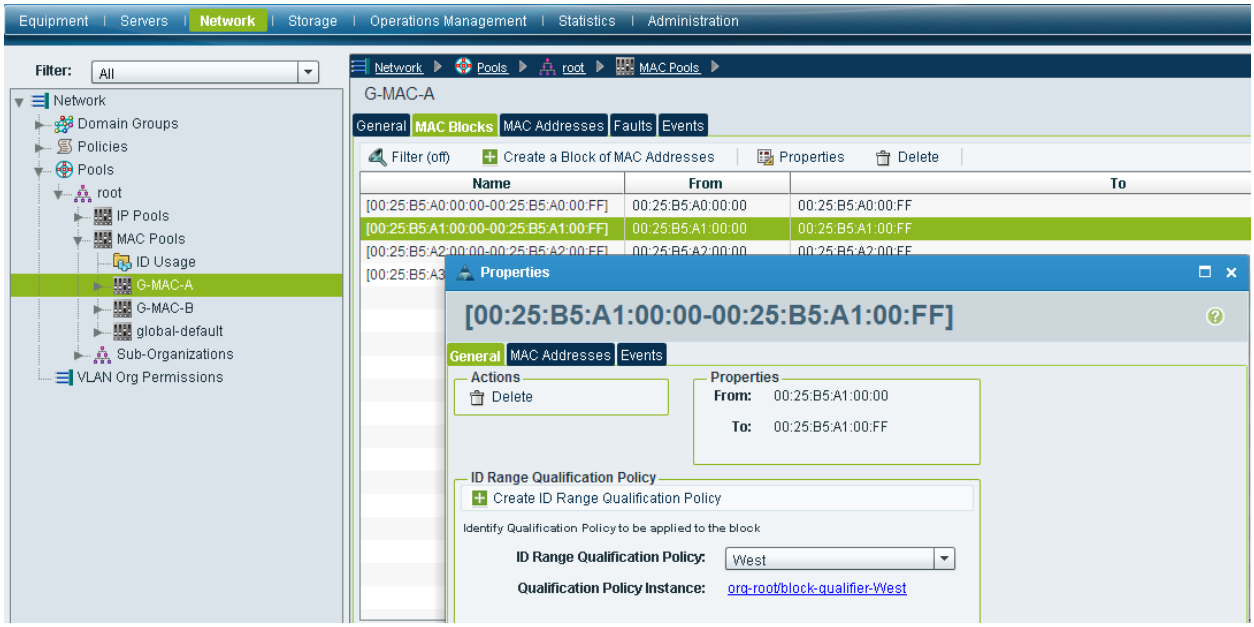
f) ID Range Qualifications

Rather than all domains consuming IDs from pools in an undifferentiated manner, UCS Central provides the ability to segregate ID blocks within a pool for a Local Service Profiles within a particular DG[12]. In this way, one or more domains from a particular DG can be assured of consuming a discrete range of identifiers, as illustrated below.



Creating ID Range Qualification Policies for Domain Groups

[12] ID Range Qualifications are not available for Global Service Profiles.



Referring to ID Range Qualifications Within an ID Block

7. Global Operational Policies

This section refers to Global Operational Policies and not Service-Profile oriented policies.

UCS Central provides global operational policies for multiple UCS domains --- but all participation of global policies is on an "opt-in" basis, with respect to the local UCS manager. UCS Central does not "take" control of global policies, unless such control is first delegated from the local administrator. Note that a local administrator can subsequently "pull back" control by "opting out" of global management for a given policy at a later time. Simply stated, the presence of UCS Central need not materially alter the management model for a UCS domain.

All administrative policies are under local domain control by default and remain that way until the following three things occur:

1. The local domain is registered to UCS Central
2. The local domain is made part of a DG in UCS Central
3. The local domain administrator explicitly promotes a given policy from "Local" to "Global" resolution.

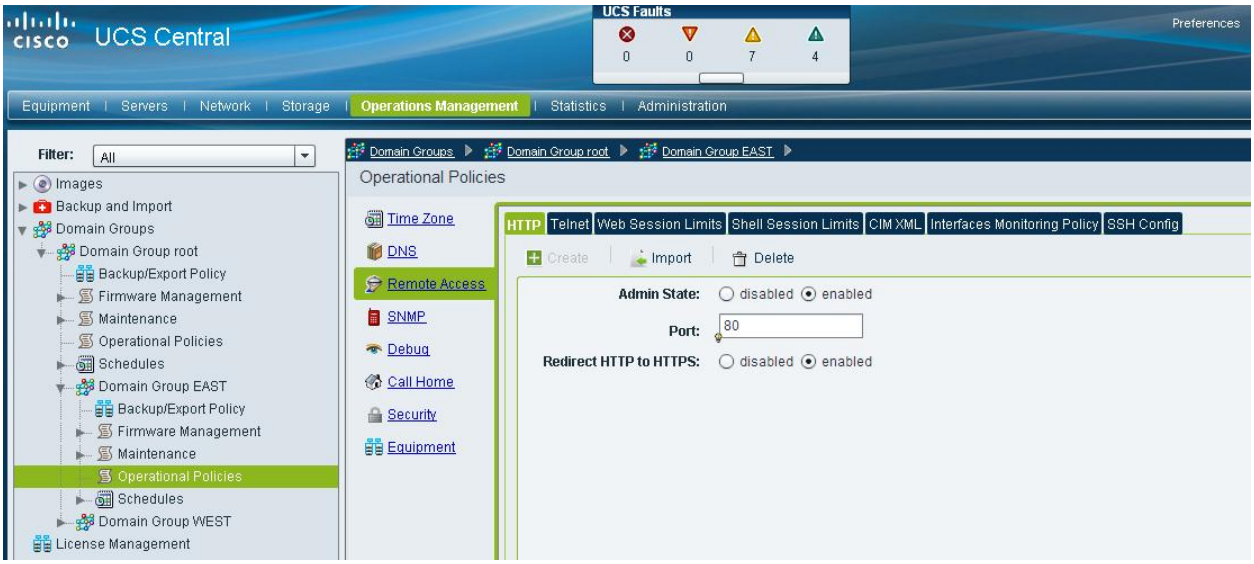
There is no dependency between the various policy promotion decisions. For example, Infrastructure/Catalogue Firmware management can be globalized, while Fault Policies can still be managed locally. All the policy options visible from "Admin -> Communication Management -> UCS Central" are all independent from each other.

Once policy is promoted from local to global, then the policy definition can only be changed at the UCS Central level. This is by design, to enforce the desired consistency across domains. However, administrators may at any time decide to return to locally resolved policies. A best practice would be to try and minimize the number of transitions between local and global for policies.

Best Practice

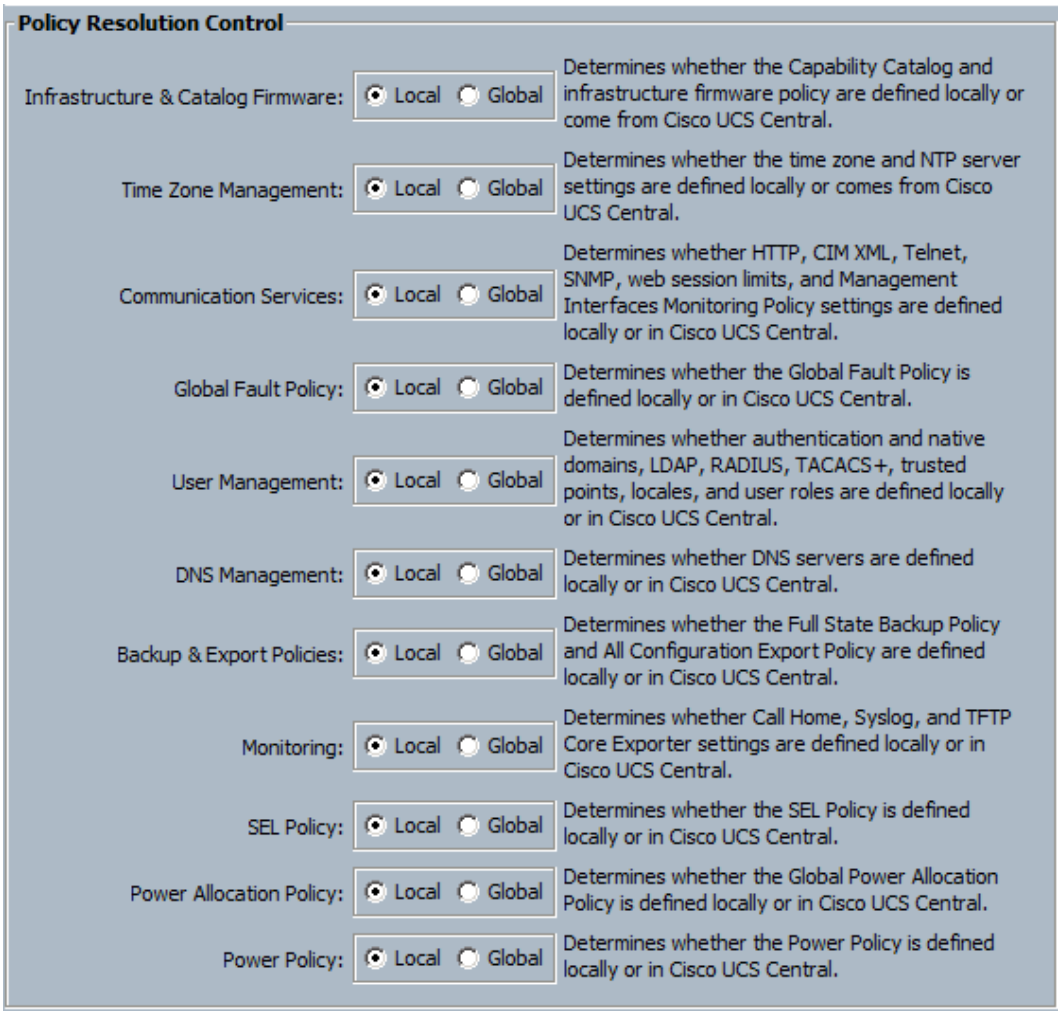
An overall best practice would be to maintain the default local policy resolution and to gain comfort and understanding, prior to a broader adoption of global policies. Global policy adoption should be done on an individual policy basis, phased over time, as familiarity and comfort are gained.

