

FORMAÇÃO EM CIBERSEGURANÇA

CISCO ISE - BASICS (CONCEITOS E OVERVIEW)

CIBERSEGURANCA.CISCO.COM.BR

JANEIRO/2025

DISCLAIMER

Esse material não tem qualquer relação oficial com a empresa CISCO. Ele foi criado por um profissional que trabalha há 20 anos com os equipamentos e soluções do fabricante.

A configuração mostrada não é uma recomendação. O autor não se responsabiliza por má utilização do material, que tem objetivo exclusivamente educativo (use-o para testar e aprender a ferramenta).

Esse ebook foi constituído a partir de artigos publicados de 2019 a 2021 no blog da TechRebels no medium.com pelo mesmo autor.

A versão utilizada do Cisco ISE na época era a 2.1, mas o conceito, telas e configuração continuam válidas para as versões atuais 3.x.

INTRODUÇÃO

Bom, pra quem não conhece, o Cisco ISE (Identity Services Engine) é o software de gestão de políticas e identidades da Cisco. Com ele:

Você centraliza e unifica o controle de acesso seguro à sua rede

- O ISE é o software central – onde todas as bases de usuário interna ou externa (AD por exemplo) – que irá permitir e controlar todo o acesso à sua rede. Além disso, todas as políticas de autenticação, autorização e accounting, também serão definidas nele. O que tal usuário, ou grupo, pode acessar e o quanto ele consegue fazer, além de logar cada ação, será definido no Cisco ISE.

Aumenta a visibilidade e identificação de dispositivos

- Através de vários tipos de probes diferentes, o ISE é capaz de identificar o sistema operacional de cada endpoint, seja computadores pessoais, smartphones, dispositivos como impressoras e inúmeros outros. Essa identificação automática permitirá que você construa regras baseadas também no tipo de dispositivo da sua rede.

Permite implementar rede Guest e BYOD

- Gerência centralizada dos usuários guest da sua rede, permitindo self-register (registro próprio) integrado com Facebook e LinkedIn, através de sponsor (quando uma pessoa da empresa precisa autorizar a criação da conta) ou simplesmente entrando com um usuário e senha previamente criados.

Aumenta a segurança da rede

- Permite que access-lists de firewall por exemplo sejam criadas não utilizando um IP de origem e destino, mas pessoas, usuários da rede. Além disso, regras de postura, verificando patches de atualização do Sistema Operacional, versão de base do AV e muitos outros irão aumentar a segurança do seu ambiente.

PARTE 1

VERSÕES

Além dos appliances SNS e das versões Small, Medium e Large de VMs, a Cisco disponibiliza para trial e PoC uma versão mini do ISE que vem com os 3 tipos de licenças habilitadas para até 100 endpoints. Essa licença tem duração de 90 dias, o que é um excelente tempo pra treinar ou mostrar o valor da ferramenta nos clientes ou na sua empresa.

À partir da versão 2.2 (no momento que escrevo esse artigo a versão 2.7 acabou de ser lançada) é necessário 8 GB de RAM para subir o ISE Evaluation. Como meu modesto notebook possui apenas essa quantidade de memória, vamos mostrar a versão 2.1, que necessita de apenas 4Gb de RAM e que para os recursos e funcionalidades que falaremos é suficiente.

A diferença à partir da versão 2.2 é de uma nova interface gráfica para o set de políticas. Ela está bem mais moderna, limpa e objetiva. Se você aprender com essa interface da 2.1, que não é nada ruim, não terá nenhuma dificuldade em se adaptar às novas telas



INSTALAÇÃO

Faça o download do .ova (no nosso caso o ISE mini) direto do site da Cisco (cisco.com/go/download) e importe esse arquivo no seu VMware Workstation por exemplo. Após ligar a máquina, o primeiro passo é digitar setup no lugar do nome do usuário (o usuário padrão admin será criado e sua senha definida durante esse processo).

