TESTE DE CONFORMIDADE

PREGÃO ELETRÔNICO Nº001/2023 - SEDUC/GO

PROCESSO Nº 2020.0000.604.5301

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

OBSERVAÇÕES

Devido à perda de qualidade e resolução na conversão para arquivo .PDF, disponibilizamos o endereço do repositório em nuvem contendo o arquivo no formado .DOC. Este arquivo mantém a qualidade das imagens, facilitando a visualização completa.

URL: https://owncloud.compwire.com.br/index.php/s/aLGkTKtH0PQ7YU5

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

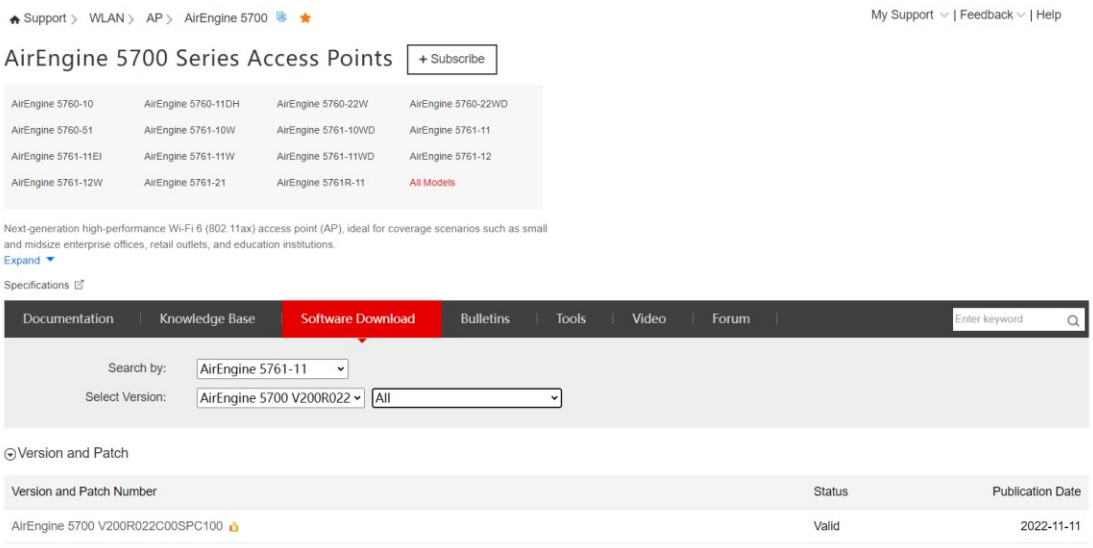
EQUIPAMENTOS UTILIZADOS NOS TESTES

Ponto de Acesso sem fio Tipo 1

Marca: Huawei

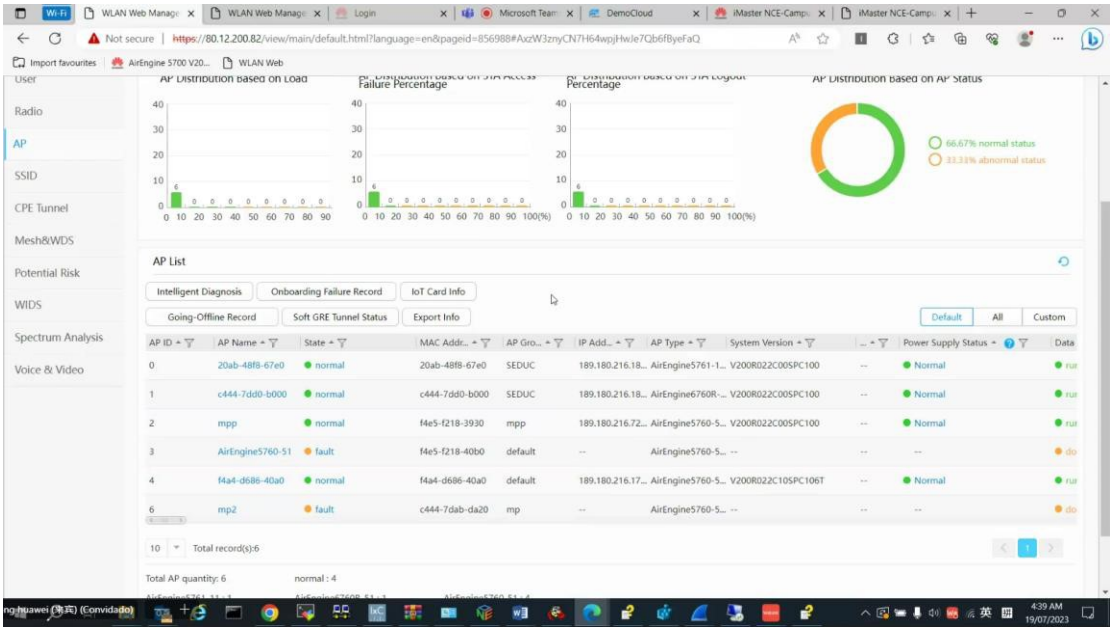
Modelo: AirEngine 5761-11

Software utilizado: AirEngine 5700 V200R022C00SPC100



Evidência:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

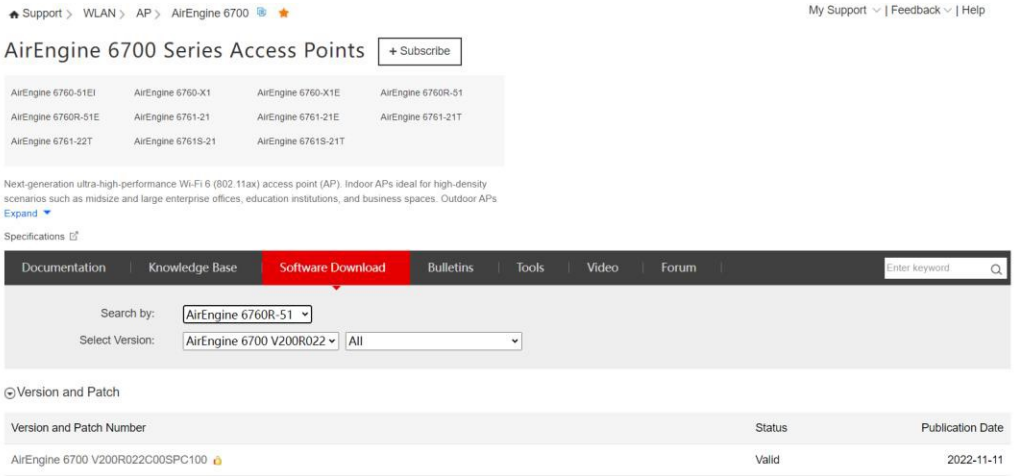


Ponto de Acesso sem fio Tipo 2

Marca: Huawei

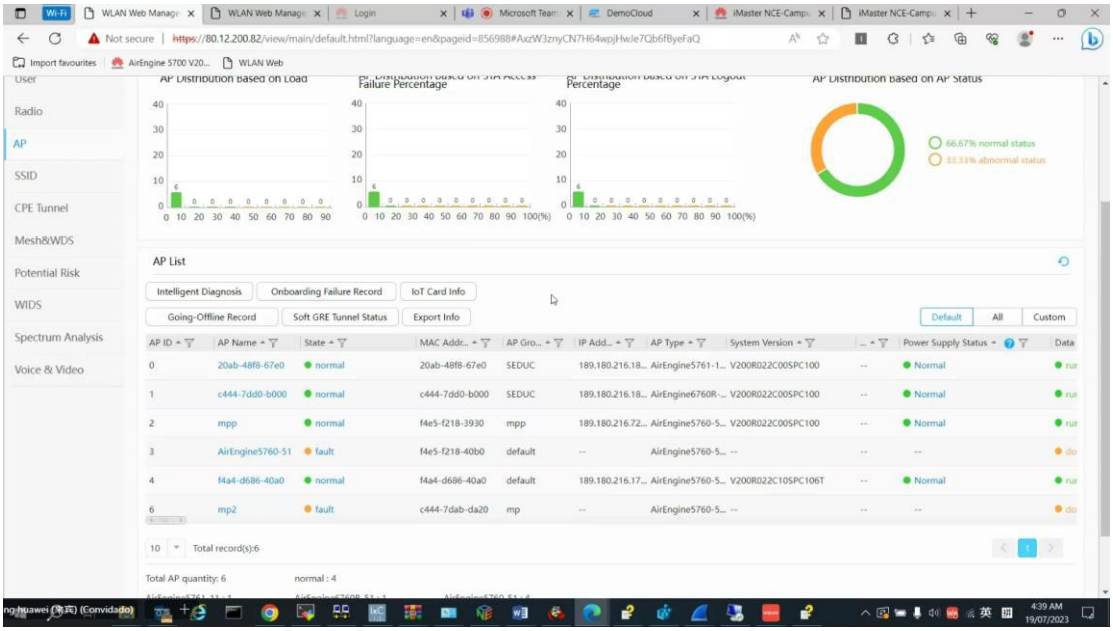
Modelo: AirEngine 6760R-51

Software utilizado: AirEngine 6700 V200R022C00SPC100



Evidência:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES



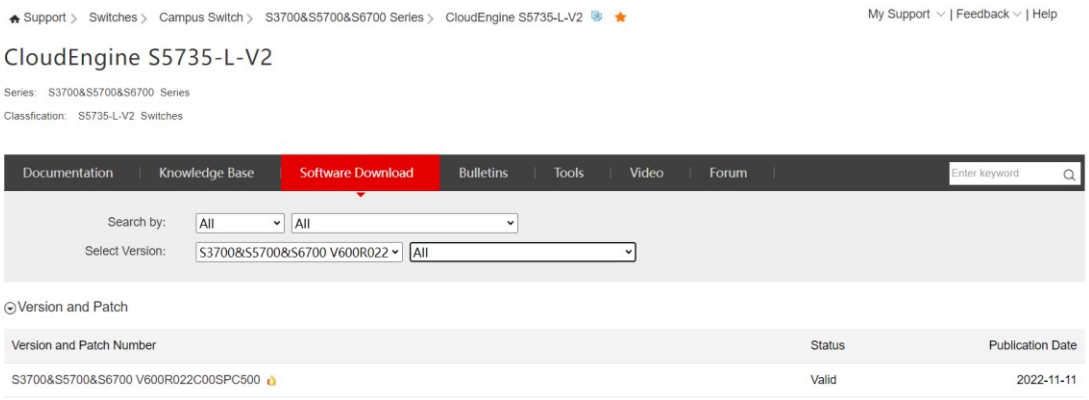
Switch Tipo 01 e Tipo 02 (Obs. Nos testes utilizamos o modelo PoE, referente ao Tipo 01)

Marca: Huawei

Modelo Tipo 01: CloudEngine S5735-L24P4S-A-V2

Modelo Tipo 01: CloudEngine S5735-L24T4S-A-V2

Software utilizado: S3700&S5700&S6700 V600R022C00SPC500



Evidência:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

```
<S5735-L24P4S-A-V2_14079E0F>dis version
Huawei YunShan OS
Version 1.22.0.1 (S5700 V600R022C01SPC500)
Copyright (C) 2021-2022 Huawei Technologies Co., Ltd.
HUAWEI CloudEngine S5735-L-V2 uptime is 0 day, 0 hour, 8 minutes

S5735-L24P4S-A-V2(Master) 1 : uptime is  0 day, 0 hour, 7 minutes
        StartupTime 2023/07/18   18:50:28
Memory       Size     : 2048 M bytes
Flash        Size     : 1024 M bytes
S5735-L24P4S-A-V2 version information:
1.PCB        Version  : ES5D2V28S036 VER A
2.MAB        Version  : 0
3.Board      Type     : S5735-L24P4S-A-V2
4.BIOS       Version  : 825
5.CPLD       Version  : 257
```

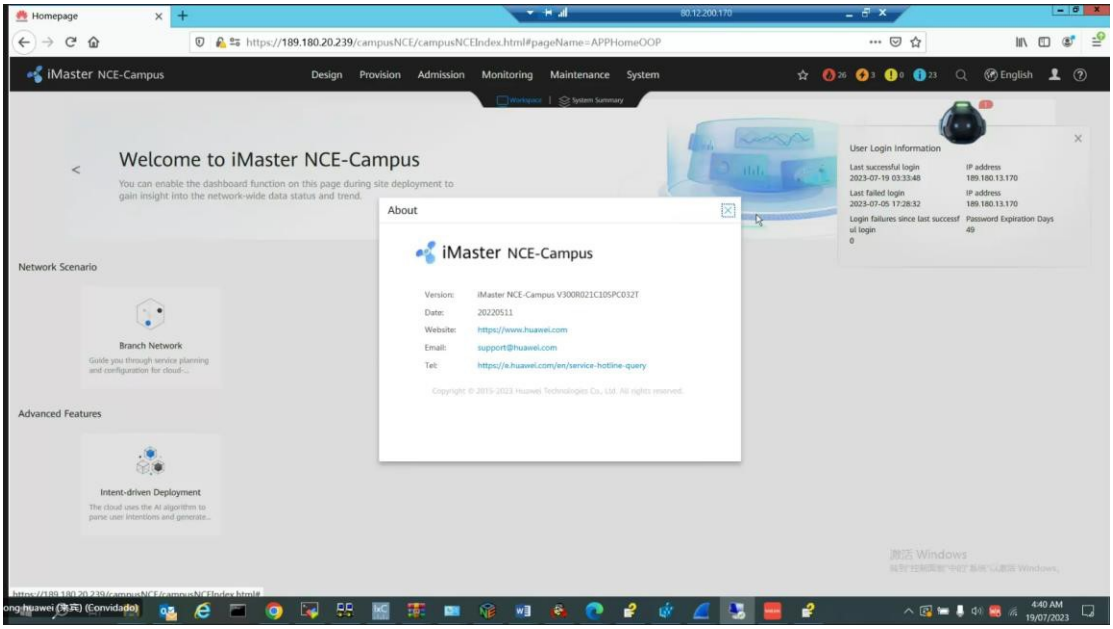
Solução de gerenciamento e controle de Switches e APs

Marca: Huawei

Modelo: CloudCampus Solution

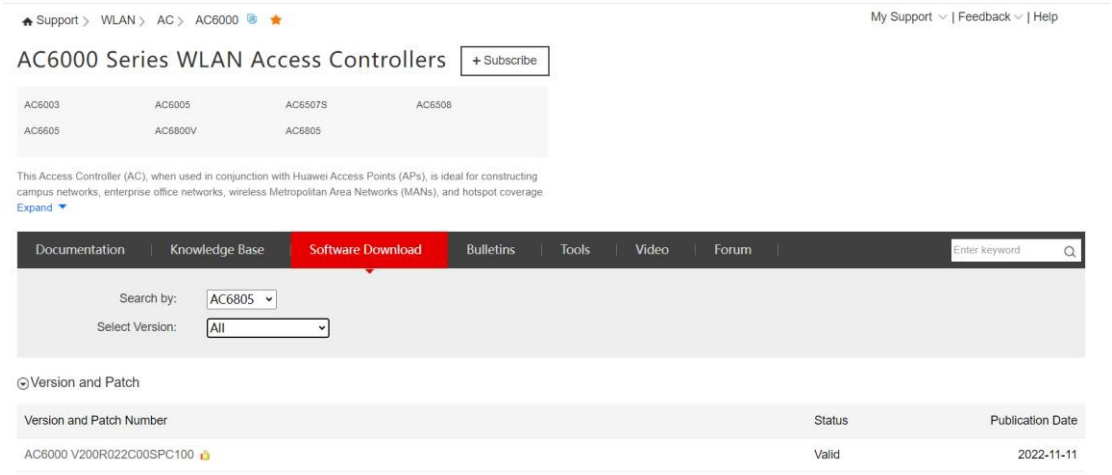
Software utilizado: iMaster NCE-Campus V300R021C10

Evidência:

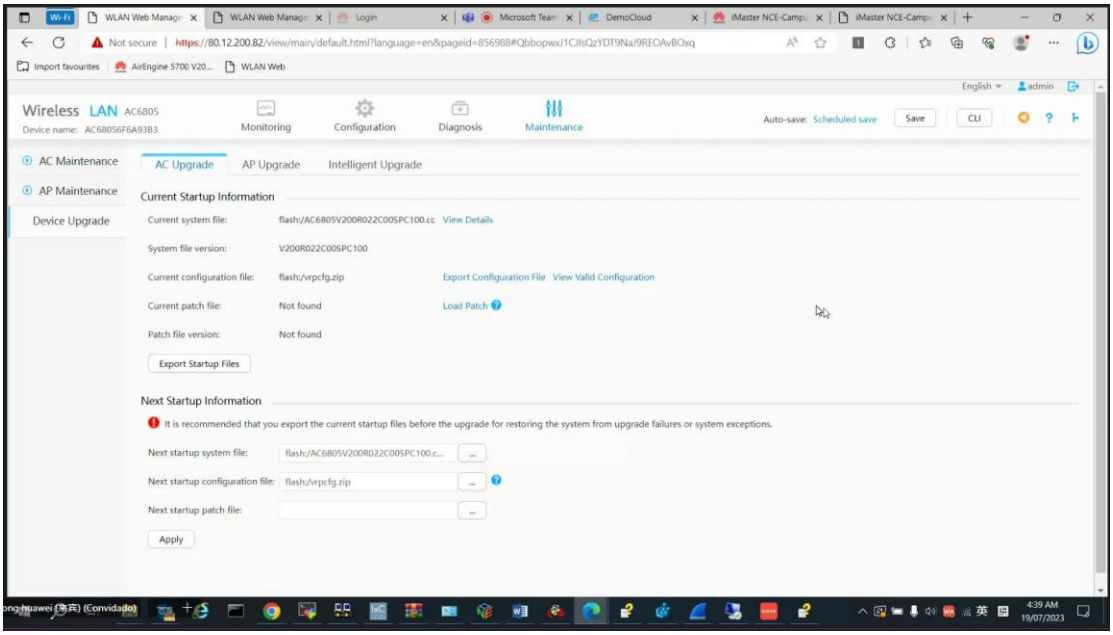


Software utilizado: AC6000 V200R022C00SPC100

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES



Evidência:



PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

CADERNO DE TESTES

Itens que não utilizam configuração como comprovação:

5.6 Ponto de Acesso sem fio Tipo 1

5.6.2.1 Possuir capacidade de montagem em parede e teto, devendo ser fornecidos todos os acessórios necessários para estas montagens;

Comprovação visual – Documentação complementar:

Super Tópico - Installing Indoor Settled Aps
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_TOPIC_0000001408815222&lang=en

Understanding Mounting Brackets e Installation Scenarios
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_TOPIC_0000001458975033&lang=en

Determining the Installation Position
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_TOPIC_0000001408815234&lang=en

5.6.2.2 Deve suportar a utilização de sistema antifurto do tipo Kensington ou similar;

Comprovação visual - Documentação complementar:

Hardware Information (AirEngine 5761-11) - Ports
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_CONCEPT_0000001388948464&lang=en

Anti-Theft e Removal
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_TOPIC_0000001458855053&lang=en

5.6.2.3 Deve acompanhar todos os recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (podendo ser utilizado cabo de segurança com chave ou similar);

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Equipamento de segurança fornecido junto a proposta - Documentação complementar:

Anti-Theft e Removal
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_TOPIC_0000001458855053&lang=en

5.6.2.6 Deve possuir um ou mais Leds indicadores de estado de operação;

Comprovação visual – Documentação complementar:

Product description – Indoor Settled AP - AirEngine 5761-11 – Hardware information – Indicators e Buttons
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_CONCEPT_0000001388948464&lang=en

5.6.2.7 Não deve possuir antenas aparentes, que sejam rosqueáveis, evitando a remoção das antenas;

Product description – Indoor Settled AP - AirEngine 5761-11 – Hardware information – Appearance
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_CONCEPT_0000001388948464&lang=en

5.7 Ponto de Acesso sem fio Tipo 2

5.7.2.1 Possuir capacidade de montagem em parede, teto e mastro, devendo ser fornecidos todos os acessórios necessários para estas montagens;

5.7.2.2 Deve acompanhar kit para montagem em parede, o kit deve ter recursos necessários para não permitir a retirada do equipamento por pessoas não autorizadas (podendo ser utilizado cabo de segurança com chave ou similar);

5.7.2.4 Possui grau de proteção mínimo IP67, outdoor;

Comprovação documental

Product description – Outdoor AP - AirEngine 6760R-51 – Hardware information – Technical Specifications
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_CONCEPT_0000001439108181&lang=en

Ingress protection level (dustproof/waterproof) - IP68

5.7.2.7 Deve possuir um ou mais Leds indicadores de estado de operação;

Comprovação visual – Documentação complementar:

Product description – Outdoor AP - AirEngine 6760R-51 – Hardware information – Appearance
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100210441&id=EN-US_CONCEPT_0000001439108181&lang=en

Itens que necessitam de configuração:

Access point sem fio, funcionalidades básicas

Capacidade PoE

5.6.2.5 Possuir capacidade de alimentação PoE 802.3af, 802.3at ou 802.3bt;

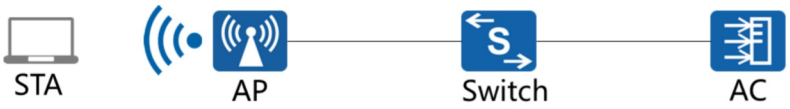
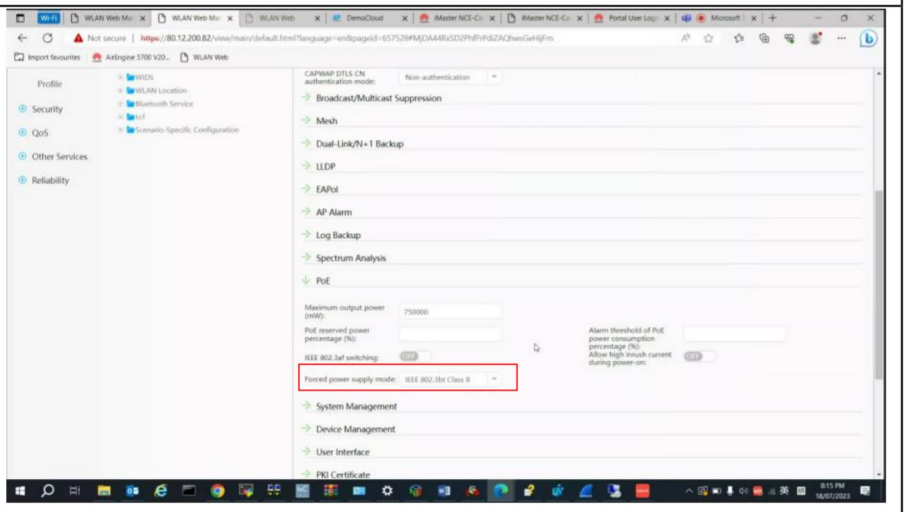
5.7.2.5 Possuir capacidade de alimentação PoE 802.3af, 802.3at ou 802.3bt;

5.8.1 Possuir capacidade de fornecer alimentação PoE 802.3af, 802.3at ou 802.3bt;

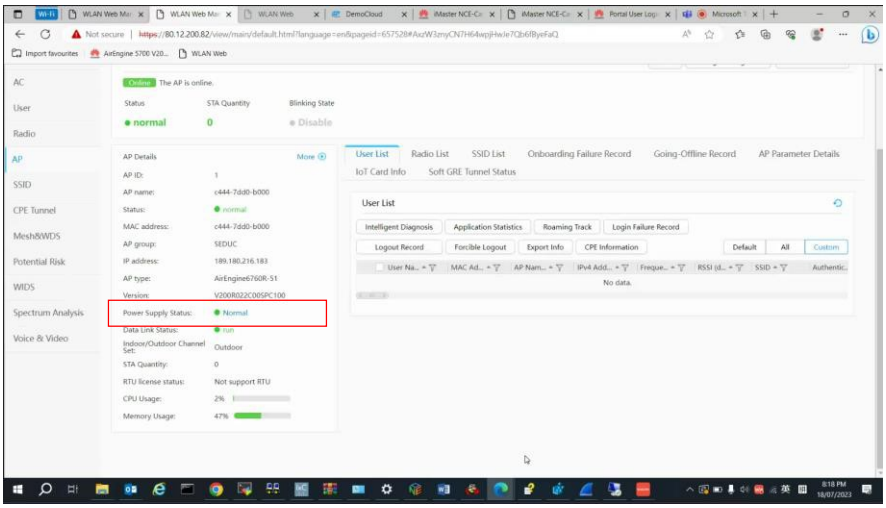
5.8.2 Deve possuir capacidade de energizar no mínimo 2 Access Point Tipo 2 e 10 Access Point Tipo 1 ou 12 Access Point Tipo 1 simultaneamente;

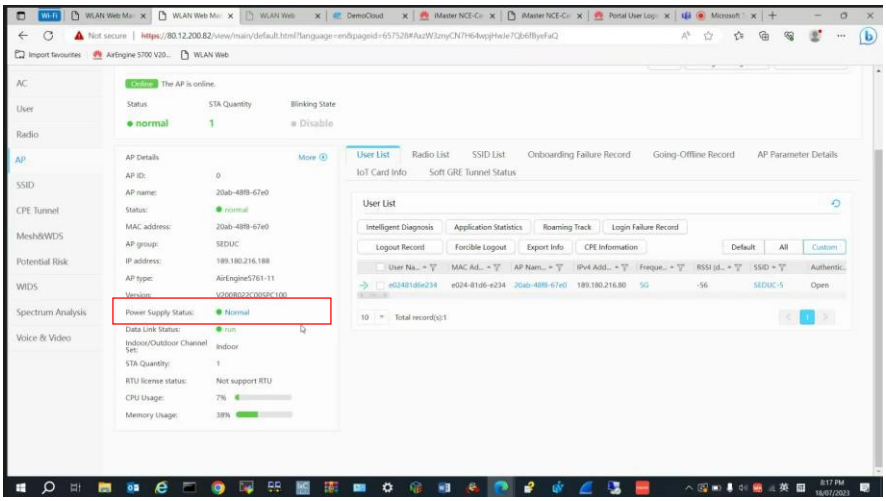
5.8.3 O Switch deve ser capaz de alimentar os Access Points Tipo 1 sem a necessidade de componentes adicionais;

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

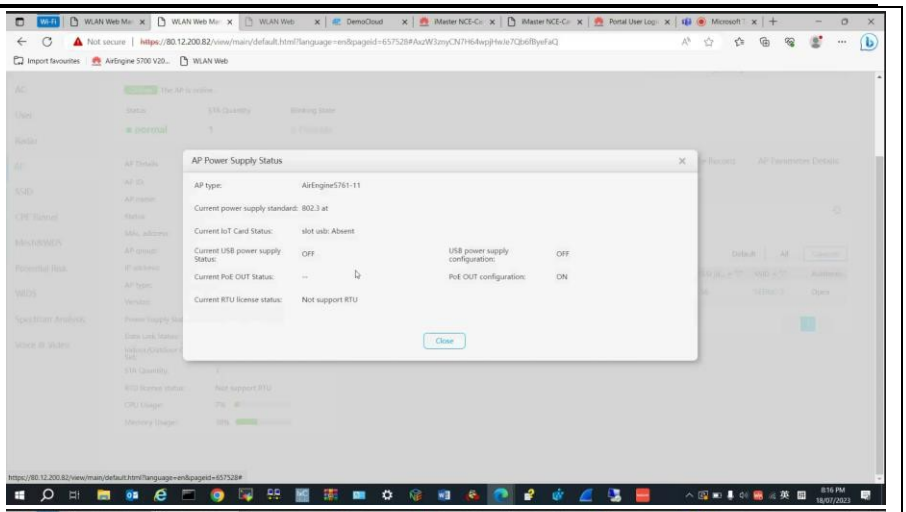
Item de teste	**Capacidade de alimentação PoE**
Objetivo do teste	Validar que o access point sem fio esteja de acordo com 802.3 bt/at
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Verifique o estado do AP quando alimentado no modo 802.3bt. 2) Mude o modo de alimentação do AP para o modo 802.3at.
Resultado esperado	1) O AP está operacional; o status de energia é mostrado. 2) O AP está operacional; o status de energia é mostrado.
Resultado	 Figura 1 – Acessando a controladora wireless (AC), é possível forçar qual o padrão de energia, será solicitado pelos pontos de acesso (AP). No

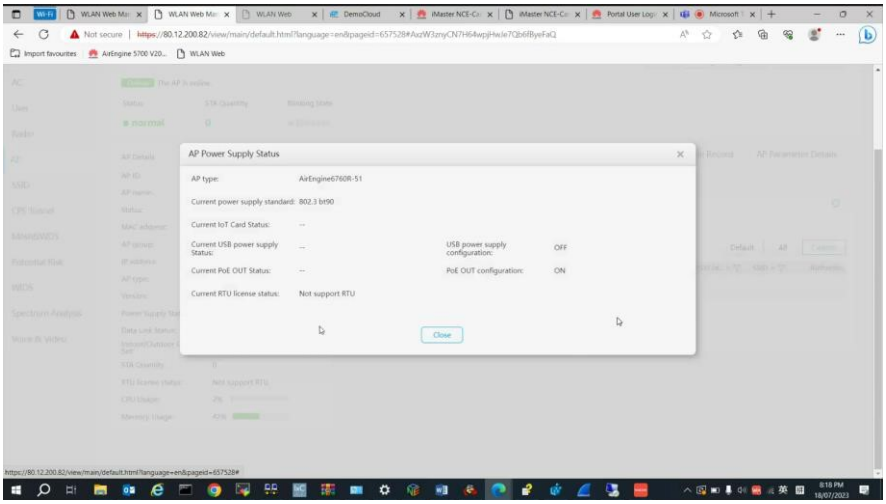
teste, foi aplicado o modo IEEE 802.3bt, para que sempre seja utilizado quando o AP suportar essa capacidade.





Figuras 2 e 3 – Na listagem dos APs, dentro da controladora, podemos ver as informações detalhadas de cada um, dentre elas, o status da fonte de energia em “Power Supply Status:”. Ambos os modelos, com o status “Normal”.





Figuras 4 e 5 – Checando as informações do descritas no “AP Power Supply Status”, é possível checar o tipo de energia e o padrão utilizado em cada ponto de acesso.

Para o modelo AirEngine 5761-11, 802.3at

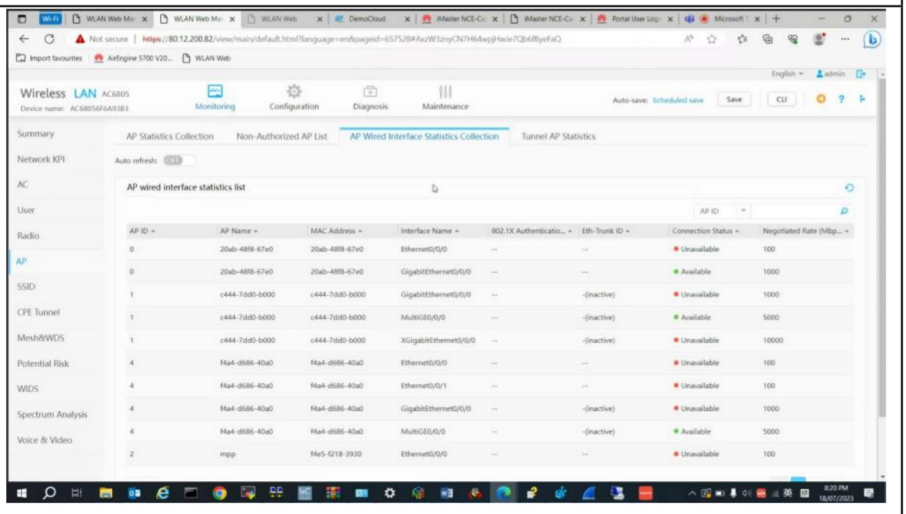
Para o modelo AirEngine 6760R-51, 802.3bt

Negociação de portas

5.6.3.1 Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior;

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

5.7.3.1 Possuir no mínimo 1 interface 10/100/1000 Base-T ou superior;

Item de teste	**Negociação de portas**
Objetivo do teste	Validar que o access point sem fio tenha pelo menos 1 interface 10/100/1000 Base-T ou acima;
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Verifique a velocidade da porta cabeada no AP.
Resultado esperado	1) O AP está operacional; a velocidade da porta é mostrada.
Resultado	 Figura 1 – Na controladora, é possivel checar a listagem de interfaces dos pontos de acesso, bem como a negociação dessas interfaces.