UCS administrators are encouraged to take increasing advantage of policy consistency and central policy enforcement, whenever possible. Global consistency and policy enforcements are among the key architectural goals for UCS Central. By consolidating policy definition and configuration within UCS Central, the administrative burdens of local UCS administrators will be reduced. Keep in mind that any opportunity to define and manage policy at a higher and more central-level will promote greater administrative scalability. Administrators are encouraged to design policy towards simplicity, and to centralize policy definition, whenever possible, as a general best practice.



Screenshot above shows Global Operational Policies

Screenshot below shows how the Policy Resolution Control for Operational Policies could be"Globalized"



UCS Manager Reference	UCS Central Reference	UCSM GUI Navigation
Infrastructure & Catalog Firmware	Operations Management -> [DG] -> Infrastructure Firmware	Equipment -> Firmware Auto Install
Time Zone Management	Operational Policies -> [DG] -> Time Zone	Admin -> Timezone Management
Communication Services	Operational Policies -> [DG] -> Remote Access	Admin -> Communication Management -> Communication Services
Global Fault Policy	Operational Policies -> [DG] -> Debug -> Global Fault Policy	Admin -> Faults/Events/Audit -> Settings
User Management	Operational Policies -> [DG] -> Security	Admin -> User Management
DNS Management	Operational Policies -> [DG] -> DNS	Admin -> Communications Management -> DNS Management
Backup and Export Policies	Operational Policies -> [DG] -> Backup/Export Policy	Admin -> All -> Backup and Export Policy
Monitoring	Operational Policies -> [DG] -> Call Home **and** Debug	Admin -> Faults/Events -> Syslog Faults/Events -> Settings -> TFTP Core Exporter Communications Mgmt -> Call Home
SEL Policy	Operational Policies -> [DG] -> Equipment -> SEL Policy	Equipment -> Policies -> SEL Policy
Power Allocation	Operational Policies -> [DG] -> Equipment -> Global Power Allocation Policy	Equipment -> Policies -> Global Policies -> Global Power Allocation Policy
Power Policy	Operational Policies -> [DG] -> Equipment -> Power Policy	Equipment -> Policies -> Global Policies -> Power Policy

Table above show the correspondence of references between UCS Central and UCS Manager. The "UCSM GUI Navigation" column shows where the references will be "greyed-out" in the GUI, once the policies are configured to resolve globally at UCS Central and once the domain becomes part of a Domain Group.

a) General Best Practice

Best Practice

Take advantage of the Domain Group hierarchy to minimize the number of Operational Policies defined. Operational Policies could be segmented in to non-disruptive (e.g. "DNS", "Timezone", "CallHome", etc), and potentially disruptive (e.g. "Firmware Management"). Administrators are encouraged to put as much non-disruptive common policy configuration as high up in the DG hierarchy as possible. Similarly, any potentially disruptive Operational Policies should be put as low in the DG hierarchy as possible.

b) Authentication

Currently, configuration of Authentication domains and schemes are done individually, per UCS domain. UCS Central provides the ability to globalize the configuration of Authentication across all UCS domains.

If so desired and appropriate, DG's could be defined, based on different authentication configuration.

General best practices are to aim for simplicity and to minimize/centralize the number of authentication schemes/definitions, whenever possible. Similarly, if access to multiple authentication schemes/definitions is required, then aim for simplicity when constructing the mapping of authentication schemes/definitions on to UCS Central DGs.

c) Monitoring (SNMP, Syslog, Call Home)

Generally, the field of system health and monitoring (SNMP, Syslog, Call Home, etc) are all reasonable candidates for common Global Policy. The simplest way to implement this is defining SNMP, syslog, and Call Home policies as Operational Policies as high up in the DG hierarchy as possible. All domains in the subordinate DG's would then inherit these global policy definitions.

d) DNS management

Typically, DNS management is defined at a global/corporate level. Therefore, DNS "domain" names and DNS servers are easy candidates for Global Policy management, typically defined as high up in the DG hierarchy's Operational Policies as possible.

e) RBAC

RBAC is typically linked in to global/corporate level authentication, such as LDAP/AD. For UCS Central, continuing to enforce central control on access would be a preferred best practice, whenever possible.

If central authentication and role management is not currently in place, then administrators would be encouraged to define role-based access within UCS Central, as high up in the DG hierarchy's Operational Policies as possible, as a best practice.

f) Power Management

Policies around Power Management include two different policies:

- "Global Power Allocation Policy". Determines whether caps are applied at the chassis level, or manually overridden at the individual blade level
- "Power Policy". Chassis-level configuration of "N+1", "Grid", or "Non-redundant" for the physical AC power.

The "Power Policy" is likely the best candidate for central policy definition.

However, the "Global Power Allocation Policy" is possibly the most sensitive to environmental/location dependencies, with no obvious best practice to offer. For example:

- Power budgets per rack could vary amongst different datacenters and locations.
- Some sites may have taken advantage of Power Groups to create power caps that span multiple racks, specific to a given datacenter layout.

"Power Policy" is likely the most dependent on local constraints. Definition schemes, such as creating broadly scoped policy to restrict power on a per-rack basis would be the most simple. However, its practicality is going to be site specific and hard to generalize.

g) Importing Operational Policies

Best Practice

For "Operational Policies" under "Operational Management", many of the policies have the option of importing policy definitions from existing domains. In general, this is an easy and convenient way of "promoting" a locally defined policy in to UCS Central, and then ensuring consistency by applying the new global policy across multiple domains.

8. UCS Central Adoption : Approaches and Challenges

Successful adoption of UCS Central requires a sense of comfort that can only come with familiarity and a sense of orientation. While UCS Central has a great deal in common with UCSM, there are also some differences and challenges, outlined in this section.

a) UCSM Platform Emulator

The best way to get oriented and gain familiarity while averting all risk is to take advantage of the UCSM Platform Emulator. The UCSM Platform Emulator (PE) runs as a virtual machine, yet is a complete instance of the UCS Manager that maintains the UCS Management Information Tree, Data Management Engine, and exports the UCS XML/API. In addition, the PE has the ability to import both the physical hardware configuration as well as the logical configuration of an actual UCS domain.

Best Practice

With the PE, UCS administrators can effectively model their entire UCS environment, along with UCS Central. In this way, all configuration changes, testing, etc. can be done in a "safe sandbox", without any impact to actual production domains.

For testing any integration with UCS Central, be sure to use the 2.1(2a) version of the PE.

b) New UCS Deployments ("Greenfield")

Once comfortable with the UCS Central management model, the best practice is to adopt UCS Central with Global Pools/Policies/ServiceProfiles for any new UCS domain deployments going forward. Environments with no previous UCS footprint are strongly urged to use UCS Central with Global Service Profiles/Pools/Policies during the adoption and deployment of Cisco UCS and to avoid adoption of local objects when possible. Global Service Profiles refer exclusively to the Global Pools and Global Policies.

c) Migration of Existing Deployments ("Brownfield")

Administrators are encouraged to adopt UCS Central for new workloads that get deployed in existing UCS domains. By following the best practices, administrators can "opt-in" to the UCS Central global management model gradually over time, while not posing any disruption to existing workloads.

Administrators also have the ability to construct Global Pools/Policies/GSP-Templates that correspond to the attributes and profiles of their existing local workload. Such a transformation needs to be done manually for now, but gives administrators the opportunity to gain familiarity and orientation with UCS Central.

When adopting UCS Central for UCS domains with existing workloads, please take note of current caveats and limitations[13]. In particular, existing workload should be left in a locally managed mode for the time being.

