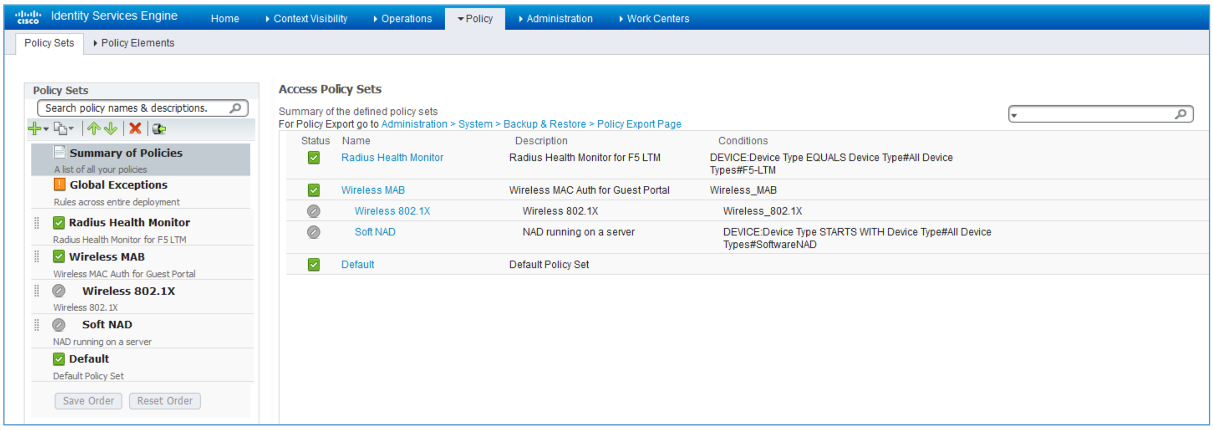
Policy Set changes after upgrade to ISE 2.3

It’s documented in the ISE 2.3 Release Notes, as well as in the ISE 2.3 Upgrade Guide. However those documents are difficult to understand, let alone, to get used to the new look and feel of the ISE 2.3 Policy Sets. Here are some examples of the pre- and post-upgrade

Radius Policy Sets

Before



Policy Sets

Search policy names & descriptions.

Summary of Policies
A list of all your policies

Global Exceptions
Rules across entire deployment

☑ **Radius Health Monitor**
Radius Health Monitor for F5 LTM

☑ **Wireless MAB**
Wireless MAC Auth for Guest Portal

⊘ **Wireless 802.1X**
Wireless 802. 1X

⊘ **Soft NAD**
NAD running on a server

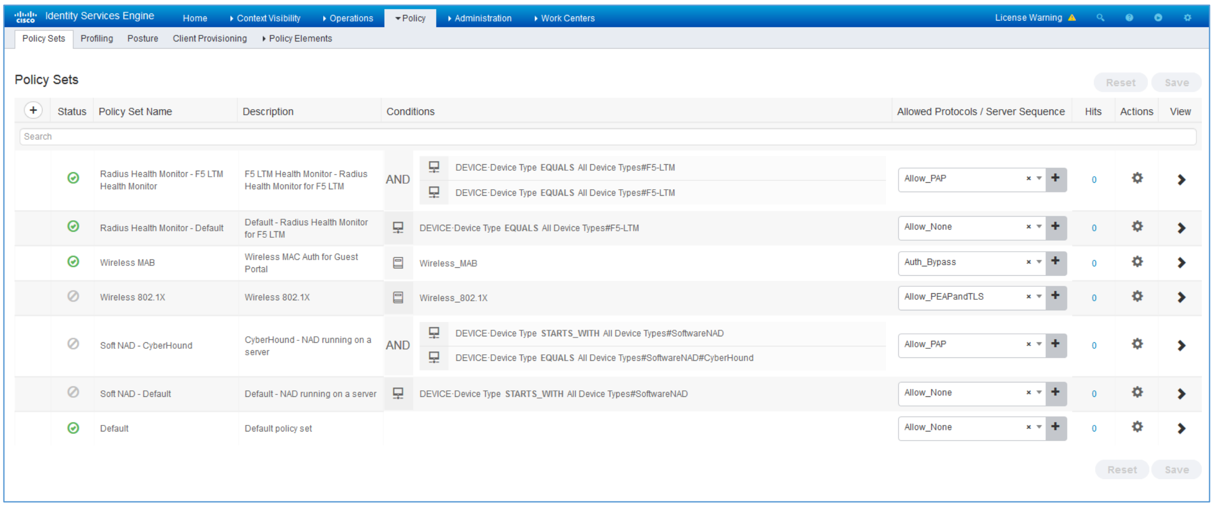
☑ **Default**
Default Policy Set

Access Policy Sets

Summary of the defined policy sets
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description	Conditions
☑	Radius Health Monitor	Radius Health Monitor for F5 LTM	DEVICE:Device Type EQUALS Device Type#All Device Types#F5-LTM
☑	Wireless MAB	Wireless MAC Auth for Guest Portal	Wireless_MAB
⊘	Wireless 802.1X	Wireless 802.1X	Wireless_802.1X
⊘	Soft NAD	NAD running on a server	DEVICE:Device Type STARTS WITH Device Type#All Device Types#SoftwareNAD
☑	Default	Default Policy Set	