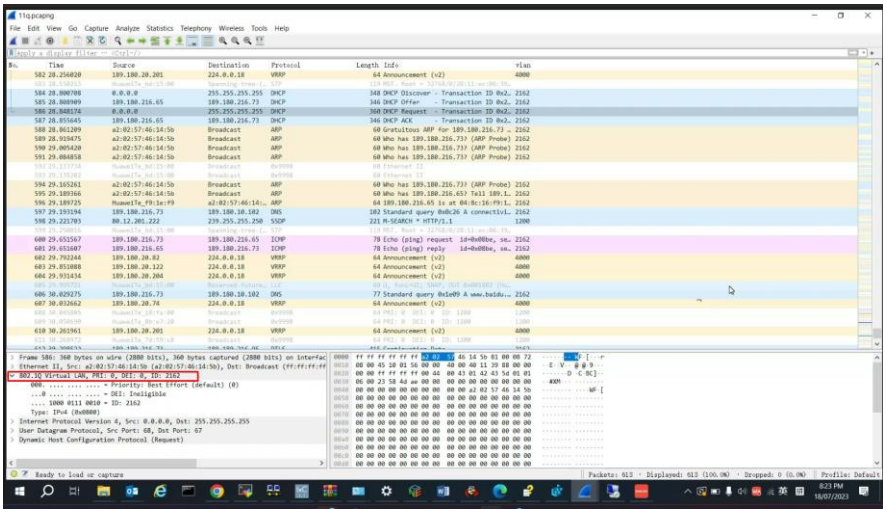
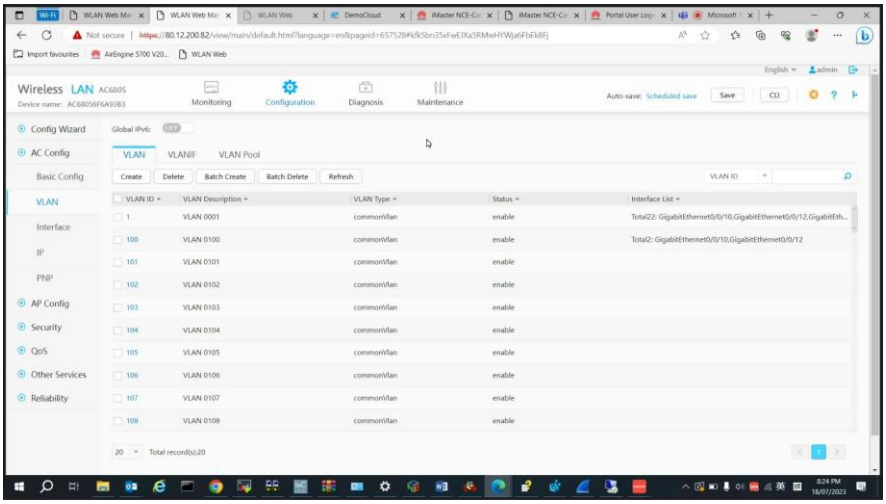
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

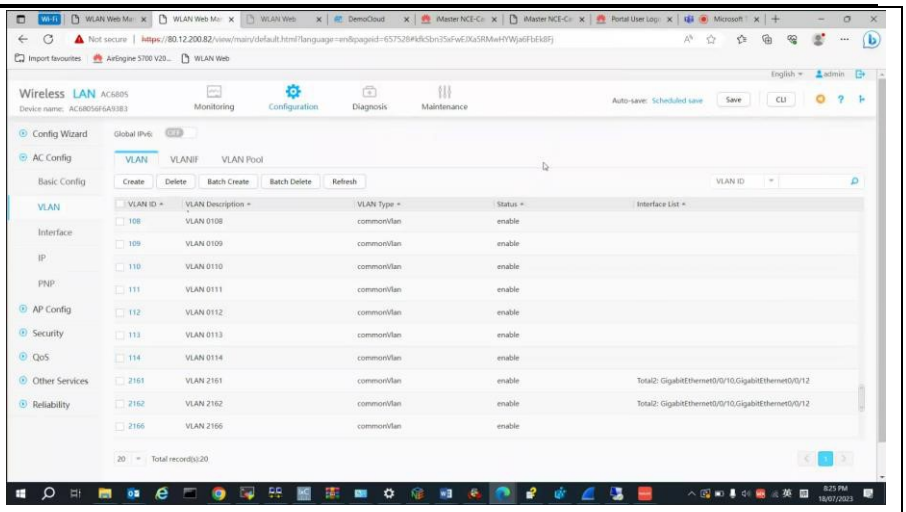
Múltiplas VLANs

5.6.3.2 Suportar VLANs conforme o padrão IEEE 802.1Q;

5.7.3.2 Suportar VLANs confirme o padrão IEEE 802.1Q;

Item de teste	**Múltiplas VLANs**
Objetivo do teste	Validar que o access point sem fio suporte VLANs de acordo com o padrão IEEE 802.1Q; e que suporte a criação de pelo menos 16 (dezesseis) VLANs;
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Após as configurações de SSID da AC, realize uma captura de pacottes na; 2) Crie 16 VLANs e add use them as service vlan for SSIDs.
Resultado esperado	1) O pacote mostra a marcação de vlan 802.1q. 2) 16 VLANs estão disponíveis no AP.

Resultado	 Figura 1 – Na captura de pacotes mostrada durante os testes, foi evidenciado a aplicação do tag, com a VLAN ID 2162. 



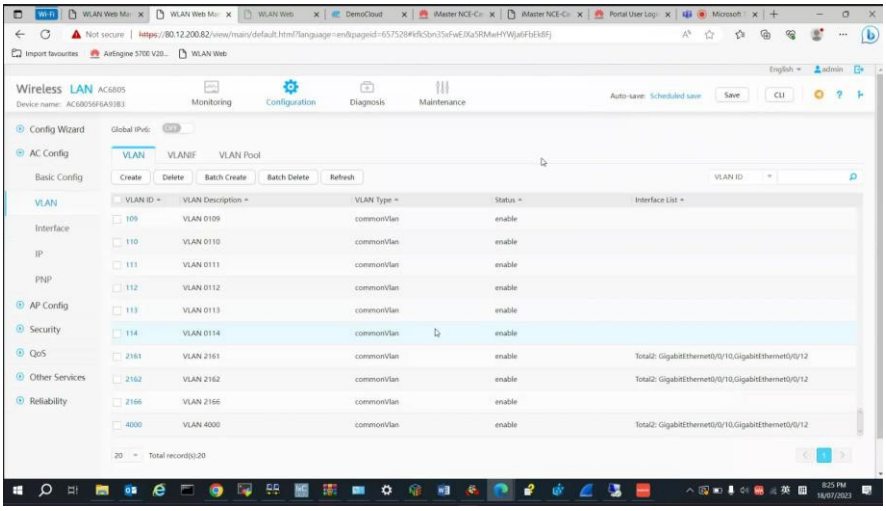
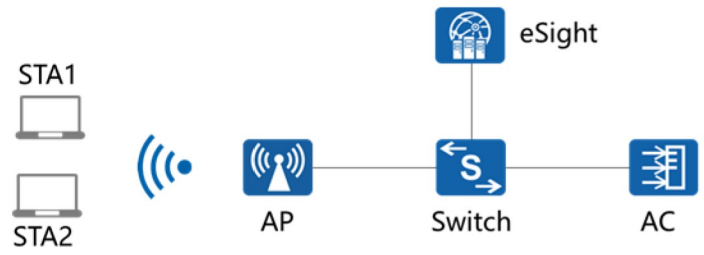
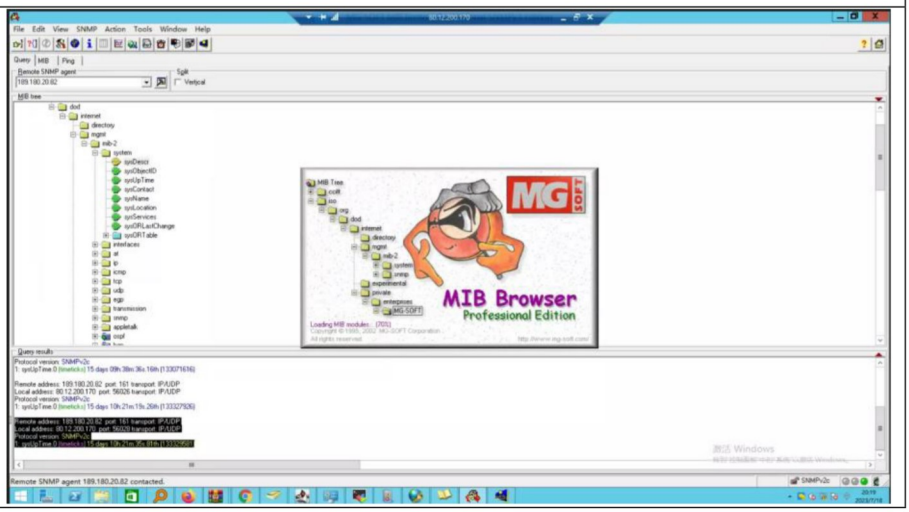


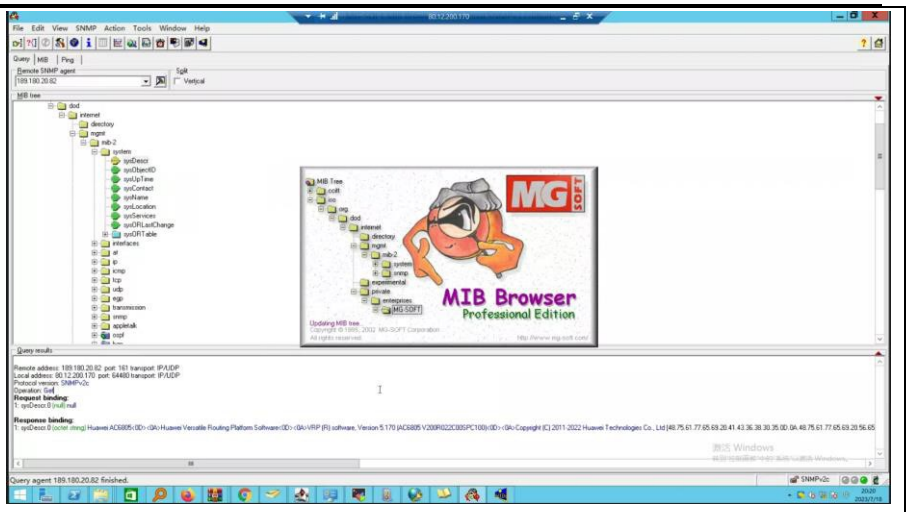
Figura 2, 3 e 4 – Na controladora, foram configuradas várias VLANs diferentes, contabilizando um total de 20 VLANs configuradas e aplicadas aos APs registrados.

Sistema de WLAN suporta a função de SNMP

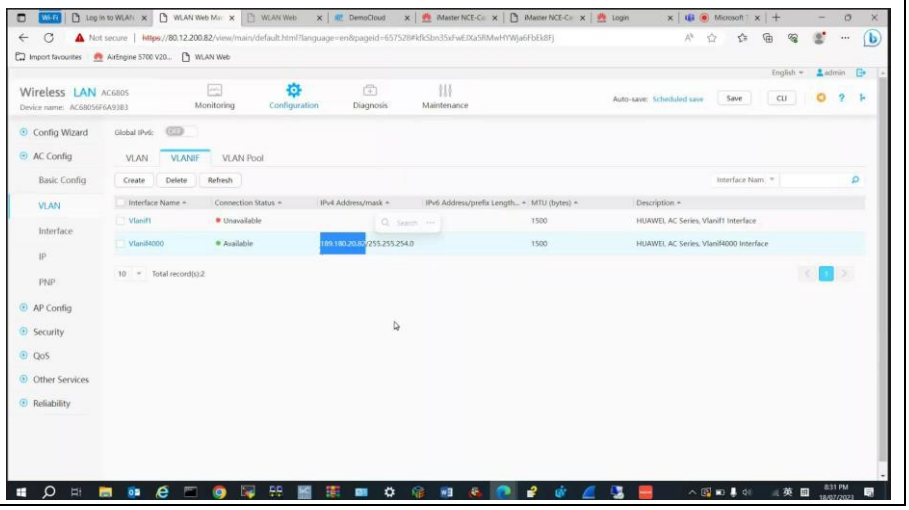
Item de teste	Sistema de WLAN suporta a função de SNMP

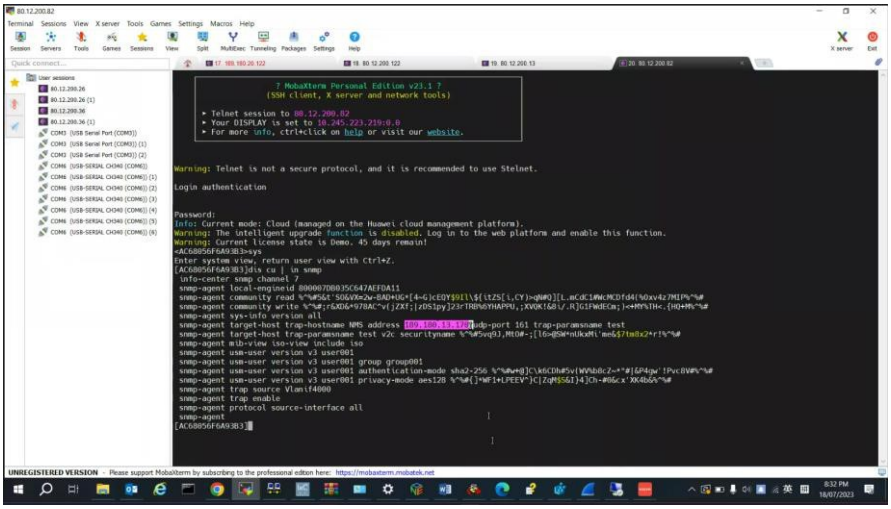
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Objetivo do teste	Validar que o sistema de WLAN suporta a função de SNMP
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Habilite a função SNMP na WAC, 2) Configure NMS para gerenciar a WAC;
Resultado esperado	1) AC gerenciada via SNMP (NMS) 2) Verifica-se informação de alarme no servidor SNMP (NMS)
Resultado	



Figuras 1 e 2 – Visualização de todas as MIBs disponíveis na AC, através do protocolo SNMPv2c.





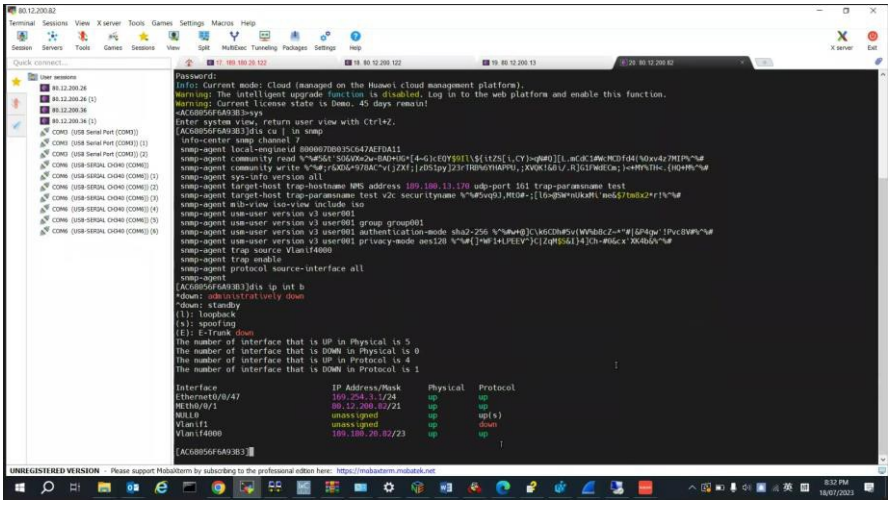


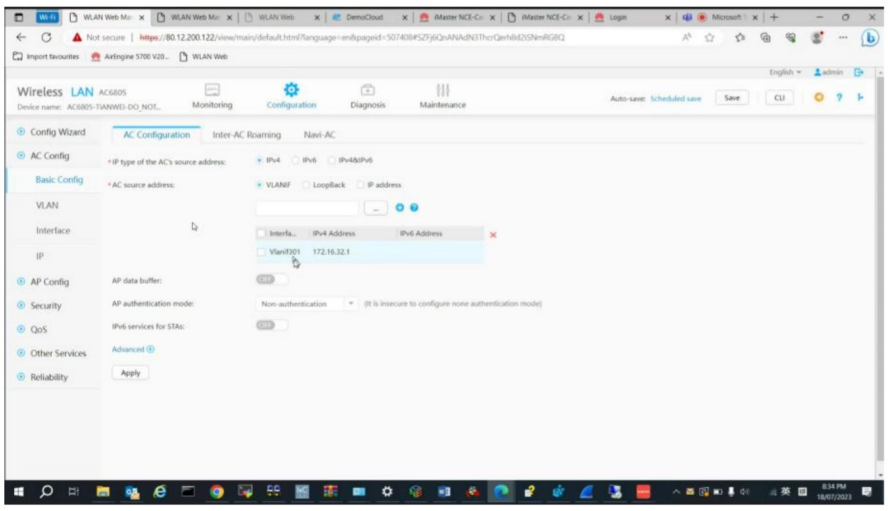
Figura 3, 4 e 5 – Configurações de endereçamento IP de gerenciamento da AC, o mesmo utilizado pelo NMS.

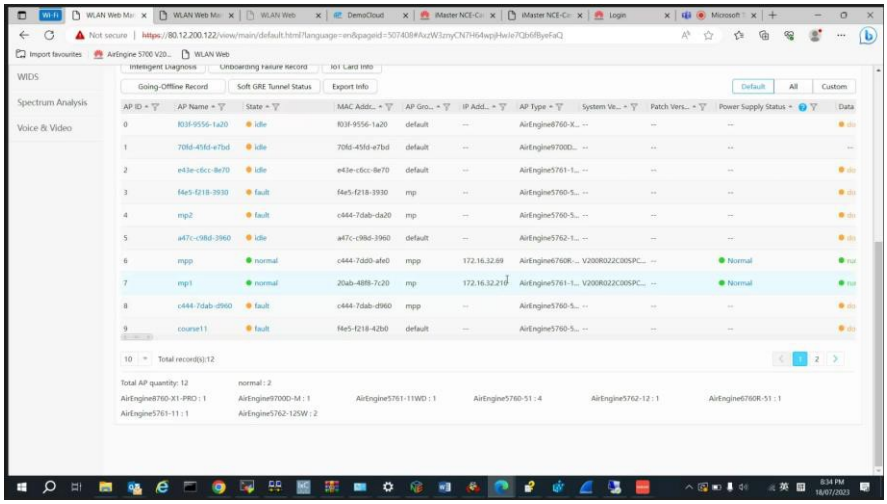
Layer 2 CAPWAP AC Discovery | Descoberta de AC por CAPWAP na camada 2

5.6.3.6. Deve implementar cliente DHCP, para configuração automática de rede;

5.7.3.6. Deve implementar cliente DHCP, para configuração automática de rede;

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Item de teste	Layer 2 CAPWAP WAC Discovery
Objetivo do teste	Validar que o Sistema WLAN suporta descoberta da AC por CAPWAP na camada 2
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure os parametros na AC: o AP obtem endereço IP do servidor DHCP. 2) O AP e AC estão na mesma subrede; 3) Verifique as configurações do AP.
Resultado esperado	1) O AP aparece como online na AC, dentro da mesma faixa de rede;
Resultado	 Figura 1 – Os APs gerenciados pelo controlador AC podem aprender o endereço IP especificado ou o endereço IP da interface especificada para

	configurar um túnel CAPWAP com o AC. Essa configuração foi evidênciada alterando os parametros em “AC source address”, configurando o endereço para a formação do tunel CAPWAP.  Figura 2 – Checando as informações dos APs descobertos, os APs com ID 6 e 7, receberam de forma automática, via protocolo DHCP, os endereços de IP da mesma faixa que foi configurada no “AC source address”.

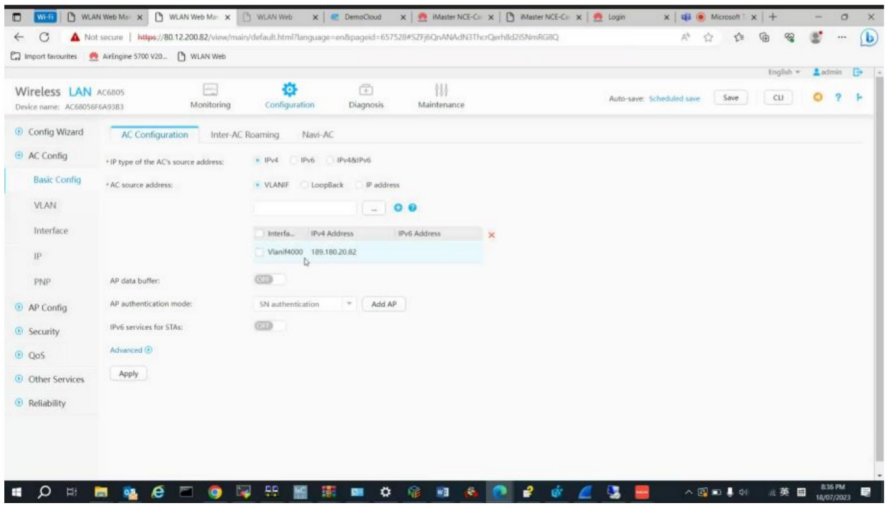
Layer 3 CAPWAP ac Discovery (DHCP Option 43) | Descoberta de AC por CAPWAP na camada 3 usando DHCP Option 43

5.6.3.6. Deve implementar cliente DHCP, para configuração automática de rede;

5.7.3.6. Deve implementar cliente DHCP, para configuração automática de rede;

Item de teste	Descoberta de WAC por CAPWAP na camada 3 usando DHCP Option 43
Objetivo do teste	Validar que o Sistema WLAN suporta Descoberta de AC por CAPWAP na camada 3 usando DHCP Option 43

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure os parametros na AC: o AP obtem endereço IP do servidor DHCP. 2) O AP e AC estão em redes distintas; 3) Verifique as configurações do AP.
Resultado esperado	1) O AP aparece como online na AC, dentro da uma faixa de rede diferente da AC;
Resultado	 Figura 1 – Os APs gerenciados pelo controlador AC podem aprender o endereço IP especificado ou o endereço IP da interface especificada para configurar um túnel CAPWAP com o AC. Essa configuração foi

evidênciada alterando os parametros em “AC source address”, configurando o endereço para a formação do tunel CAPWAP

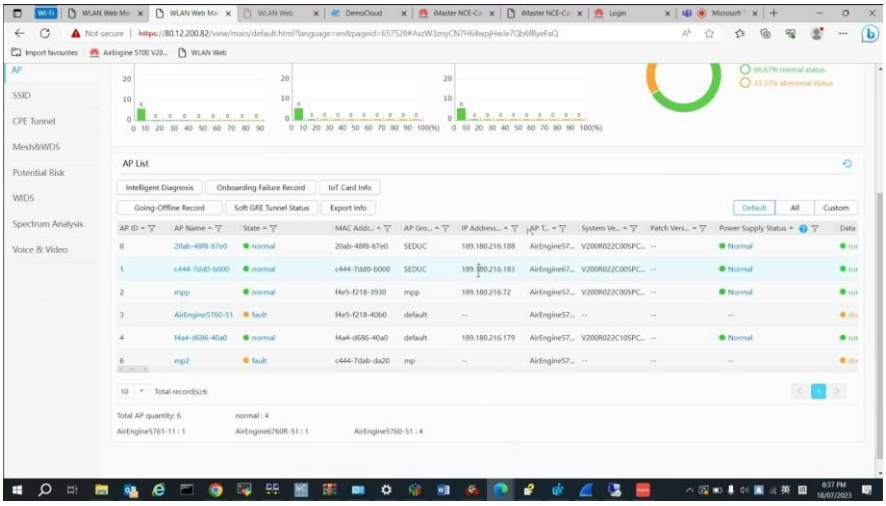


Figura 2 – Checando as informações dos APs descobertos, os APs com ID 0 e 1, receberam de forma automática, via protocolo DHCP, os endereços de IP, de uma VLAN diferente da que foi configurada no “AC source address”.

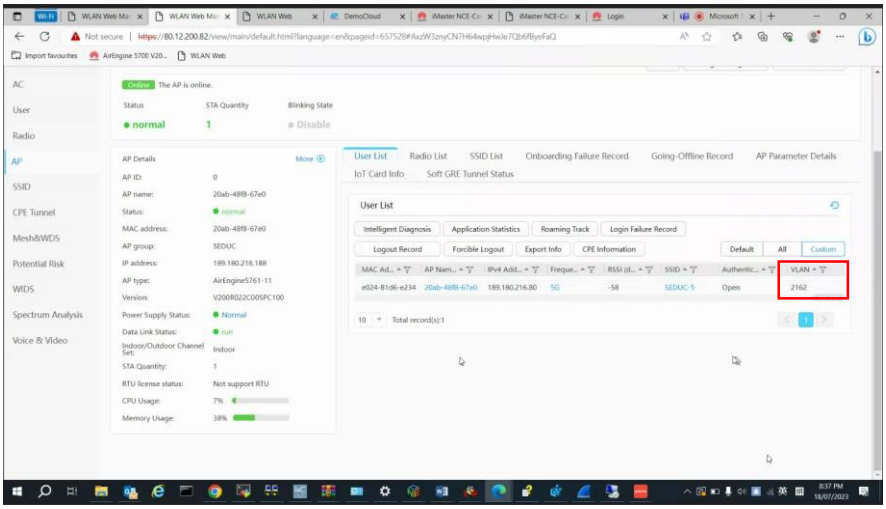
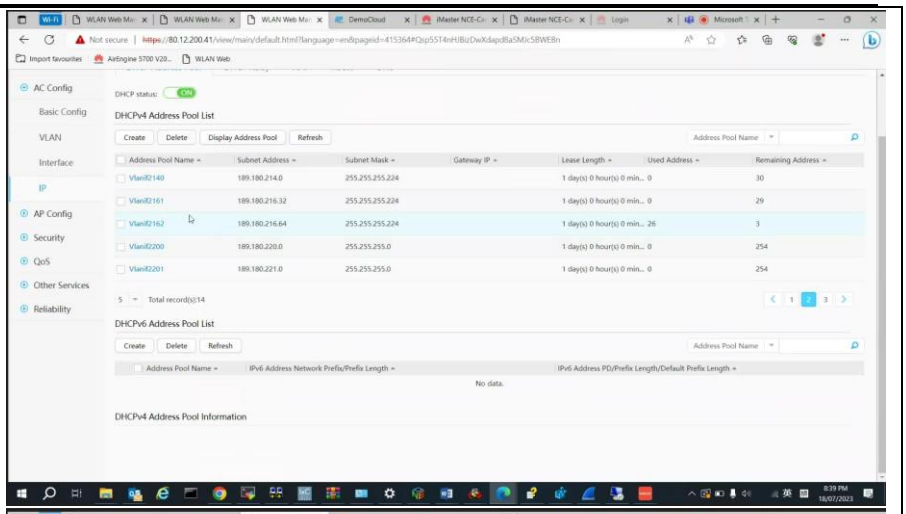
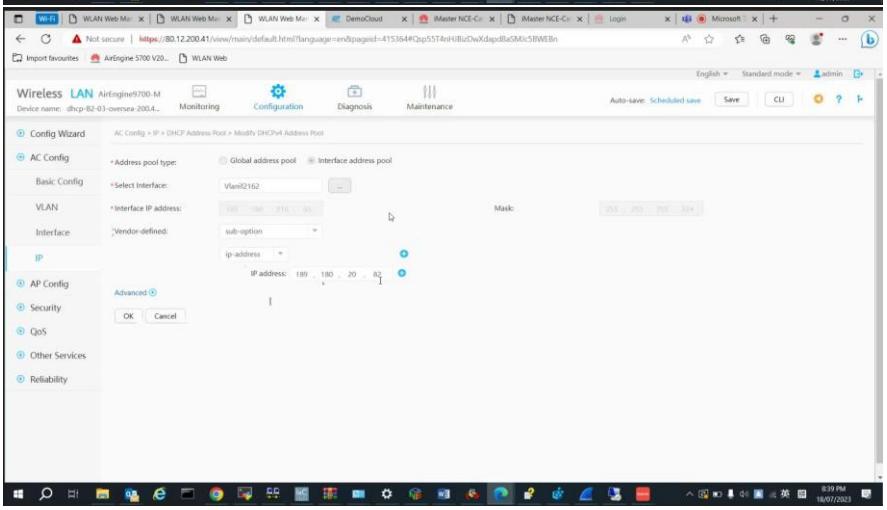


Figura 3 – Analisando as informações do AP ID 0, evidenciamos que seu funcionamento estava com o status de normal, e que a VLAN utilizada para a sua gerência, possui o ID 2162.





Figuras 4 e 5 – Na controladora, podemos ver os pools de DHCP disponiveis. Dentre eles, o pool com VLAN ID 2162.

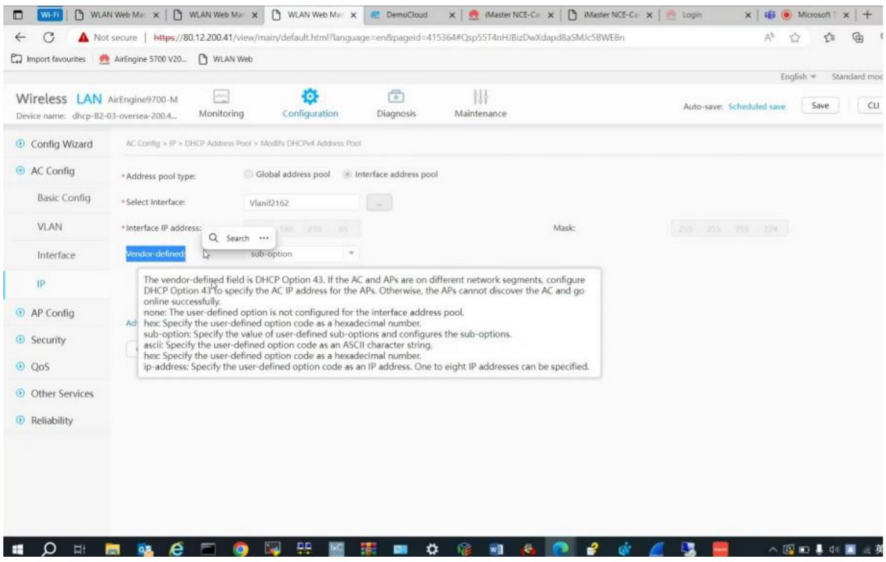


Figura 6 - Nas suas configurações, foi evidenciado a utilização do parametro “sub-options”, com a opção 43.