UCS Central is designed to be the focal point of UCS Management going forward. For datacenters with existing UCS domains, adoption of UCS Central should be strongly considered for simplifying future growth management challenges.

d) Local Affinity Issues

As policy and control becomes centralized in UCS Central, certain challenges may arise that highlight affinity for local resources and control points. These are referred to as "Local Affinity" issues, with respect to local/individual domains. Here is a list of common affinity points, along with possible workarounds[14]:

- **External IP Pools** : These are the addresses for out-of-band management of physical blades (KVM, Power, etc.). However, UCS Central does not automatically associate these addresses to blades, as UCS Manager does. Workaround: Use Management IP Addresses associated with Service Profiles (or Templates), so that Global External IP Pools can be referenced. Ensure that all UCS domains and all External IP addresses are on a common subnet.
- **Boot Policies**: These have hard association to WWPNs of a specific Storage Array, making it hard to configure Global Service Profiles with the same boot policies on a worldwide basis, potentially across different Storage Arrays. Workaround: Use the same workaround as today with UCSM today : create SP Templates that are named as SP-StorageArray pairs.

9. Backup of UCS Central

Backup of UCS Central configuration on a regular basis is essential. The UCS Central management model is an extension of the core UCS management model. But there are constructs within UCS Central that are not present within the base UCS model. For example, the construct of "Domain Groups" is only present within UCS Central. Without proper/regular backups, there is no automatic way to reconstruct DG configuration.

Similarly, since Operational Policies terminate on DGs, without proper/regular backups of UCS Central, there is no automatic way to reconstruct the mapping of these Operational Policies on to DGs and the subordinate, individual UCS domains.

[13] See Sections 15 and 16 ("Take Note" and "Known Caveats")

[14] External IP Pools and Boot Policies are targeted for "alias" capability in an upcoming release, similar to the existing "ID Range Qualification" policies for Domain Groups.

Given the small size of a UCS Central backup (usually much less than 1 MB), backups should be scheduled once a day, or should correspond to the number and frequency of configuration changes.

10. Backup of UCS Domains

UCS Administrators would be advised to use their existing backup frequency as a starting reference point. Management through UCS Central does not change the need for taking regular/frequent UCS backups. But management through UCS Central does help simplify and automate individual backup operations.

Backup and Export Policies are defined per DG. However, a best practice would be to define these policies in the "root" DG, so that backups can be easily and automatically taken for all domains.

Typical backups of individual UCS domains might be ~100 KB, which is easily small enough to justify frequent backups. (Full-state binary backups might be ~2MB).

11. Upgrading UCS Central

Please review all available release notes at time of upgrade.
http://www.cisco.com/en/US/products/ps12502/prod_installation_guides_list.html

Please note there are version compatibility requirements between UCS Central 1.0(1a) and 1.1(1a):

- UCS Central 1.0(1a) supports communication with UCSM 2.1.1 and UCSM 2.1.2
- UCS Central 1.1(1a) supports communication **only** with UCSM 2.1.2

Therefore, prior to attempting an upgrade of UCS Central to 1.1(1a), all registered UCS domains must first be upgraded to UCSM 2.1.2

Two approaches exist for upgrading from UCS Central 1.0. You can either upgrade the existing VM in place using the ISO method, or upgrade by creating and migrating to an entirely new instance of UCS Central.

a) In-place Upgrade

The in-place ISO upgrade method is documented in the Upgrade/Installation Guide.

Before Upgrading UCS Central, take a snapshot of the VM using Snapshot Manager if you plan to do an in-place upgrade, to preserve the state of 1.0(1a) VM, in case

there is a need to revert to original state. Customers should also take a full state backup and a config-all backup of the 1.0(1a) VM in UCS Central, prior to upgrade.

b) New VM Upgrade

Best Practices recommend that customers preserve the existing 1.0(1a) instance as a backup. In this case, the upgrade sequence would be:

- Take UCS Central "config-all" Backup of the 1.0(1a) instance. Make sure the Backup State is "enabled".
- Power-off (but do not delete) the 1.0(1a) UCS Central VM
- Deploy the 1.1(1a) UCS Central VM with the same network configuration and shared secret
- Do an "Import" from the "config-all" backup file, using the "merge" option (do not use the "replace" option). Make sure the Import State is "enabled".
- Do a sanity check on Domain Groups, Global Pools and Operational Policies to ensure consistency of the restore operation.
- (Optionally) Eventually unregister and delete the original VM from disk (or leave powered-off as an archive)

The local UCS domains will lose visibility to UCS Central, but should change state back to "registered" once upgrade is complete. An "Unregister / Register" cycle is not expected with UCS Central upgrades, but may be required.

Be sure to use the "merge" (not "replace") when importing UCS Central configuration from version 1.0(1a).

Ensure that the archived 1.0(1a) VM and the new 1.1(1a) VM are never running concurrently.

Keep in mind the version compatibility requirements of both UCSM and the Host OS, in case a downgrade is needed of either UCS Central or UCSM.

12. Statistics Database Support

The 1.1(1a) release now provides support for statistics to be maintained for long-term historical trending, using either the internal UCS Central database, or an external database. The external databases supported as of 1.1(1a) are Oracle and Postgres.

Use of an external database can be configured at any time after an installation or upgrade of 1.1(1a). Furthermore, the database type can be changed after the fact, though must be done

out-of-band with respect to UCS Central and will involve a complete database export/import operation. Any database conversion would need to be done at the SQL/database level. Configuration of an external database can only be done through the CLI. Please refer to the CLI Configuration Guide.

The following guidelines should be used to help size an external database[15]:

- Collecting statistics data from 20 UCS Domains each with 5 Chassis (800 servers total) for 1 year requires a minimum of 400GB storage on the database server.
- Collecting statistics data from 100 UCS Domains each with 5 Chassis (4000 servers total) for 1 year requires a minimum of 2TB storage on the database server.

UCS Central does not backup the externally connected Statistics Database. Backup of the Statistics Database must be managed independently from UCS Central.

A preconfigured Postgres database appliance is available on http://communites.cisco.com/ucsm for Demo's and Proof-of-Concept testing --- but is not supported for production environments.

13. Firmware Management for UCS domains

Upgrading UCS domains has typically been a manual process, up til now[16]. The 2.1 release of UCSM has a new "Firmware Auto Install" feature, to help automate tasks that were previously manual[17]. UCS Central builds upon this new feature to help in automating firmware upgrades across potentially multiple UCS domains.

Please keep in mind there are two types of "firmware". Infrastructure firmware refers to the images that run in the I/O Modules, the Fabric Interconnects and the UCS Manager. Server firmware refers to the images that run on a physical server's BIOS, CIMC, Adaptors and Controllers. As with UCS Manager in general, the best practices for server firmware are to leverage Host Firmware Packages as part of the Service Profile definition, to guarantee configuration consistency at the application level.

Several important points need to be clear, regarding this capability:

a) Service degradation and/or disruption

Any UCS infrastructure firmware upgrade will still cause at minimum a service degradation, as each Fabric Interconnect must sequentially go through a reboot cycle. Administrators and Operators are urged to ensure that appropriate

[15] Generally plan on 0.5GB per server per year
[16] Unless you used Eric William's UCS Firmware Upgrade script: http://developer.cisco.com/web/unifiedcomputing/community/-/blogs/cisco-ucs-powertool-examples
[17] The "autoinstall" feature is not recommended for upgrading to UCSM 2.1(2a)

application-level "availability" schemes are in place, such as NIC teaming/bonding and host-based storage multi-pathing.

b) Pending Acknowledgement

Upgrading Firmware and rebooting FI's require explicit acknowledgement from the UCS Central administrator. Administrators should pay attention for "Pending Acknowledgements" under "Schedules"[18] for the DG's that are being upgraded. Default behavior is that all Firmware Upgrades ("infra-fw") and reboots ("fi-reboot") need to be Acknowledged before they proceed. The best vantage points for viewing progress on UCS Central is the "Active Tasks"[19] tab from the "Schedules" menu; for an individual UCS domain, follow
"Equipment -> Firmware Management -> Firmware Auto Install -> FSM".

Best Practice

There are no implicit maintenance policies for server firmware bundles. Therefore a best practice would be explicitly defining a maintenance policy that governed server firmware bundle upgrades. Best practice would be to define maintenance policies with "user-ack" chosen to avoid unexpected service interruptions.

The upgrade process does not complete in an "unattended" mode and will involve several Acknowledgements to complete.

One benefit of UCS Central is that multiple upgrades can proceed in parallel. If you are connected to the individual UCSM's, those connections will get reset, as you'd expect during an upgrade. As with standalone UCSM upgrades, the process takes roughly one hour to complete, but can run in parallel across multiple domains[20]. Upon completion, there should be no need to re-register with UCS Central.

Firmware Management can complement Host Firmware Policies. When bringing up a new UCS domain for the first time, using both infra and host firmware auto install triggered from UCS Central can ensure that a new domain is current with all low-level host firmware before being put into production.

14. Preparing for TAC

For any problems requiring a support case with Cisco TAC, be prepared to supply the output from "show tech-support". This can be done by navigating to "Administration -> Diagnostics -> Tech Support Files", and "Create and Download Tech Support File".