Nesse setup inicial iremos fazer as configurações básicas como em qualquer dispositivo de rede: IP, máscara, gateway, NTP, DNS e etc. Após isso, e a senha do usuário admin definida, o ISE irá fazer alguns testes de leitura e escrita de disco e memória (que mesmo não atendido 100% pode ser usado nessa versão Evaluation), e vai começar a criar a base de dados. Esse processo é que costuma demorar um pouco mais de tempo.



Finalizado, teremos um prompt de login, onde, após se logar, você poderá ver toda essa configuração inicial com o bom e velho comando `show running-config`.



Dica: Existe um usuário `admin` para se logar na CLI e um usuário `admin` (são iguais mesmo) pra se logar na GUI. As senhas desses usuários podem ser diferentes, e a da GUI expira (por padrão, mas pode ser alterado), então é comum que os administradores façam confusão, tentando se logar na CLI usando uma senha da GUI, ou achando que é o mesmo usuário.

Caso precise, altere a senha do `admin` da GUI com o comando: **`application reset-passwd ise admin`**

E, se preciso, altere a senha do `admin` da CLI com o comando: **`password`**

Caso perca o acesso via CLI, será necessário bootar com a ISO do ISE e seguir com a recuperação da senha. Aqui tem um doc bem explicativo do processo: <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200568-ISE-Password-Recovery-Mechanisms.pdf>



Além disso, um outro comando muito útil é o ***show application status ise***, que irá mostrar o status de cada um dos processos do ISE. Veja a seguir:

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	7154
Database Server	running	57 PROCESSES
Application Server	running	11681
Profiler Database	running	8225
ISE Indexing Engine	running	12061
AD Connector	running	12903
WT Session Database	running	3038
WT Log Collector	running	12664
WT Log Processor	running	12549
Certificate Authority Service	running	12392
EST Service	running	14947
SXP Engine Service	running	2366
TC-NAC Docker Service	disabled	
TC-NAC MongoDB Container	disabled	
TC-NAC RabbitMQ Container	disabled	
TC-NAC Core Engine Container	disabled	
MA Database	disabled	
MA Service	disabled	
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
PassiveID Service	disabled	
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	

```
ise/admin#
```

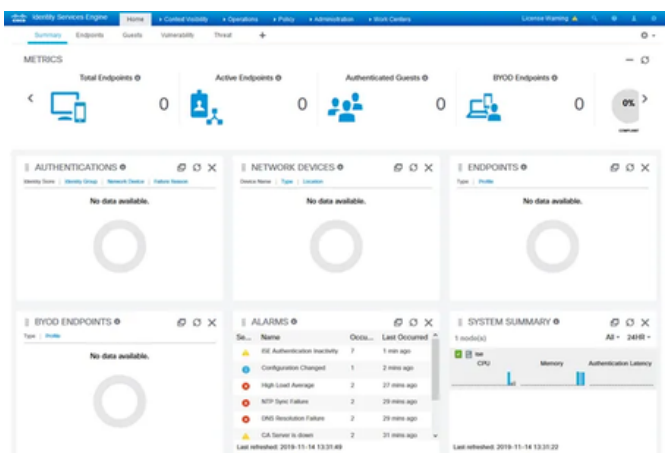
show application status ise



TOUR PELA GUI

Concluído isso, todo o restante é feito via interface gráfica. Vamos então iniciar nosso tour pelas telas e funcionalidades.

Ao se logar, você verá a aba Summary, com informações do servidor, de autenticação, BYOD, alarmes, processos do sistema, dispositivos de rede, e etc.