After



Policy Sets

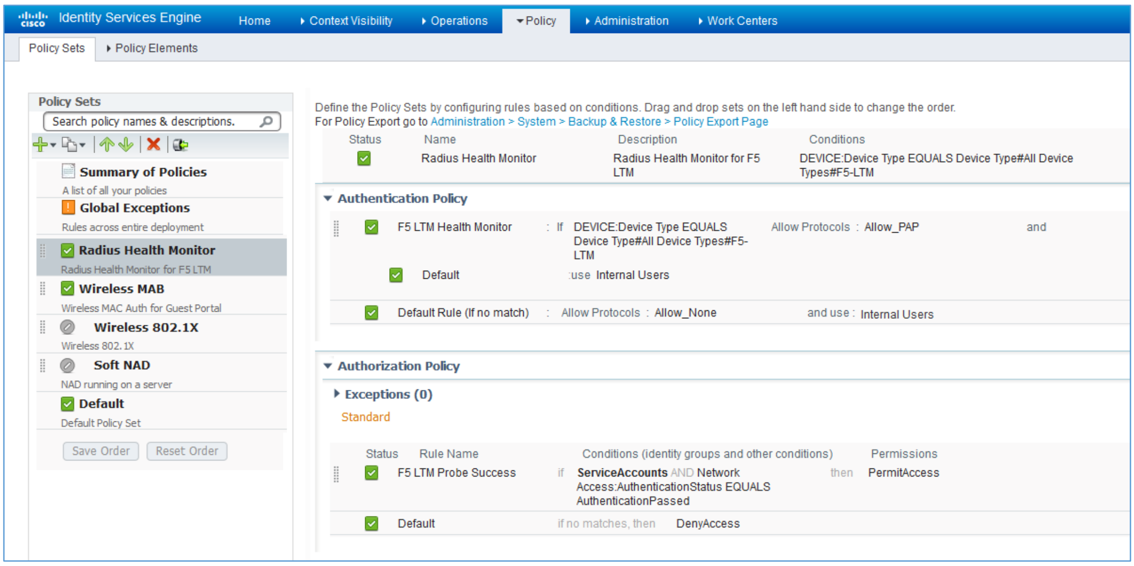
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Radius Health Monitor - F5 LTM Health Monitor	F5 LTM Health Monitor - Radius Health Monitor for F5 LTM	AND DEVICE·Device Type **EQUALS** All Device Types#F5-LTM DEVICE·Device Type **EQUALS** All Device Types#F5-LTM	Allow_PAP	0	⚙	›
✓	Radius Health Monitor - Default	Default - Radius Health Monitor for F5 LTM	DEVICE·Device Type **EQUALS** All Device Types#F5-LTM	Allow_None	0	⚙	›
✓	Wireless MAB	Wireless MAC Auth for Guest Portal	Wireless_MAB	Auth_Bypass	0	⚙	›
⊘	Wireless 802.1X	Wireless 802.1X	Wireless_802.1X	Allow_PEAPandTLS	0	⚙	›
⊘	Soft NAD - CyberHound	CyberHound - NAD running on a server	AND DEVICE·Device Type **STARTS_WITH** All Device Types#SoftwareNAD DEVICE·Device Type **EQUALS** All Device Types#SoftwareNAD#CyberHound	Allow_PAP	0	⚙	›
⊘	Soft NAD - Default	Default - NAD running on a server	DEVICE·Device Type **STARTS_WITH** All Device Types#SoftwareNAD	Allow_None	0	⚙	›
✓	Default	Default policy set		Allow_None	0	⚙	›

The first thing that strikes me as odd, is the F5 LTM Health Monitor and its AND condition – seems superfluous. And also the “Radius Health Monitor – Default” – looks like I need to delete that line, since it makes no sense here.

The same goes for any other Default Conditions that have been migrated.

Let’s Look at he F5 Health Monitor in more detail

Before



Policy Sets

Search policy names & descriptions.