Layer 3 CAPWAP AC Discovery (static IP address) | Descoberta de AC por CAPWAP nacamada 3 usando IP estático

Item de teste	Layer 3 CAPWAP AC Discovery (static Endereço IP)
Objetivo do teste	Validar que o Sistema WLAN suporta descoberta de AC por CAPWAP na camada 3 usando IP estático
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

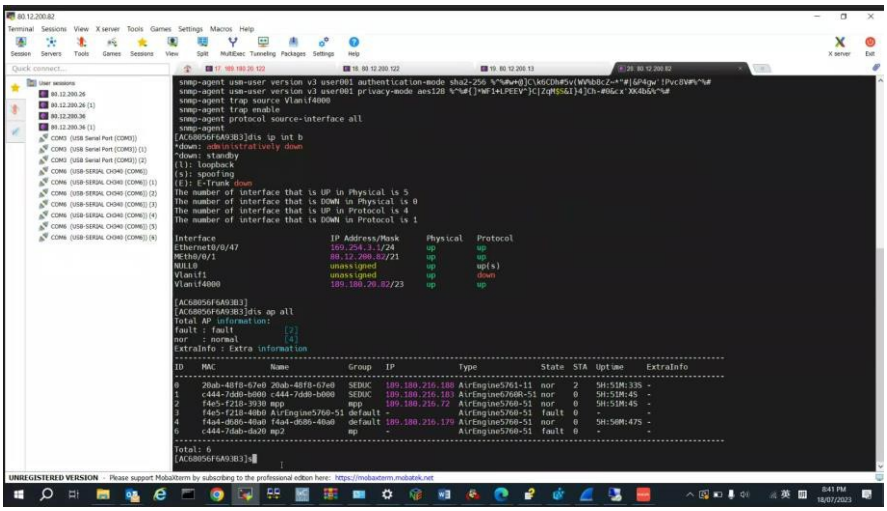
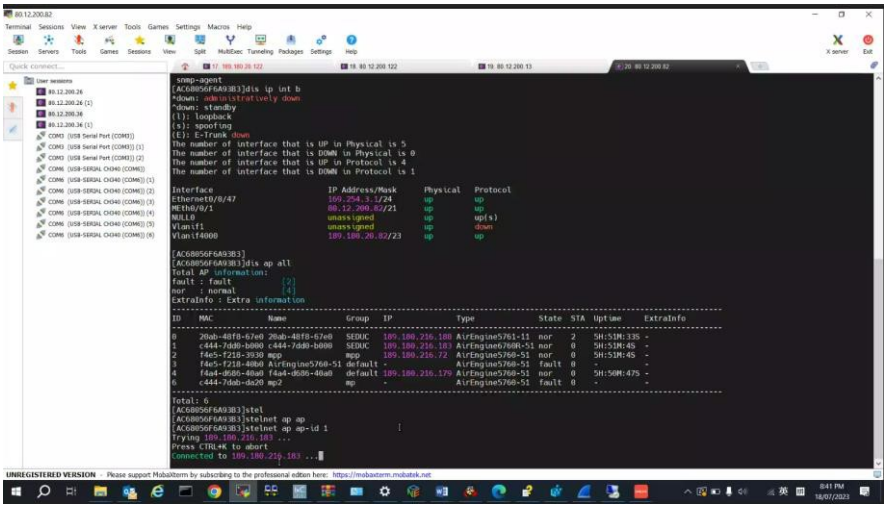
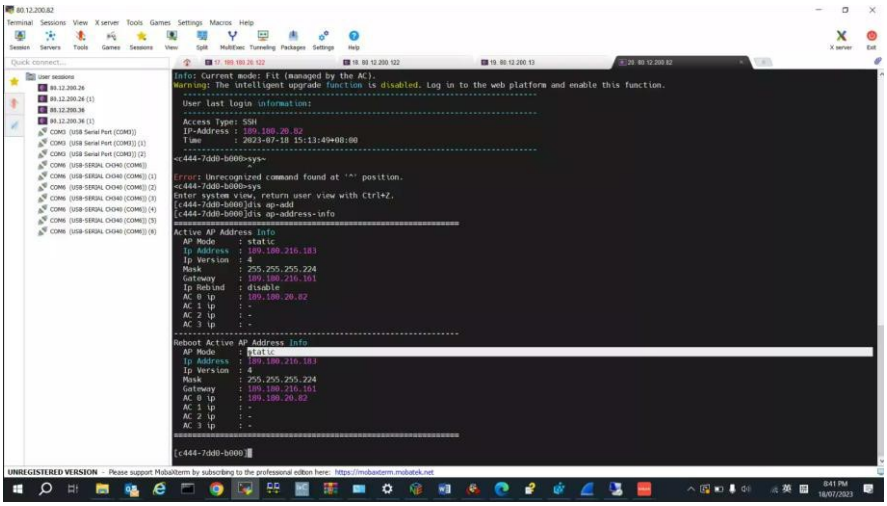
Procedimento de teste	1) Configure o endereçamento IP do AP, de forma estática. 2) O AP e AC estão em redes distintas; 3) Verifique as configurações do AP.
Resultado esperado	1) O AP aparece como online na AC, dentro da uma faixa de rede diferente da AC;
Resultado	 Figura 1 – Foi mostrada as configurações de endereçamento IP da controladora, e em seguida, a listagem de APs gerenciados, também com suas respectivas informações de endereçamento IP. 

	Figura 2 – Iniciamos um acesso via protocolo SSH, ao AP ID 1  Figura 3 – Visualizando as informações de enderaçamento IP do AP ID 0, atestamos que o IP utilizado foi configurado de forma estática, e que ainda sim foi possível formar o tunel CAPWAP, com a AC que está em outra rede.

Segurança WLAN

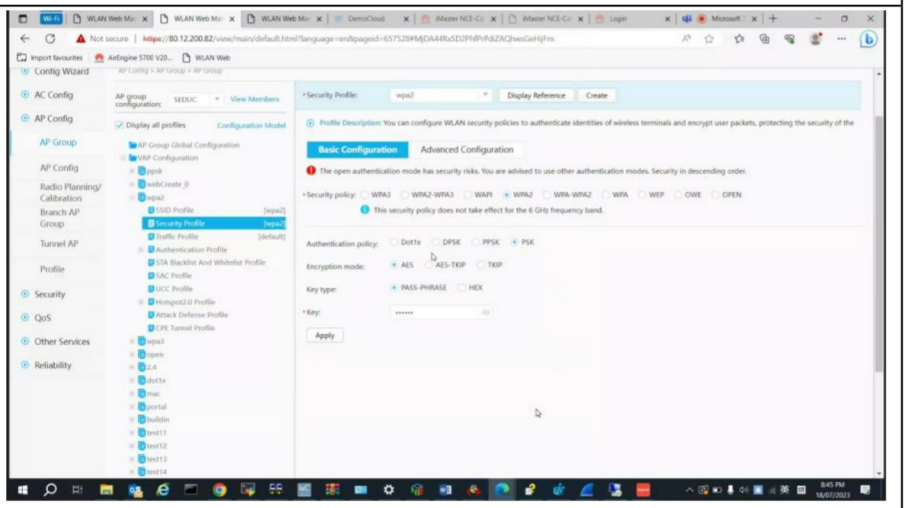
Autenticação WPA2

5.6.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

5.7.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

Item de teste	Políticas de segurança da rede WLAN (WPA2)
Objetivo do teste	Validar que o sistema WLAN suporta políticas de segurança (WEP/WPA/WPA2)
Configuração de teste	Topologia da rede:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	 Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configuração de SSID, com a politica de segurança definida para WPA2.
Resultado esperado	1) Divulgação de SSID onde a política de segurança com WPA2, foi configurada. 2) Associação de dispositivo ao SSID criado
Resultado	 Figura 1 – Na AC, foi criado um VAP Configuration com o nome “wpa2”. Os VAP Configurations, agregam todos os parametros de configuração, considerados pela AC, ao propagar um SSID. Neste utilizado no teste, foi configurado o perfil de segurança com o perfil de segurança utilizando WPA2, com criptografia AES e uma senha padrão (PASS-PHRASE)

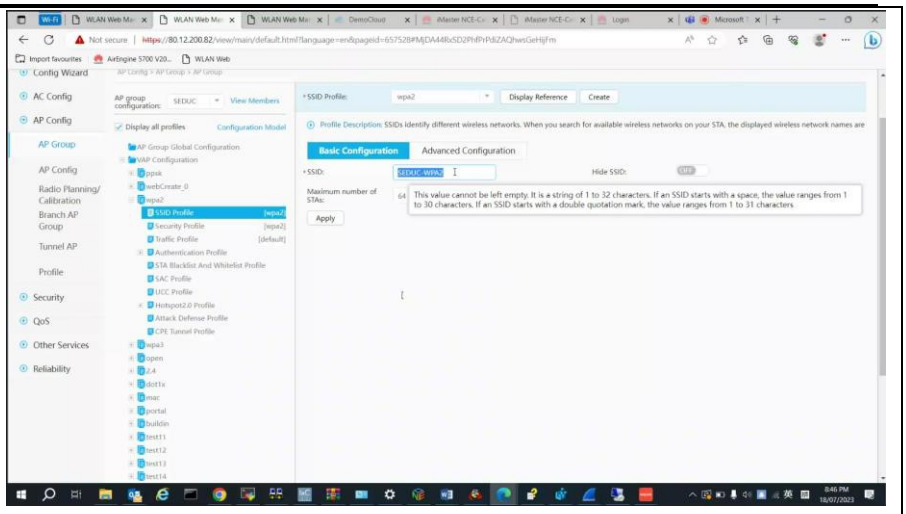
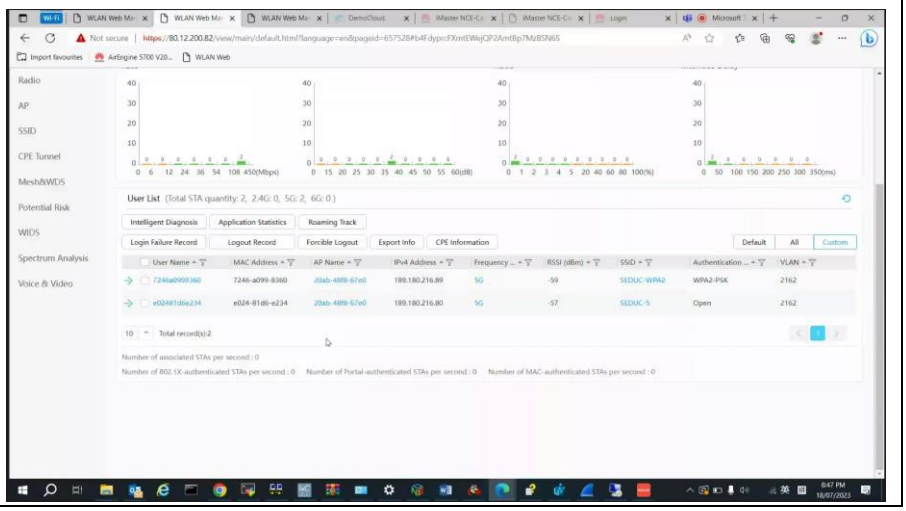
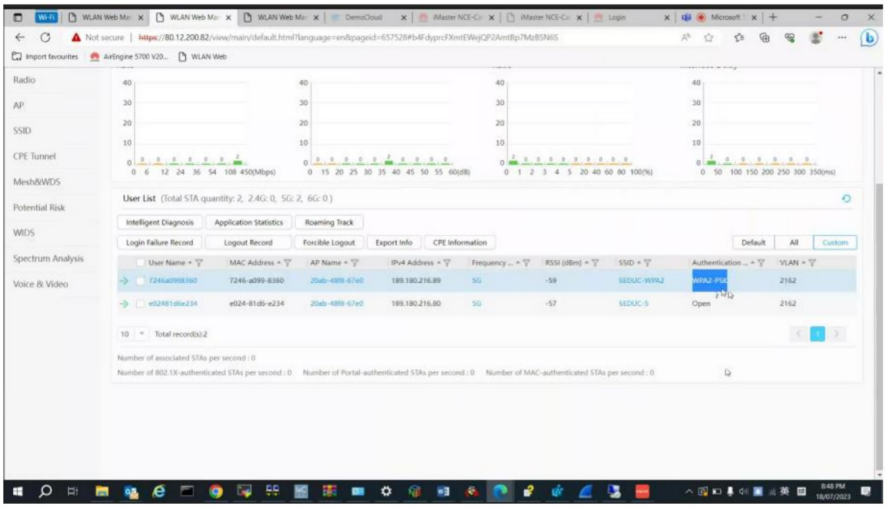


Figura 2 – Ainda no VAP Configuration de nome “wpa2”, criamos um SSID com o nome SEDUC-WPA2.



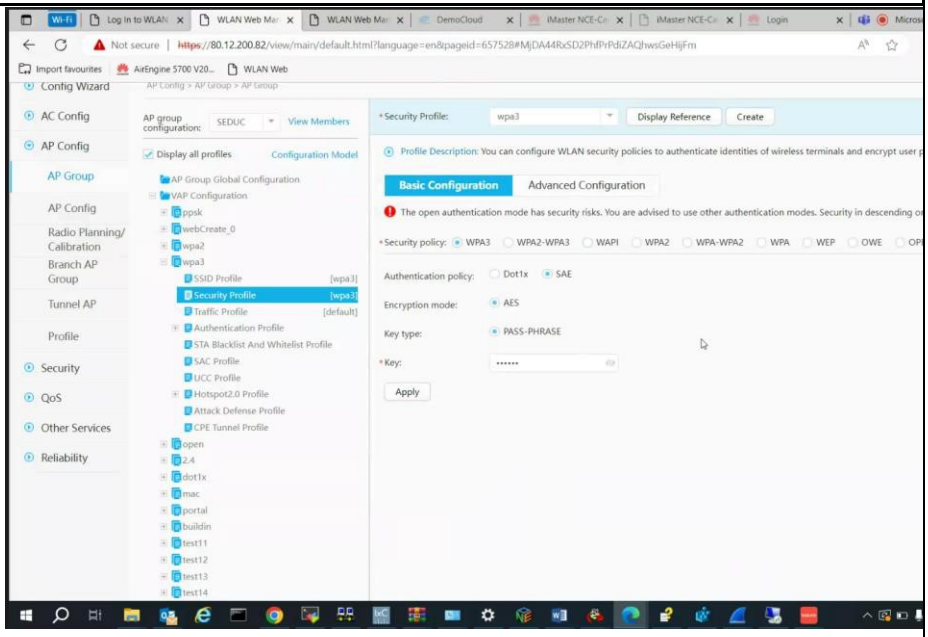
	 Figura 3 e 4 – Na listagem de dispositivos conectados (User list), podemos verificar um dispositivo associado ao SSID SEDUC-WPA2, e que o metodo de autenticação utiliado foi WPA2-PSK.

Autenticação WPA3-SAE

5.6.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

5.7.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

Item de teste	Políticas de segurança da rede WLAN (WPA3)
Objetivo do teste	Validar que o Sistema WLAN suporta autenticação WPA3-SAE
Configuração de teste	Topologia da rede: 

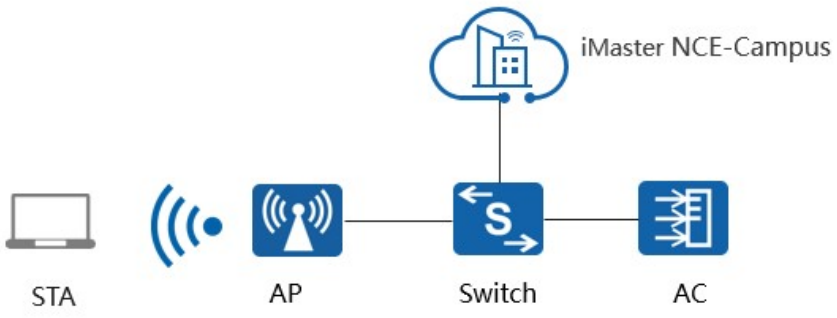
	Condições iniciais: 1) Todos os dispositivos estão funcionando normalmente. 2) Montar o ambiente de teste de acordo com a topologia acima. 3) O dispositivo cliente (STA) suporta autenticação WPA3-SAE.
Procedimento de teste	1) Configuração de SSID, com a política de segurança definida para WP3-SAE.
Resultado esperado	1) Configuração de SSID onde a política de segurança com WPA3-SAE.
Resultado	 Figura 1 – Complementando o teste anterior, também foi criado um VAP Configuration, de nome “wpa3”, onde o perfil de segurança utilizado foi o WPA3, com a politica de autenticação SAE, criptografia AES e uma senha de acesso (PASS-PHRASE).

Autenticação 802.1x

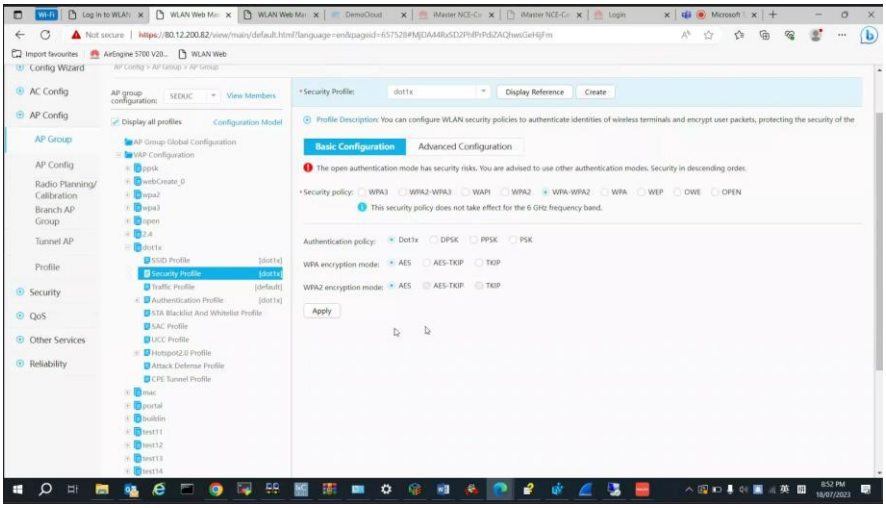
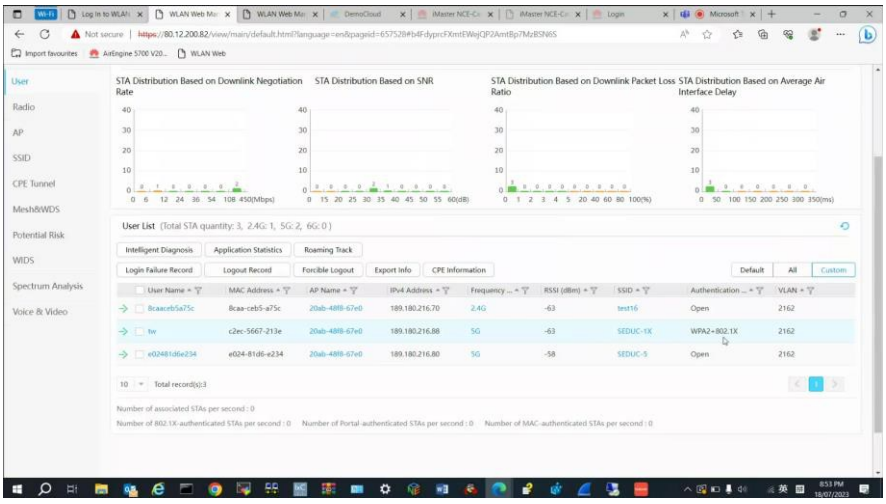
5.6.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

5.7.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

5.10.26 Implantar autenticação de dispositivos e usuários via 802.1x, Web Portal e endereço MAC na rede sem fio;

Item de teste	Políticas de segurança da rede WLAN (802.1x)
Objetivo do teste	Validar que o Sistema WLAN suporta Autenticação 802.1x
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configuração de SSID, com a política de segurança definida para Dot1x (802.1x). 2) Autenticar usuários através de 802.1x
Resultado esperado	1) Configuração de SSID onde a política de segurança é 802.1x e autenticar usuários.

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Resultado	 Figura 1 – Complementando o teste anterior, também foi criado um VAP Configuration, de nome “dot1x”, onde o perfil de segurança utilizado foi o WPA-WPA2, com a politica de autenticação Dot1x (802.1x) e criptografia AES.  Figura 2 – Foi evidenciado, na listagem de usuários conectados, o usuário “tw”, autenticado via 802.1x pelo SSID SEDUC-1X.

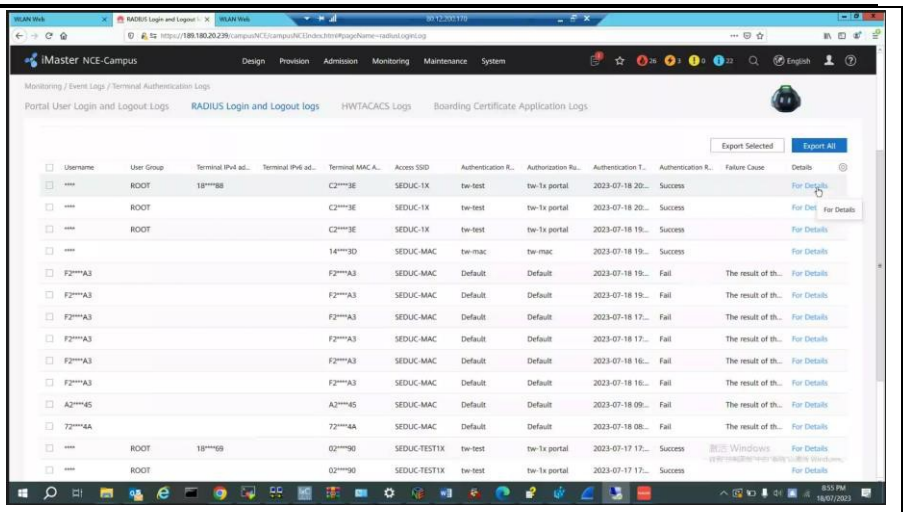


Figura 3 – Na plataforma iMaster NCE Campus, também é listado a autenticação com sucesso no SSID SEDUC-1X.

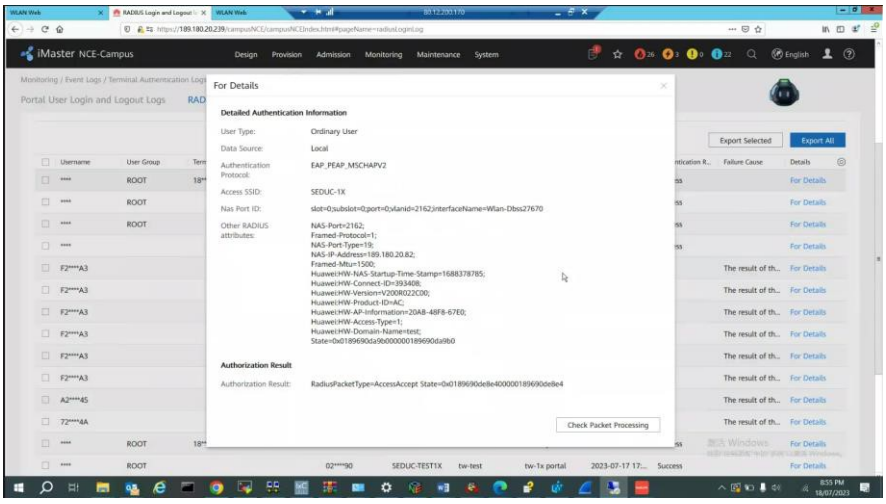
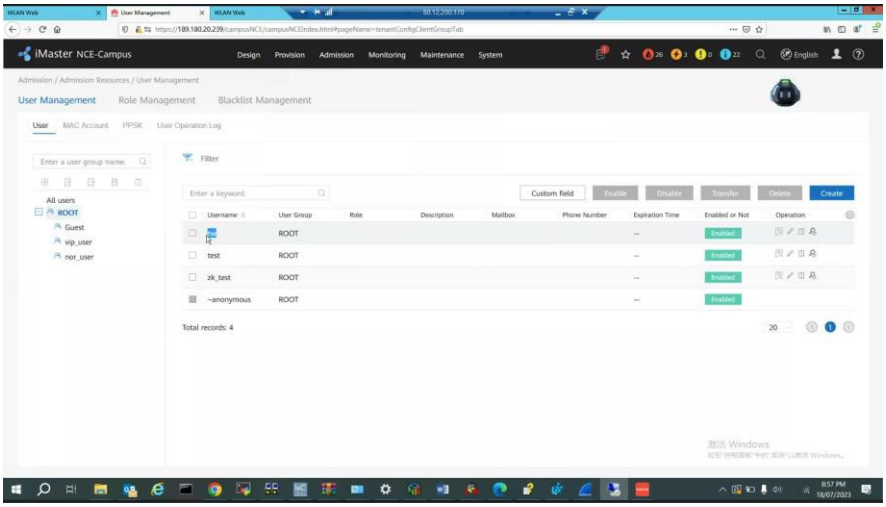
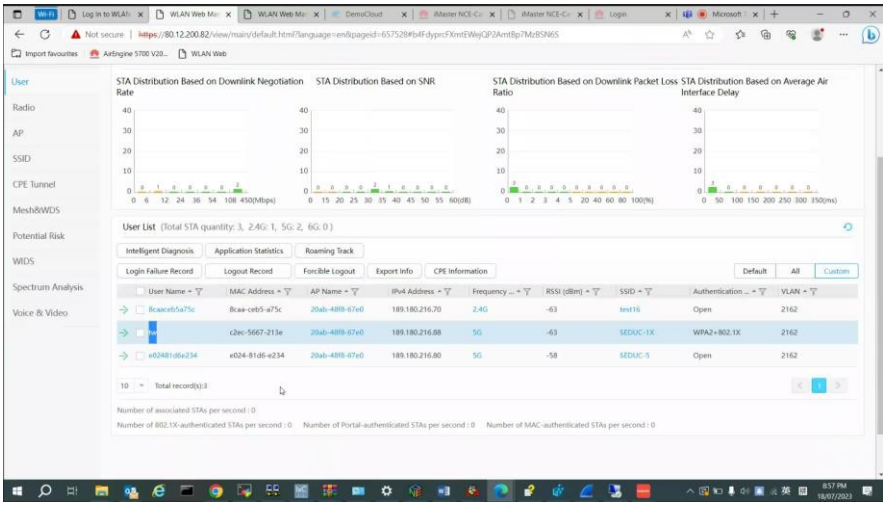


Figura 4 – Também foi evidenciado os logs do protocolo RADIUS, dentro da plataforma iMaster NCE, mostrando todo o processo de autenticação realizado com sucesso.



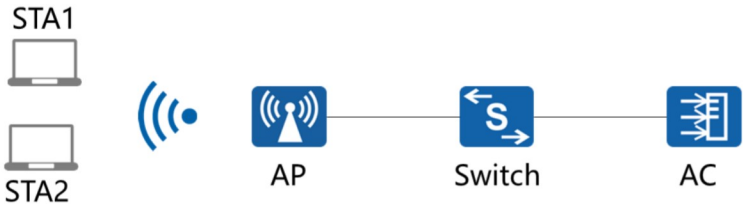


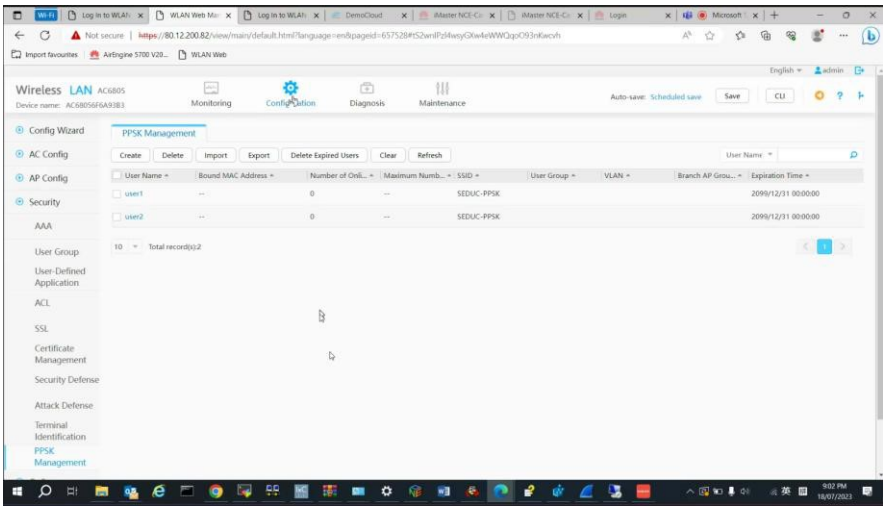
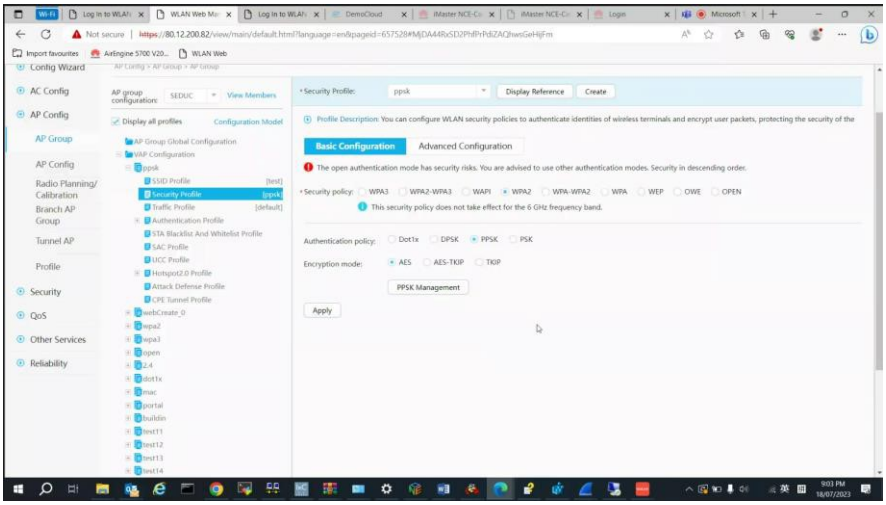
Figuras 5 e 6 – Por ultimo, finalizando o teste, foi evidenciado o mesmo usuário “tw”, utilizado para a autenticação, na base de dados da plataforma iMaster NCE Campus, e na listagem de usuários conectados da controladora.

Autenticação WPA/WPA2-PPSK

5.6.6 Implementar chave de compartilhada exclusiva (Exemplo: PPSK, Identity PSK, ePSK, MPSK, DPSK ou similar do fabricante)

5.7.6 Implementar chave de compartilhada exclusiva (Exemplo: PPSK, Identity PSK, ePSK, MPSK, DPSK ou similar do fabricante)

Item de teste	Autenticação WPA/WPA2-PPSK
Objetivo do teste	Validar que o Sistema WLAN suporta Autenticação WPA/WPA2-PPSK
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configuração de SSID, com a política de segurança definida para WPA2-PPSK. 2) Autenticar usuários através de WPA2-PPSK
Resultado esperado	1) Configuração de SSID onde a política de segurança é WPA2-PPSK e auenticar usuários.

Resultado	 Figura 1 – Na controladora, foram criados dois usuários com diferentes PPSK (Private Pre-Shared Key), que são chaves de acesso privadas ou individuais.  Figura 2 – Em seguida, também foi criado um VAP Configuration, de nome “ppsk”, onde o perfil de segurança utilizado foi o WPA2, com a politica de autenticação PPSK e criptografia AES.