[18] Also visible under the InfraPack -> Pending-ack for each DG.
[19] Also visible in the InfraPack -> Status for each DG.
[20] The concurrency setting can be provided in the InfraPack tab(for infra firmware upgrades) and in the maintenance policy schedule(for server firmware upgrades)

15. Take Note (N.B.)

This section lists challenges that admins should be aware of, but which don't constitute product "Caveats"

a) Local Visibility of Global Objects

When Global Objects are created, they are not presented nor pushed in to UCSM automatically. Global IDs and Global Policies may be visible from the UCSM GUI drop-down menus when creating/modifying local objects. But Global Objects, once created, will not appear automatically in the UCSM GUI. Global Objects become visible in the UCSM GUI once Global Service Profiles are deployed to a server. At deployment-time, a read-only copy of the Global Object gets "pulled down" by the local UCSM, and are then visible in the GUI.

b) Maintenance Policies (local and global)

"User-ack" or "timer-automatic" is generally recommended universally, to avoid unexpected service interruption. If you want the user acknowledgement for service interruption to happen locally within UCSM, then create and use Maintenance Policies based on "user-ack". If you want the acknowledgement to happen within UCS Central, then chose "timer-automatic", and select a Schedule that uses the "user-ack"option.

c) Host OS versions from UCS Central 1.0(1a) to 1.1(1a)

UCS Central 1.0(1a) is supported on the following Host OS versions:

- VMWare: ESX4.0u2, 4.1u1, 5.0
- Windows: W2K8 R2 SP1

UCS Central 1.1(1a) requires the following Host OS versions:

- VMWare: ESX4.1u2, 5.0, 5.1
- Windows: W2K8R2 SP1, W2012

If upgrading from UCS Central 1.0(1a), be sure to upgrade the Host OS, if needed, before upgrading UCS Central.

d) External Statistics Database Backup

UCS Central does not backup the externally connected Statistics Database. Backup of the Statistics Database must be managed independently from UCS Central.

e) UCSM may require a forced Time sync

UCSM may appear to not sync the time, immediately after setting NTP.

UCSM can be forced to sync with NTP immediately, by setting the NTP Server in Admin tab, followed by attempting to set clock from the CLI with the following sequence:

- "scope system"
- "scope services"
- "set clock x x x x x" (Ex: "set clock may 22 2013 13 44 00")

A message should follow, indicating "Clock synchronization successful", with UCSM time reflecting the change. Next registration attempt should then succeed.

f) Avoid Hypervisor Contention

Since UCS Central runs as a virtual appliance, it is subject to resource sharing, governed by the host OS hypervisor. One way to promote reasonable performance characteristics is to make use of "resource pools" in either the VMware or Hyper-V environments. The purpose of using "resource pools" is to make sure that CPU and/or Memory contention is avoided or minimized for UCS Central. To ensure that UCS Central is appropriately favored, it can be placed in its own dedicated resource pool, with both CPU and Memory Shares settings set to "High", instead of the default "Normal". Please refer to the Installation/Upgrade Guide.

g) High-Availability Cluster-mode

High-availability (H/A) with UCS Central in Cluster-mode refers to a single instance of UCS Central. H/A mode is not the same and should not be confused with Disaster-recovery (DR) mode, which implies two distinct instances.

H/A with UCS Central can be achieved by:

- Installing a new UCS Central 1.1(1a) instance as an H/A cluster
- Converting standalone UCS Central 1.1(1a) to an H/A cluster.
- First upgrading a 1.0(1a) instance to 1.1(1a) and then enabling H/A cluster mode

Upgrades from 1.0(1a) can only be done in Standalone mode.
Be sure to refer to the Installation/Upgrade Guide, before attempting.

When deploying in Cluster-mode, make sure that:

- Both VMs are on separate physical hosts with access to shared storage.
- Both VMs are running the same version of ESX or HyperV.
- Both VMs are running the same version of UCS Central.
- Both VMs are on the same sub-net.

Cluster H/A mode does require the configuration of a Shared LUN, presented as a raw device. This will require configuration privileges on the SAN in order to:

- Zone both hypervisor clustered hosts with the Storage Array from the SAN switch
- Provide access to the Shared LUN for the clustered hosts from the Storage Array (LUN masking)

Ensure sure that:

- Thick Provisioning is used for the Shared LUN (not Thin Provisioning)
- Access to the Shared LUN is exclusive for the 2 clustered hosts (not being used by any other hosts)
- LUN is not configured in multi-pathing mode on the hosts (e.g. LUN should be mapped in Fixed I/O mode on ESX hosts)

For best performance of the shared storage:

- Configure high speed SAN connections to enable fastest access
- Select the best performing RAID type for the shared LUN
- Make sure the storage is write-cache enabled and properly configured[21].

Take care if using features such as suspend/resume or restoring VM snapshots, which could create a shared storage "conflict of ownership". Shared storage is always mounted on the Primary VM. Having the Secondary VM claim ownership while the Primary is still active may result in a crash or the cluster going down.

16. Known Caveats as of 1.1(1a)

This section will list all known caveats for the current release --- 1.1(1a). Addressing these caveats is a high-priority.

a) UCS Central Admin policies in the “root” DG

The current release presents Operational Policies for the management of UCS Central itself under the “root” DG in Operations Management. Configuration of Locales and Locally Authenticated UCS Central users is placed under Admin tab. Configuration which is applicable for both UCSM and UCS Central is still present under Operational Policies tab.

Workaround: Do not populate the “root” DG with domains. Create/Populate DGs below the “root” DG, so as to avoid policy conflicts with UCS Central itself.

[21] For example, an EMC storage array should have the following cache configuration: Page Size: 8KB, Low watermark: 60%, High Watermark: 80%

b) LDAP Authentication

Please refer to Section "Best Practices: UCS Central Authentication" for more detail.

c) Global Org merging for Locales

In the current release, "orgs" that have service profiles are presented from UCSM to UCS Central as visible, but as read-only local objects. "Locales" in UCS Central possess true multi-tenancy, in that user visibility to org's and DG's is truly limited to the "locale's" corresponding to those org-DG pairs.

However, global "locales" can only be created on global orgs. Therefore, for sites using "orgs" and desiring true multi-tenancy, the following sequence is recommended:

1) Create Global Orgs in UCS Central for all UCS domains prior to actually registering with UCS Central
2) Register UCS domain with UCS Central. The local/global org namespace will get merged upon registration
3) Create Global Locales in UCS Central that map to the Global Orgs.

Admins not following this procedure will not be able to create global "locales" with true multi-tenancy. Any mistakes here may require unregister/re-register cycling, along with re-creation of the global orgs, in order to correct. As a workaround, creating a Global Org from the Network or Storage tab in UCS Central may allow Global Locales to be created without the re-register/re-create cycle.

d) Adopting Global MAC/WWxN Pools

The UCSM 2.1(2a) release along with the UCS Central 1.1(1a) release **will** cause service interruptions and ID re-assignment when Service Profile VNICs/VHBAs are changed from local to global ID pool references[22]. The previous version of this document erroneously indicated that service interruptions could be avoided if updating templates were used.

This problem will be addressed with urgency in UCSM 2.1(3)

To avoid possible service interruptions, the best approach is to let existing local SP's remain as local SP's, until the reach the end of their lifecycle. Any new SP's should be created as GSP's.

[22] Bug CSCud44377

e) Global UUID Pools

Transitioning to Global UUID pools creates particular challenges.

Prefixes. UUID Prefixes are defined at the domain level; UUID Suffixes can be used to create blocks within pools. Adopting Global UUIDs that are supersets of all local UUID pools would require creating at minimum one Global UUID pool per UCS domain. Therefore, the number of Global UUID Pools would be equal to the number of domains, at minimum, yielding no consolidation in the number of pools.

Orgs. Global Pools are based on Orgs. But UUID prefixes are based on Domains (internal IDs from the fabric interconnects). There is no mapping between Orgs and Domains, making it difficult to generalize a best practice.

Adoption. With the existing release existing Service Profiles cannot easily and seamlessly adopt to using Global UUIDs without incuring a reconfiguration cycle and a server reboot.

Workaround: Let existing local SP's remain as local SP's, until the reach the end of their lifecycle. Any new SP's should be created as GSP's.

f) Domain Group Re-assignment from Domain Group Policy

Changing the Domain Group Policy (subsequent to domain registration) no longer automatically re-assigns domains to DGs. DG re-assignment of domains will now only be affected by an explicit "Re-evaluate Membership" action on a given domain. This change in behavior was implemented in 1.1(1a) to reduce the impact of human errors.

g) Server Pool members aren't masked by RBAC

Viewing members of a Global Server Pool are not currently masked by RBAC. As a workaround, please use the "Equipment View" for viewing Server inventory. Viewing servers through the Global Server Pool view may allow visibility to pool members, for which any access and configuration may actually be constrained, due to RBAC.

h) UCS Faults Summary occasionally goes blank

This is a known problem. Please refresh your browser session.

i) Host FW Package and Maintenance Policies

During the 1.0(1a) release, Host FW Packages and Maintenance policies were erroneously structured within the Domain Group context. Due to the resulting

backward compatibility issues, Host Firmware Packages & Maintenance Policies are now both visible and configurable from a Domain Groups context as well as Orgs context.

