

A background image showing a hand plugging a cable into a server rack. The image is partially obscured by blue geometric shapes. The hand is in the foreground, and the server rack is in the background. The overall color scheme is blue and black.

ASBUILT INSTALAÇÃO CISCO ISE

MAG

2021

Sumário

1. Objetivo	3
2. Descrição	3
3. Equipamentos	4
4. Cisco ISE	5
Licenciamento	5
Design Solução.....	5
Integração Active Directory	6
Network Device	7
Autenticação 802.1x.....	8
Autenticação TACACS	9
Logs	13

1. Objetivo

O objetivo desse documento é descrever todo o projeto que foi implementado na empresa utilizando a tecnologia Cisco ISE.

Este documento contém a descrição completa do projeto proposto, incluindo todas as informações que foram utilizadas na solução, detalhando os equipamentos, a configuração de cada elemento e a validação da instalação.

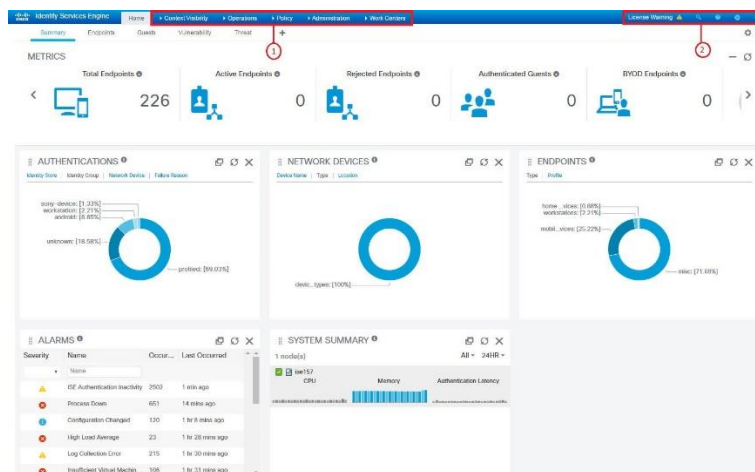
2. Descrição

A MAG possuía um Cisco ACS que se encontrava obsoleto e apresentando problemas na sua utilização e diante desse cenário foi adquirido um Cisco ISE para que o mesmo realize as funções atuais do ACS que são autenticação dos equipamentos da empresa utilizando o TACACS e a autenticação da rede wireless utilizando 802.1x

3. Equipamentos

Cisco Identity Services Engine (ISE)

O Cisco ISE permite que você forneça acesso de rede altamente seguro a usuários e dispositivos. Ele ajuda a obter visibilidade do que está acontecendo na sua rede, como quem está conectado, quais aplicativos estão instalados e em execução e muito mais. Ele também compartilha dados contextuais vitais, como identidades, ameaças e vulnerabilidades de usuários e dispositivos, com soluções integradas dos parceiros de tecnologia da Cisco, para que você possa identificar, conter e corrigir ameaças.




4. Cisco ISE

O Cisco ISE está sendo utilizado na rede da MAG para realizar a autenticação do protocolo 802.1x na rede wireless e também para autenticar o acesso aos dispositivos através do TACACS. Abaixo temos todas as configurações que foram realizadas no Cisco ISE para que o mesmo conseguisse realizar a autenticação de acordo com as especificações da MAG.