- ☐ **Summary of Policies** – A list of all your policies
- **Global Exceptions** – Rules across entire deployment
- ☑ **Radius Health Monitor** – Radius Health Monitor for F5 LTM
- ☑ **Wireless MAB** – Wireless MAC Auth for Guest Portal
- **Wireless 802.1X** – Wireless 802.1X
- **Soft NAD** – NAD running on a server
- ☑ **Default** – Default Policy Set

Save Order | Reset Order

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description	Conditions
☑	Radius Health Monitor	Radius Health Monitor for F5 LTM	DEVICE:Device Type EQUALS Device Type#All Device Types#F5-LTM

Authentication Policy

☑ F5 LTM Health Monitor : If DEVICE:Device Type EQUALS Device Type#All Device Types#F5-LTM Allow Protocols : Allow_PAP and
☑ Default :use Internal Users

☑ Default Rule (If no match) : Allow Protocols : Allow_None and use : Internal Users

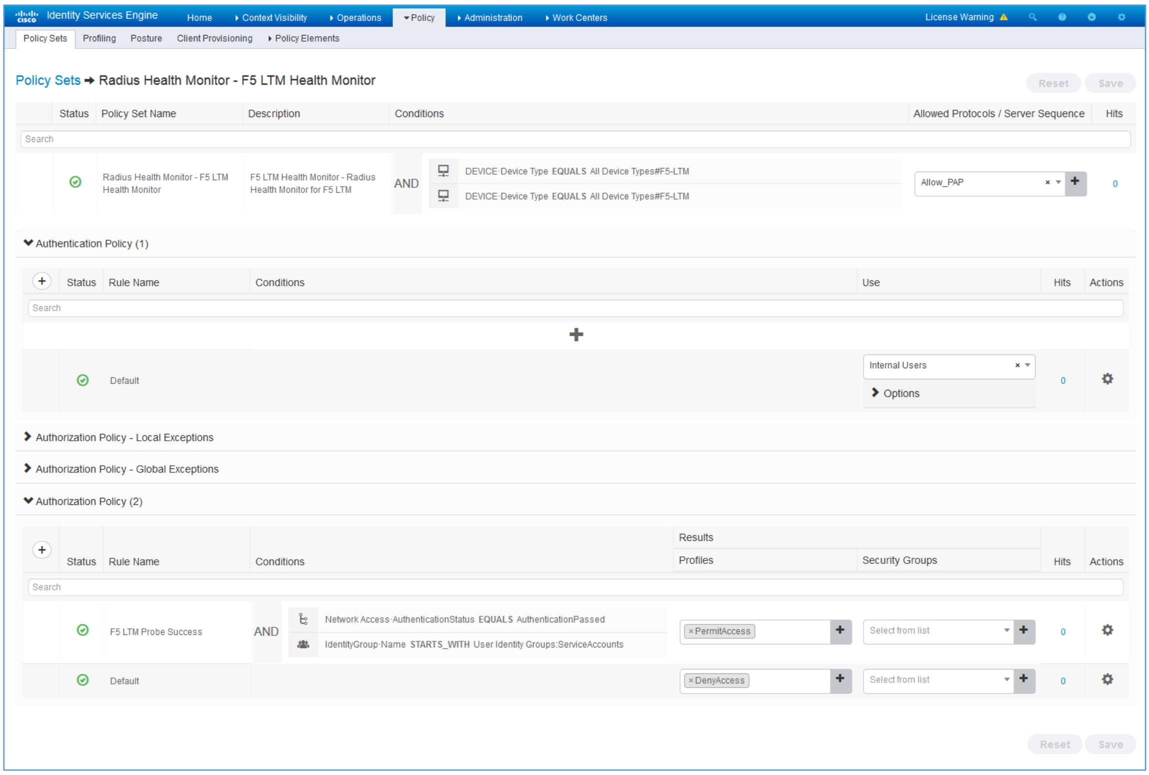
Authorization Policy

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	F5 LTM Probe Success	if	**ServiceAccounts** AND Network Access:AuthenticationStatus EQUALS AuthenticationPassed	then	PermitAccess
☑	Default	if no matches, then			DenyAccess

After



Policy Sets ➡ Radius Health Monitor - F5 LTM Health Monitor

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Radius Health Monitor - F5 LTM Health Monitor	F5 LTM Health Monitor - Radius Health Monitor for F5 LTM	AND DEVICE·Device Type EQUALS All Device Types#F5-LTM DEVICE·Device Type EQUALS All Device Types#F5-LTM	Allow_PAP	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users Options	0	⚙