The expected behavior for 1.1(1a) is:

- Global Service Profiles will only refer to the Host FW Package that is defined under Org context
- Local Service Profile (created in UCSM) can only refer to the Host FW Package from the Domain Group context --- same as release 1.0(1a)
- After a Global Service Profile is associated with a Server, the Host FW Package and Maintenance Policy (and any other referenced policies) are "pulled" from UCSM to UCS Central.
- Subsequently, a Local Service Profile can then refer to either the Host FW Package and Maintenance Policy from either the Org or Domain Group context.
- Global Service Profiles will only reference Host FW Packages and Maintenance Policies from Org context.

This behavior is due to backward compatibility issues with the 1.0(1a) release, where Maintenance policies, Host FW packages, and Schedulers are defined under the Domain Group context.

Best Practice

The Best Practice would be to configure and use Host FW Packages and Maintenance Policies exclusively from the Org context.

j) VLAN can appear unreferenced

If using "Modify VLAN Org Permissions" from the Network tab to limit VLAN scope across Orgs, and the VLAN is subsequently deleted, then other Global Service Profile VNICs within the referenced Orgs will still see the unreferenced "VLAN alias", presenting itself as a VLAN.

Workaround is to ensure that any VLAN alias gets deleted prior to deleting the respective VLAN itself.

k) Default FCoE VLAN ID is "1" for VSANs

When creating new VSANs from the "SAN Cloud", the default FCoE VLAN ID value is "1", which is in conflict with the "global-default" VLAN ID value.

Be sure to change the FCoE VLAN ID when creating new VSANs, and specify a VLAN that is not currently in use anywhere else.

l) VLANs and VSANs may persist locally

If VLANs/VSANs were created globally and subsequently pushed down through a GSP deployment, then they may persist in the local domain's MIT, even after the domain has de-registered.

m) Local UCS backups will not have global references

If backups are taken at the local UCSM level, then these backups will not have any references to Global objects that are managed by UCS Central.

If using UCS Central, then Backup/Export Policies should be used, with Backup operations managed exclusively by UCS Central.

n) Localization and Globalization

There is no way for Pools, Policies, and SPs to be automatically localized nor globalized. Migrating Local Objects to Global (or vice-versa) must be done manually.

o) SDK Support

The 1.1(1a) release does not include a Cisco developed SDK for automation. As such, there is no PowerTool or Python SDK that supports monitoring/configuring UCS Central in an automated fashion.

17. Summary

With great power comes great responsibility.

Please be careful.

Jeff Silberman is a Data Center Architect and part of the original UCS Technical Marketing Team, who has been focused on Server and I/O virtualization for the past 12 years. Jeff has authored the original "UCS Best Practice/Quickstart Guide", the "UCS Test Drive" and the "UCS Deep Dive Methodology". At Cisco, Jeff has been responsible for managing hundreds of customer proof of concepts, product reviews/demos, technical "Deep Dives" with UCS, and numerous Cisco Live presentations. Prior to Cisco, Jeff spent four years at NetApp in the Advanced Product Development Group, bringing some of the industry's first Unified Fabric solutions to market for Oracle®/NetApp environments.

18. Appendix I (Registration Troubleshooting)

If registration does not complete successfully, the following should be ensured after the UCS Central VM has been deployed:

1. Configure NTP server within UCS Central, via Operational Policies for the "root" Domain Group.
2. Regenerate certificates in UCS Central via CLI :
   ```
   connect local-mgmt
   re-generate certificate
   ```
3. Regenerate certificates in UCSM by cycling the http/https "Admin" state to restart the internal webserver
4. Ensure NTP server is configured in UCS domain, if not already configured
5. Register UCS domain with UCS Central

Registration from a UCS domain is typically[23] done through "Admin -> Communication Management -> UCS Central" in the UCSM GUI.

In UCSM, the shared secret is configured during registration and can be modified subsequently ("**`connect local-mgmt; set shared-secret`**"). If the shared secret is changed on UCS Central, then administrators should re-register with the new shared secret in all managed UCS domains.

In the event that local domains fail to complete registration to UCS Central, "keyring" regeneration in UCSM may be required. Example, if you are using the "default" keyring in UCSM, the UCSM CLI commands to fix this are:

```
scope security
scope keyring default
set regenerate yes
commit-buffer
```

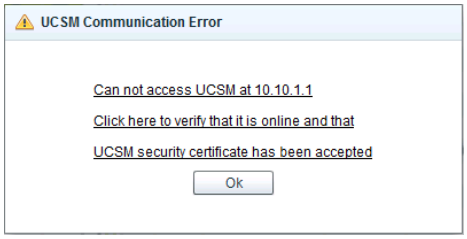
Additional certificate issues may result in failure to cross-launch UCSM GUI and KVM sessions, or failure in querying faults from UCS Central. In these cases, toggling the HTTP to HTTPS redirection from Admin -> Communication Services may fix the problem.

[23] Also available through latest PowerShell provider, corresponding to UCSM 2.1

19. Appendix II (Certificate Troubleshooting)

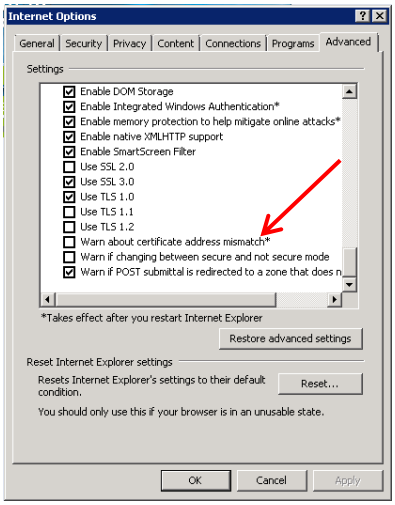
Cisco UCS Central – Troubleshooting Certificate errors
Version 1.0 - Jan 17, 2013

Many features of the UCS Central management interface rely on https certificates (from each UCS Domain being managed by UCS Central) to be available and imported on the client machine.
These certificates are used by the browser managing UCS Central for invoking features such as KVM Launch, UCSM GUI Launch, and query of particular faults/alerts in the UCS Fault Summary. If the certificates are not imported properly, have expired, or if the Web Browser being used has certain security settings enabled, the user may encounter the errors seen below:

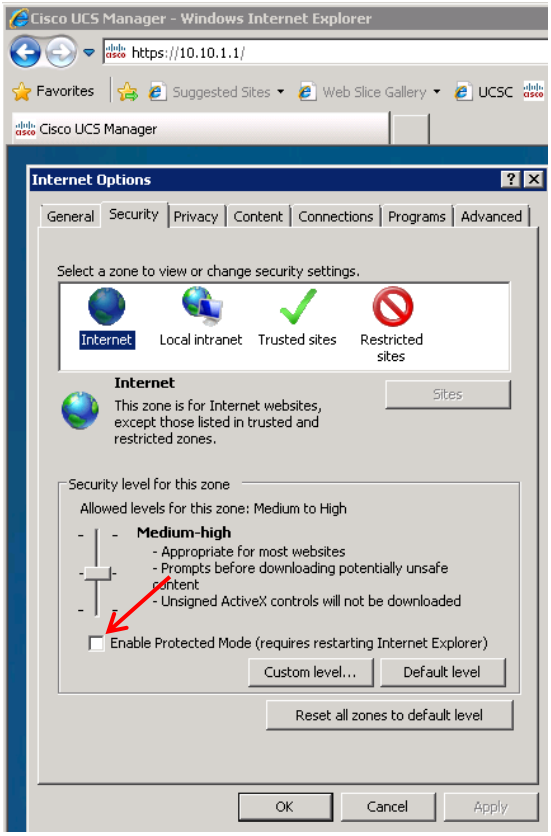


Internet Explorer

1. Be sure that IE is configured to NOT warn about a certificate address mismatch
    a. In IE: Tools → Internet Options → Advanced – at the very bottom in the section "Security", be sure to uncheck "Warn about certificate address mismatch" (Requires restart of IE)

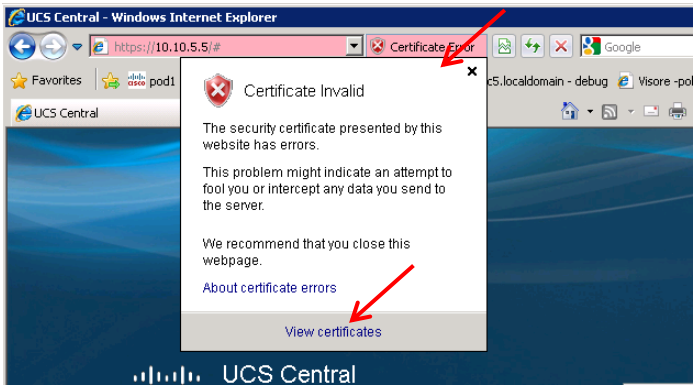


2. You may need to turn off “Protected Mode” so that Certificates can be imported.
    a. Tools → Options → Security Tab → uncheck the Enable Protected Mode checkbox for each zone:

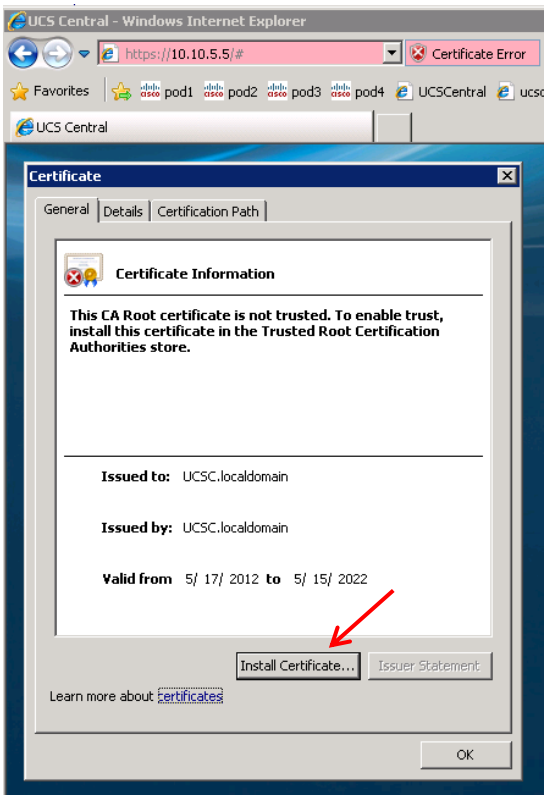


3. Upon initial connection to any UCS Central or UCS Manager, you will receive a Certificate Error. Import the presented certificate using this process:

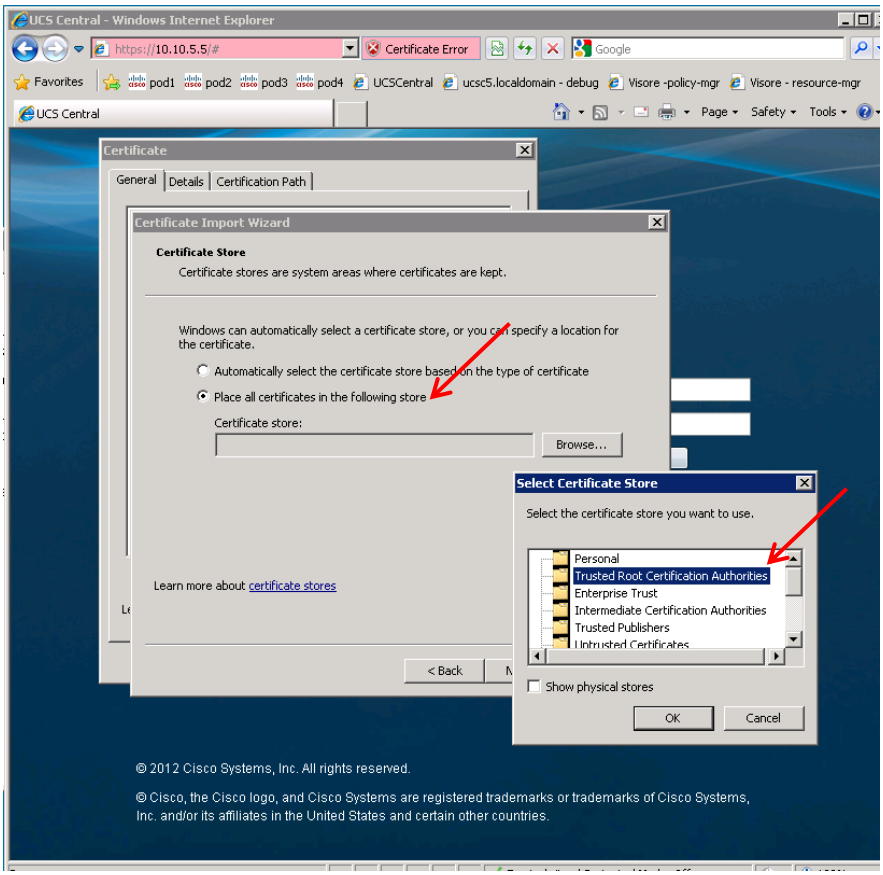
Click the Certificate error, then click view Certificates, followed by clicking Import



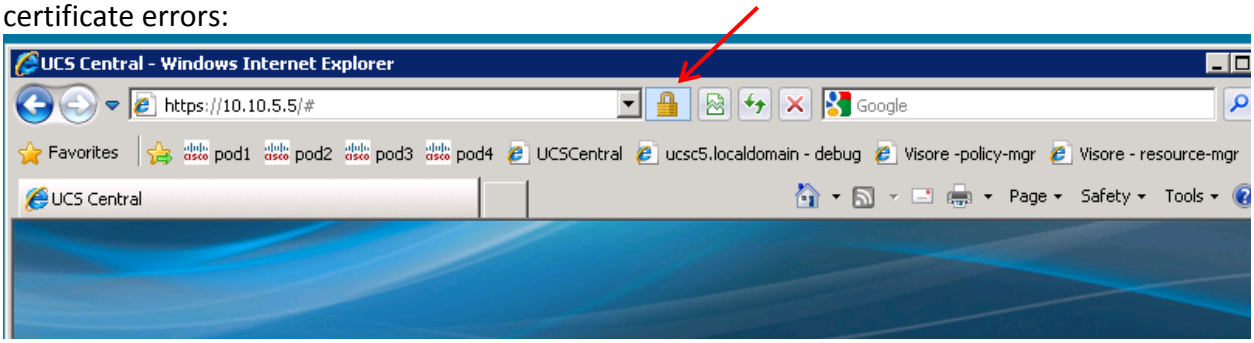
Then click Install Certificate:



Click next and select “Place all Certificates in the following store” radio button



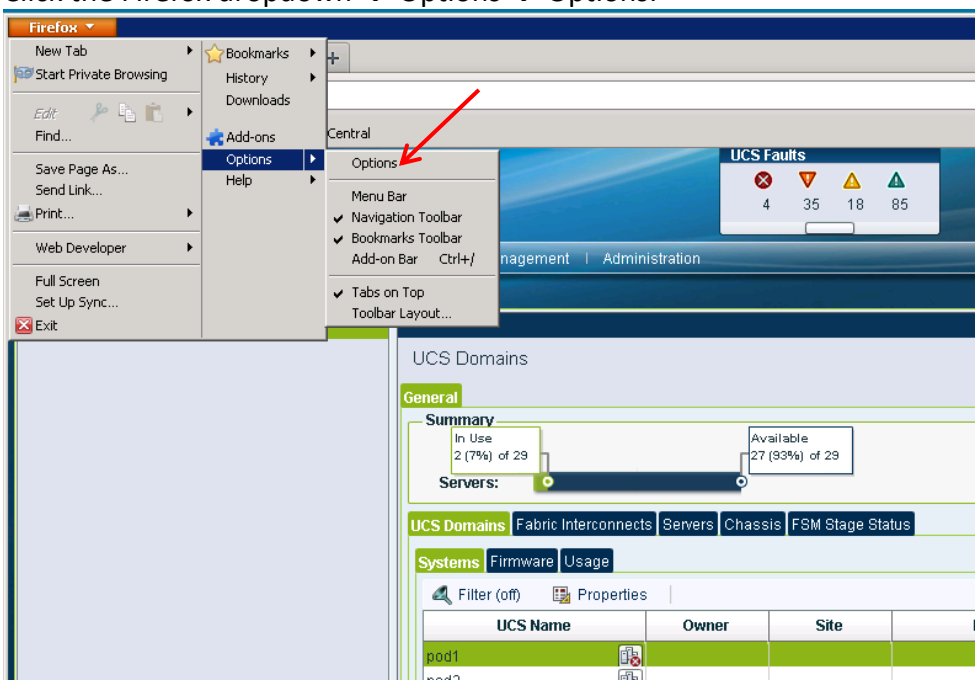
Click OK, Finish, and then **RESTART IE** – when you connect again in you should not see the certificate errors:

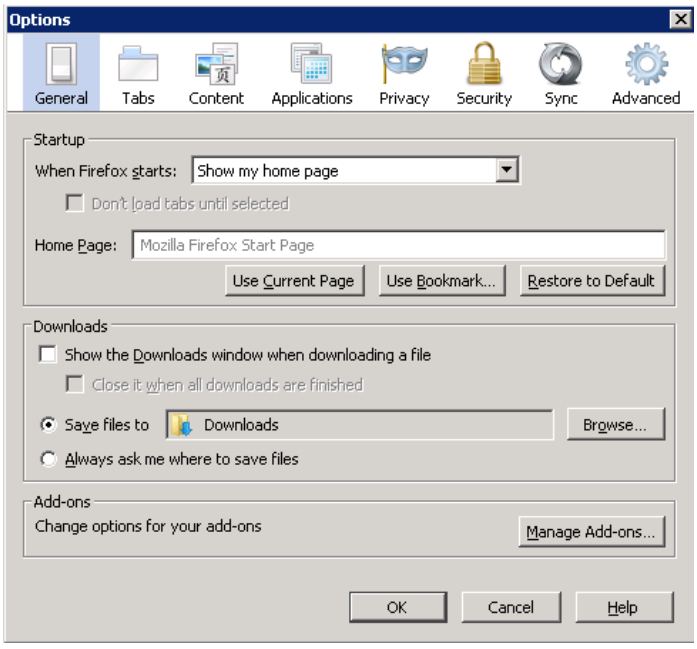


Mozilla Firefox

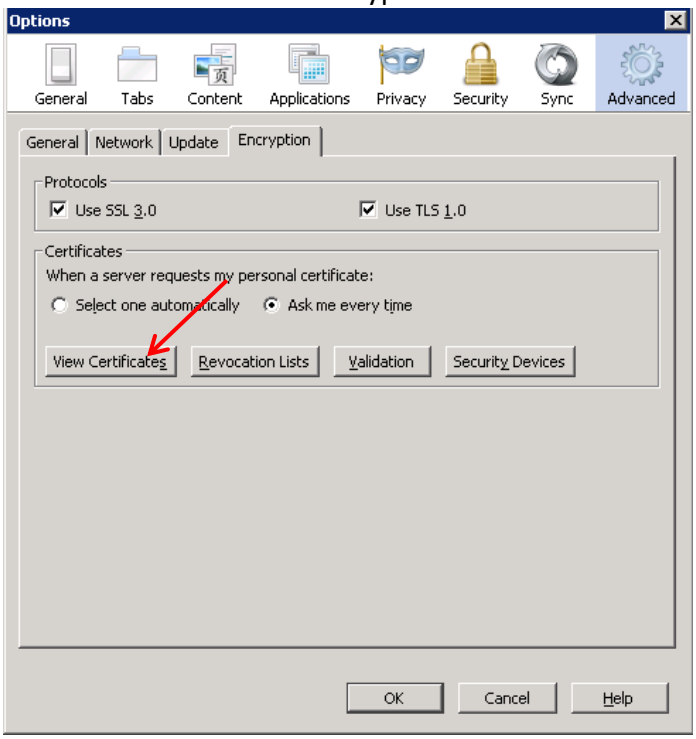
Steps to clear out all Certificates / cache:

Click the Firefox dropdown → Options → Options:

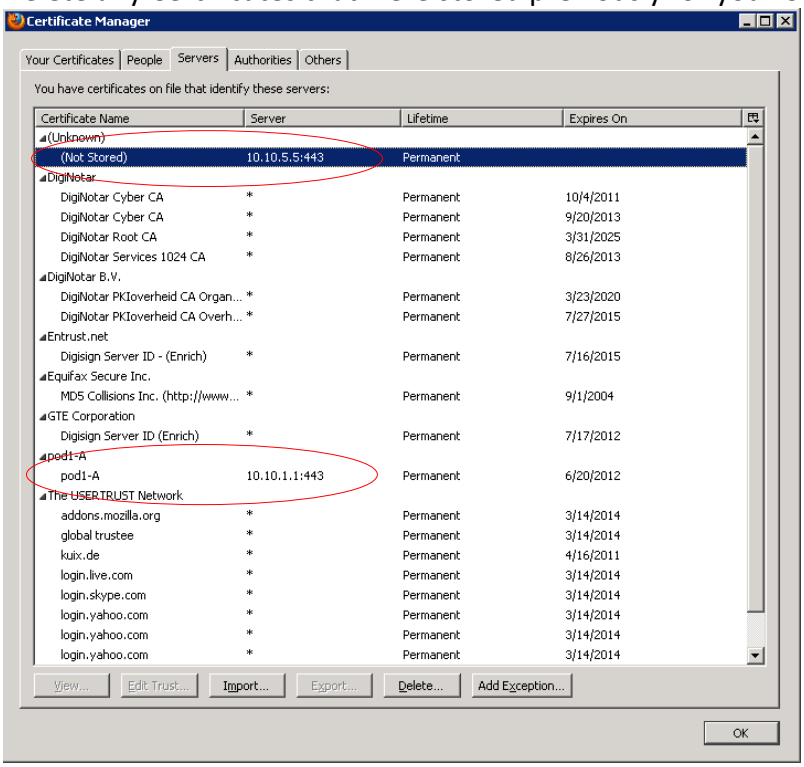




Next click Advanced → Encryption → View Certificates:

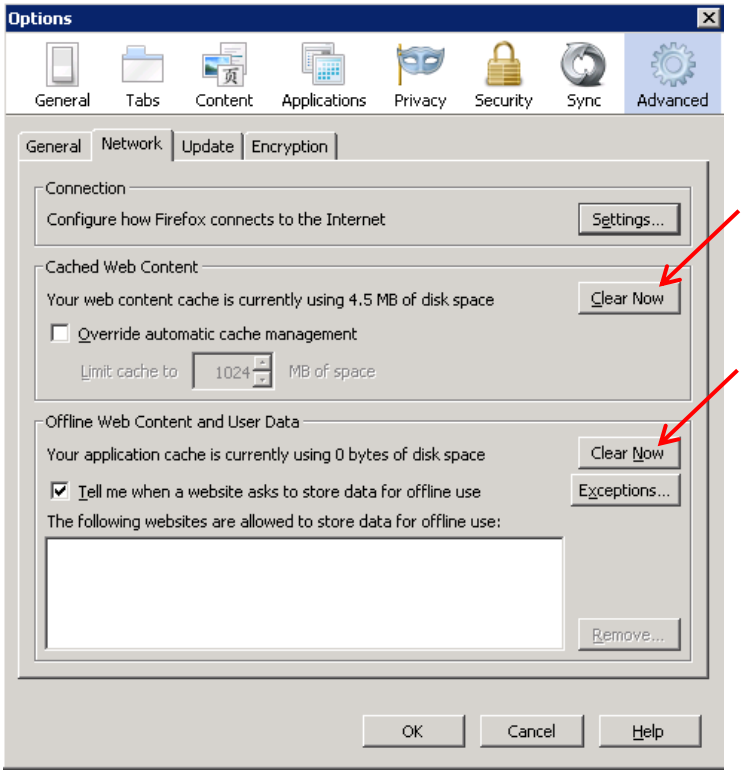


Delete any Certificates that were stored previously for your UCS or UCSCentral systems (only)



Once complete, clear the Web Cache. Click the Firefox dropdown → Options → Options, and then click The Advanced button, then Network tab.

- Click both of the "Clear Now" button s on this page – then click OK to close.

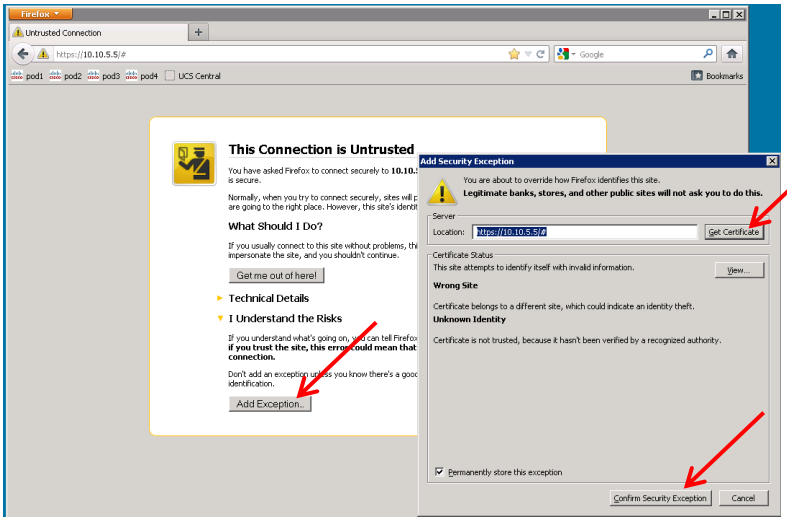


You should now be able to connect to UCSCentral (import certificate) and launch UCSM.