Licenciamento

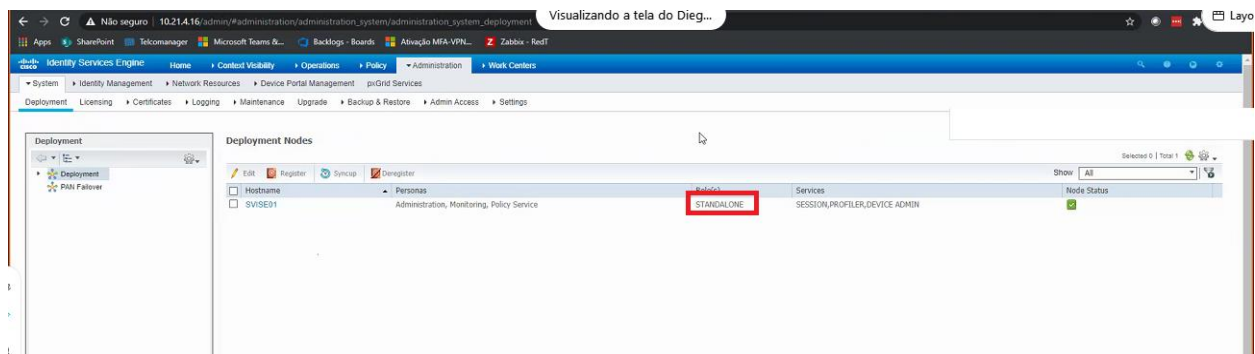
A MAG adquiriu o licenciamento BASE para 1500 dispositivo, a licença para 1 dispositivos virtuais médium e a licença de device admin (TACACS). Abaixo temos os serviços permitidos pelas licenças.

		Device Admin*	Base				Plus				ISE Apex + AnyConnect Apex			
Benefit	Use case	TACACS+	RADIUS / 802.1x	AAA	Group-Based Policy Scalable Group tagging	Guest services	Rapid threat containment	ANC/EPS	Device profiling and feed service	BYOD with CA	pxGrid context sharing	MDM / EMM	Threat-Centric NAC	Posture (endpoint compliance and remediation)
Control all access from one place	Guest Provide unique guest permissions to visitors			●	●	●								
	Secure access Control user access and ensure device authentication		●		●									
	Device Admin Differentiate access for device administrators	●												
 See and share rich user and device details	BYOD Seamlessly onboard devices with the right access		●	●	●				●	●				
	Visibility See when, where, and why users are on your network		●	●	●				●					
	Integration Share information with other products		●	●	●	●			●		●			
 Stop threats from getting in and spreading	Compliance Ensure that endpoints meet network standards		●	●	●							●		●
	Segmentation Limit exposure with pre-defined access segmentation		●	●	●									
	Containment Reduce risk with rapid threat containment		●	●	●	●	●	●	●					
 Prevention	Prevention Prevent breaches at the endpoint level		●	●	●								●	
			Control (AAA Group-Based Policy)				Context (Profiling pxGrid)				Compliance (Posture MDM)			