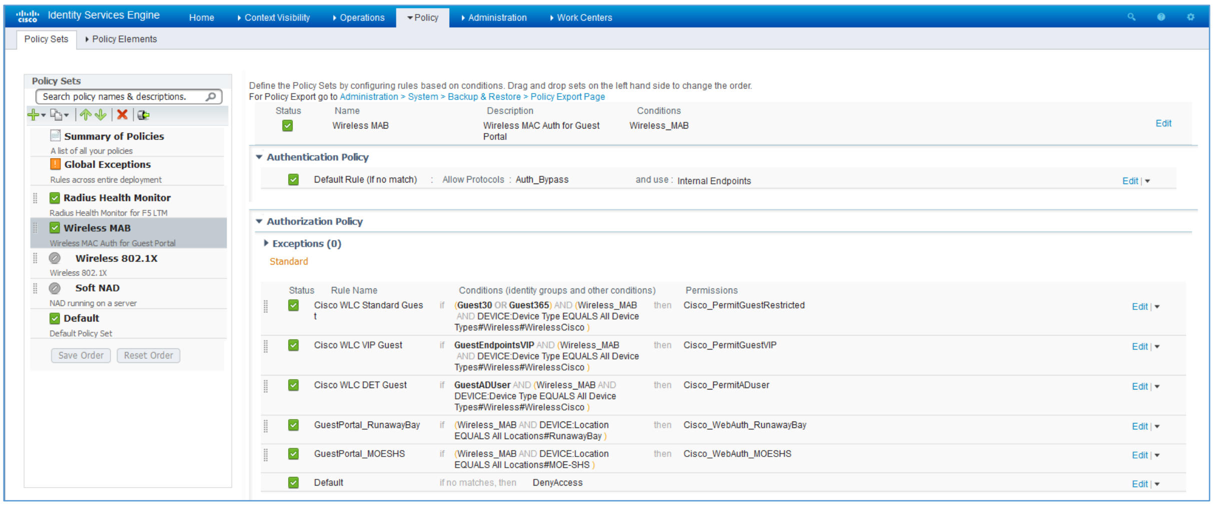
Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	F5 LTM Probe Success	AND Network Access·AuthenticationStatus EQUALS AuthenticationPassed IdentityGroup·Name STARTS_WITH User Identity Groups:ServiceAccounts	PermitAccess	Select from list	0	⚙
✓	Default		DenyAccess	Select from list	0	⚙

Before



Policy Sets

- ☐ **Summary of Policies** — A list of all your policies
- **Global Exceptions** — Rules across entire deployment
- ☑ **Radius Health Monitor** — Radius Health Monitor for F5 LTM
- ☑ **Wireless MAB** — Wireless MAC Auth for Guest Portal
- **Wireless 802.1X** — Wireless 802. 1X
- **Soft NAD** — NAD running on a server
- ☑ **Default** — Default Policy Set

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description	Conditions	
☑	Wireless MAB	Wireless MAC Auth for Guest Portal	Wireless_MAB	Edit

Authentication Policy

☑ Default Rule (If no match) : Allow Protocols : Auth_Bypass and use : Internal Endpoints Edit |