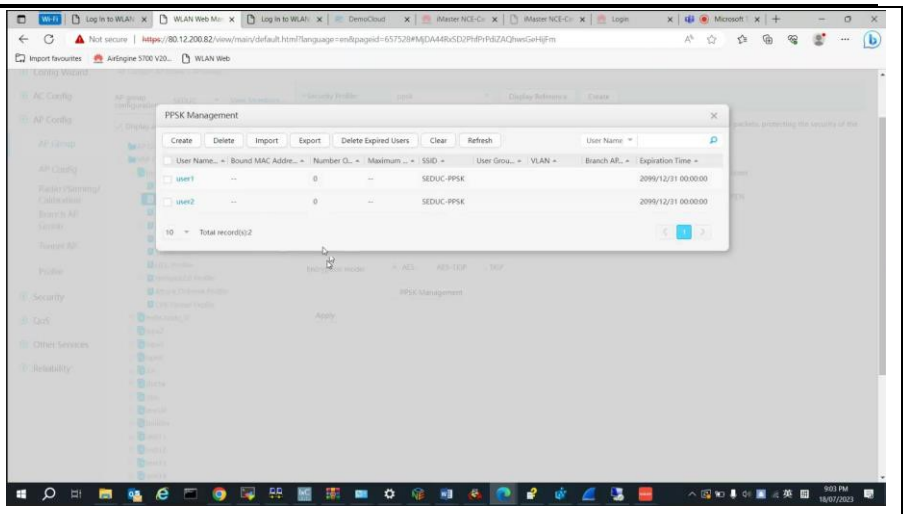


Figura 3 – Nesta mesma tela de configuração, também foi evidenciado o gerenciamento dos usuários e senhas tipo PPSK.

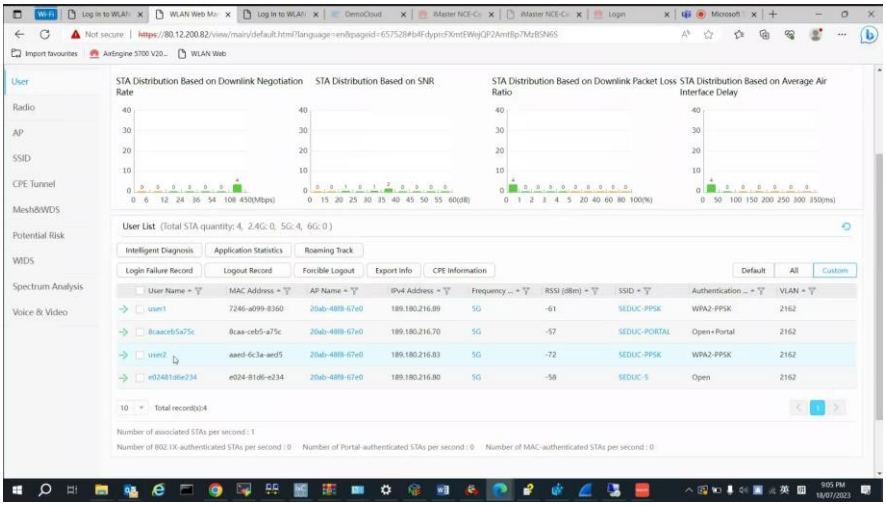


Figura 4 – Na listagem de dispositivos conectados, temos os dois usuários criados com a politica PPSK, associados ao SSID SEDUC-PPSK.

Radio

Fluxo 2.4Ghz e 5Ghz

5.6.7.1 Fluxo 2.4Ghz e 5Ghz: no mínimo 2x2

5.6.7.4 Implementar funcionamento simultâneo em 2,4GHz e 5GHz;

5.7.7.1 Fluxo 5Ghz: 4x4
5.7.7.4 Implementar funcionamento simultâneo em 2,4GHz e 5GHz;

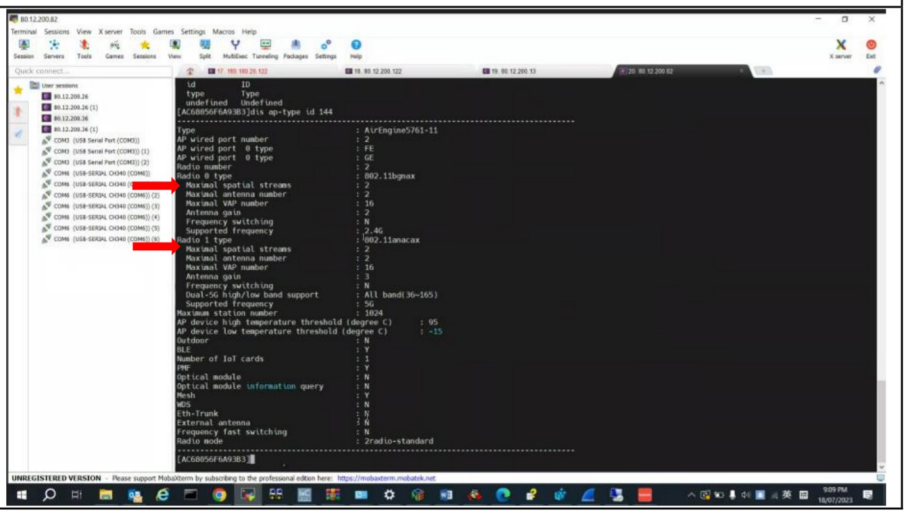
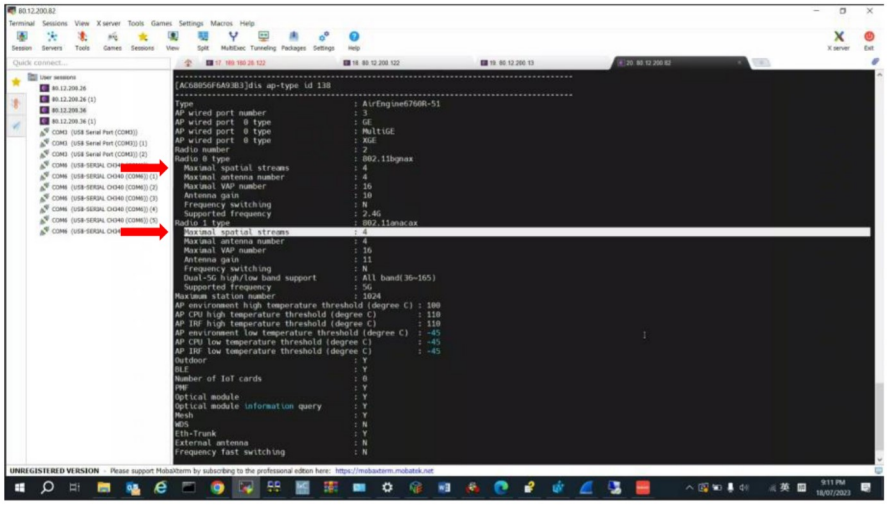
Item de teste	**Fluxo 2.4Ghz e 5Ghz**
Objetivo do teste	Validar que o AP 5761-11 tenha fluxo nas frequências 2.4Ghz e 5Ghz: pelo menos 2x2; 6760R-51 tenha fluxo na frequência 5Ghz em 4x4
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Verifique os spatial streams no AP.
Resultado esperado	1) AP está online; 5761-11 tem fluxos nas frequências 2.4Ghz e 5Ghz em pelo menos 2x2; 6760r-51 tem fluxo na frequência 5Ghz em 4x4
Resultado	

	Figura 1 – Via CLI, foi listada todas as informações do AP modelo AirEngine 5761-11. Nestas informações, é possível checar a quantidade de spatial streams suportada por rádio.  Figura 2 – Via CLI, foi listada todas as informações do AP modelo AirEngine 6760R-51. Nestas informações, é possível checar a quantidade de spatial streams suportada por rádio.

Maximum access user | Máximo de usuários simultâneos

Item de teste	**Máximo de usuários simultâneos**
Objetivo do teste	Validar que o access point sem fio suporta pelo menos 512 clientes por unidade de AP.
Configuração de teste	Topologia da rede:  Condições iniciais:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

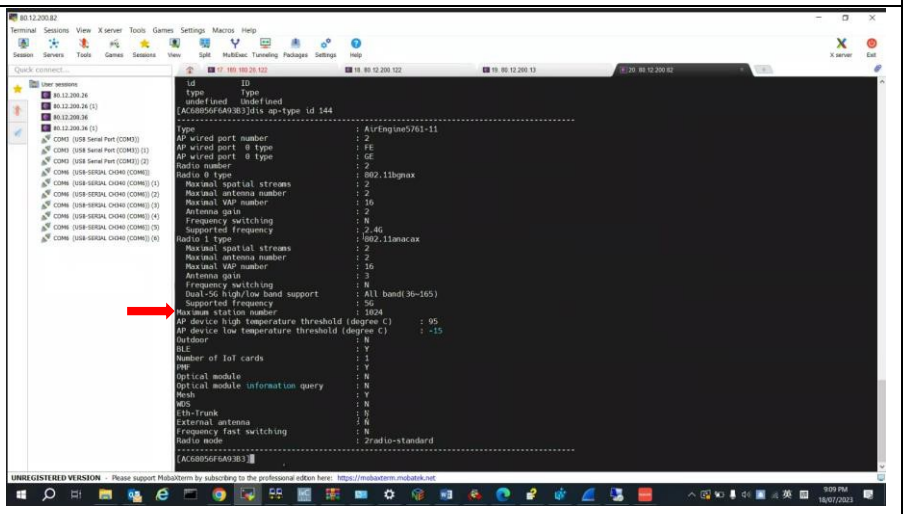
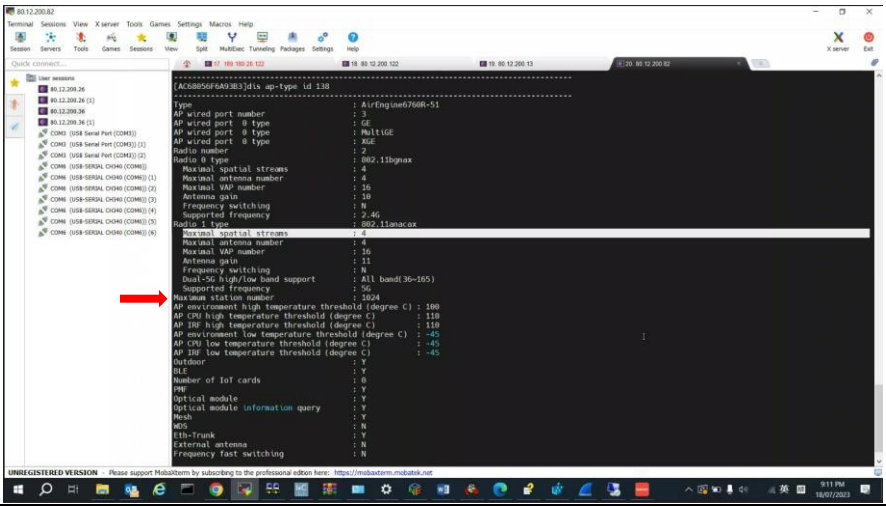
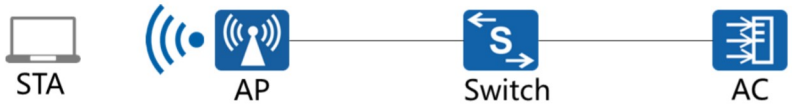
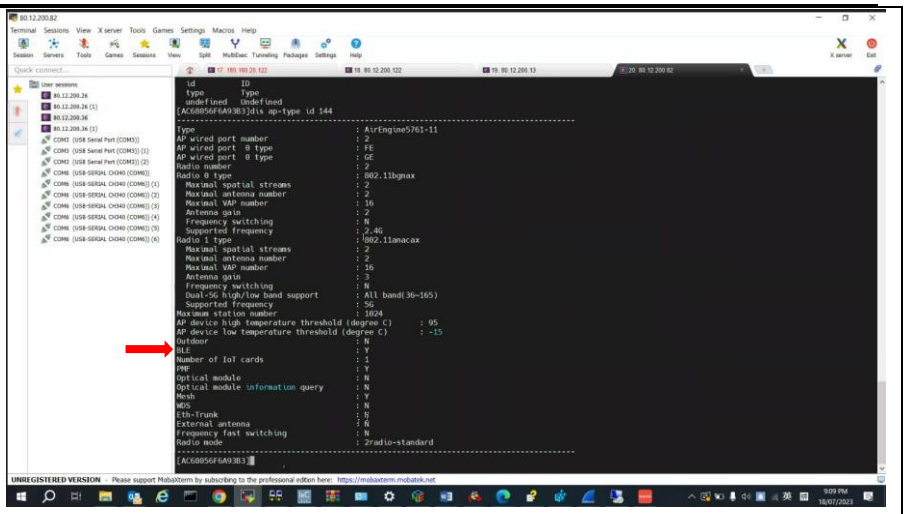
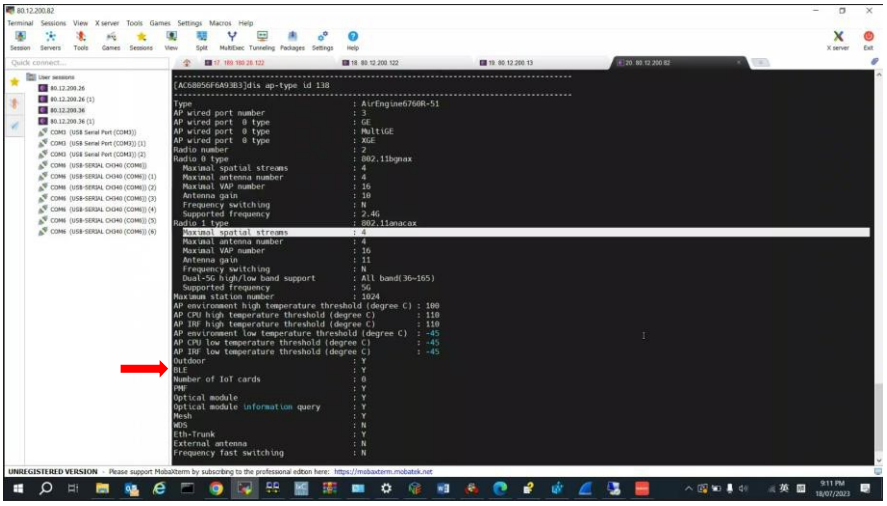
	1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Verifique a quantidade máxima de terminais suportados por AP.
Resultado esperado	2) O AP mostra a informação que suporta mais de 512 terminais.
Resultado	 Figura 1 – Via CLI, foi listada todas as informações do AP modelo AirEngine 5761-11. Nestas informações, é possível checar a quantidade de terminais suportados (station number). 

	Figura 2 – Via CLI, foi listada todas as informações do AP modelo AirEngine 6760R-51. Nestas informações, é possível checar a quantidade de terminais suportados (station number).

Bluetooth Low-Energy (BLE) radio | Rádio Bluetooth de baixo consumo energético (BLE)

Item de teste	**Bluetooth Low-Energy (BLE) radio | Rádio Bluetooth de baixo consumo energético**
Objetivo do teste	**Validar que o a access point sem fio suporte rádio Bluetooth de baixo consumo energético (BLE)**
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Verifique o suporte a BLE.
Resultado esperado	1) O AP mostra a informação que suporta radio do tipo Bluetooth Low-Energy.

Resultado	 Figura 1 – Via CLI, foi listada todas as informações do AP modelo AirEngine 5761-11. Nestas informações, é possível checar o suporte a tecnologia BLE.  Figura 2 – Via CLI, foi listada todas as informações do AP modelo AirEngine 6760R-51. Nestas informações, é possível checar o suporte a tecnologia BLE.

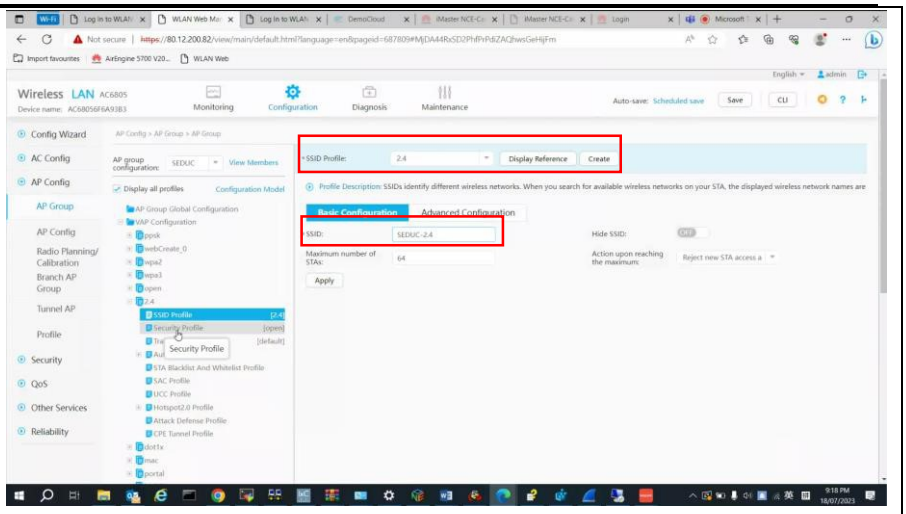
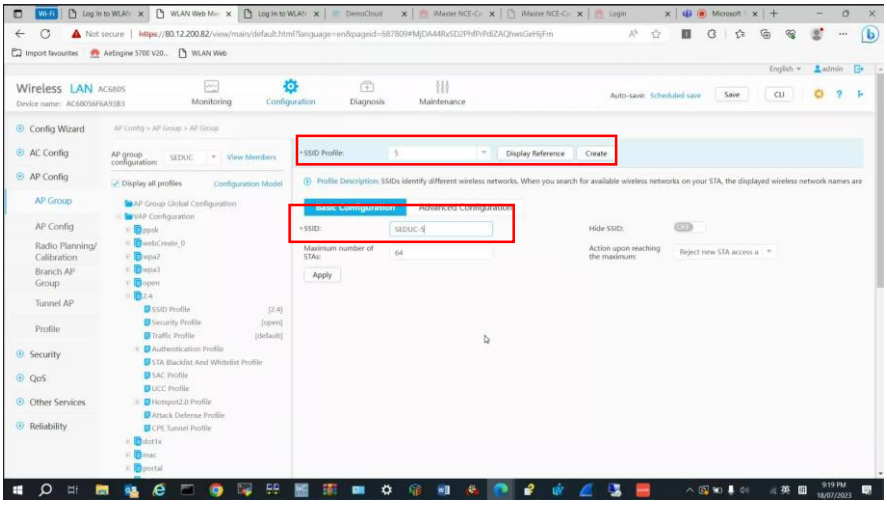
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

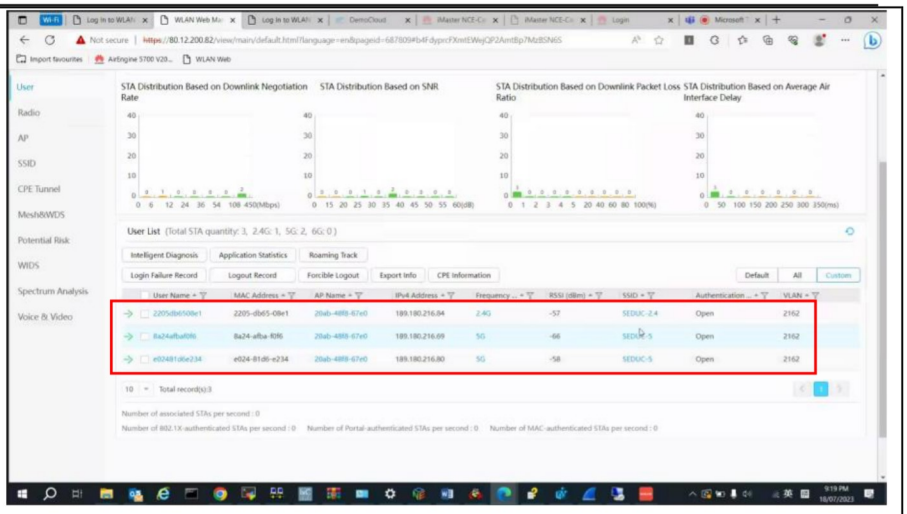
Funcionamento simultâneo em 2.4GHz e 5GHz;

5.6.7.4 Implementar funcionamento simultâneo em 2,4GHz e 5GHz;

5.7.7.4 Implementar funcionamento simultâneo em 2,4GHz e 5GHz;

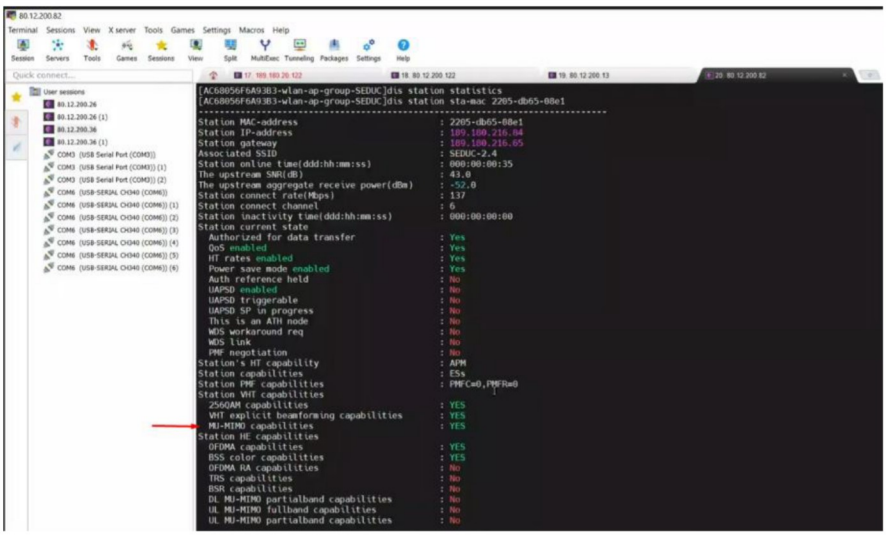
Item de teste	**Funcionamento simultâneo em 2.4GHz e 5GHz;**
Objetivo do teste	**Validar que o Sistema WLAN suporta funcionamento simultâneo em 2,4GHz e 5GHz**
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure ac corretamente, para que o AP propague dois SSIDs. Sendo um no rádio de 2.4GHz, e outro, no rádio de 5 GHz. 2) Conecte o os dispositivos em cada SSID.
Resultado esperado	1) Os SSIDs “SEDUC-2.4” no rádio de 2.4GHz e ”SEDUC-5” no rádio de 5 GHz podem ser descobertos nos dispositivos clientes (STAs); 2) Os dispositivos clientes (STAs) conectam-se SSIDs respectivamente

Resultado	 Figura 1 – Na controladora, foi configurado um VAP Configuration onde o perfil de SSID foi selecionado para operar apenas em banda 2.4GHz. O nome do SSID, é SEDUC-2.4  Figura 2 – Na controladora, foi configurado um VAP Configuration onde o perfil de SSID foi selecionado para operar apenas em banda 5GHz. O nome do SSID, é SEDUC-5

	 Figura 3 – Na listagem de usuários associados, foi possível atestar que existem dispositivos conectados ao mesmo AP (checar o MAC ADDRESS), nos dois SSIDs criados, e suas respectivas frequências.

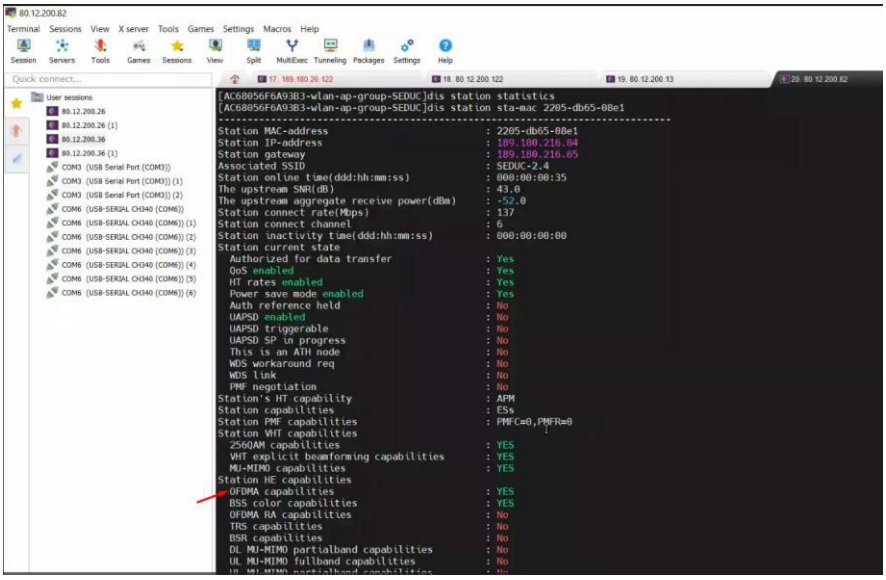
Suporte MU-MIMO

Item de teste	Teste de suporte a MU-MIMO
Objetivo do teste	Valiadar o suporte a MU-MIMO
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos clientes devem suportar 802.11ax 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure a AC corretamente, e propague associe um dispositivo ao SSID.

Resultado esperado	1) Listar as informações do dispositivo associado ao SSID
Resultado	 Figura 1 – Via CLI, foi listada através do comando “display station sta-mac 2205-db-65-08e1”, todas as informações de um dispositivo conectado ao SSID SEDUC-2.4, criado no procedimento anterior. Na saída deste comando é possível atestar o suporte a tecnologia MU-MIMO.

OFDMA

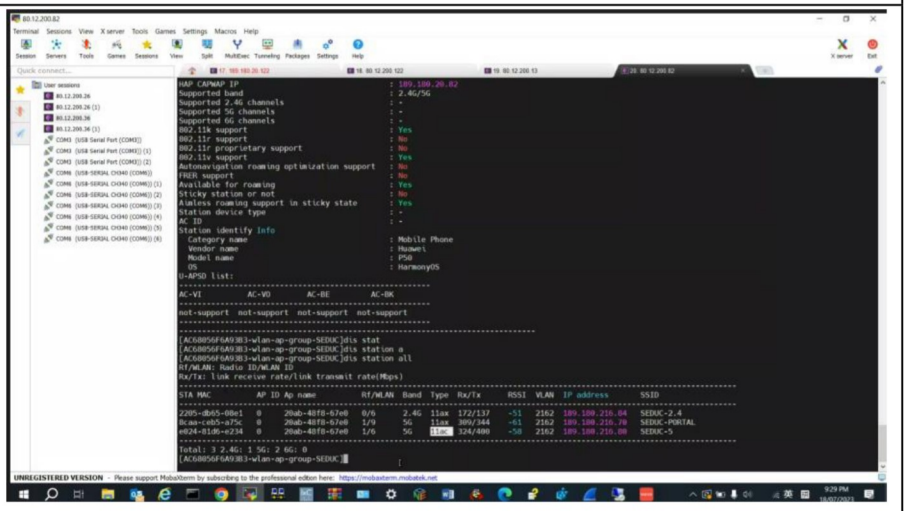
Item de teste	Teste de suporte a OFMDA
Objetivo do teste	Validar o suporte a OFDMA
Configuração de teste	Topologia da rede:  Condições iniciais:

	3) Todos os dispositivos clientes devem suportar 802.11ax 4) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure a AC corretamente, e propague associe um dispositivo ao SSID.
Resultado esperado	2) Listar as informações do dispositivo associado ao SSID
Resultado	 Figura 1 – Via CLI, foi listada através do comando “display station sta-mac 2205-db-65-08e1”, todas as informações de um dispositivo conectado ao SSID SEDUC-2.4, criado no procedimento anterior. Na saída deste comando é possível atestar o suporte a tecnologia OFDMA.

802.11a/b/g/n/ac/ax múltiplos padrões de radio.

Item de teste	802.11a/b/g/n/ac/ax múltiplos padrões de radio.

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Objetivo do teste	Validar que o Sistema WLAN suporta os padrões 802.11a/b/g/n/ac/ax
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure a AC corretamente, e propague associe um dispositivo ao SSID.
Resultado esperado	1) Listar as informações do dispositivo associado ao SSID
Resultado	 Figura 1 – Via CLI, foi listada através do comando “display station station all”, todas as informações de um dispositivo conectados. Dentre essas informações, é listado o padrão 802.11 suportado.