Design Solução

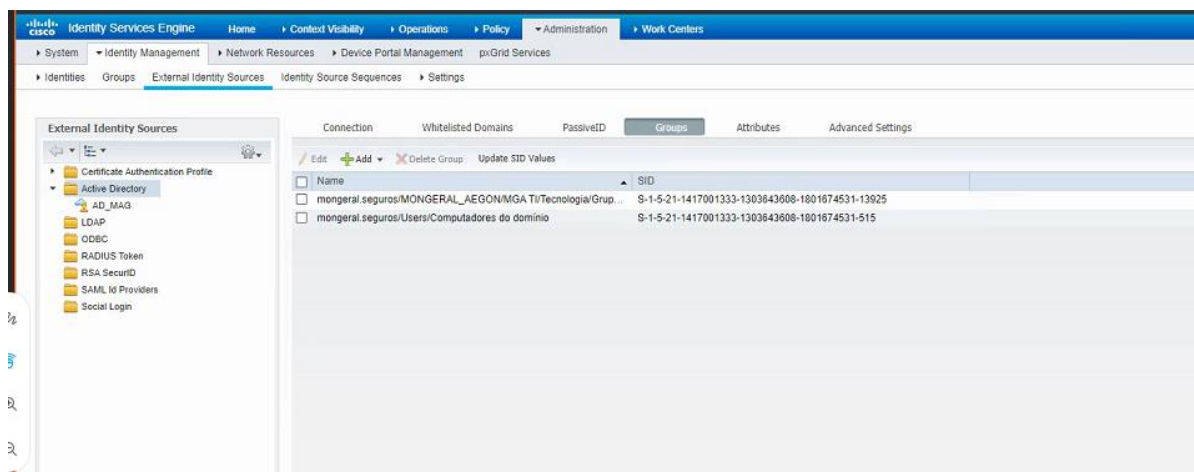
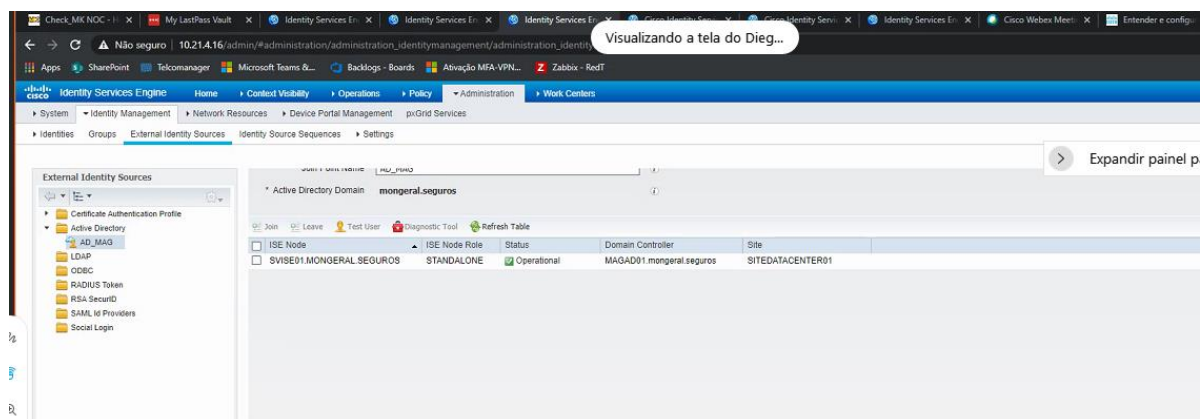
Como a empresa só adquiriu um Cisco ISE, a solução escolhida para ser implementada no MAG foi o modelo Standalone, onde o único node tem a função de administração (PAN), monitoria (Mnt) e police servisse (PSN)





Integração Active Directory

Para a autenticação dos equipamentos utilizar as contas do AD foi necessário realizar a integração do Cisco ISE com o AD, a partir dessa integração o Cisco ISE consegue ler usuários e grupos criados no AD. Essa integração ainda inclui uma troca de assinaturas de certificado.





Identity Services Engine Home | **Context Visibility** | Operations | Policy | Administration | Work Centers

Network Access | Guest Access | TrustSec | Device Administration | Password

Overview | Identities | User Identity Groups | External Sources | **Network Resources** | Policy Elements | Device Admin Policy Sets | Reports | Settings