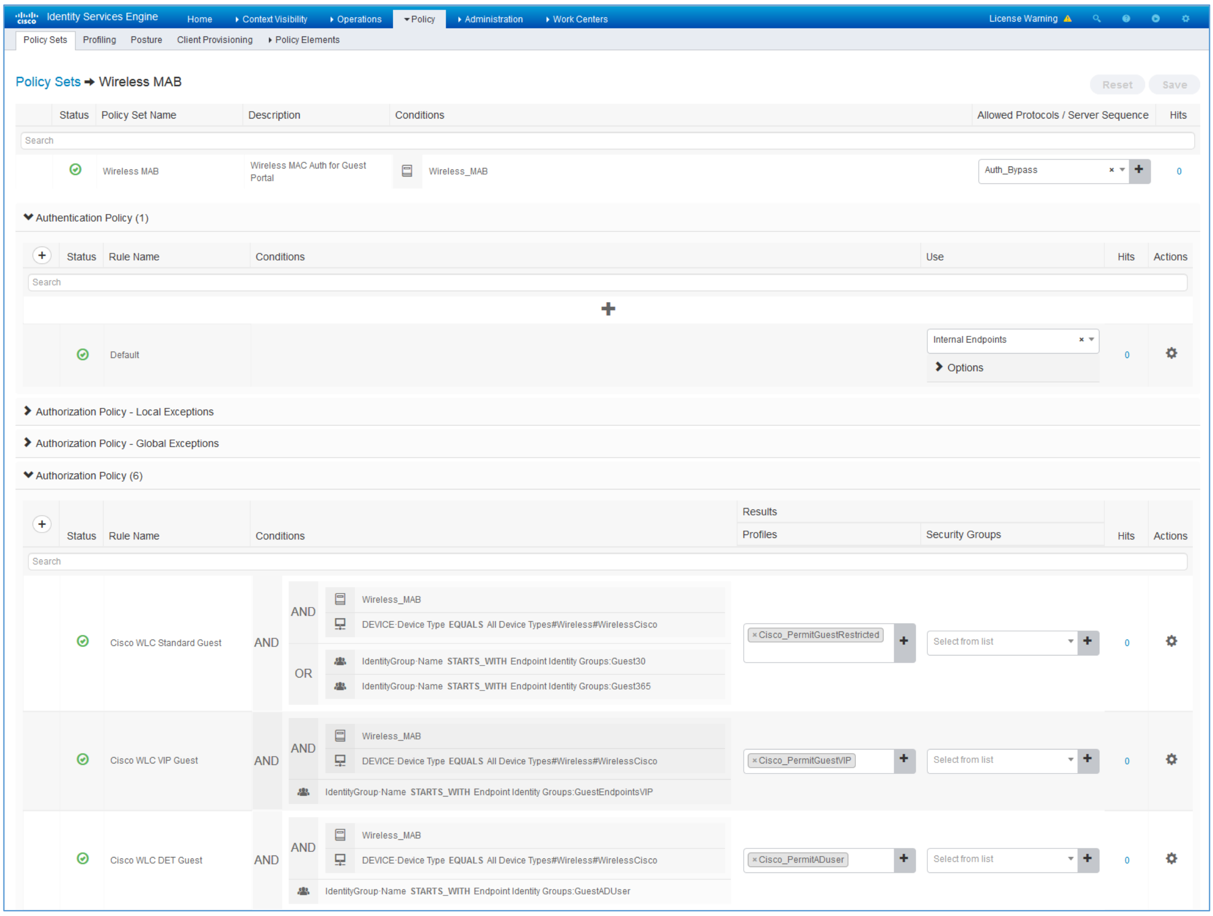
Authorization Policy

Exceptions (0)

Standard

	Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
	☑	Cisco WLC Standard Gues t	if	(**Guest30** OR **Guest365**) AND (Wireless_MAB AND DEVICE:Device Type EQUALS All Device Types#Wireless#WirelessCisco)	then	Cisco_PermitGuestRestricted	Edit |
	☑	Cisco WLC VIP Guest	if	**GuestEndpointsVIP** AND (Wireless_MAB AND DEVICE:Device Type EQUALS All Device Types#Wireless#WirelessCisco)	then	Cisco_PermitGuestVIP	Edit |
	☑	Cisco WLC DET Guest	if	**GuestADUser** AND (Wireless_MAB AND DEVICE:Device Type EQUALS All Device Types#Wireless#WirelessCisco)	then	Cisco_PermitADuser	Edit |
	☑	GuestPortal_RunawayBay	if	(Wireless_MAB AND DEVICE:Location EQUALS All Locations#RunawayBay)	then	Cisco_WebAuth_RunawayBay	Edit |
	☑	GuestPortal_MOESHS	if	(Wireless_MAB AND DEVICE:Location EQUALS All Locations#MOE-SHS)	then	Cisco_WebAuth_MOESHS	Edit |
	☑	Default		if no matches, then		DenyAccess	Edit |

After



Policy Sets → Wireless MAB

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Wireless MAB	Wireless MAC Auth for Guest Portal	Wireless_MAB	Auth_Bypass	0

Authentication Policy (1)

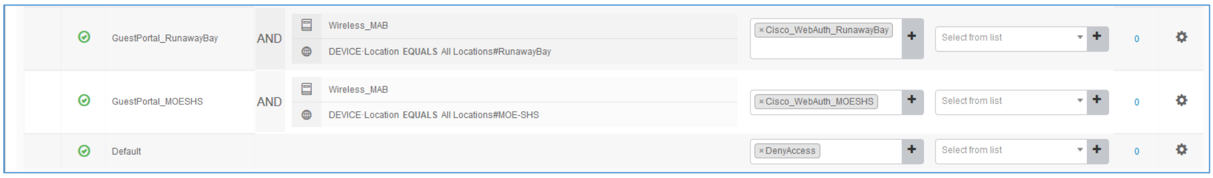
Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Endpoints Options	0	