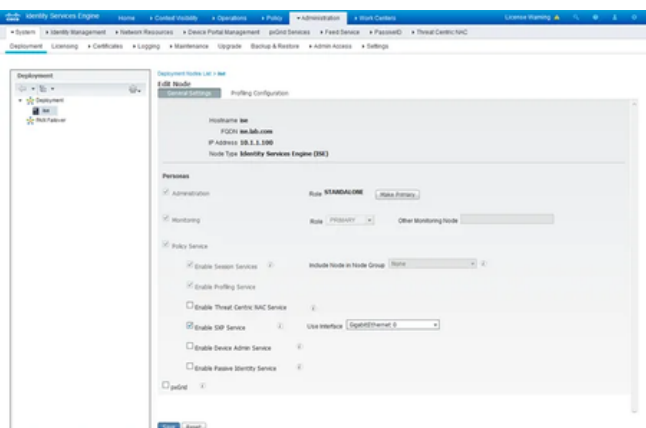
Summary

Na sequência, vamos para o menu Administration e Deployment. É aqui que será configurado o ISE primário e secundário para alta disponibilidade “manual” em ativo/passivo ou ainda acrescentando um health node e fazendo uma alta disponibilidade automática.



Você também poderá definir aqui se o ISE irá rodar em modo standalone ou não, apontar os diversos PSNs (nós de política) que normalmente ficam espalhados em sites diferentes, e etc.

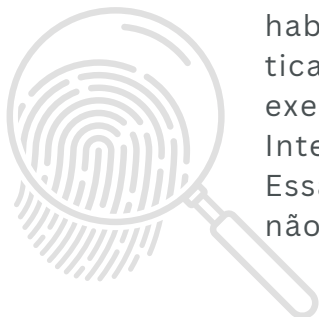
É nessa aba também que você habilita alguns serviços que não vêm configurados por padrão, como o TrustSec, pxGrid, TACACS+, etc.

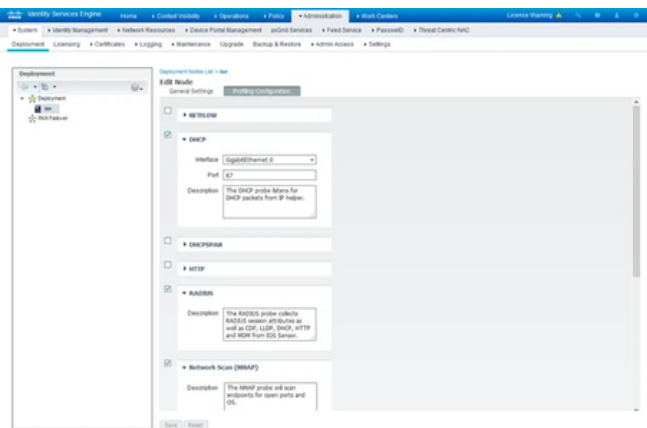


Deployment – imagem 1

Ainda em Deployment, a segunda aba permite selecionarmos quais meios o ISE irá usar para fazer o Profiling, ou seja identificar e categorizar os dispositivos. Caso não haja probes suficientes habilitadas (não quer dizer que você deva tancar todas), uma máquina Windows 7 por exemplo seria identificada apenas como Intel-based device.

Essas probes abaixo vêm por padrão, caso não utilize, elas podem ser desabilitadas.



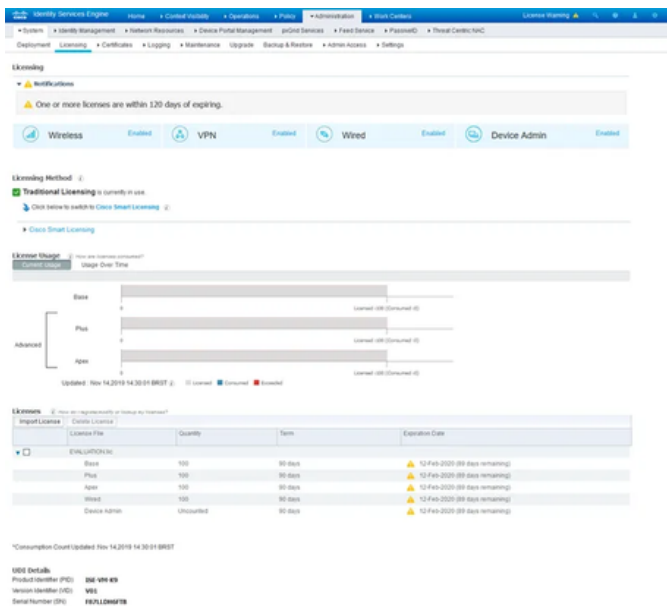


Deployment – imagem 2

A próxima aba mostra os detalhes do licenciamento. Existem duas formas possíveis: pelo smart licensing ou traditional licensing (o bom e velho PAK da Cisco).