Network Devices

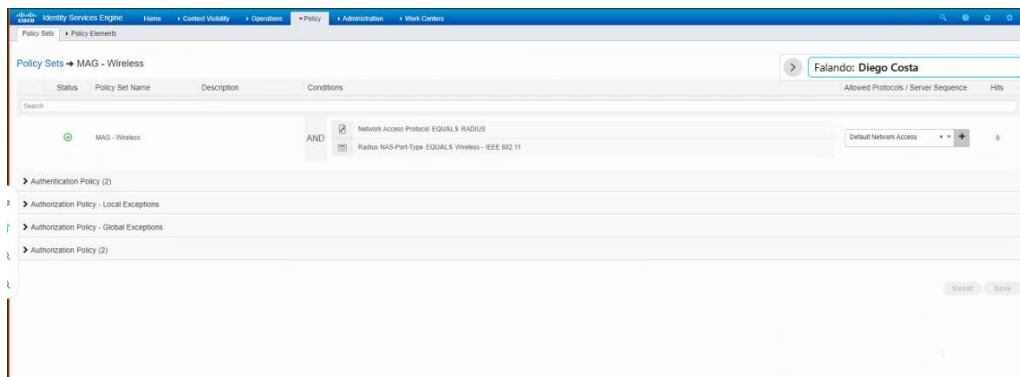
Expandir paine

Name	IP/Mask	Profile Name	Location	Type	Description
NK-MONGE	10.25.10.248/32	Cisco	Matriz	All Device Types	
NK-MONGE	10.25.10.249/32	Cisco	Matriz	All Device Types	
NK-MONGE	10.25.10.251/32	Cisco	Matriz	All Device Types	
NK-MONGE	10.25.10.252/32	Cisco	Matriz	All Device Types	
NEXUS9K-1	10.21.4.2/32	Cisco	Matriz	All Device Types	
NEXUS9K-1_2	169.254.10.6/32	Cisco	Matriz	All Device Types	
NEXUS9K-2	10.21.4.3/32	Cisco	Matriz	All Device Types	
NEXUS9K-2_2	169.254.10.10	Cisco	Matriz	All Device Types	
SFMT2WLQ1	10.25.30.253/32	Cisco	Matriz	All Device Types	
SFMT2WLQ2	10.25.30.252/32	Cisco	Matriz	All Device Types	
SVDATMG134	10.21.25.160/32	Cisco	Matriz	All Device Types	
SW-1oAND	10.25.10.101/32	Cisco	Matriz	All Device Types	
SW-2oAND	10.25.10.102/32	Cisco	Matriz	All Device Types	
SW-3oAND	10.25.10.103/32	Cisco	Matriz	All Device Types	
SW-4oAND	10.25.10.104/32	Cisco	Matriz	All Device Types	
SW-5oAND	10.25.10.105/32	Cisco	Matriz	All Device Types	
SW-6oAND	10.25.10.106/32	Cisco	Matriz	All Device Types	
SW-7oAND	10.25.10.107/32	Cisco	Matriz	All Device Types	
SW-7oAND02	10.25.10.109/32	Cisco	Matriz	All Device Types	
SW-9oAND	10.25.10.108/32	Cisco	Matriz	All Device Types	
SW-ANIX-1a	10.25.10.120/32	Cisco	Matriz	All Device Types	
SW-ANIX-1a	10.25.10.123/32	Cisco	Matriz	All Device Types	
SW-ANIX-2a	10.25.10.124/32	Cisco	Matriz	All Device Types	
SW-ANIX-2a	10.25.10.125/32	Cisco	Matriz	All Device Types	
SW-ANIX-3a	10.25.10.126/32	Cisco	Matriz	All Device Types	
SW-ANIX-TE	10.25.10.120/32	Cisco	Matriz	All Device Types	
SW-ANIX-TE	10.25.10.121/32	Cisco	Matriz	All Device Types	
SW-ANIX-TE	10.25.10.119/32	Cisco	Matriz	All Device Types	
SW-ANIX-1A	10.25.10.130/32	Cisco	Matriz	All Device Types	

Autenticação 802.1x

A empresa possui uma rede wireless que é autenticada através do protocolo Radius (802.1x). De acordo com as necessidades da empresa foram configuradas políticas.

MAG Wireless -> Verifica se o NAS-Port Type é igual a Wireless IEEE802.11



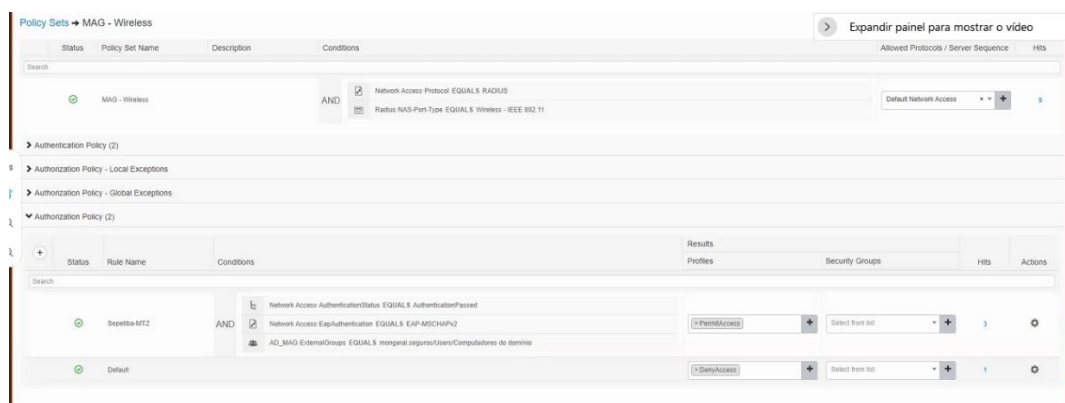
Autenticação

Wireless DOT1X -> Verifica se a conexão foi iniciada utilizando o protocolo 802.1x e se a mesma tem o fator de autenticação no AD da MAG (Certificado).