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

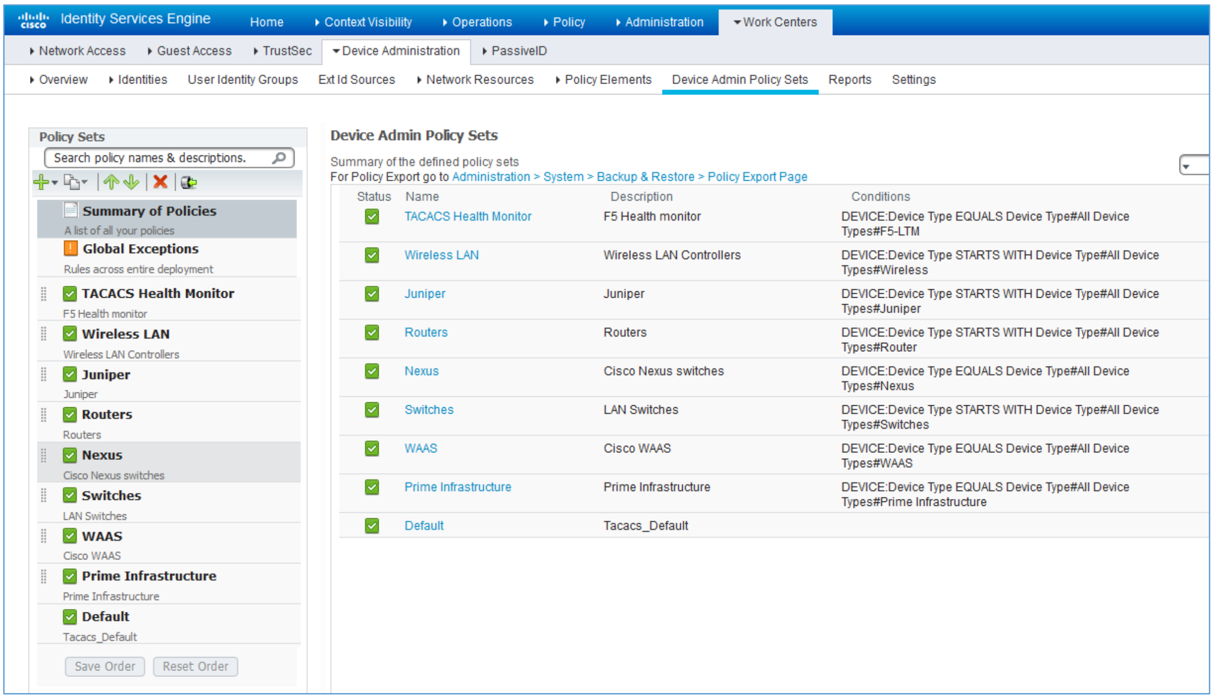
Authorization Policy (6)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
✓	Cisco WLC Standard Guest	AND AND: Wireless_MAB DEVICE·Device Type EQUALS All Device Types#Wireless#WirelessCisco OR: IdentityGroup·Name STARTS_WITH Endpoint Identity Groups:Guest30 IdentityGroup·Name STARTS_WITH Endpoint Identity Groups:Guest365	Cisco_PermitGuestRestricted	Select from list	0	
✓	Cisco WLC VIP Guest	AND AND: Wireless_MAB DEVICE·Device Type EQUALS All Device Types#Wireless#WirelessCisco IdentityGroup·Name STARTS_WITH Endpoint Identity Groups:GuestEndpointsVIP	Cisco_PermitGuestVIP	Select from list	0	
✓	Cisco WLC DET Guest	AND AND: Wireless_MAB DEVICE·Device Type EQUALS All Device Types#Wireless#WirelessCisco IdentityGroup·Name STARTS_WITH Endpoint Identity Groups:GuestADUser	Cisco_PermitADuser	Select from list	0	
✓	GuestPortal_RunawayBay	AND Wireless_MAB DEVICE·Location EQUALS All Locations#RunawayBay	Cisco_WebAuth_RunawayBay	Select from list	0	
✓	GuestPortal_MOESHS	AND Wireless_MAB DEVICE·Location EQUALS All Locations#MOE-SHS	Cisco_WebAuth_MOESHS	Select from list	0	
✓	Default		DenyAccess	Select from list	0	



TACACS Policy Sets

Before – simplicity …



Policy Sets

Search policy names & descriptions.