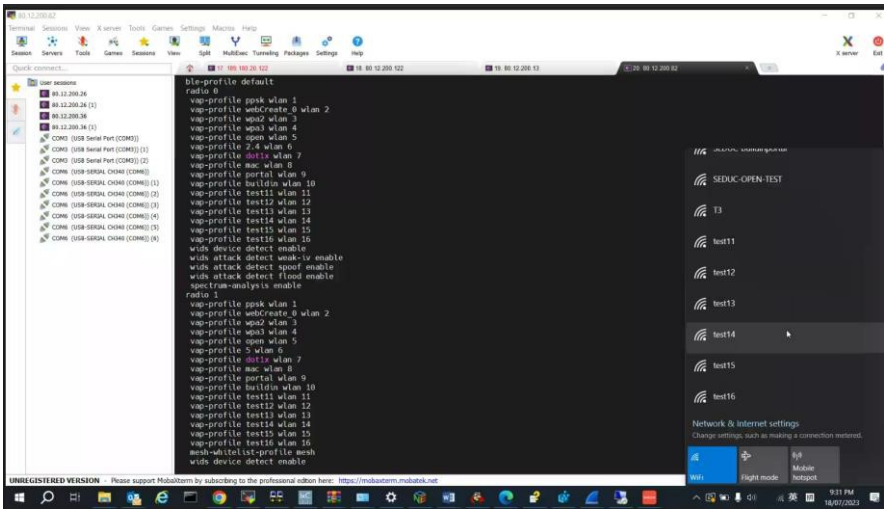
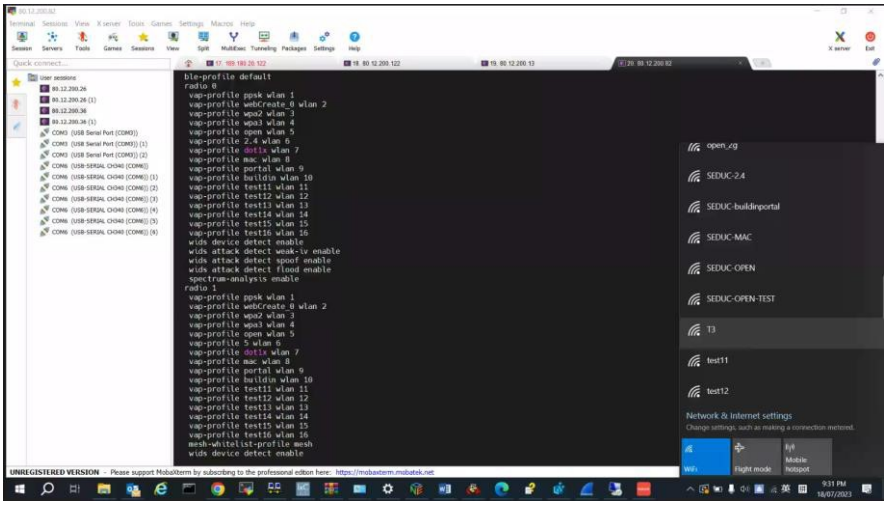
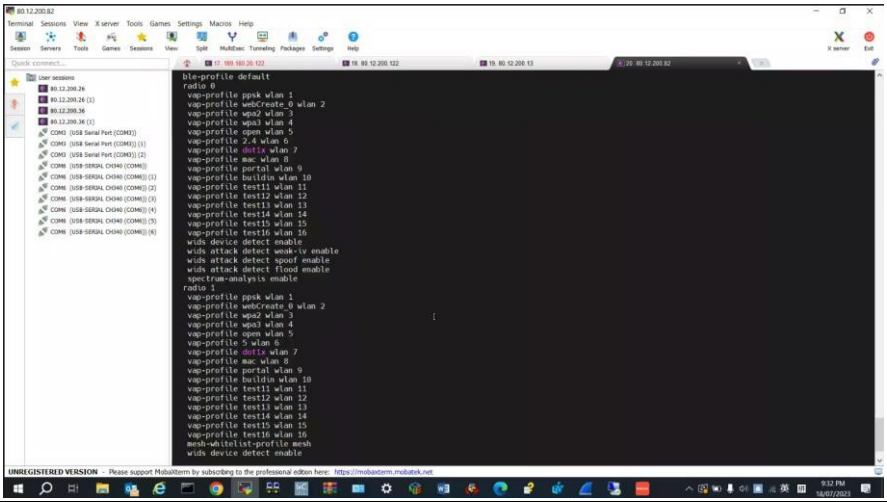
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

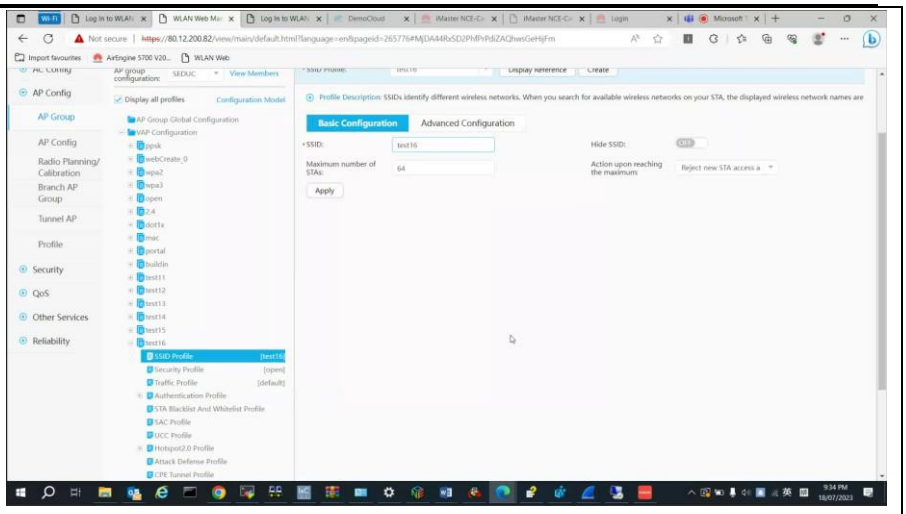
Multiplas SSIDs

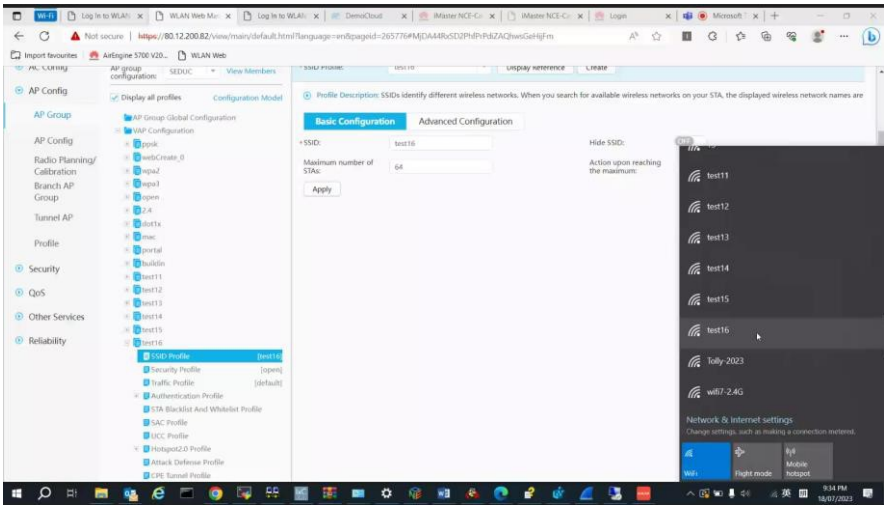
5.6.7.8 Capacidade de implementar no mínimo 16 SSID;

Item de teste	Multi-SSIDs
Objetivo do teste	Validar que o Sistema WLAN suporta pelo menos 16 SSIDs
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configurar corretamente a AC e propagar 16 SSIDs diferentes através dos pontos de acesso.
Resultado esperado	1) Os 16 sinais diferentes podem ser detectados.

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Resultado	  



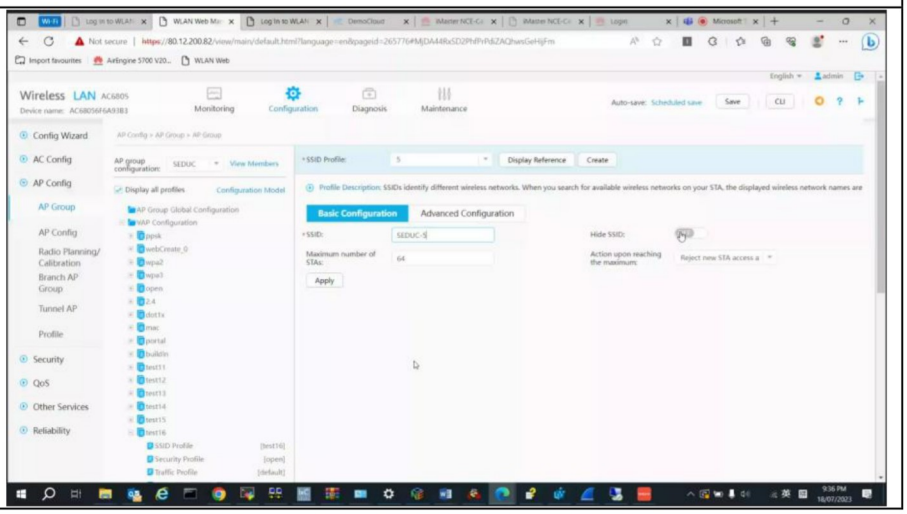


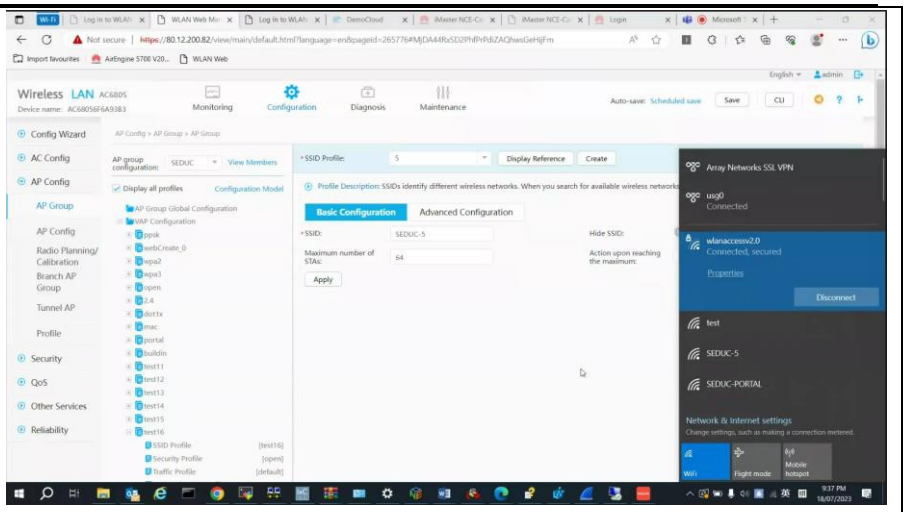
Figuras 1, 2, 3, 4 e 5 – Listagem via CLI, WEB e através do laptop utilizado no teste, dos 16 SSIDs configurados e disponiveis.

SSID oculto

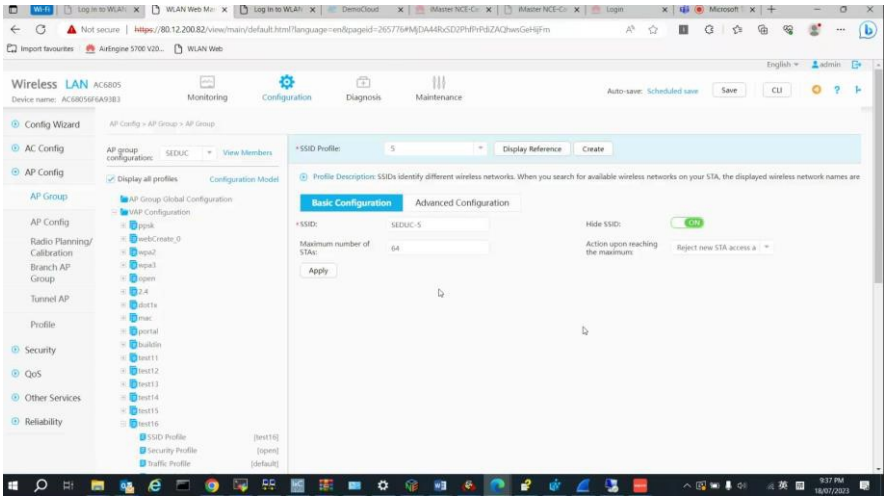
5.6.7.9 Deve permitir habilitar e desabilitar a divulgação do SSID;

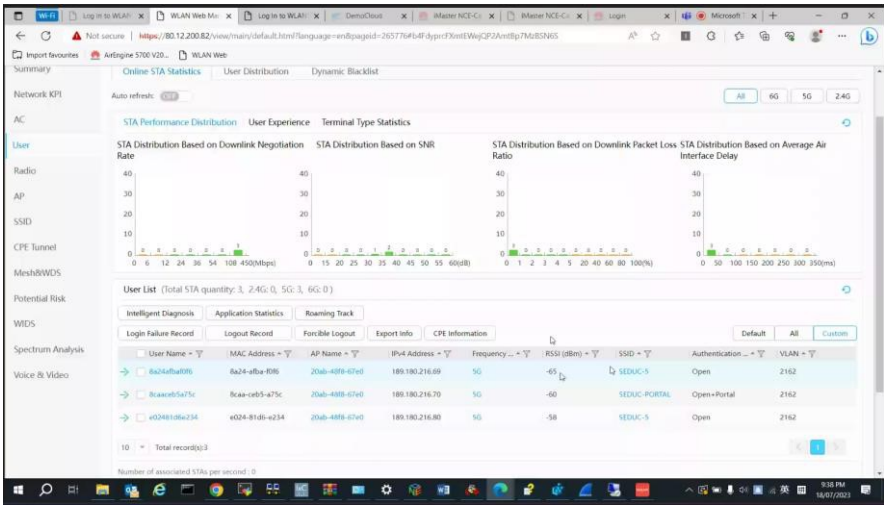
5.7.7.9 Deve permitir habilitar e desabilitar a divulgação do SSID;

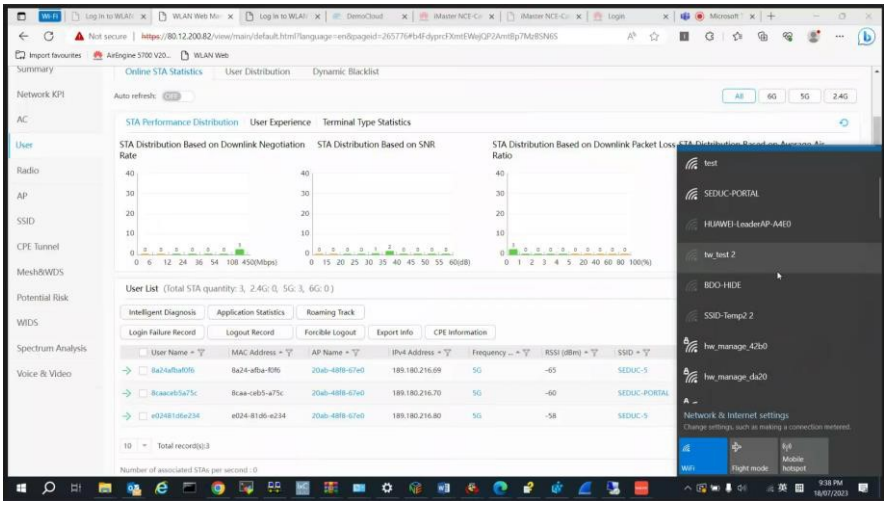
Item de teste	SSID oculto
Objetivo do teste	Validar que o Sistema WLAN suporta SSID função oculto.
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configurar corretamente a AC para propagar um SSID oculto através dos pontos de acesso 2) Desabilitar a propagação de SSID
Resultado esperado	1) O SSID oculto pode ser descoberto pelo STA; 2) Após desabilitar os radios, os SSIDs não serão mais detectados
Resultado	



Figuras 1 e 2 – O SSID SEDUC-5, configurado e sendo propagado e detectado pelo laptop.







Figuras 3, 4 e 5 – Foi selecionada a opção “Hide SSID”, e o o laptop parou de detectar o SSID.

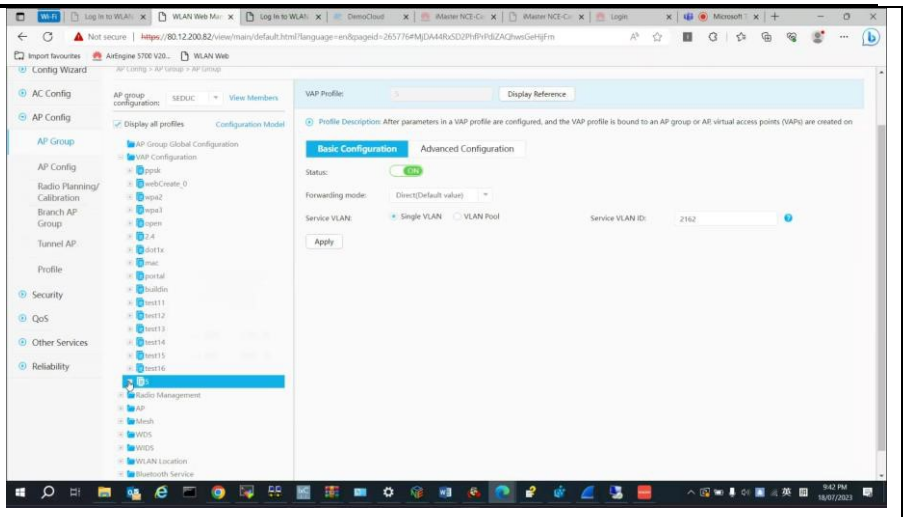


Figura 6 – Ainda nas configurações, é possivel selecionar a opção "Status", onde quando o status é "ON", os radios estão em operação, e "OFF", os radios estão desligados.

Calibração automática de rádios - Alocação dinâmica de canais e ajuste de potência DCA &TPC

5.6.7.10 Deve possuir capacidade de selecionar automaticamente o canal de transmissão;

5.6.7.11 Deve permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF (rádio frequência) conforme as características do ambiente, evitando intervenção manual;

5.7.7.10 Deve possuir capacidade de selecionar automaticamente o canal de transmissão;

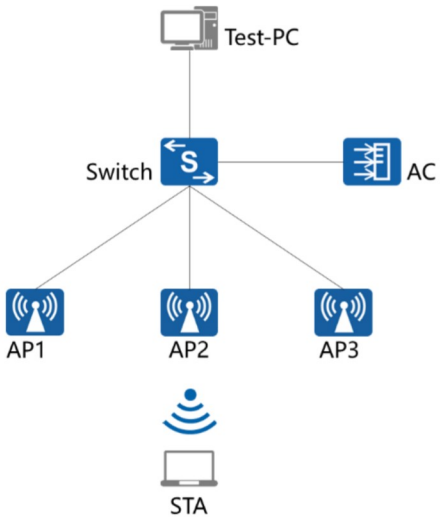
5.7.7.11 Deve permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF (rádio frequência) conforme as características do ambiente, evitando intervenção manual;

5.10.19 Na ocorrência de inoperância de um Ponto de Acesso, a solução deverá ajustar

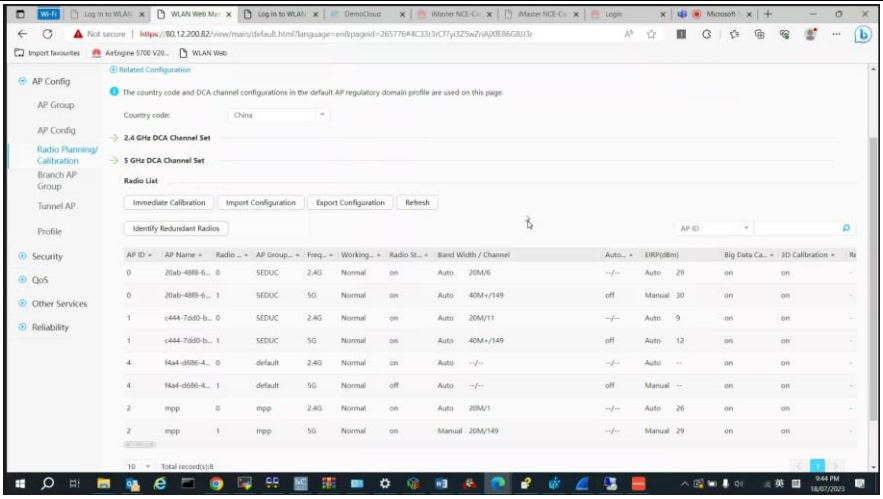
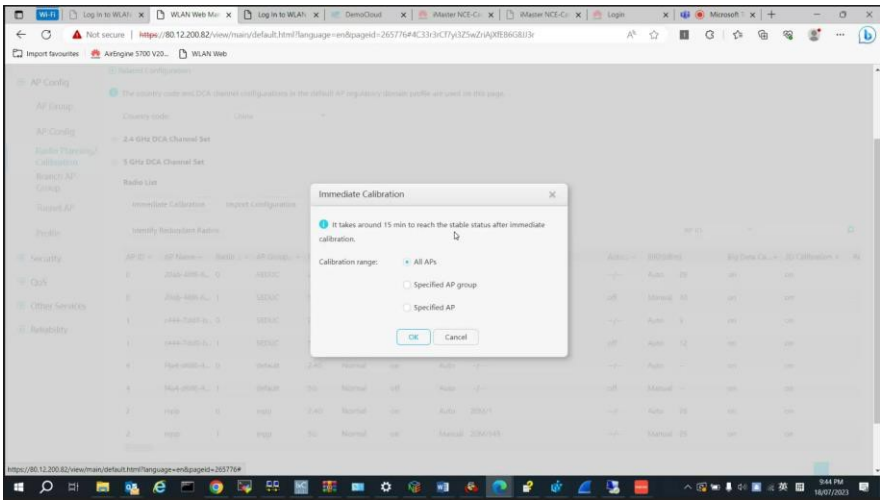
automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;

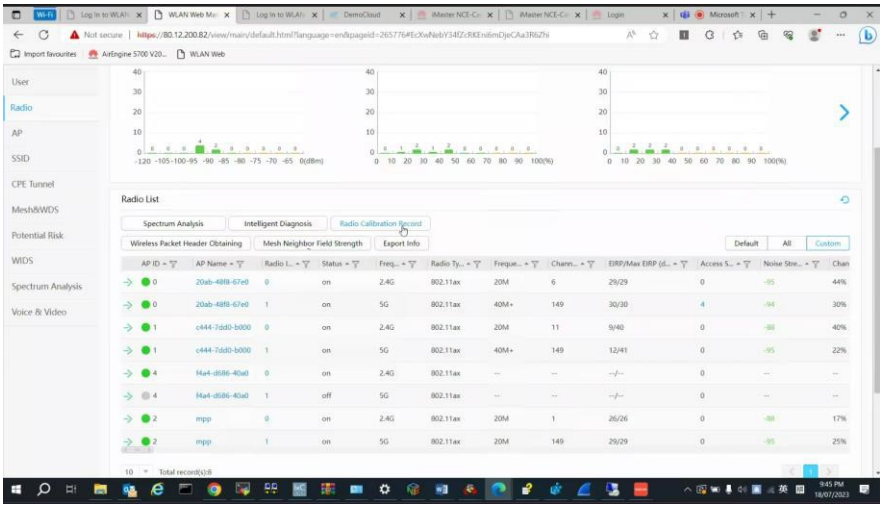
5.10.20 Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede de acordo com as condições de RF;

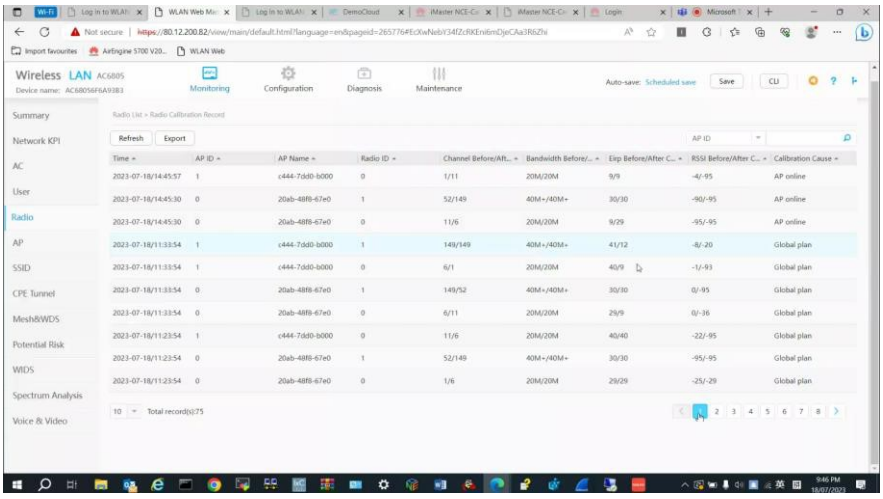
5.10.21 Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática;

Item de teste	Calibração de Rádio
Objetivo do teste	Validar que o Sistema WLAN suporta calibração de rádio
Teste environment	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure a AC corretamente 2) Habilite a função Radio Calibration;

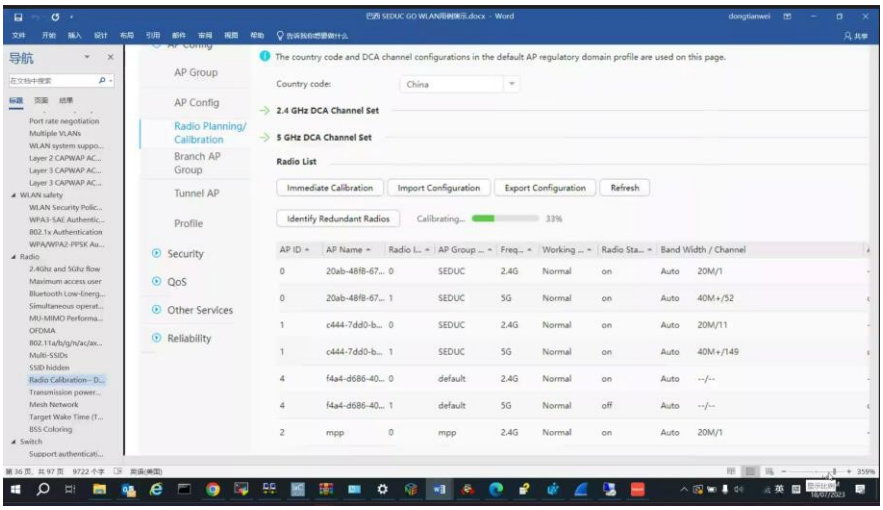
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Resultado esperado	1) Registrar informações de rádio sobre todos os APs; 2) O canal AP e a potência de trânsito foram ajustados de forma dinâmica.
Resultado	 





Figuras 1, 2, 3 e 4 – Na controladora, na opção “Radio Planning/Calibration”, foi mostrado todo o detalhamento da rede com os ajustes dinâmicos realizados. As colunas mostram o antes e depois de cada ajuste, considerando canal, largura de banda, potência, sensibilidade e etc.

	 Figura 5 – Conforme indicado durante a sessão, a calibração não foi feita no momento do teste, para que não houvesse intermitência no ambiente da homologação. A imagem mostra o momento exato que esse teste foi realizado pelo time técnico, e como é seu procedimento.

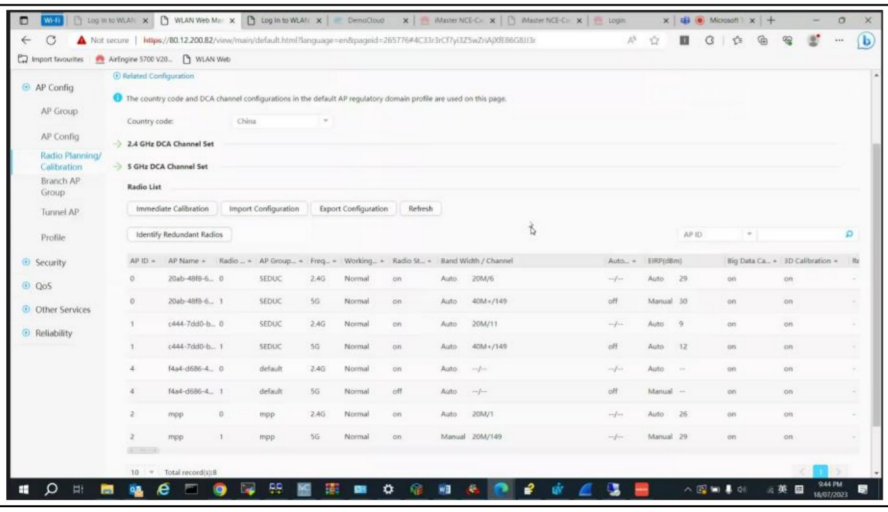
Alteração da potência de transmissão

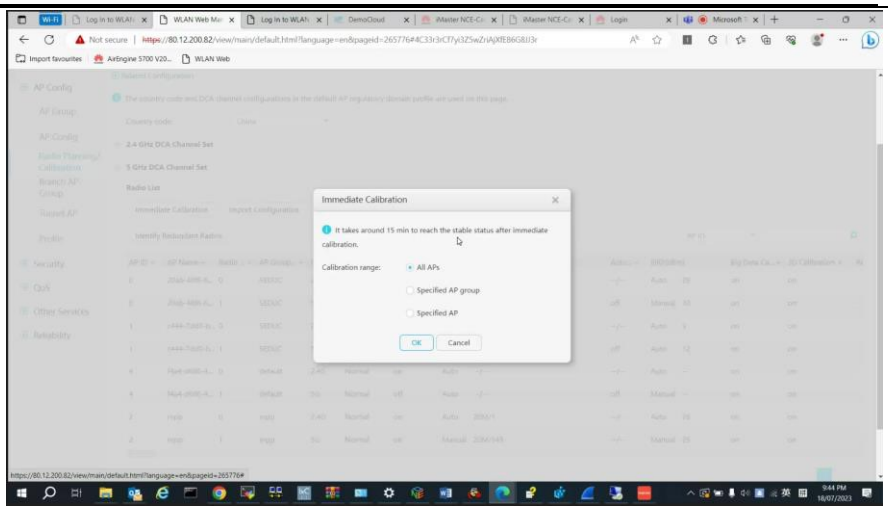
5.6.7.11 Deve permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF (rádio frequência) conforme as características do ambiente, evitando intervenção manual;

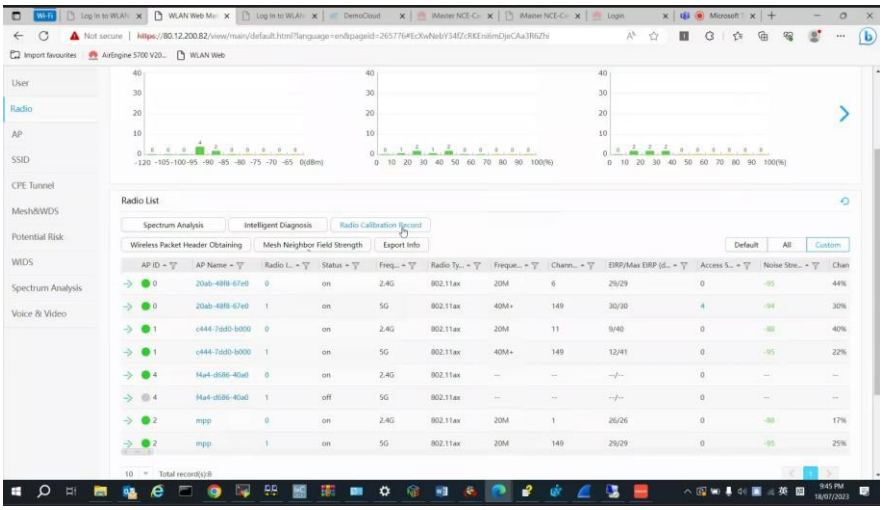
5.7.7.11 Deve permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF (rádio frequência) conforme as características do ambiente, evitando intervenção manual;

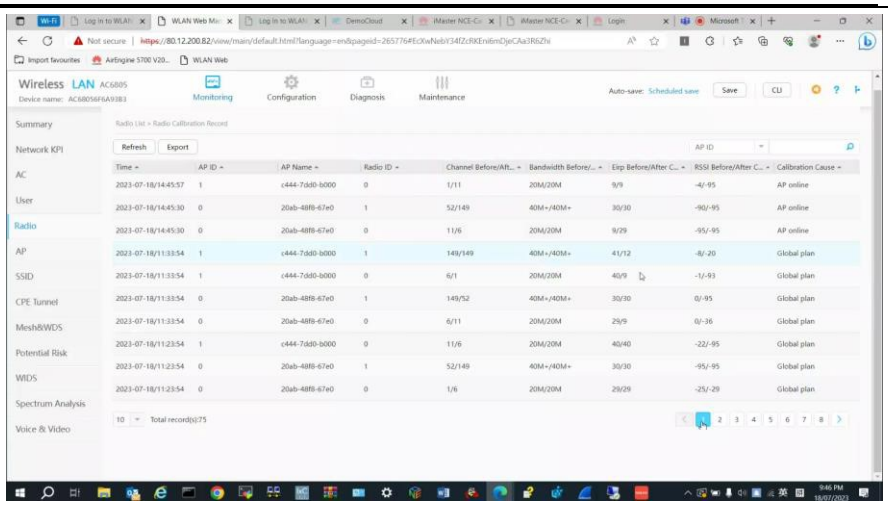
Item de teste	Alteração da potência de transmissão

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Objetivo do teste	Validar se a potência de transmissão do AP pode ser modificada e se o intervalo de potência está dentro da legislação local.
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure a AC corretamente 2) Habilite a função Radio Calibration;
Resultado esperado	1) Registrar informações de rádio sobre todos os APs; 2) O canal AP e a potência de trânsito foram ajustados de forma dinâmica.
Resultado	


Immediate Calibration
It takes around 15 min to reach the stable status after immediate calibration.
Calibration range:
All APs
Specified AP group
Specified AP
OK
Cancel


User
Radio
AP
SSID
CPE Tunnel
Mesh&WDS
Potential Risk
WIDS
Spectrum Analysis
Voice & Video
Radio List
Spectrum Analysis
Intelligent Diagnosis
Radio Calibration Record
Wireless Packet Header Obtaining
Mesh Neighbor Field Strength
Export Info
Default
All
Custom



Figuras 1, 2, 3 e 4 – Na controladora, na opção “Radio Planning/Calibration”, foi mostrado todo o detalhamento da rede com os ajustes dinâmicos realizados. As colunas mostram o antes e depois de cada ajuste, considerando canal, largura de banda, potência, sensibilidade e etc.