Autorização

Sepetiba-MTZ -> Verifica se a conexão foi aceita na fase de autenticação e posteriormente verifica se o protocolo de segurança é o MSCHAPv2, e se a máquina está dentro do grupo do AD (Computadores de Domínio). Caso a conexão atenda todos os requisitos é permitido acessar a rede.

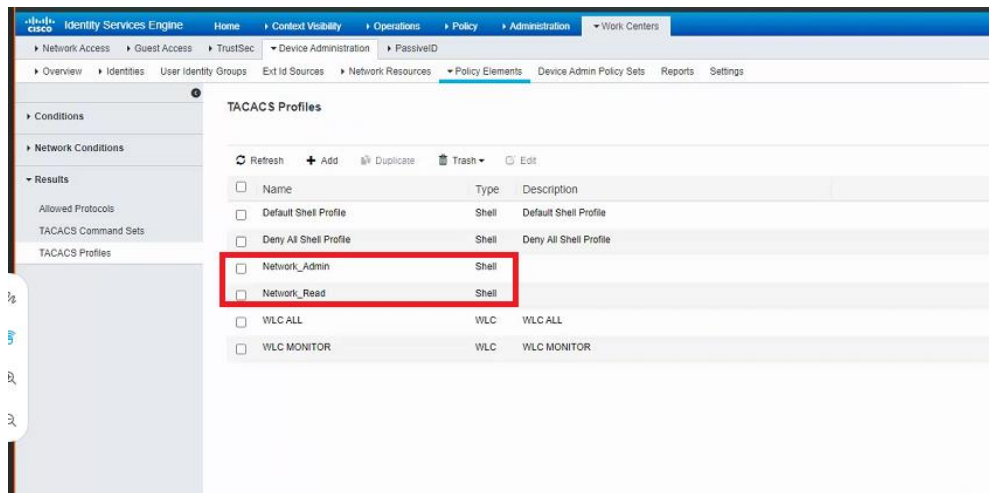


Autenticação TACACS

Para se autenticar nos equipamentos, empresa utiliza as contas dos usuários de grupos do AD, e de acordo com esse cenário foram criados 2 grupos no Cisco ISE com privilégios diferentes de acesso aos equipamentos.

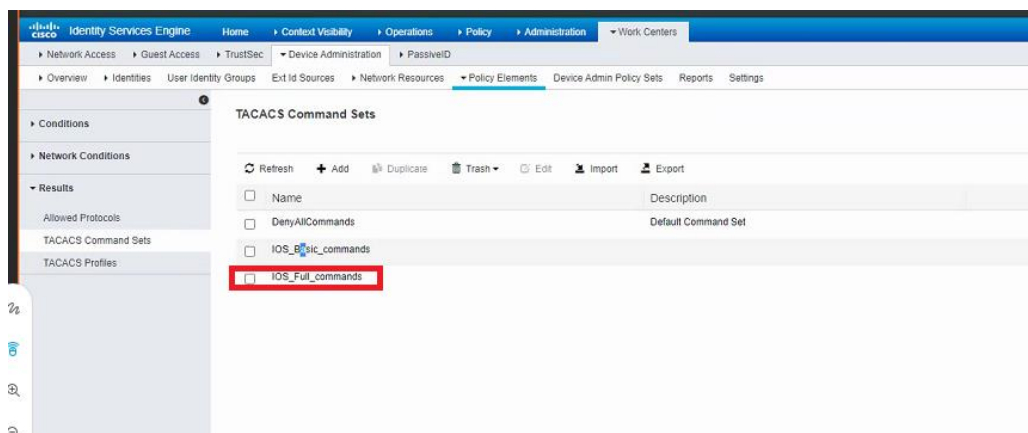
Network Admin -> Acesso total aos equipamentos

Network Read -> Acesso somente com comandos pré-estabelecidos



Network Admin

Grupo criado e associado a profile IOS Full Commands, permitindo o acesso completo com privilégio 15.