Repare nos detalhes do licenciamento das licenças Base, Plus e Apex para 100 endpoints com duração de 90 dias. Tudo 100% habilitado pra você testar e treinar!





The screenshot displays the Cisco ISE Licensing page. At the top, a navigation bar includes links for System, Identity Management, Network Resources, Device Policy Management, pUDD Services, Field Service, Password, Threat Control/IOC, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. The main content area is titled 'Licensing' and features a 'Notifications' section with a warning: 'One or more licenses are within 120 days of expiring.' Below this, there are status indicators for 'Wireless', 'VPN', 'Wired', and 'Device Admin', all marked as 'Enabled'. The 'Licensing Method' section indicates 'Traditional Licensing is currently in use' and provides a link to 'Click here to switch to Cisco Smart Licensing'. The 'License Usage' section shows a 'Usage Over Time' chart for 'Basic', 'Plus', and 'App' licenses, with a legend for 'Unlimited', 'Consumed', and 'Reserved'. The 'Licenses' table lists the following data:

Input License	License File	Quantity	Term	Expiration Date
<input checked="" type="checkbox"/>	ENTRUSTONIC			
	Basic	100	90 days	⚠️ 10-Feb-2020 (89 days remaining)
	Plus	100	90 days	⚠️ 10-Feb-2020 (89 days remaining)
	App	100	90 days	⚠️ 10-Feb-2020 (89 days remaining)
	Wired	100	90 days	⚠️ 10-Feb-2020 (89 days remaining)
	Device Admin	Unlimited	90 days	⚠️ 10-Feb-2020 (89 days remaining)

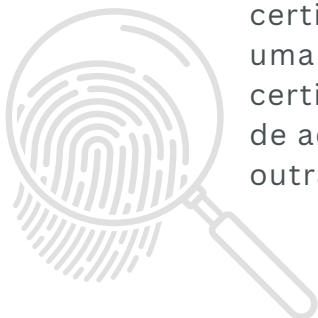
At the bottom, the 'Consumption Count' is updated as of Feb 14, 2019 14:30:01 BRST. The 'ISE Details' section provides the following information:

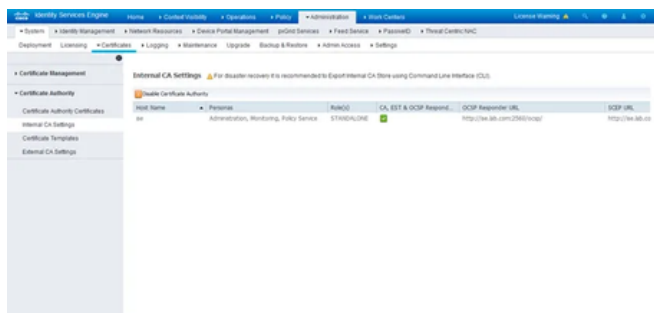
- Product Identifier (PID): ISE-491-49
- Version Identifier (VID): 5.0.1
- Serial Number (SN): F8JL10M9718

Licensing

O ISE também pode ser utilizado como uma CA. Como ele normalmente é configurado em HA, pode ser uma boa alternativa para as empresas que ainda não possuem uma CA.

Caso você precise instalar um certificado válido, é também nessa seção que será feito. No momento da importação do certificado (após gerar o CSR), irá aparecer uma janela para você escolher se esse certificado é para um portal guest, portal de administração do próprio ISE, entre outras.