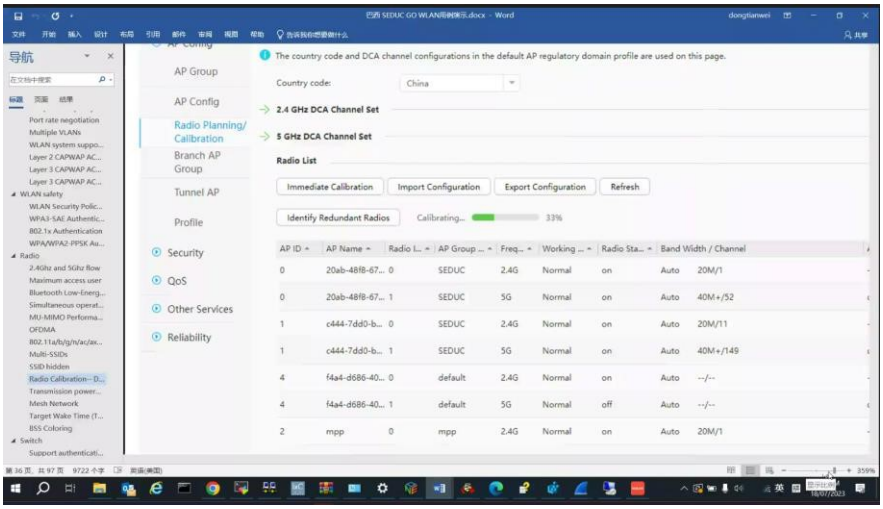


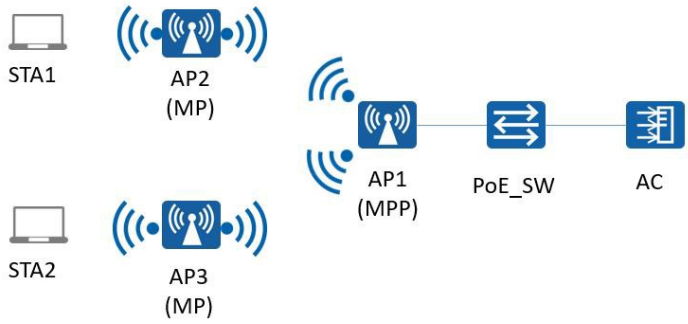
Figura 5 – Conforme indicado durante a sessão, a calibração não foi feita no momento do teste, para que não houvesse intermitência no ambiente da homologação. A imagem mostra o momento exato que esse teste foi realizado pelo time técnico, e como é seu procedimento.

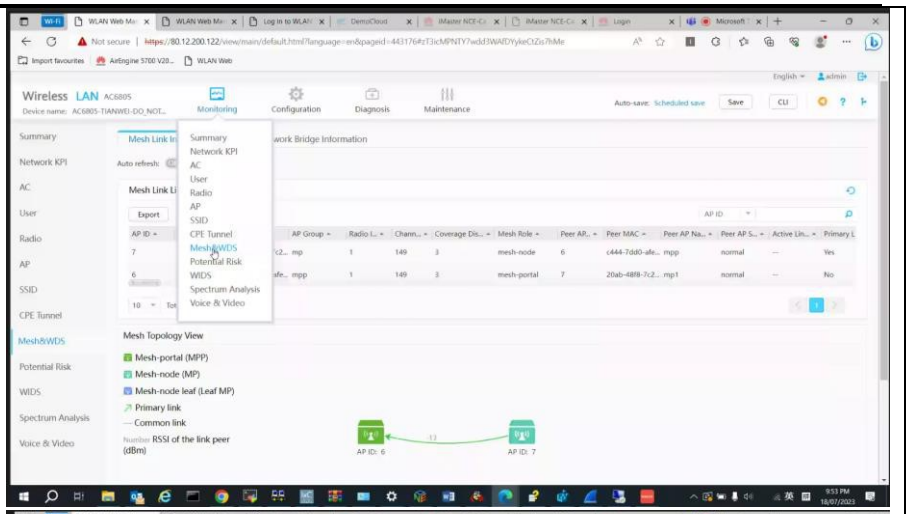
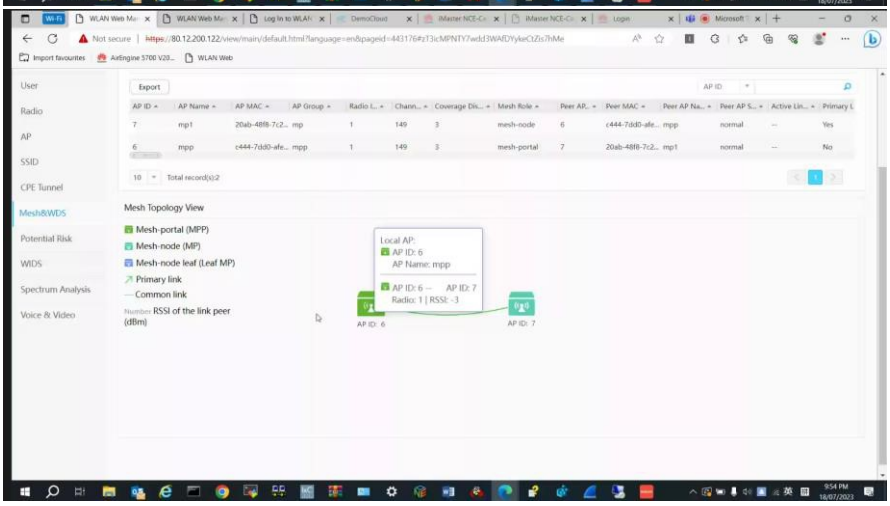
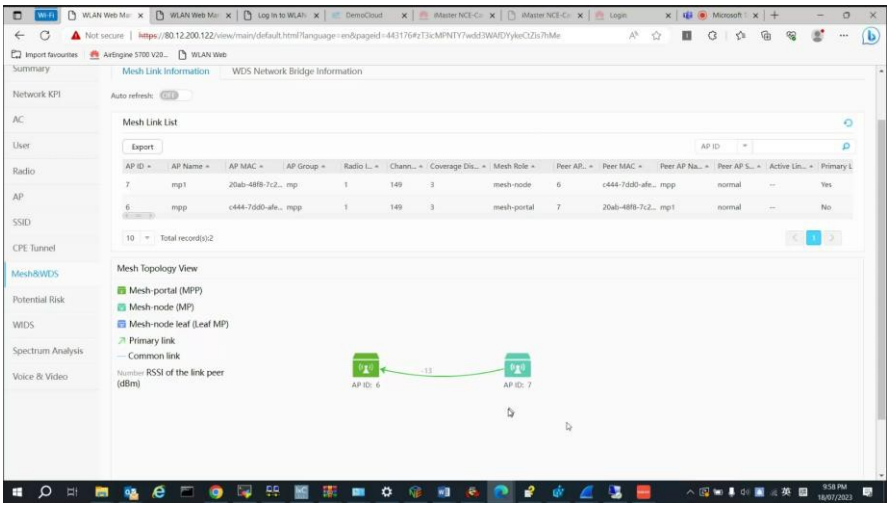
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

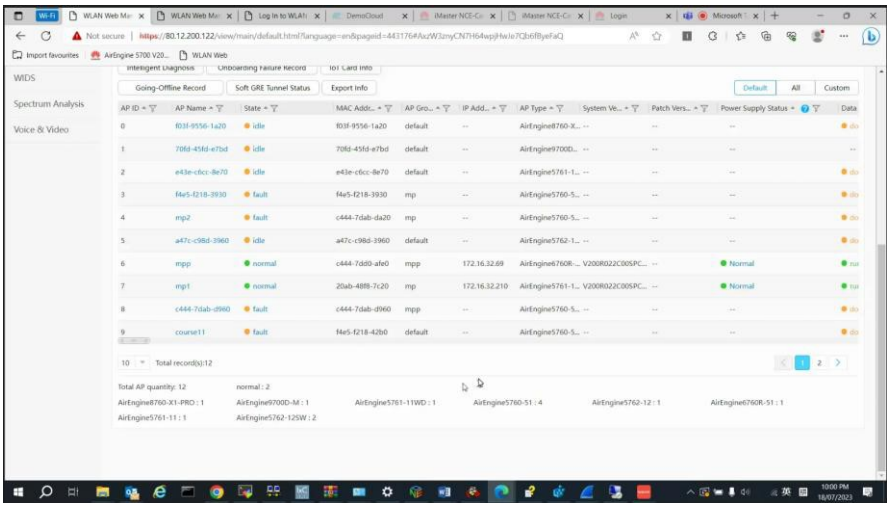
Mesh Network

5.6.7.14 Deve permitir operação em modo Mesh, garantindo o estabelecimento daconexão por meio do rádio Wi-Fi com outros pontos de acesso;

5.7.7.14 Deve permitir operação em modo Mesh, garantindo o estabelecimento daconexão por meio do rádio Wi-Fi com outros pontos de acesso;

Item de teste	Rede Mesh
Objetivo do teste	Validar que o Sistema WLAN suporta Rede Mesh
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configurar a função Mesh na AC e APs
Resultado esperado	1) Verificar informação de link mesh na AC e sua operação;

Resultado	   Figuras 1, 2 e 3 – Foi evidenciado na dashboard da controladora, dois pontos de acesso, operando em modo Mesh, sem a utilização de nenhum

	link físico entre eles. O AP ID 7, com a função de “Mesh-node (MP)” e o AP ID 6 com a função de “Mesh-portal (MPP)”  Figura 4 – Na listagem de todos os APs disponíveis e gerenciados, o funcionamento do AP ID 6 e 7, aparecem com o status de operação normal.

Target Wake Time (TWT)

5.6.7.15 Deve implementar recurso de Target Wake Time (TWT);

5.7.7.15 Deve implementar recurso de Target Wake Time (TWT);

Item de teste	Target Wake Time (TWT)
Objetivo do teste	Validar que o Sistema WLAN suporta TWT

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

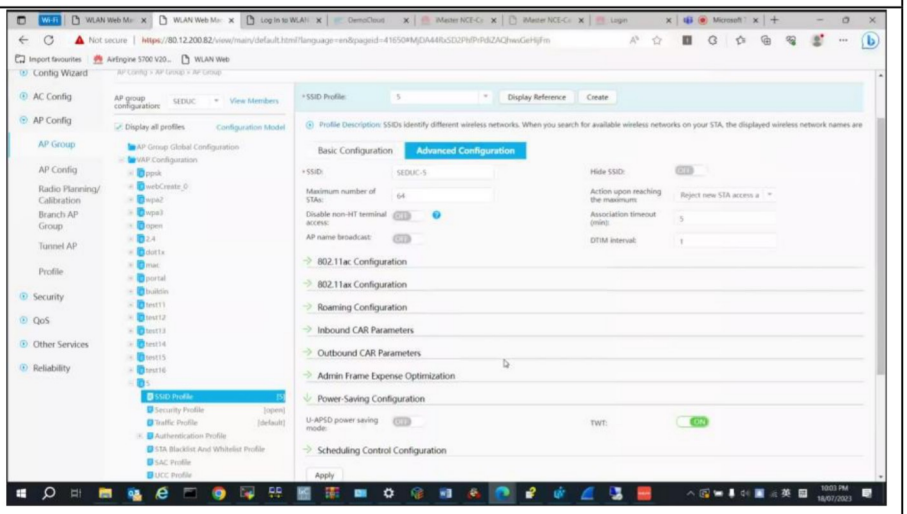
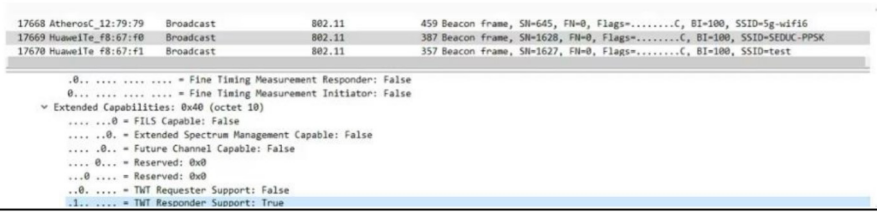
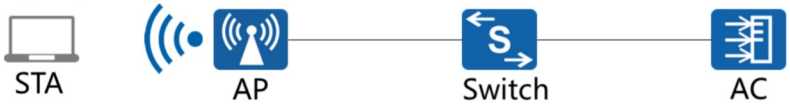
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure a AC corretamente, 2) Habilite TWT
Resultado esperado	1) O status TWT pode ser verificado nos detalhes de perfil SSID. 2) Frames referentes a tecnologia TWT capturados
Resultado	 Figura 1 – Dentro do VAP Configuration, nas opções de “Power-Saving Configuration”, foi mostrado onde habilitar a opção de TWT. 

	Figura 2 – Foi evidenciado através de uma captura de pacotes, um dispositivo associado ao SSID SEDUC-PPSK, criado anteriormente para outro teste, os frames referentes ao TWT.

BSS Coloring

5.6.7.17 Deve suportar BSS Coloring;

5.7.7.17 Deve suportar BSS Coloring;

Item de teste	**BSS Coloring**
Objetivo do teste	**Validar se o AP suporta acoloração BSS**
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure a AC corretamente, 2) Habilite BSS Coloring
Resultado esperado	1) O status TWT pode ser verificado nos detalhes de perfil SSID. 2) Pacotes referentes a tecnologia TWT capturados

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Resultado

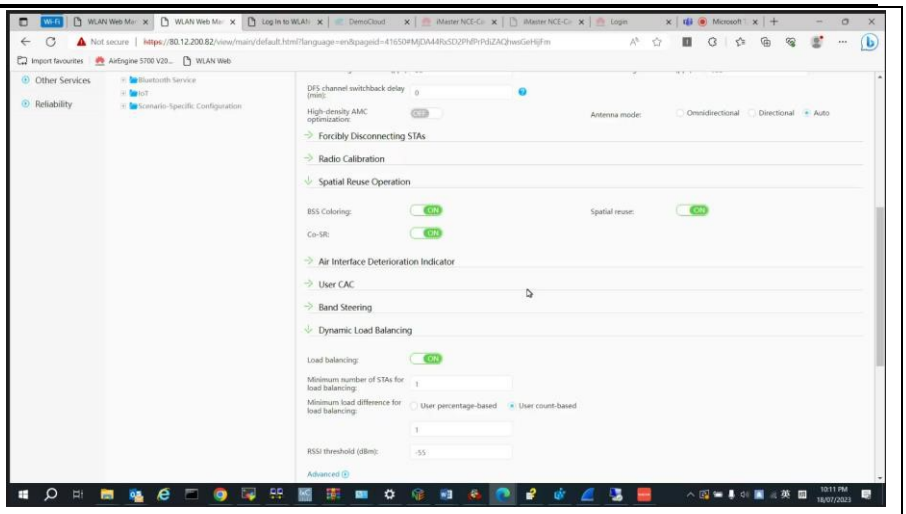


Figura 1 – Dentro do VAP Configuration, nas opções de “Spatial Reuse Operation”, foi mostrado onde habilitar a opção de BSS Coloring.

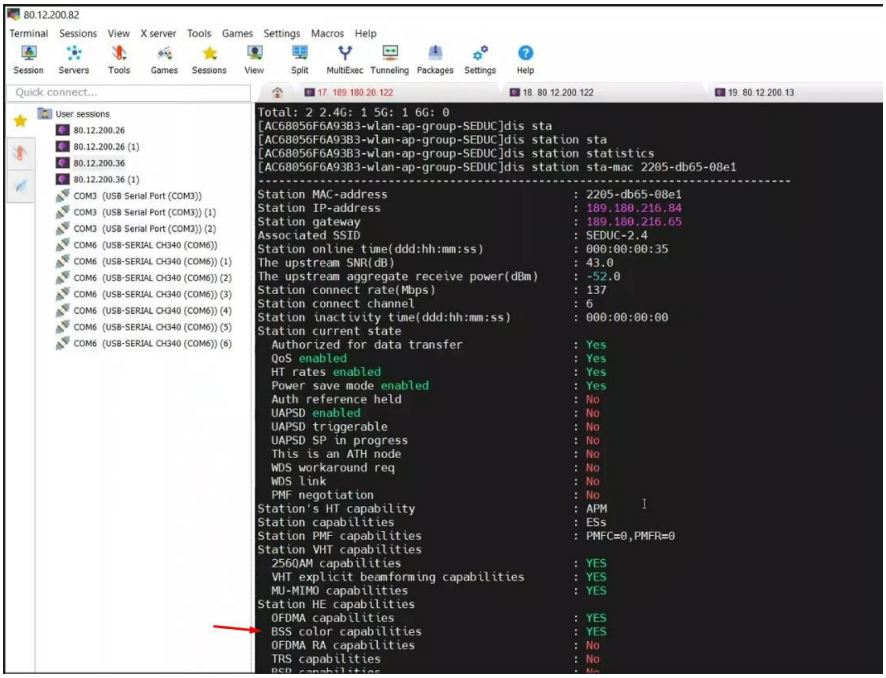


Figura 1 – Via CLI, foi listada através do comando “display station sta-mac 2205-db-65-08e1”, todas as informações de um dispositivo conectado ao SSID SEDUC-2.4, criado no procedimento anterior.

	Na saída deste comando é possível atestar o suporte a tecnologia BSS Coloring.

Switch

Itens que não necessitam de configuração para comprovação:

5.8 Switch Tipo 01

5.8.5 Possuir no mínimo 24(vinte e quatro) PoE portas Gigabit RJ45;

Comprovação visual – Documentação complementar:

CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

- S5735-L24P4S-A-V2
- 24 x 10/100/1000Base-T ports
- 802.3af (15.4 W per port): 24
- 802.3at (30 W per port): 13

5.8.6 Possuir no mínimo 4(quatro) portas SFP 1 Gbps ou superior;

Comprovação visual – Documentação complementar:

CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

- S5735-L24P4S-A-V2
- 4 x GE SFP ports

5.8.8 Possuir Leds indicativos de funcionamento da fonte de alimentação e status das portas;

Comprovação visual - Documentação complementar:

Product description – Hardware description – Chassis – S5735-L24P4S-A-V2 – Indicators e buttons
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-

US_CONCEPT_0000001386247636&lang=en

5.8.9 Deve ocupar 1U do Rack;

Comprovação Visual – Documentação complementar:

Product description – Hardware description – Chassis – S5735-L24P4S-A-V2 – Technical specifications:
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US_CONCEPT_0000001386247636&lang=en

Chassis height [U] 1 U

5.8.15 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência;

Comprovação visual – Documentação complementar:

CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

- ac input: 100 V ac to 240 V ac, 50/60 Hz

5.8.29 Deverá estar licenciado para a gerência e controle do item Solução de gerenciamento e controle;

Comprovação documental:
CloudCampus N1 Business Model Datasheet.pdf

5.9 Switch Tipo 02

5.9.2 Possuir no mínimo 24 portas 10/100/1000 Base-T;

Comprovação visual - Documentação complementar:

CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

- S5735-L24T4S-A-V2
- 24 x 10/100/1000Base-T ports

5.9.3 Possuir no mínimo 4(quatro) portas SFP 1 Gbps ou superior;

Comprovação visual - Documentação complementar:

CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

- S5735-L24T4S-A-V2
- 4 x GE SFP ports

5.9.5 Possuir Leds indicativos de funcionamento da fonte de alimentação e status das portas;

Comprovação visual – Documentação complementar:

Product description – Hardware description – Chassis – S5735-L24T4S-A-V2 – Indicators e buttons:
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US_CONCEPT_0000001386088048&lang=en

5.9.6 Deve ocupar 1U do Rack;

Product description – Hardware description – Chassis – S5735-L24P4S-A-V2 – Technical specifications:
https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US_CONCEPT_0000001386088048&lang=en

Chassis height [U] 1 U

5.9.12 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência;

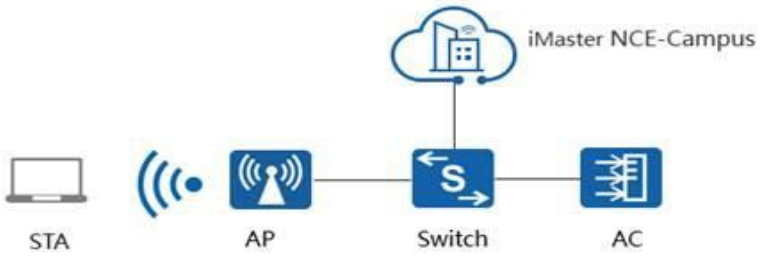
CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

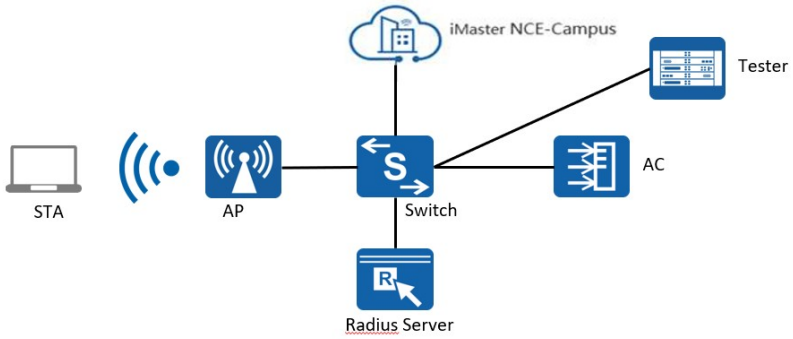
- ac input: 100 V ac to 240 V ac, 50/60 Hz

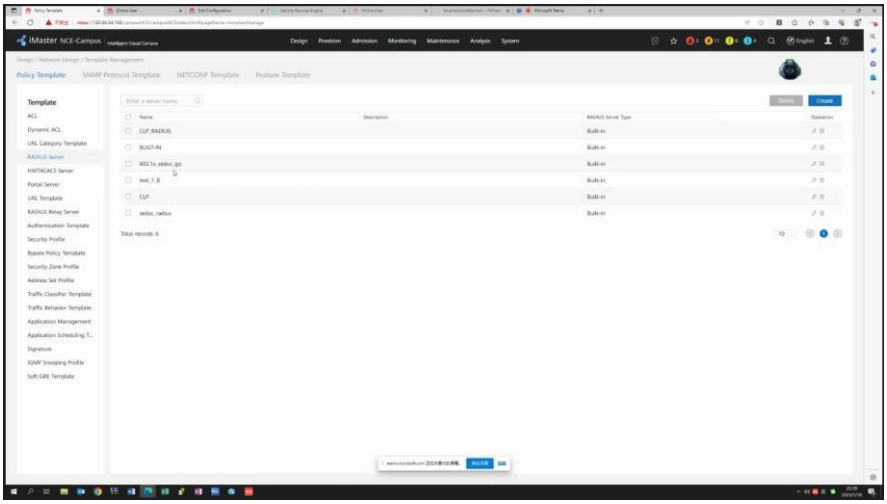
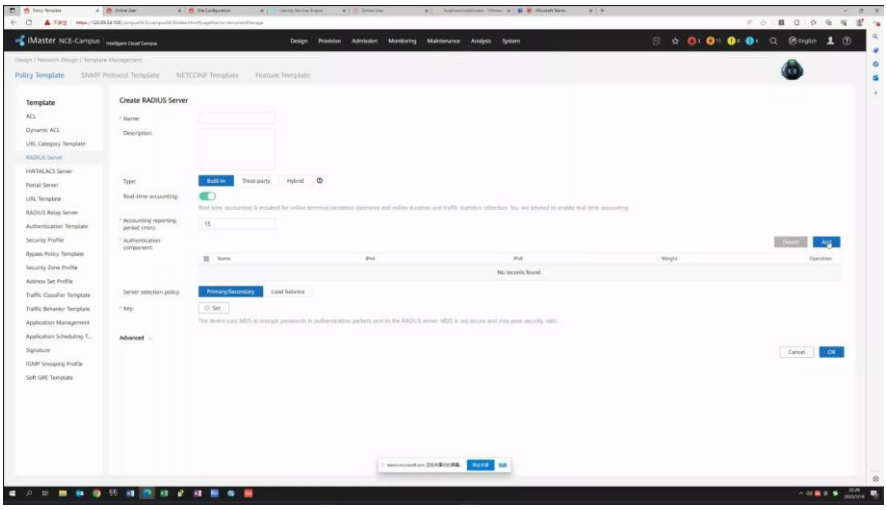
Suporte a autenticação via servidores RADIUS

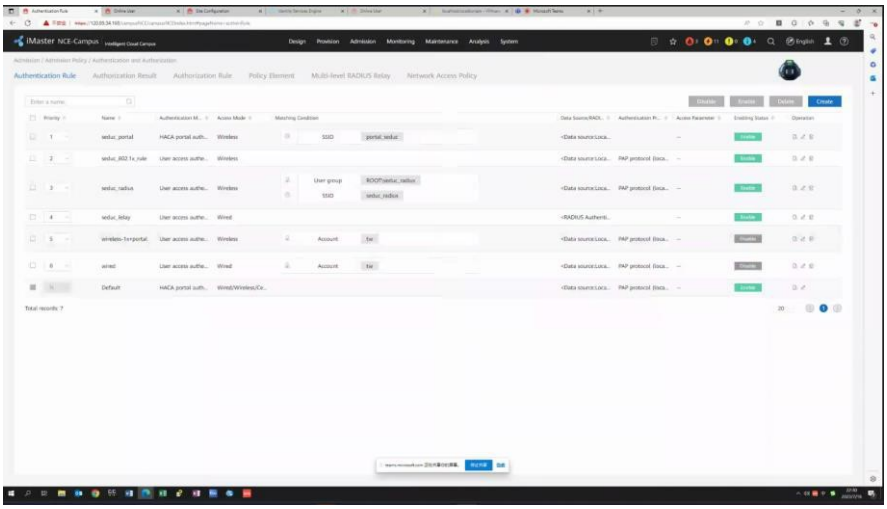
5.8.18 Suportar autenticação em servidores RADIUS ou TACACS;

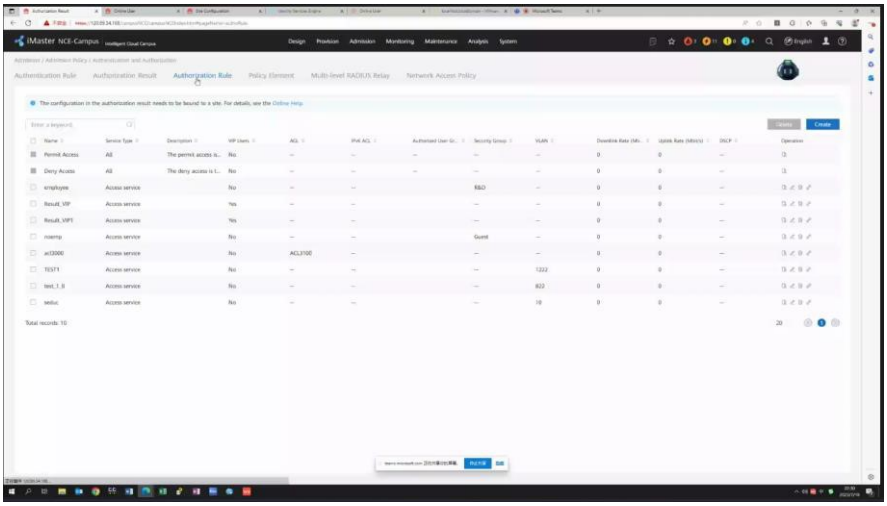
5.9.15 Suportar autenticação em servidores RADIUS ou TACACS;

Item de teste	**Suporte de autenticação para servidores RADIUS**
Objetivo do teste	Suporta autenticação para servidores RADIUS;
Configuração de teste	Topologia da rede 1:  Topologia de rede 2 (com RADIUS externo):

	 Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Selecione “Provision> Device > Site Configuration > Site > Device Login Configuration” no menu principal .Clique ”Create“; Depois, configure regras de autenticação, regras de autorização e os resultados da autorização. 2) Selecione “Provision> Device > Site Configuration” depois configure as interfaces por onde os usuários serão autenticados
Resultado esperado	1) A configuração é entregue e autenticada com sucesso.

Resultado	 Figura 1 – Dentro da plataforma iMaster NCE Campus, foi criado alguns templates de servidores Radius  Figura 2 – O procedimento para isso é baseado em inserir as informações necessárias, como a “shared secret” que vai ser compartilhada entre os dispositivos.





Figuras 3 e 4 – Ainda na plataforma, também é possível criar todas as regras de autenticação e autorização bem como o resultado esperado de cada uma.

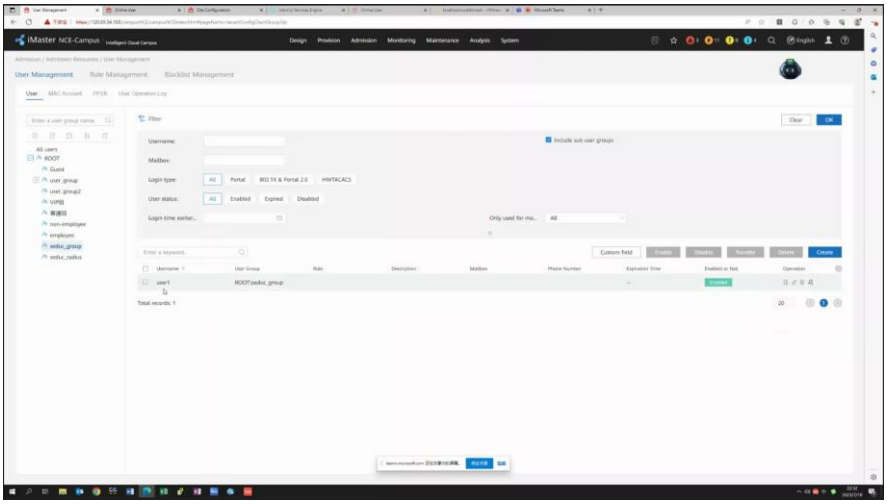


Figura 5 – Foi criado um grupo de usuários, chamado seduc_group, onde foi adicionado um usuário nomeado como user1, o qual utilizamos para autenticar o dispositivo.

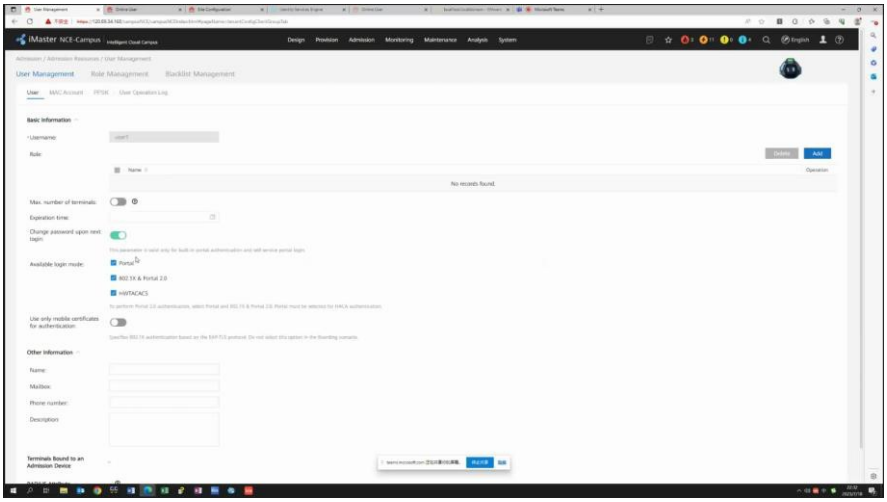


Figura 6 – Esse usuário, em suas permissões, foi configurado para que possa se autenticar via Portal, 802.1x e HWTACACS.