The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Elements > Device Admin Policy Sets > Reports > Settings. The left sidebar shows the navigation menu with 'Results' expanded, containing 'Allowed Protocols', 'TACACS Command Sets', and 'TACACS Profiles'. The main content area is titled 'TACACS Command Sets > IOS_Full_commands'. It includes a 'Command Set' section with a 'Name' field containing 'IOS_Full_commands' and an empty 'Description' field. Below this is a 'Commands' section with a checkbox 'Permit any command that is not listed below' which is checked. At the bottom, there is a table with columns 'Grant', 'Command', and 'Arguments', and a 'Cancel' button.

The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Elements > Device Admin Policy Sets > Reports > Settings. The left sidebar shows the navigation menu with 'Results' expanded, containing 'Allowed Protocols', 'TACACS Command Sets', and 'TACACS Profiles'. The main content area is titled 'TACACS Profiles > Network_Admin'. It includes a 'TACACS Profile' section with a 'Name' field containing 'Network_Admin' and an empty 'Description' field. Below this are tabs for 'Task Attribute View' (selected) and 'Raw View'. The 'Common Tasks' section has a 'Common Task Type' dropdown set to 'Shell'. It contains several checkboxes and input fields: 'Default Privilege' (checked, value 15), 'Maximum Privilege' (checked, value 15), 'Access Control List' (unchecked), 'Auto Command' (unchecked), 'No Escape' (unchecked), 'Timeout' (unchecked), and 'Idle Time' (unchecked). The 'Custom Attributes' section at the bottom has a table with columns 'Type', 'Name', and 'Value', and a 'No data found.' message.

Network Read

Grupo criado e associado a profile IOS Basic Commands, permitindo o acesso restrito, podendo executar somente comandos permitidos.

The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Elements > Device Admin Policy Sets > Reports > Settings. The left sidebar shows the navigation menu with 'Results' expanded, containing 'Allowed Protocols', 'TACACS Command Sets', and 'TACACS Profiles'. The main content area is titled 'TACACS Command Sets'. It includes a toolbar with 'Refresh', '+ Add', 'Duplicate', 'Trash', 'Edit', 'Import', and 'Export'. Below the toolbar is a table with columns 'Name' and 'Description'. The table contains three rows: 'DenyAllCommands' (Description: Default Command Set), 'IOS_Basic_commands' (highlighted with a red box), and 'IOS_Full_commands'.

TACACS Command Sets > IOS_Basic_commands

Command Set

Name:

Description:

Commands

Permit any command that is not listed below: ☐

	Command	Arguments	
<input type="checkbox"/>	Grant		
<input type="checkbox"/>	PERMIT	show inventory	
<input type="checkbox"/>	PERMIT	ping	
<input type="checkbox"/>	PERMIT	traceroute	
<input type="checkbox"/>	PERMIT	show running-config	

[Cancel](#) [Save](#)

Identity Services Engine > Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > Device Administration > PassiveID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

TACACS Profiles > Network_Read

TACACS Profile

Name:

Description:

[Task Attribute View](#) [Raw View](#)

Common Tasks

Common Task Type:

<input checked="" type="checkbox"/>	Default Privilege	<input type="text" value="1"/>	(Select 0 to 15)
<input checked="" type="checkbox"/>	Maximum Privilege	<input type="text" value="7"/>	(Select 0 to 15)
<input type="checkbox"/>	Access Control List	<input type="text"/>	
<input type="checkbox"/>	Auto Command	<input type="text"/>	
<input type="checkbox"/>	No Escape	<input type="text"/>	(Select true or false)
<input type="checkbox"/>	Timeout	<input type="text"/>	Minutes (0-9999)
<input type="checkbox"/>	Idle Time	<input type="text"/>	Minutes (0-9999)