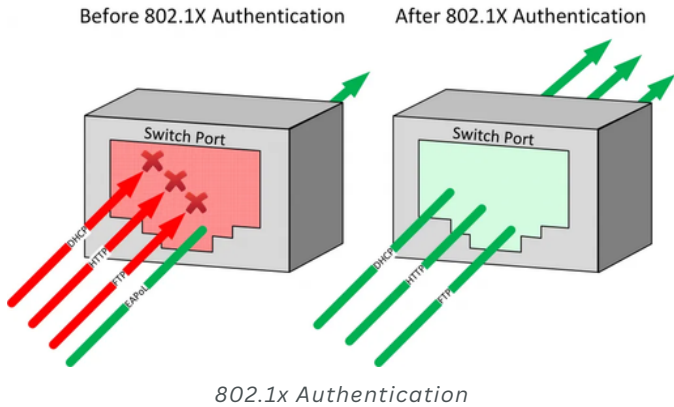
Certificates

E para concluir esse primeiro artigo, a aba Maintenance permite a instalação dos patches, que também são baixados diretamente do site da Cisco e feito upload direto para o ISE. A instalação é bem simples e é dessa forma que você manterá seu software operando sem vulnerabilidades e nas melhores condições.

A opção de Repository, permite a configuração de um repositório de software onde ficará um arquivo que será utilizado para o upgrade do ISE. Esse repositório pode ser uma unidade de CDROM, HTTP, HTTPS, SFTP, DISK LOCAL, etc.



PARTE 2



Começando pela tela *Administration > System > Admin Access* e aba *Password Policy*: Aqui fazemos a configuração da política de senha e autenticação de usuários da GUI e da CLI – usuários de acesso administrativo ao software ISE.

Repare nas possibilidades: tamanho mínimo de senha, histórico, requisito mínimo de complexidade, bloqueio após tentativas incorretas, e etc.

The screenshot shows the 'Password Policy' configuration page in the Cisco ISE Administration console. The 'Settings' section is expanded, showing the following configuration options:

- Authentication Method:** Password Policy
- Authentication:** Account Disable Policy
- Permissions:** Menu Access, Data Access, Policy
- Administrators:** Administrators
- Settings:**
 - GUI and CLI Password Policy:**
 - Minimum Length: 8 characters (Valid Range: 4 to 127)
 - Password should not contain the username or its characters in reversed order
 - Password should not contain "lsc" or its characters in reversed order
 - Password should not contain [] in its characters in reversed order
 - Password should not contain repeated characters four or more times consecutively
 - Password must contain at least one character of each of the selected type:
 - Lowercase alphabetic characters
 - Uppercase alphabetic characters
 - Numeric characters
 - Non-alphanumeric characters
 - Password History:**
 - Password must be different from the previous 5 sessions (Other enabled CLI terminals only need 1 password irrespective of value configured)
 - Control plane password valid 30 days (Valid Range: 1 to 365)
 - Password Lifetime:**
 - Admins can be required to periodically change their password
 - Administrator passwords expire 90 days after creation or last change (valid range: 1 to 3650)
 - Send an email reminder to administrators 30 days prior to password expiration (valid range: 1 to 3650)
 - Suspend or Lock Account with Inconsecutive Login Attempts

Políticas de senhas de usuários de acesso administrativo

Nessa mesma tela, em Authorization, temos uma ótima granularidade para definir o que cada usuário administrativo pode ou não fazer. Acesso a menus específicos, permissão para criar outros usuários e etc.

Essa possibilidade é bem útil caso tenhamos vários admins olhando pro ISE. Teríamos então um grupo Help Desk com possibilidade de read-only, um grupo Operadores, com permissão de troubleshooting ou review básico de autenticação, e um grupo Admin, que poderia criar e adicionar devices e novas regras — esses são apenas exemplos de possibilidades.