- **Summary of Policies** – A list of all your policies
- **Global Exceptions** – Rules across entire deployment
- ☑ **TACACS Health Monitor** – F5 Health monitor
- ☑ **Wireless LAN** – Wireless LAN Controllers
- ☑ **Juniper** – Juniper
- ☑ **Routers** – Routers
- ☑ **Nexus** – Cisco Nexus switches
- ☑ **Switches** – LAN Switches
- ☑ **WAAS** – Cisco WAAS
- ☑ **Prime Infrastructure** – Prime Infrastructure
- ☑ **Default** – Tacacs_Default

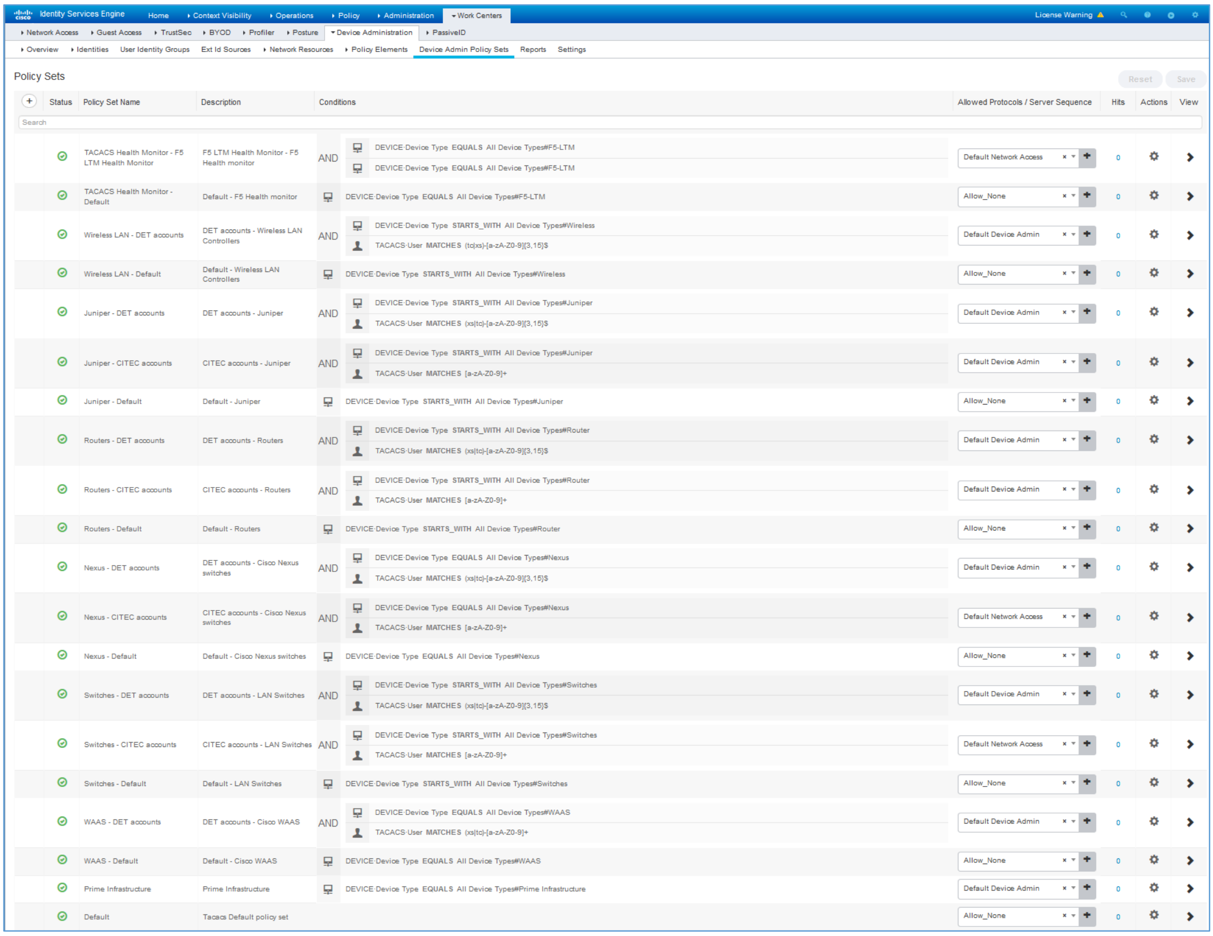
Device Admin Policy Sets

Summary of the defined policy sets

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description	Conditions
☑	TACACS Health Monitor	F5 Health monitor	DEVICE:Device Type EQUALS Device Type#All Device Types#F5-LTM
☑	Wireless LAN	Wireless LAN Controllers	DEVICE:Device Type STARTS WITH Device Type#All Device Types#Wireless
☑	Juniper	Juniper	DEVICE:Device Type STARTS WITH Device Type#All Device Types#Juniper
☑	Routers	Routers	DEVICE:Device Type STARTS WITH Device Type#All Device Types#Router
☑	Nexus	Cisco Nexus switches	DEVICE:Device Type EQUALS Device Type#All Device Types#Nexus
☑	Switches	LAN Switches	DEVICE:Device Type STARTS WITH Device Type#All Device Types#Switches
☑	WAAS	Cisco WAAS	DEVICE:Device Type EQUALS Device Type#All Device Types#WAAS
☑	Prime Infrastructure	Prime Infrastructure	DEVICE:Device Type EQUALS Device Type#All Device Types#Prime Infrastructure
☑	Default	Tacacs_Default	