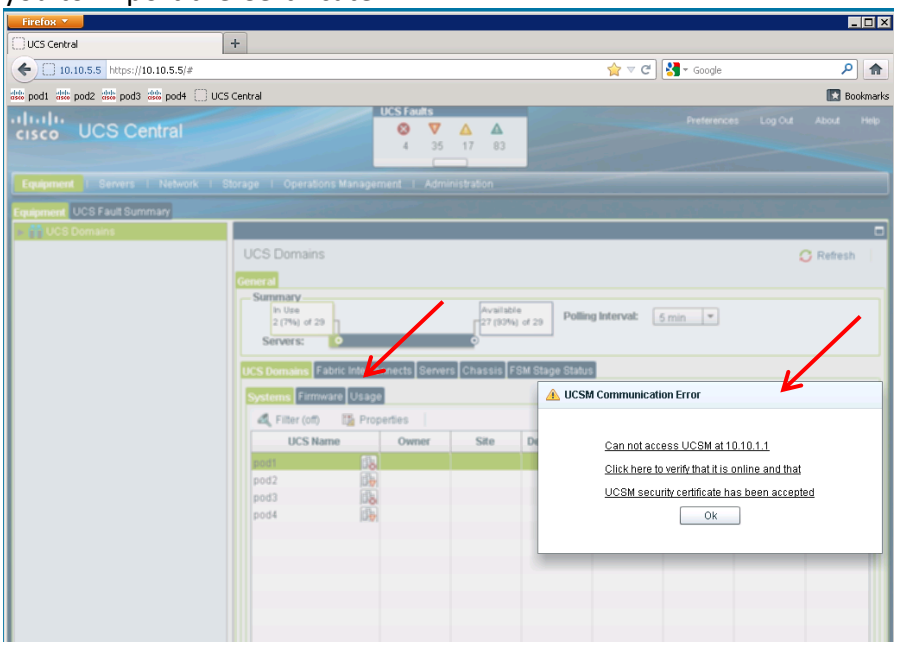
- Note: You will need to connect to each UCSM system (manually, or through UCSCentral) at least once to import the certificate, so that subsequent attempts to launch the GUI from within UCSCentral will happen without certificate errors.

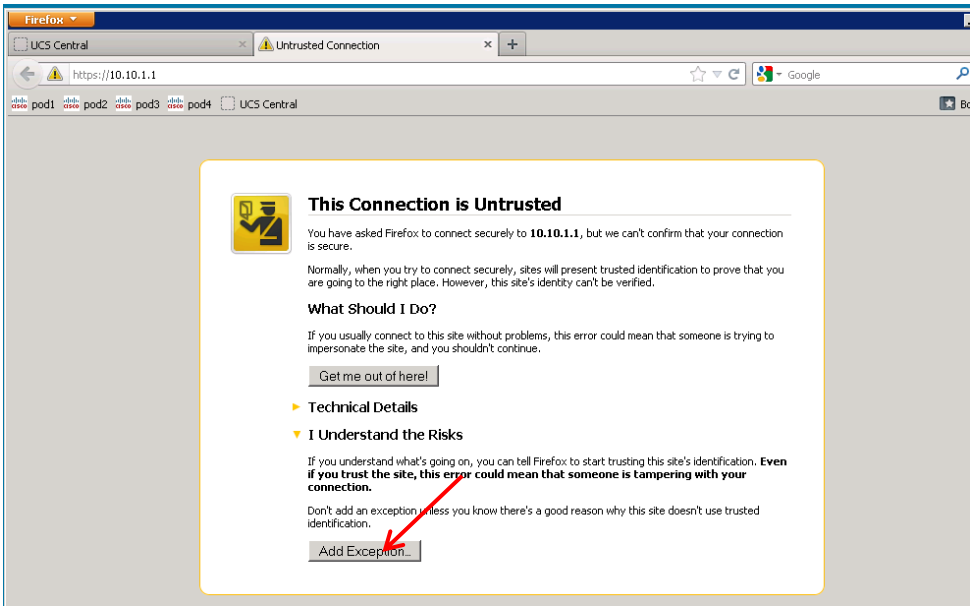
To add the certificate using Firefox:

- Click Add Exception, Get Certificate, and Confirm Security Exception as seen below



If Launching from UCS Central, Clicking the error in the link below will launch UCSM and allow you to import the Certificate





Other

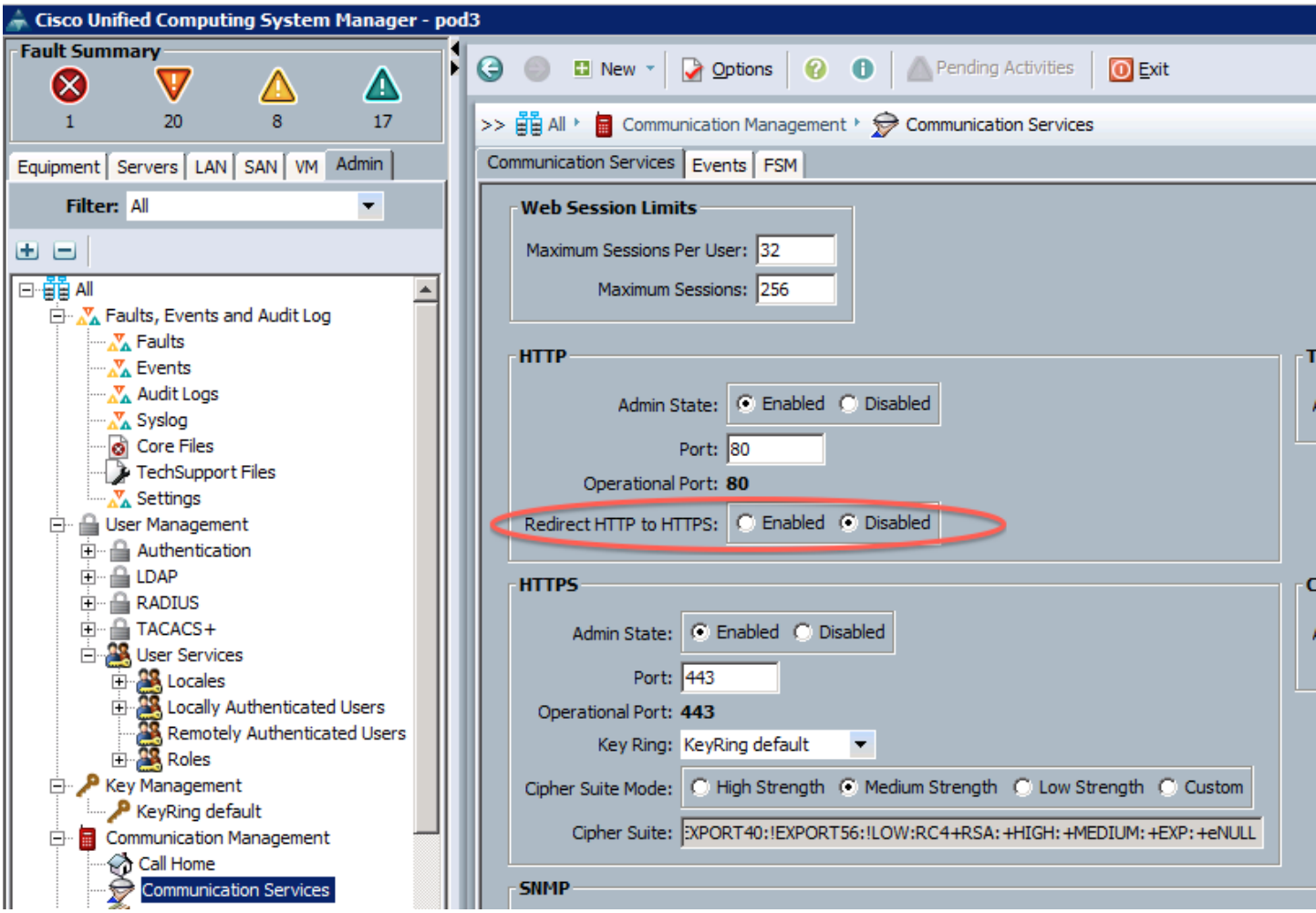
1. Expired Certificates:

Make sure that the HTTPS Certificates being presented by the Fabric Interconnects are not expired.

- If the Certificates are expired, The UCS Documentation details the process to "regenerate" new HTTPS Certificates:
- UCSM CLI commands: scope security; scope keyring <keyring_name>; set regenerate yes; commit-buffer

2. Bug affecting regeneration of new HTTPS Certificates on the Fabric Interconnects:

NOTE: There is a bug in 2.1(1a), where in some cases, after regenerating new HTTPS Certificates, that the old certificate are not published immediately to the web servers on the Fabric Interconnects. To work around this bug (until it is fixed in the next release), toggle the HTTP → HTTPS redirection setting in the Admin Tab / Communication Services:


Cisco Unified Computing System Manager - pod3
Fault Summary
1
20
8
17
Equipment
Servers
LAN
SAN
VM
Admin
Filter: All
All
Faults, Events and Audit Log
Faults
Events
Audit Logs
Syslog
Core Files
TechSupport Files
Settings
User Management
Authentication
LDAP
RADIUS
TACACS+
User Services
Locales
Locally Authenticated Users
Remotely Authenticated Users
Roles
Key Management
KeyRing default
Communication Management
Call Home
Communication Services
New
Options
Pending Activities
Exit
>> All
Communication Management
Communication Services
Communication Services
Events
FSM
Web Session Limits
Maximum Sessions Per User: 32
Maximum Sessions: 256
HTTP
Admin State: Enabled Disabled
Port: 80
Operational Port: 80
Redirect HTTP to HTTPS: Enabled Disabled
HTTPS
Admin State: Enabled Disabled
Port: 443
Operational Port: 443
Key Ring: KeyRing default
Cipher Suite Mode: High Strength Medium Strength Low Strength Custom
Cipher Suite: EXPORT40:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL
SNMP