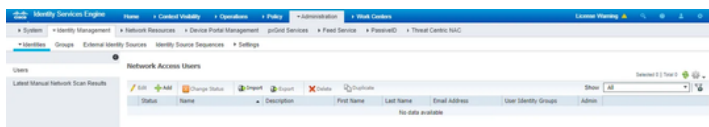
Name	Description
<input type="checkbox"/> Super Admin Menu Access	Access permission for Operations tab, Policy tab, Guest Access tab, Mobile Device Management tab and Administration tab.
<input type="checkbox"/> Policy Admin Menu Access	Access permission for Operations tab, Policy tab, Guest Access tab, Mobile Device Management tab, System and Identity Management.
<input type="checkbox"/> Predefined Admin Menu Access	Access permission for Operations tab.
<input type="checkbox"/> Identity Admin Menu Access	Access permission for Operations tab and Identity Management.
<input type="checkbox"/> Network Device Menu Access	Access permission for Operations tab and Network Resources.
<input type="checkbox"/> System Admin Menu Access	Access permission for Operations tab and System.
<input type="checkbox"/> RBAC Admin Menu Access	Access permission for Operations tab and System.
<input type="checkbox"/> Self Admin Menu Access	Access permission for Operations tab.
<input type="checkbox"/> Customizable Admin Menu Access	Access Permission to Guest Menu and Device Portal Management.
<input type="checkbox"/> TACACS+ Admin Menu Access	Access Permission to Operations, Administration and Workcenter.

Políticas de autorização para usuários administrativos

Administration > Identity Management.

Aqui já começaremos a falar dos usuários de rede, ou seja, usuários que serão utilizados para acesso a recursos da rede (seja Internet, servidores específicos, etc.), via protocolo RADIUS ou TACACS+.

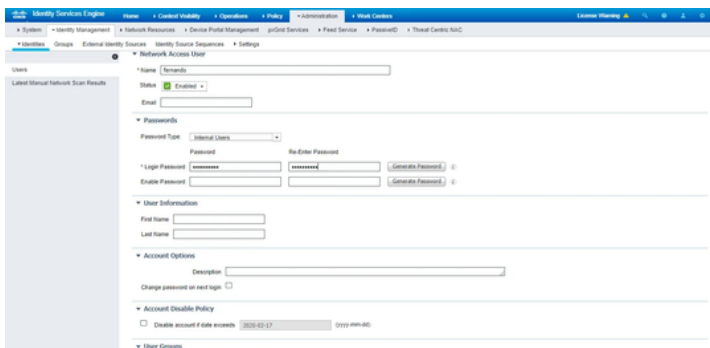




Usuários de acesso a rede

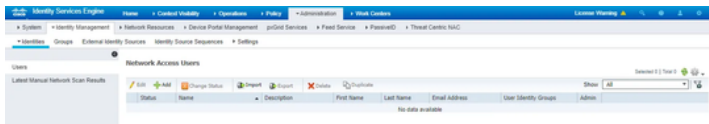
Abaixo, faremos a criação de um usuário como exemplo. Dois pontos de destaque nesse processo:

- Em Password Type, podemos utilizar uma senha que será armazenada na base de dados do ISE ou em uma base externa, como um Microsoft Active Directory (é necessário integração antes, mostraremos em artigos futuros ok?).
- E mais pra baixo, podemos adicionar esse usuário em grupos, que são criados na aba seguinte.



Criação de usuários de rede

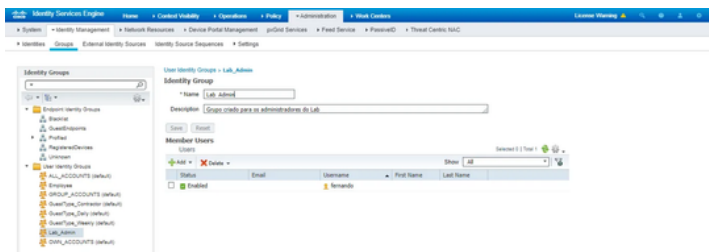




Usuários de acesso a rede

Aqui vemos dois tipos de grupos: usuários e endpoints. Isso porque o ISE autentica não só usuários como também dispositivos.