After – a complete shambles (I think it's due to my "Allow_None" allowed protocols that causes all these new Policy Sets to be created – what a pity – I liked the old ISE 2.2 :-<)



Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	TACACS Health Monitor - F5 LTM Health Monitor	F5 LTM Health Monitor - F5 Health monitor	AND DEVICE·Device Type EQUALS All Device Types#F5-LTM DEVICE·Device Type EQUALS All Device Types#F5-LTM	Default Network Access	0
✓	TACACS Health Monitor - Default	Default - F5 Health monitor	DEVICE·Device Type EQUALS All Device Types#F5-LTM	Allow_None	0
✓	Wireless LAN - DET accounts	DET accounts - Wireless LAN Controllers	AND DEVICE·Device Type STARTS_WITH All Device Types#Wireless TACACS·User MATCHES (tc|xs)-[a-zA-Z0-9]{3,15}$	Default Device Admin	0
✓	Wireless LAN - Default	Default - Wireless LAN Controllers	DEVICE·Device Type STARTS_WITH All Device Types#Wireless	Allow_None	0
✓	Juniper - DET accounts	DET accounts - Juniper	AND DEVICE·Device Type STARTS_WITH All Device Types#Juniper TACACS·User MATCHES (xs|tc)-[a-zA-Z0-9]{3,15}$	Default Device Admin	0
✓	Juniper - CITEC accounts	CITEC accounts - Juniper	AND DEVICE·Device Type STARTS_WITH All Device Types#Juniper TACACS·User MATCHES [a-zA-Z0-9]+	Default Device Admin	0
✓	Juniper - Default	Default - Juniper	DEVICE·Device Type STARTS_WITH All Device Types#Juniper	Allow_None	0
✓	Routers - DET accounts	DET accounts - Routers	AND DEVICE·Device Type STARTS_WITH All Device Types#Router TACACS·User MATCHES (xs|tc)-[a-zA-Z0-9]{3,15}$	Default Device Admin	0
✓	Routers - CITEC accounts	CITEC accounts - Routers	AND DEVICE·Device Type STARTS_WITH All Device Types#Router TACACS·User MATCHES [a-zA-Z0-9]+	Default Device Admin	0
✓	Routers - Default	Default - Routers	DEVICE·Device Type STARTS_WITH All Device Types#Router	Allow_None	0
✓	Nexus - DET accounts	DET accounts - Cisco Nexus switches	AND DEVICE·Device Type EQUALS All Device Types#Nexus TACACS·User MATCHES (xs|tc)-[a-zA-Z0-9]{3,15}$	Default Device Admin	0
✓	Nexus - CITEC accounts	CITEC accounts - Cisco Nexus switches	AND DEVICE·Device Type EQUALS All Device Types#Nexus TACACS·User MATCHES [a-zA-Z0-9]+	Default Network Access	0
✓	Nexus - Default	Default - Cisco Nexus switches	DEVICE·Device Type EQUALS All Device Types#Nexus	Allow_None	0
✓	Switches - DET accounts	DET accounts - LAN Switches	AND DEVICE·Device Type STARTS_WITH All Device Types#Switches TACACS·User MATCHES (xs|tc)-[a-zA-Z0-9]{3,15}$	Default Device Admin	0
✓	Switches - CITEC accounts	CITEC accounts - LAN Switches	AND DEVICE·Device Type STARTS_WITH All Device Types#Switches TACACS·User MATCHES [a-zA-Z0-9]+	Default Network Access	0
✓	Switches - Default	Default - LAN Switches	DEVICE·Device Type STARTS_WITH All Device Types#Switches	Allow_None	0
✓	WAAS - DET accounts	DET accounts - Cisco WAAS	AND DEVICE·Device Type EQUALS All Device Types#WAAS TACACS·User MATCHES (xs|tc)-[a-zA-Z0-9]+	Default Device Admin	0
✓	WAAS - Default	Default - Cisco WAAS	DEVICE·Device Type EQUALS All Device Types#WAAS	Allow_None	0
✓	Prime Infrastructure	Prime Infrastructure	DEVICE·Device Type EQUALS All Device Types#Prime Infrastructure	Default Device Admin	0
✓	Default	Tacacs Default policy set		Allow_None	0