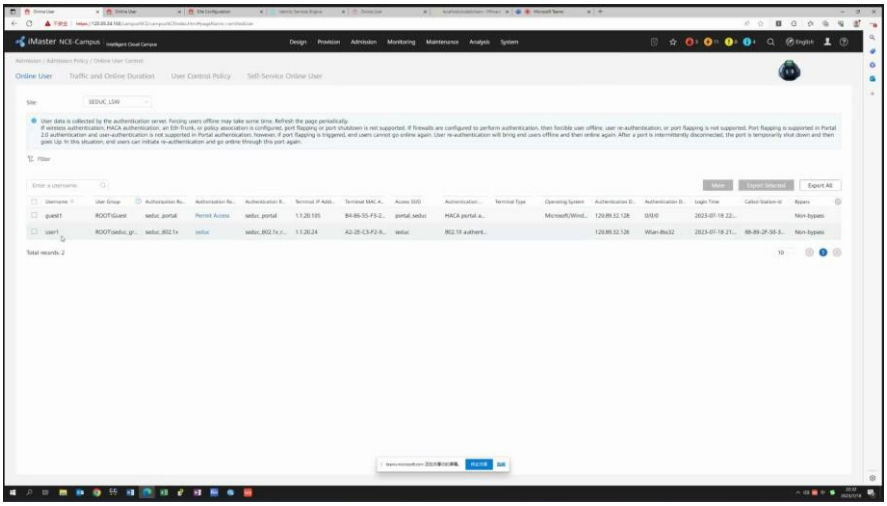


Figura 9 – Por ultimo, foi evidenciado o usuário user1, autenticado a rede via 802.1x.

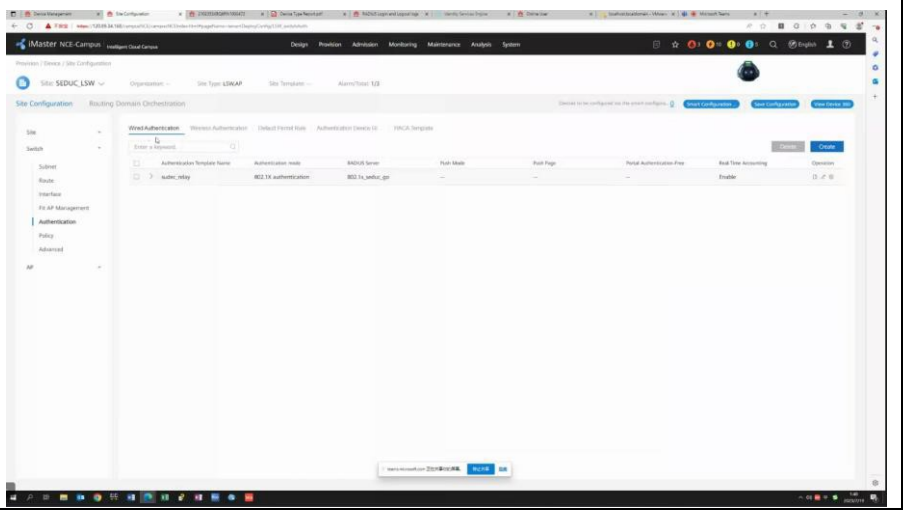


Figura 10 – Nas configurações do switch, através da plataforma iMaster NCE Campus, foi atrelado um servidor de Radius (externo), para a autenticação de usuários na rede cabeada.

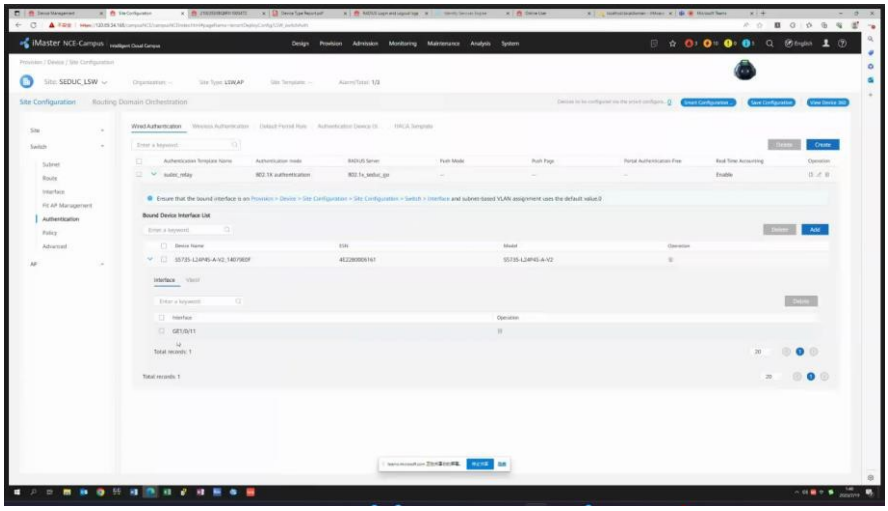


Figura 11 – Em seguida, foi feita associação da interface GE1/0/11, ao servidor.

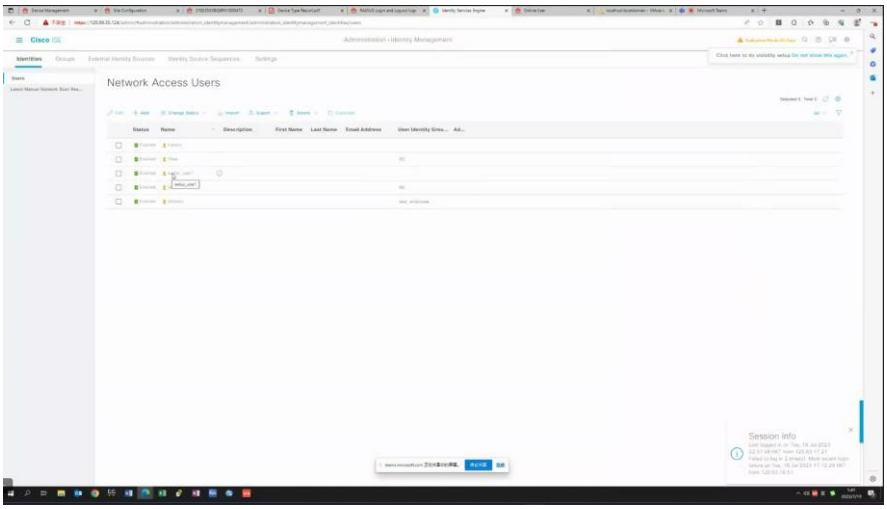
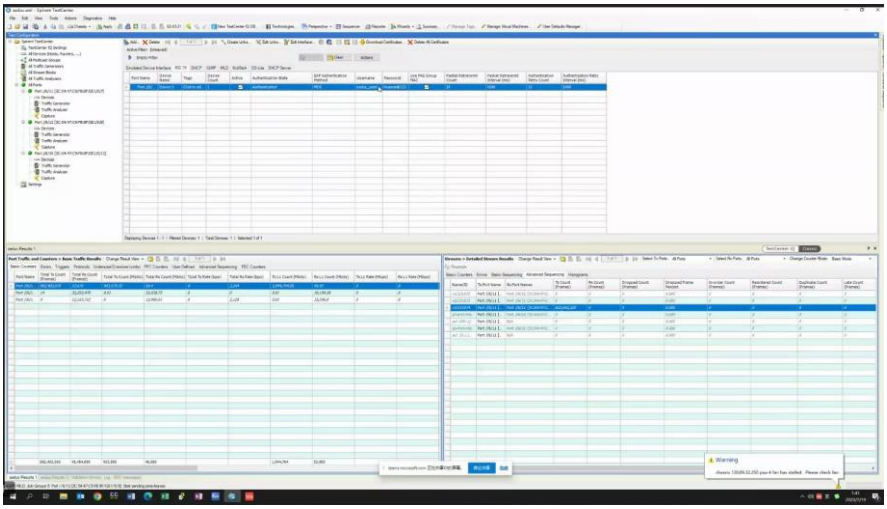


Figura 12 – No servidor de Radius (nos testes, utilizamos o software Cisco ISE), foi criado o usuário seduc_user1.



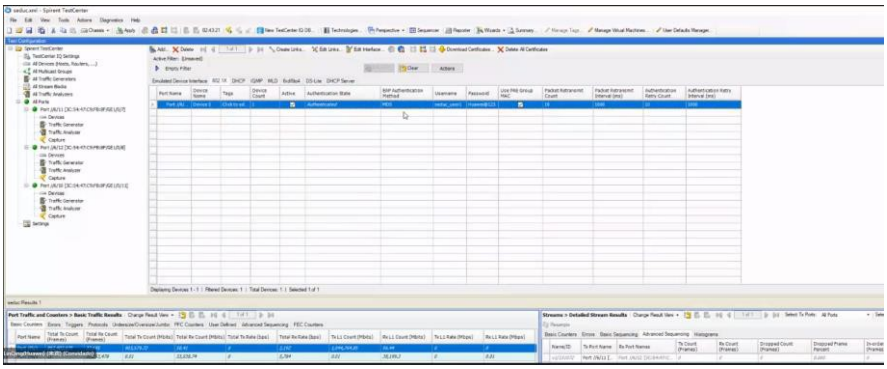


Figura 13 e 14 – Com o auxilio de um gerador de tráfego, foi simulada uma autenticação, utilizando o mesmo usuário criado no passo anterior.

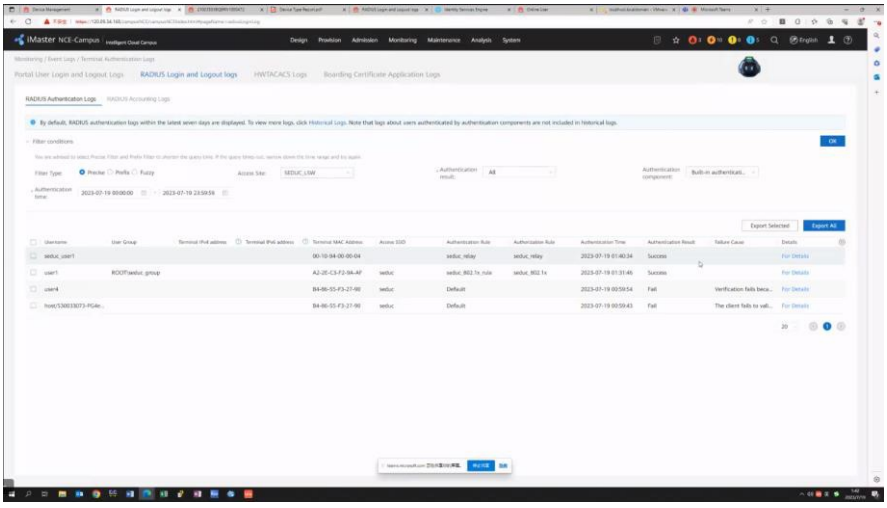


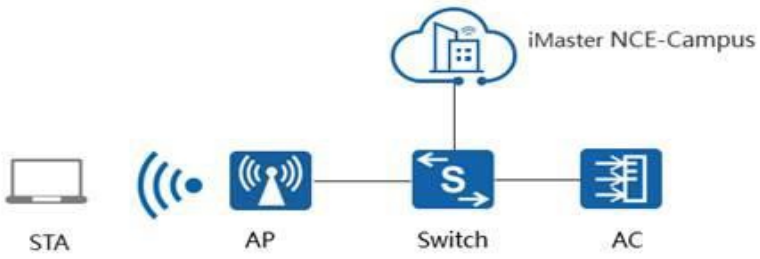
Figura 15 – Na plataforma iMaster NCE Campus, conseguimos listar os usuários conectados e autenticados via 802.1x. O usuário em destaque é o mesmo utilizado, com o nome seduc_user1.

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

LLDP e LLDP-MED

5.8.22. Implementar LLDP e LLDP-MED;

5.9.19. Implementar LLDP e LLDP-MED;

Item de teste	**LLDP e LLDP-MED**
Objetivo do teste	**Implementar LLDP e LLDP-MED;**
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Exibir as o suporte a LLDP no equipamento

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

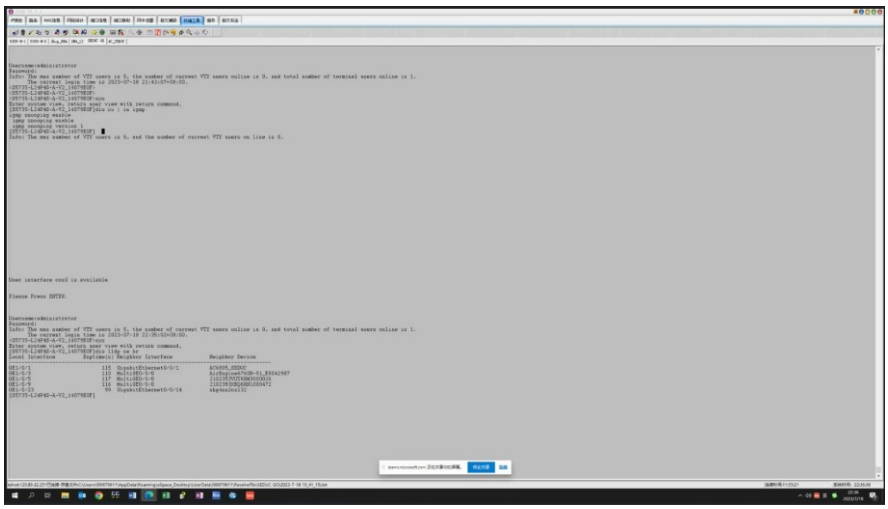
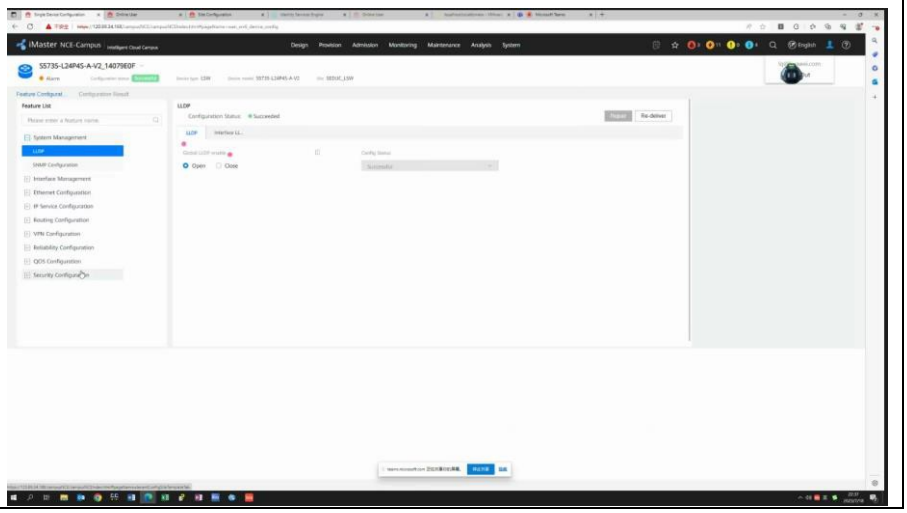
Resultado esperado	1) Exibir o suporte a LLDP, via CLI e via plataforma de gerenciamento iMaster NCE Campus
Resultado	 Figura 1 – Acessando a CLI do equipamento, foi inserido o comando “display lldp neighbor” e foram listados os dispositivos conectados as interfaces do switch. 

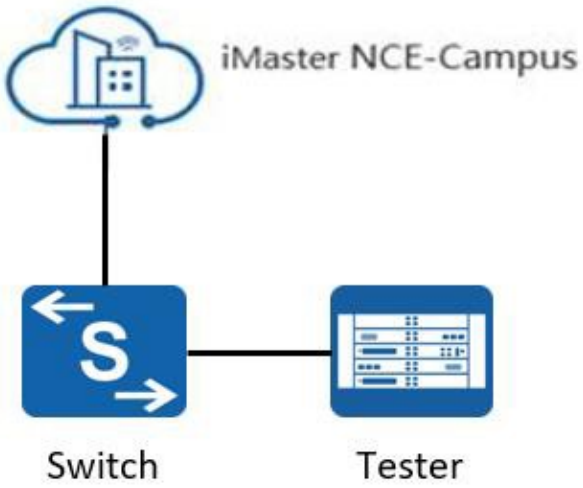
	Figura 2 – Na plataforma de gerenciamento iMaster NCE Campus, também foi mostrado onde podemos habilitar globalmente a função LLDP nos equipamentos.

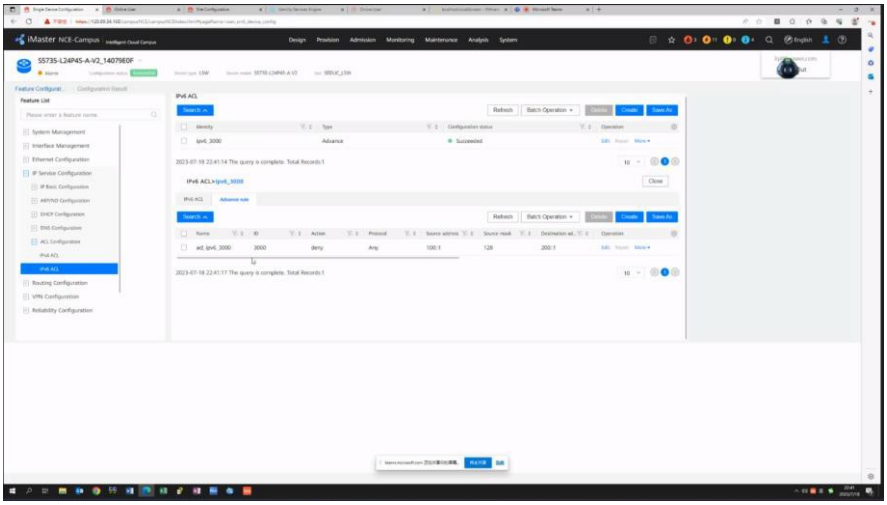
ACL

5.8.24. Deve Implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino ou VLAN;

5.9.21. Deve Implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino ou VLAN;

Item de teste	**ACL**
Objetivo do teste	Deve implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, endereço MAC de origem/destino ou VLAN;
Configuração de teste	Topologia da rede:

	 Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Enviar dois fluxos via gerador de trafégo, um dos quais está em conformidade com a política criada pela ACL e o outro não.
Resultado esperado	1) Aconfiguração é entregue com sucesso. 2) O tráfego que corresponde às regras ACL é processado com base nas políticas correspondentes.

Resultado	 Figura 1 – Na plataforma de gerenciamento iMaster NCE Campus, foi configurada uma ACL avançada para IPv6, com o nome de acl_ipv6_3000 e ID 3000. As regras desta ACL, estão negando qualquer protocolo (ou todo tipo de tráfego) da origem 100::1/128 para para o destino 200::1/128.

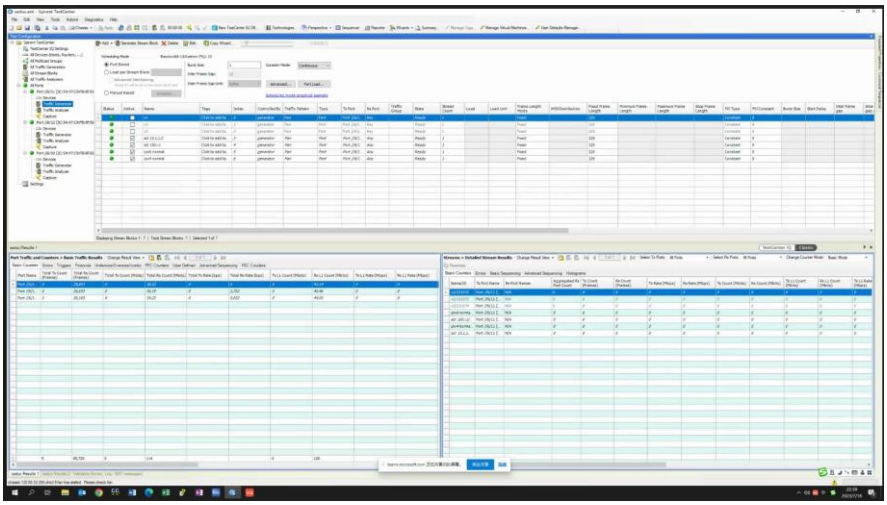
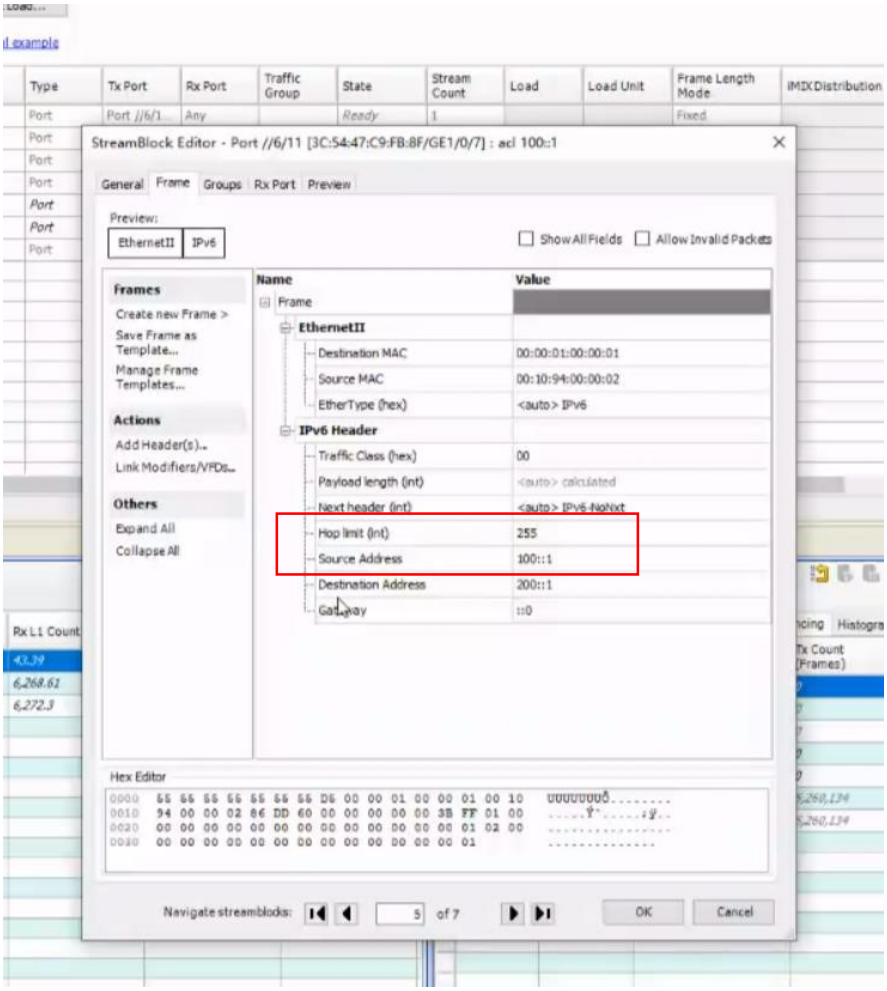


Figura 2 – Utilizando a ACL criada, com o auxilio do gerador de trafego, preparamos dois fluxos onde um foi negado pela ACL e o outro não.



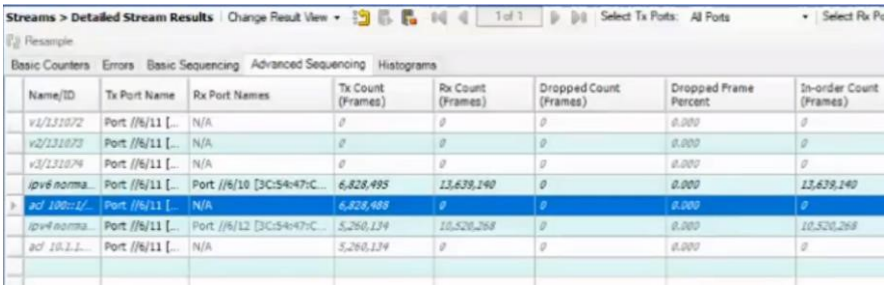


Figura 3, 4 e 5 – Os testes selecionados, mostram os fluxos recebidos pelo switch. O fluxo chamado de “acl 100::1”, criado para ser testado (figura 4), esta detalhando os IPs de origem e destino. Na figura 5, estão

listadas as estatísticas do teste em azul. Esse tráfego, está dando match nas regras da ACL 3000 e consequentemente, negando o trafego IPv6 dos IPs inseridos.

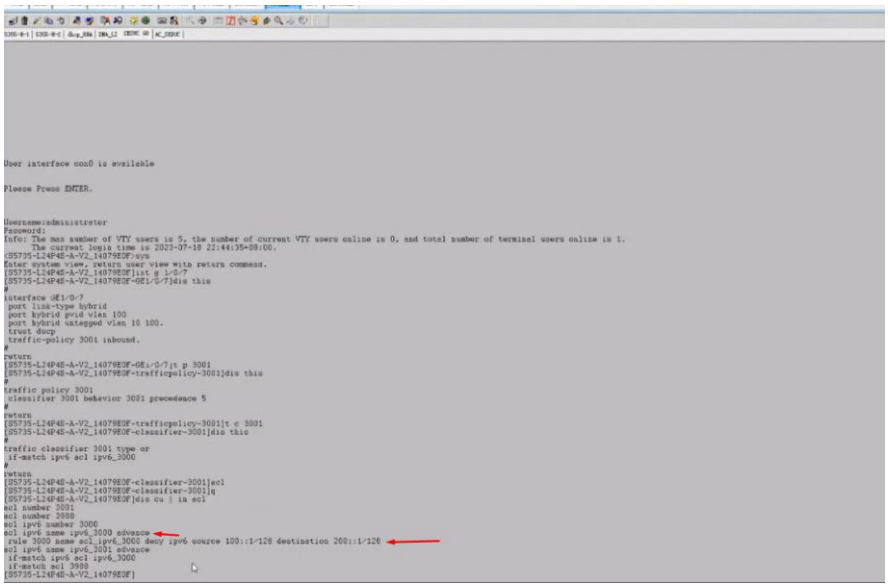
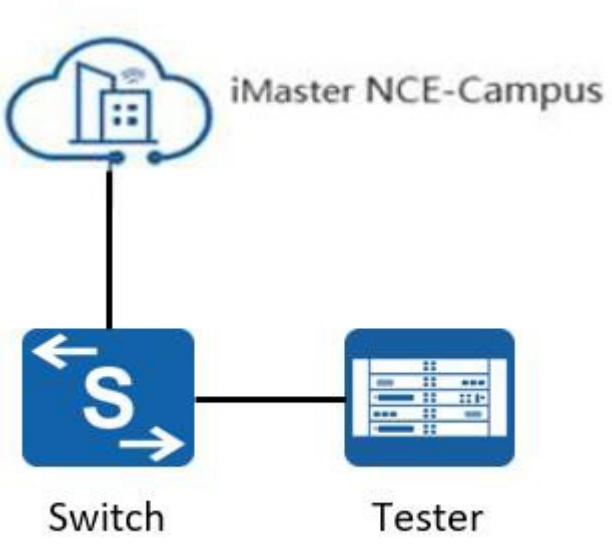


Figura 6 – Checando a CLI do switch, mostramos a sequência de ações para a implementação das regras. Primeiro foi definida a ACL, com as permissões e/ou bloqueios. Segundo, configuramos em Traffic Classifier, para que seja validada as regras da ACL. Terceiro, inserimos o Traffic Classifier dentro de um Traffic Policy, e em seguida é aplicada a interface do equipamento.

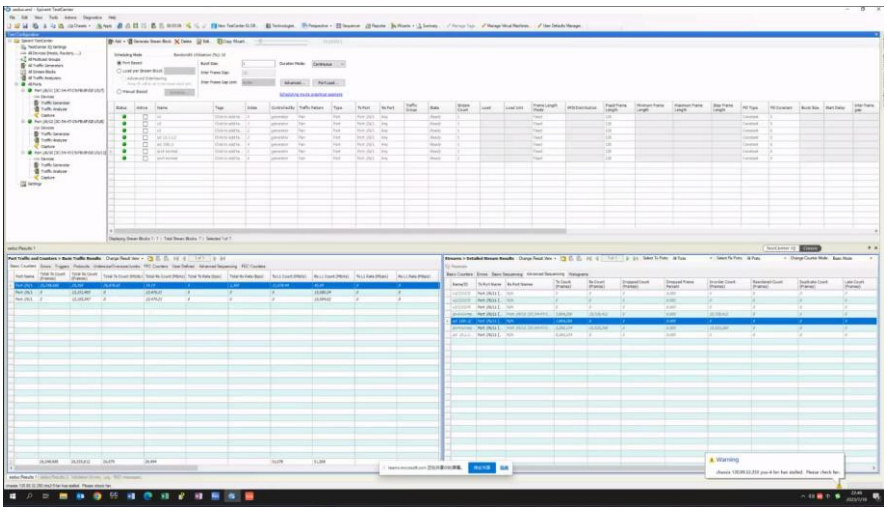
IGMP snooping

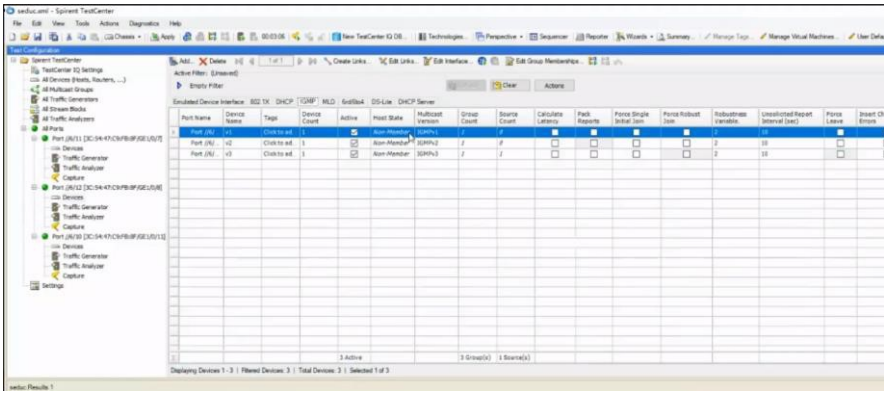
5.8.26. Implementar IGMP v1, IGMP v2 e IGMP v3 snooping;

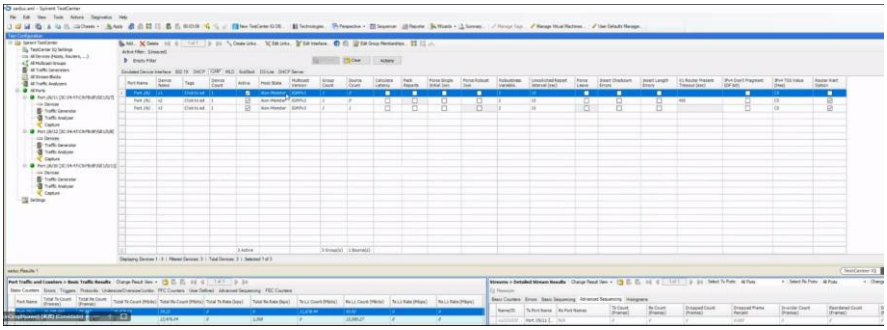
5.9.23. Implementar IGMP v1, IGMP v2 e IGMP v3 snooping;

Item de teste	**IGMP snooping**
Objetivo do teste	**Implementar o snooping IGMP v1, IGMP v2 e IGMP v3;**
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) 1) O dispositivo testado é conectado ao testador através de duas interfaces. A função de IGMP snooping está ativada no dispositivo testado. A interface 1 do testador simula uma fonte de multicast e a interface 2 simula um cliente de multicast para se juntar a um grupo de multicast.
Resultado esperado	1) Tport_2 do testador junta-se ao grupo multicast e tem uma tabela de encaminhamento multicast da camada 2. Tport_2 do testador recebe fluxos de dados multicast. 2) Tport_2 no testador não pode receber dados multicast.
Resultado	





Figuras 1, 2 e 3 – O IGMP Snooping ele foi aplicado em duas interfaces correspondentes, onde foi simulado um tráfego de multicast.