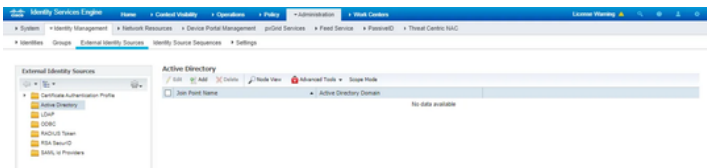
Esses dispositivos podem ser criados manualmente ou automaticamente, através da funcionalidade de Profiling que comentamos no artigo anterior (link). Dessa forma, como o ISE pode identificar iPhones, máquinas Windows 7, Linux, Smartphone Samsung, impressoras HP entre outros, podemos criar regras permitindo que apenas um tipo de equipamento acesse determinado recurso na rede. Granularidade total!



Grupos de Identidade – Endpoints e Usuários

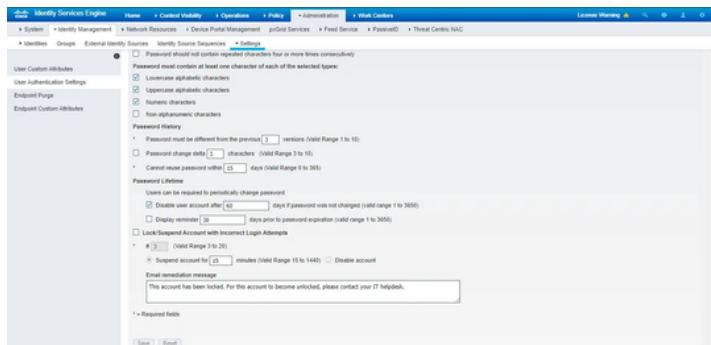


A próxima tela External identity Sources, é onde configuramos a integração de uma base de usuários externa com o ISE. Em destaque o Active Directory que é o mais usual.



Bases de usuários externas

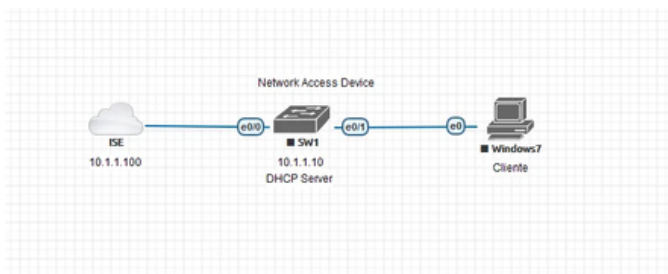
A próxima tela é a Identity Sources Sequences que trataremos mais pra frente, e a última é a Settings, bem parecida com a tela que falamos no início do artigo. Aqui, nós definiremos a política de usuários para acesso aos recursos da rede, diferente do acesso administrativo ao ISE que falamos acima.



Política de senha de usuários de rede



Bom, agora que já temos um usuário e um grupo no ISE, vamos configurar o NAD (Network Access Device). O dispositivo que irá consultar o ISE para confirmar a autenticação e aplicar a política de autorização.



Topologia de rede simples

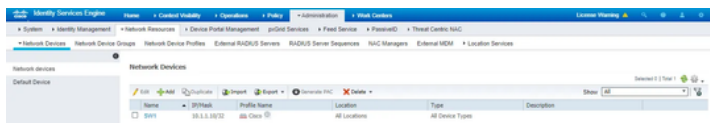
Aqui estamos só tratando da criação do NAD, o processo todo de autenticação será no próximo artigo blz?

Vamos adicionar então nome, IP, e senha do RADIUS.

Adicionando um dispositivo



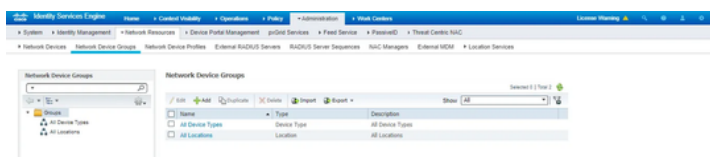
Na lista, ele irá aparecer dessa forma:



Name	Profile Name	Location	Type	Description
SW1	SW1	All Locations	All Device Types	

Lista de dispositivos criados

Os NADs também podem ser alocados em grupos, seja por tipo ou localização. Planejar é fundamental para a organização da rede.