Custom Attributes

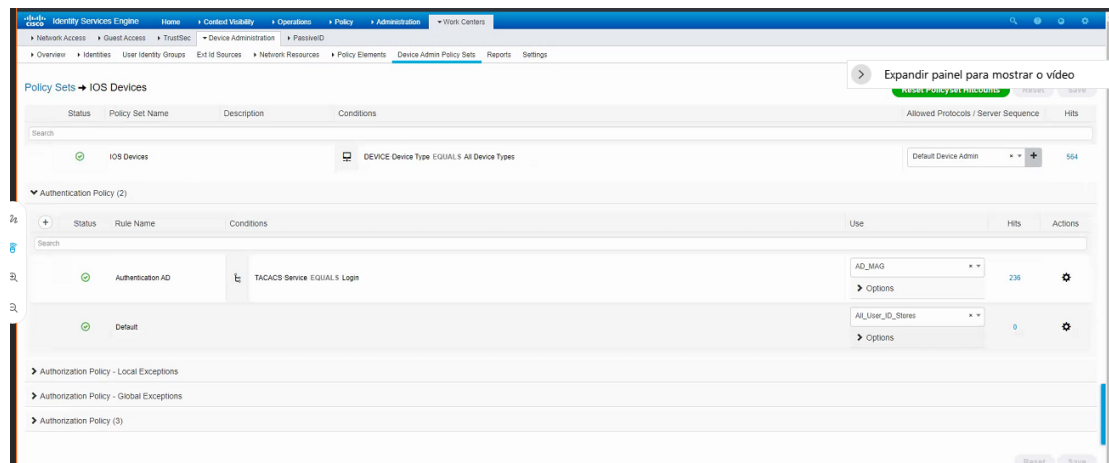
Type	Name	Value
No data found.		

[Add](#) [Trash](#) [Edit](#)

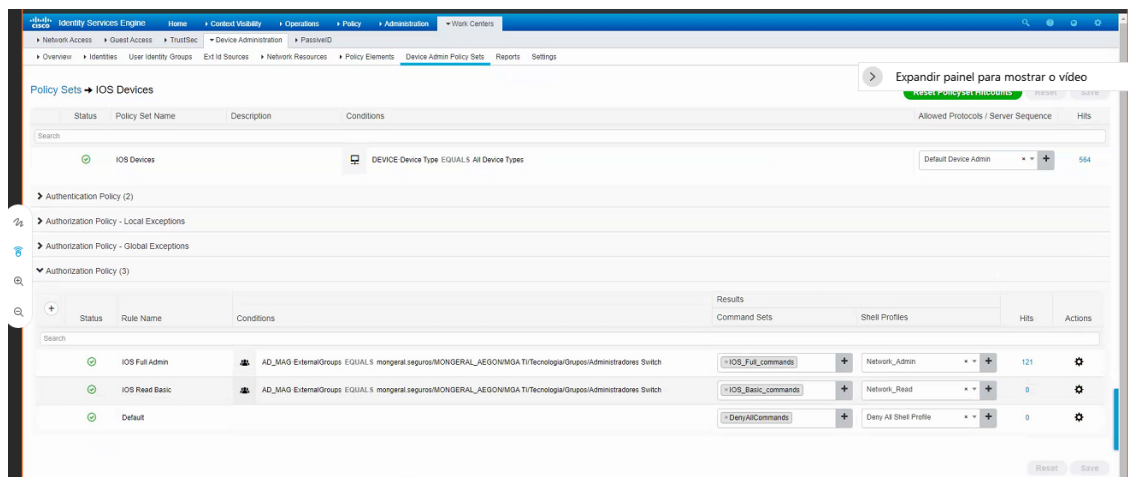
Polices

Com os grupos criados e associados as respectivas profiles, esses foram aplicados nas políticas, associado o grupo do ISE aos grupos do AD

Autenticação



Autorização



OBS. Não existia ainda o grupo do AD para o grupo do ISE Network Read, então foi incluso o grupo atual e a MAG irá realizar a troca posteriormente