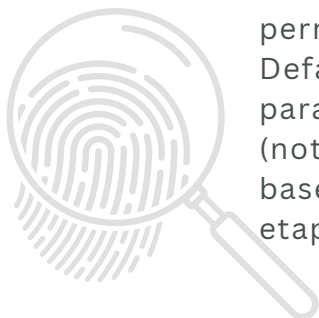
Name	Type	Description
All Device Types	All Device Types	
All Locations	Locations	All Locations

Organizando os dispositivos

E, finalmente, vamos pra tela Policy aba Authentication.

Esse é o padrão do ISE nessa versão. A primeira regra é de MAB – Mac Authentication Bypass, que autentica o MAC Address, ou seja, estamos falando de camada 2.

Traduzindo a regra, significa: **SE** a autenticação for para MAC Address cabeada (wired) ou wireless, em protocolos permitidos na regra padrão de nome Default Network Access – falaremos mais para frente dela – e, caso esse dispositivo (notebook, celular, etc.) estiver criado na base do ISE, aí ele passará para a próxima etapa: **Autorização**.



The screenshot shows the 'Authentication Policy' configuration page in Cisco ISE. The 'Policy Type' is set to 'Simple'. The policy is named 'Default' and is associated with the 'Internal Endpoints' group. The policy is applied to the 'Default Network Access' profile. The policy is defined by the following rules:

Rule Name	Conditions	Permissions
Default	Wireless_SSI EX OR Wireless_SSI OR	DenyAccess
Default	Wireless_SSI Match-Protocols DefaultNetworkAccess and	DenyAccess
Default Rule (if no match)	and use AllUser_ID_Stores	DenyAccess

Política padrão de autenticação

Agora que já sabemos que o usuário foi autenticado com sucesso, vamos definir **O QUE ELE PODE FAZER**. Essa configuração é feita na tela Authorization.

Abaixo, as regras padrão do ISE nessa versão 2.1.

The screenshot shows the 'Authorization Policy' configuration page in Cisco ISE. The policy is named 'Default' and is associated with the 'First Matched Rule Applies' rule type. The policy is applied to the 'Default Network Access' profile. The policy is defined by the following rules:

Rule Name	Conditions (identity groups and other conditions)	Permissions
Wireless Back List Default	Blacklist AND Wireless_Access	DenyAccess
Prohibit Cisco IP Phones	Cisco_IP_Phone	DenyAccess
Prohibit Non Cisco IP Phones	Non_Cisco_Prohibit_Phones	DenyAccess
Compliant_Device_Access	Network_Access_Authentication_Framed AND Compliant_Device	PermitAccess
Employee_EAP_TLS	Wireless_SSI EX AND BYOD_Registered AND EAP_TLS AND MAC_SAR	PermitAccess AND BYOD
Employee_Onboarding	Wireless_SSI EX AND EAP_MSCHAPV2	DenyAccess
WiFi_Guest_Access	Guest_Flow AND Wireless_SSI	PermitAccess AND Guest
WiFi_Retrived_to_Guest_Login	Wireless_SSI	DenyAccess
Basic_Authentication_Access	Network_Access_Authentication_Framed	PermitAccess
Default	First Matched Rule	DenyAccess

Política padrão de autorização



AGRADECIMENTOS

Gostaria de agradecer a todos os leitores e seguidores do blog TechRebels nesses anos todos. Foi sensacional ter tido a chance de conhecer alguns pessoalmente.

Espero que o conteúdo possa ajudar muito mais pessoas a aprender sobre essa solução que continua dominando o mercado e não para de crescer em funcionalidades e adoção!

Se você recebeu esse ebook de um amigo, dê uma olhada nos treinamentos que temos disponíveis no ciberseguranca.cisco.com.br.

Grande abraço e muito sucesso!!!



[linkedin.com/in/fmp7/](https://www.linkedin.com/in/fmp7/)