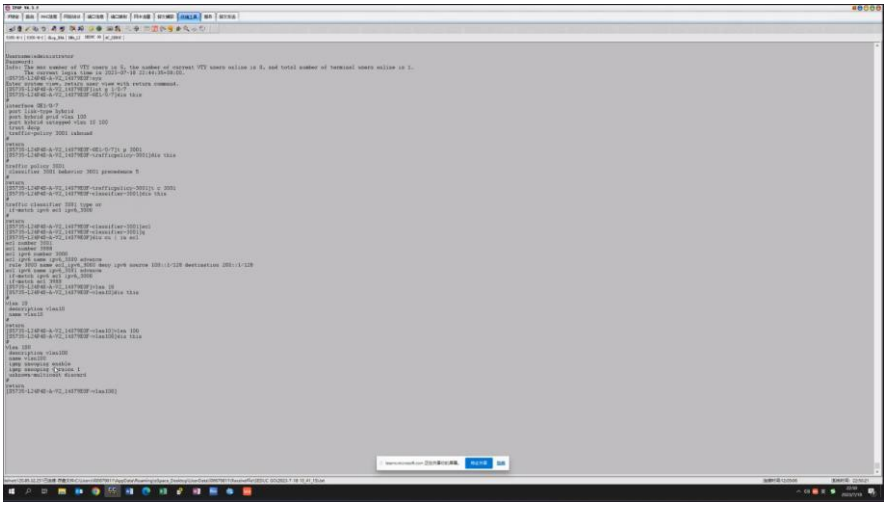
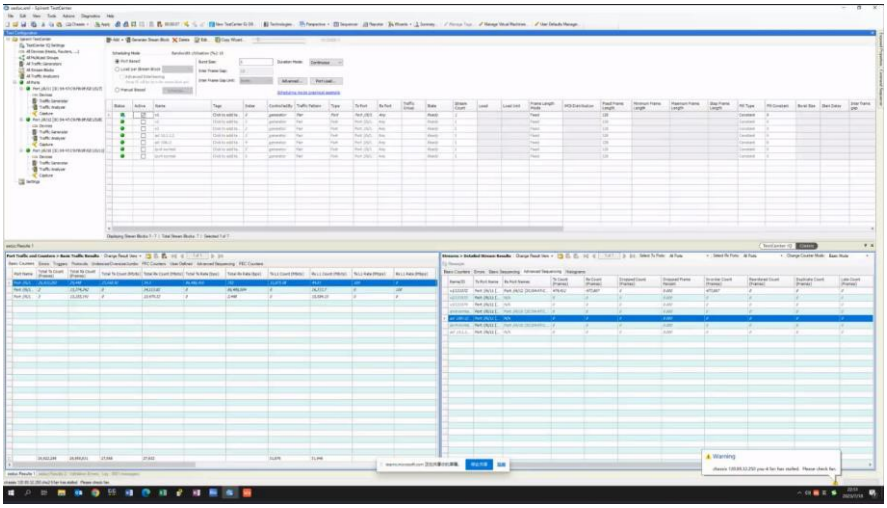


Figura 4 – No switch, foi configurado o IGMP snooping versão 1, dentro da VLAN 100, onde o IGMP Snooping, basicamente irá identificar os grupos de multicast disponiveis.



Figuras 6, 7 e 8 – O tráfego simulado foi iniciado no gerador, e pode ser visto nas estatísticas das interfaces correspondentes.

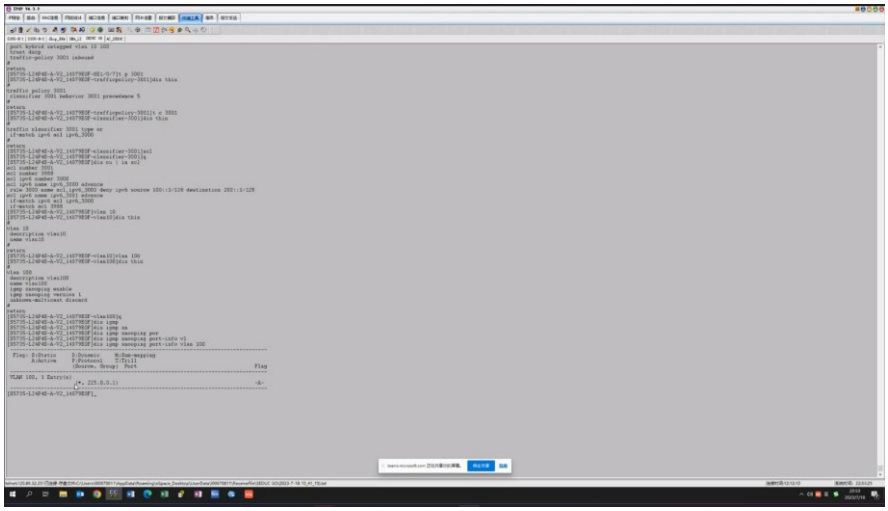


Figura 9 – Novamente no switch, através do comando “display igmp snooping port info”, é mostrado um grupo identificado para a VLAN 100.

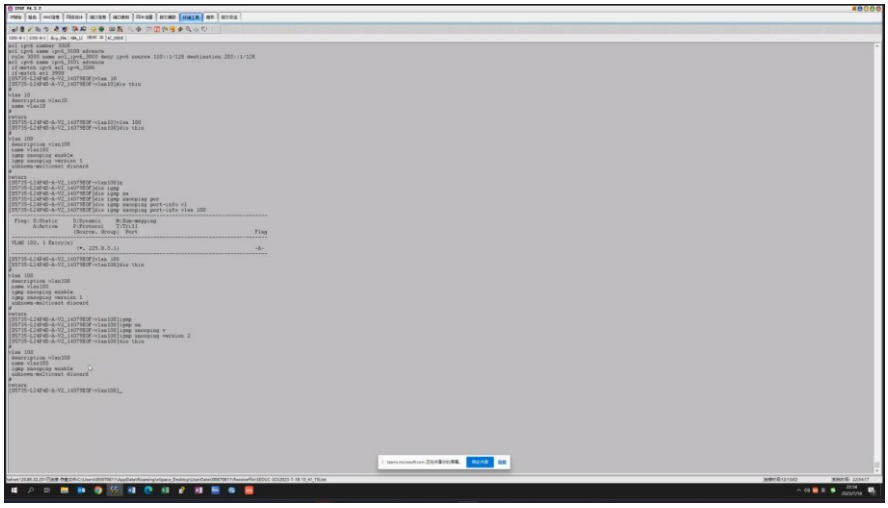


Figura 10 – Ainda no switch, alteramos a versão do IGMP Snooping. Agora para a versão 2.

Obs. O padrão utilizado é o IGMP Snooping V2, então os equipamentos não mostram explicitamante a versão. Isso só é mostrado para as versões 1 e 3, as quais não são o padrão.

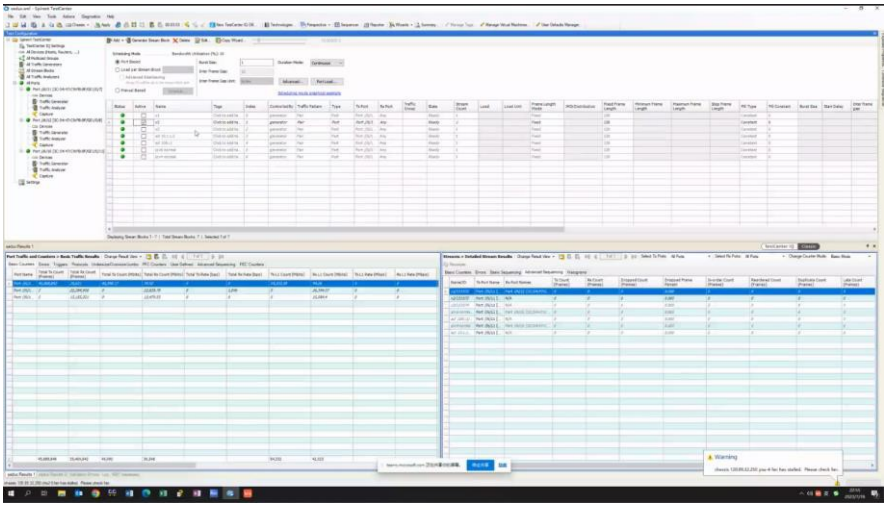


Figura 11 – No gerador, foi iniciado o trafego multicast, agora para IGMP Snooping versão 2.

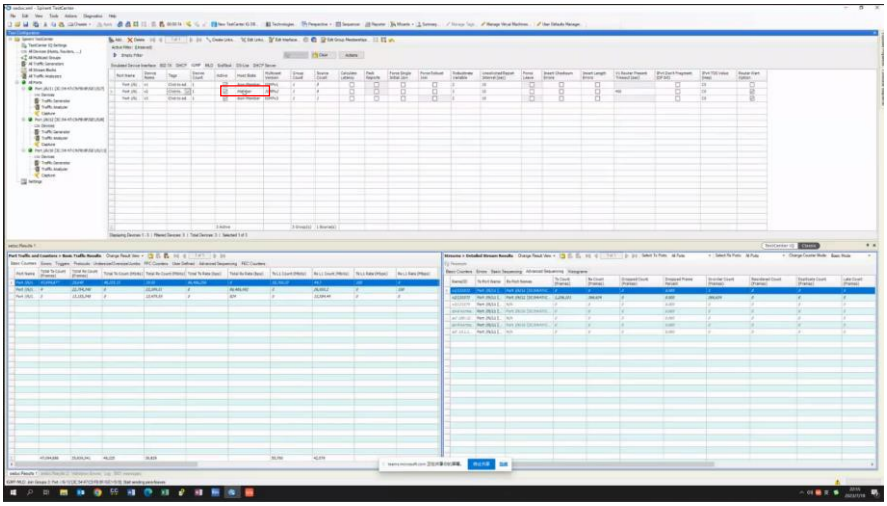


Figura 13 – No gerador, foi evidenciado que a interface é parte do grupo IGMP V2 criado

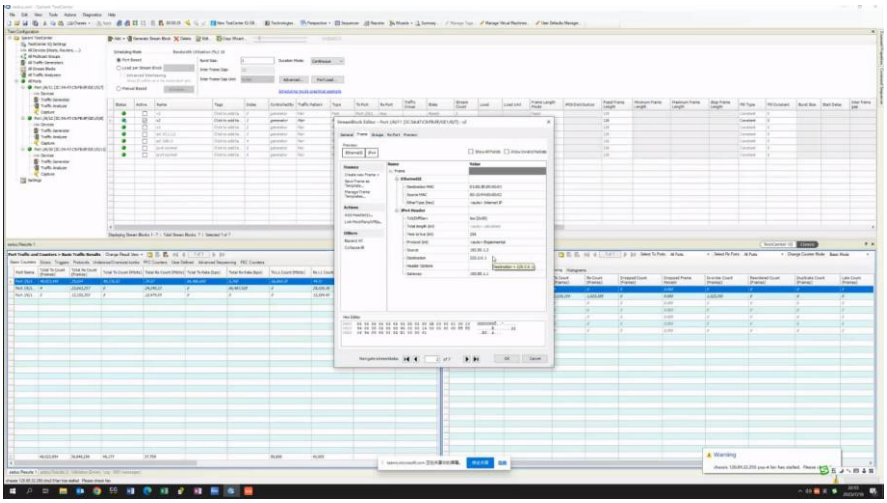


Figura 14 – O destino multicast é o 225.0.0.1

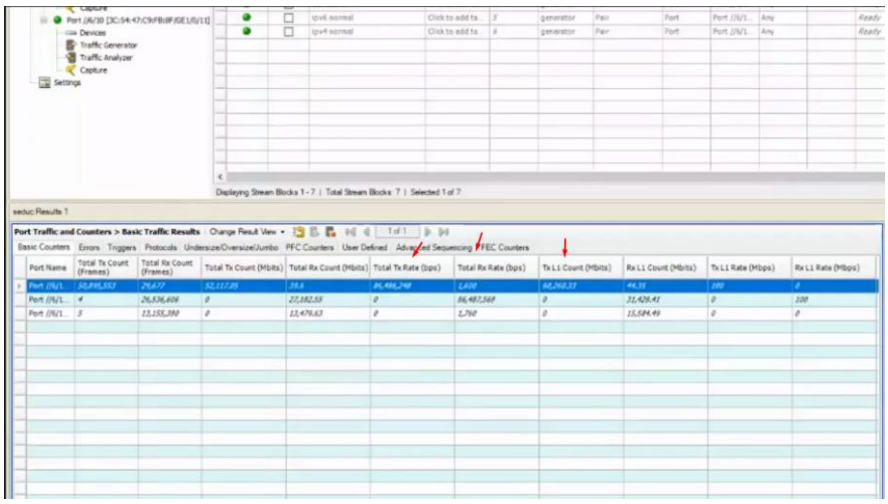
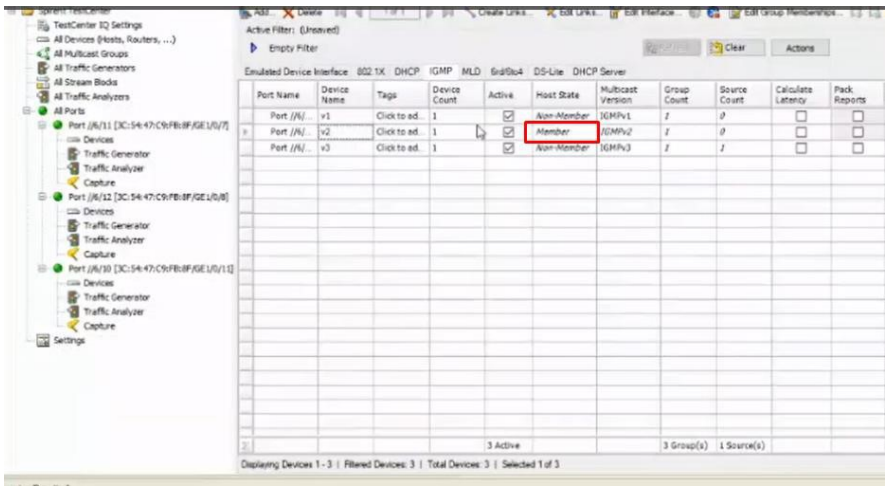
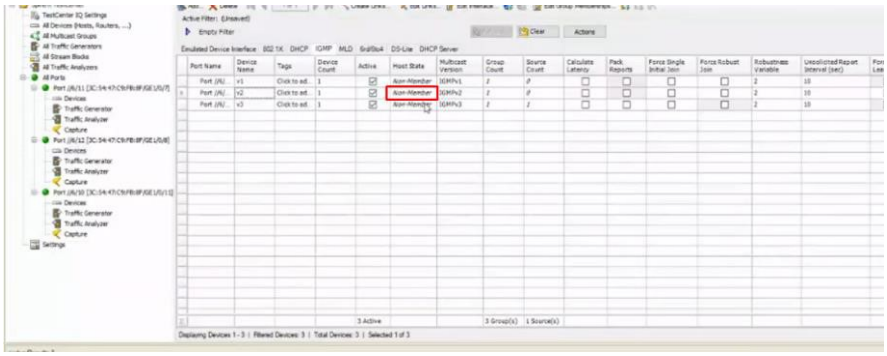
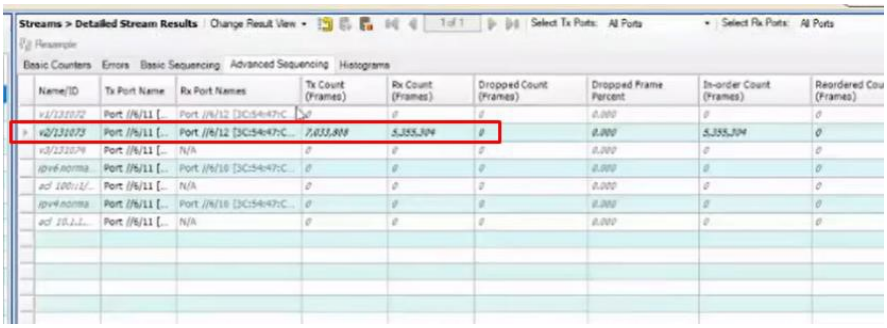


Figura 15 – No gerador, é possivel identificar que esse tráfego está sendo encaminhado normalmente.





Figuras 16 e 17 – Em seguida, foi simulado uma mensagem de “LEAVE”, para este grupo IGMP V2, e logo as interfaces alteraram o status de “MEMBER” para “NON MEMBER”



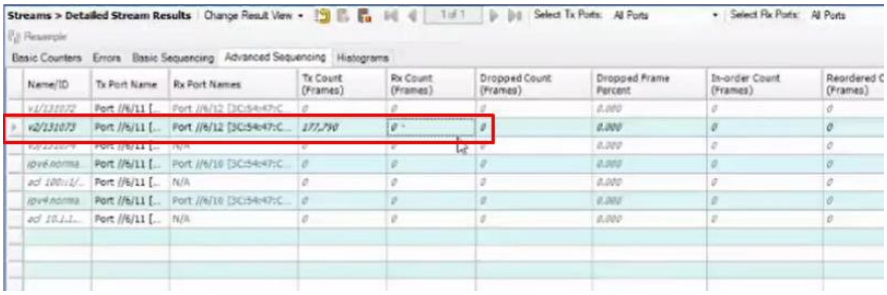


Figura 18 (antes do LEAVE) e 19 (depois do LEAVE) – Feito isso, os contadores mostrando o trafego enviado, ficaram zerados.

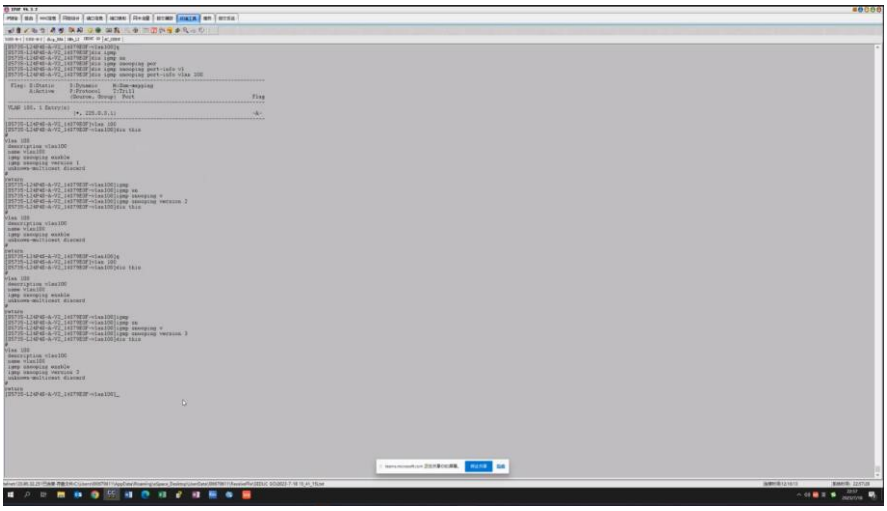
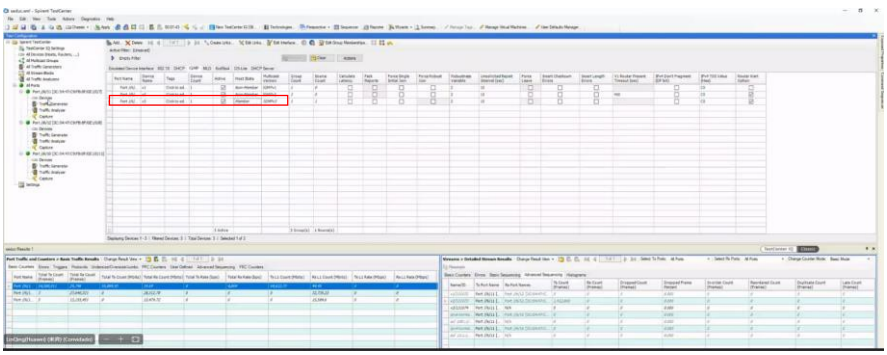
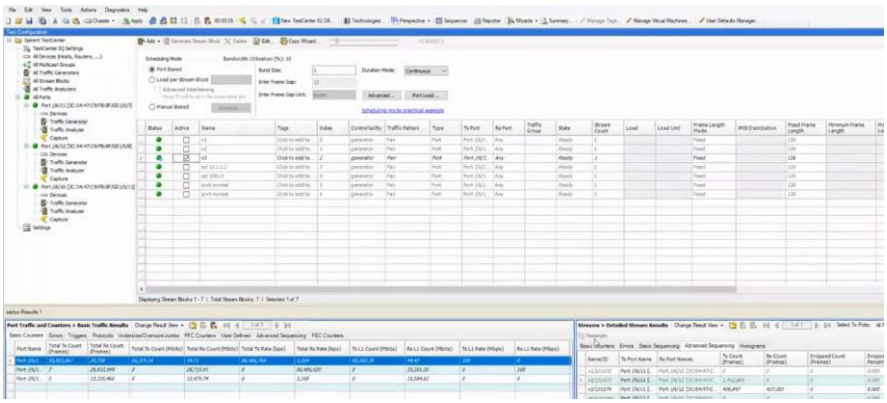


Figura 20 – De volta ao switch foi alterada a versão do IGMP Snooping para versão 3.





Figuras 21 e 22 – A interface do gerador foi adicionada ao grupo multicast e agora é um membro. Em seguida o o trafego começa a ser enviado nas estatisticas do gerador.

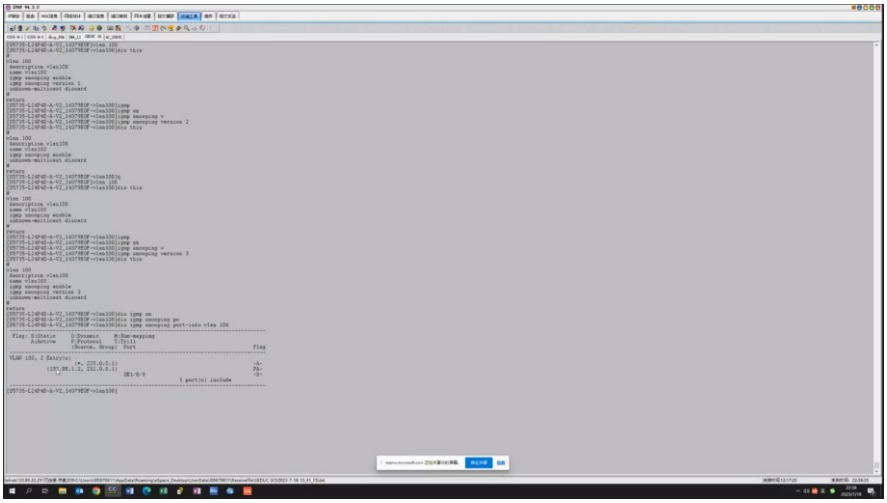
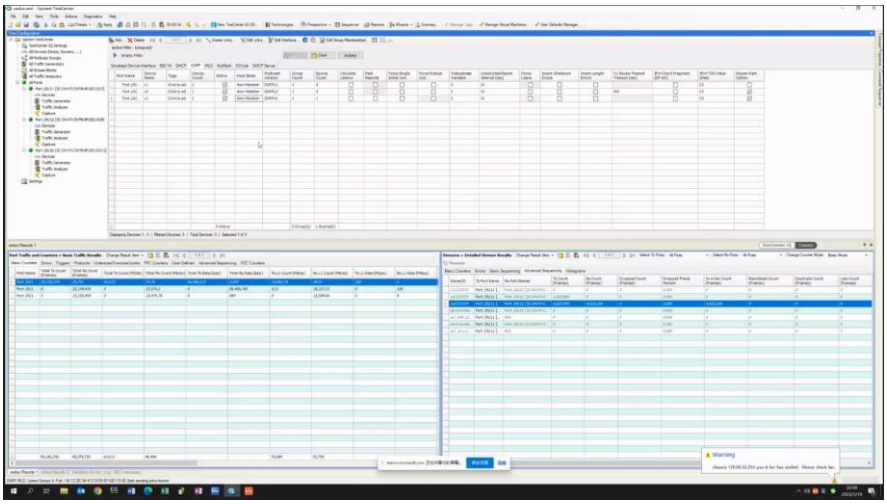


Figura 23 – Executando o comando “igmp snooping port-info vlan 100”, é mostrado que agora os membros na interface que está recebendo o tráfego multicast.

	 Figura 24 – Novamente, foi simulado uma mensagem de “LEAVE”, para este grupo IGMP V3, e logo as interfaces alteraram o status de “MEMBER” para “NON MEMBER”, e seus contadores, ficaram como zero.

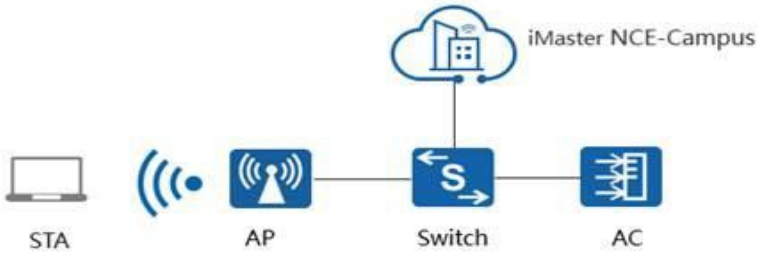
Autenticação 802.1x

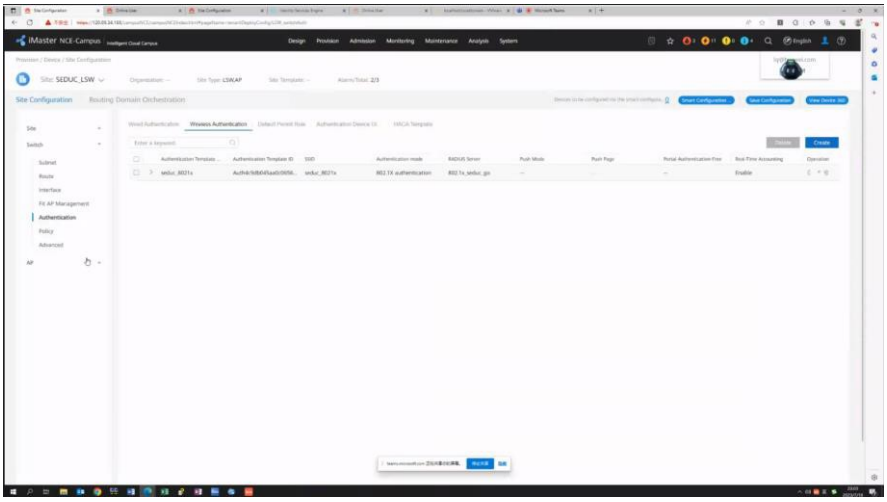
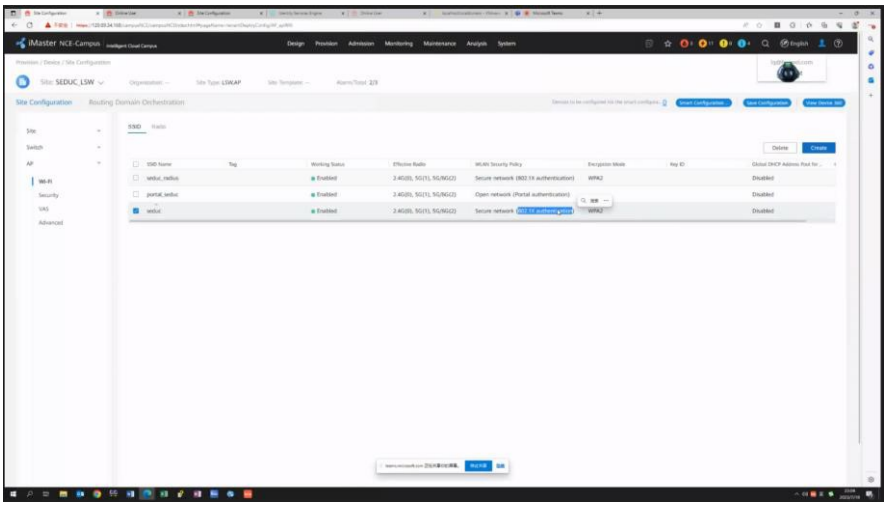
5.8.28 Implementar IEEE 802.1x para autenticação do usuário, permitindo à associação dinâmica do usuário a determinada VLAN;

5.10.26 Implantar autenticação de dispositivos e usuários via **802.1x**, Web Portal e endereço MAC na rede sem fio;

Item de teste	**Autenticação 802.1x (5.8.28)**

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Objetivo do teste	Implementar IEEE 802.1x para autenticação de usuários, permitindo a associação dinâmica de utilizadores a uma determinada VLAN;
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Conectar usuários via 802.1x
Resultado esperado	1) A autenticação 802.1X é bem sucedida e o usuário pode acessar a rede;

Resultado	 Figura 1 – Foi associado ao switch o template de servidor RADIUS  Figura 2 – No ponto de acesso, foi criado um SSID chamado seduc, com a politica de segurança “Secure networks (802.1x Authentication).”

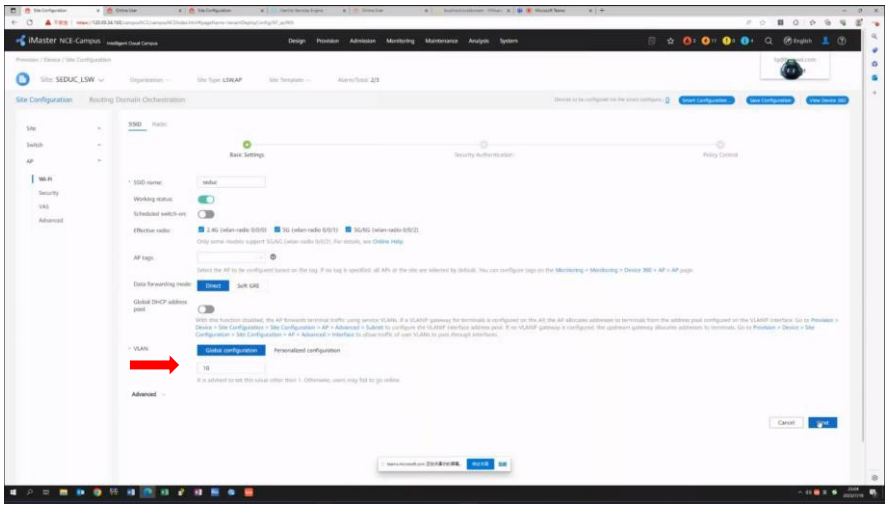
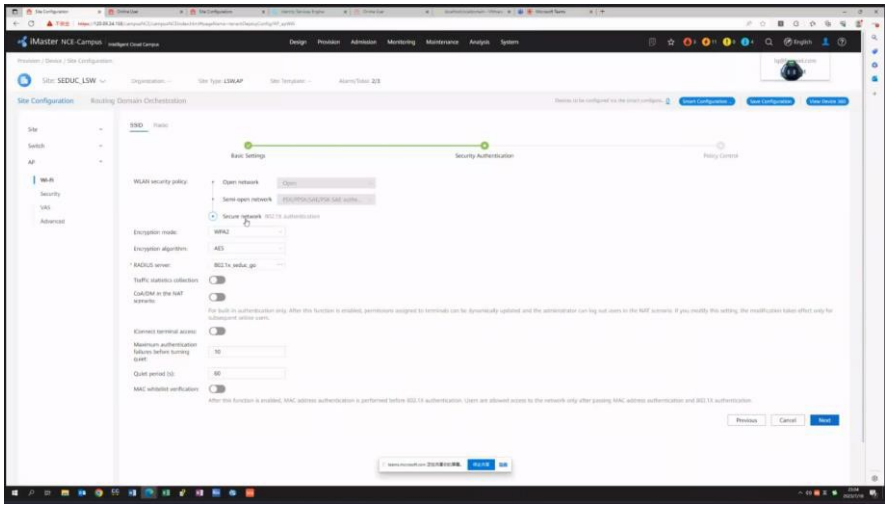
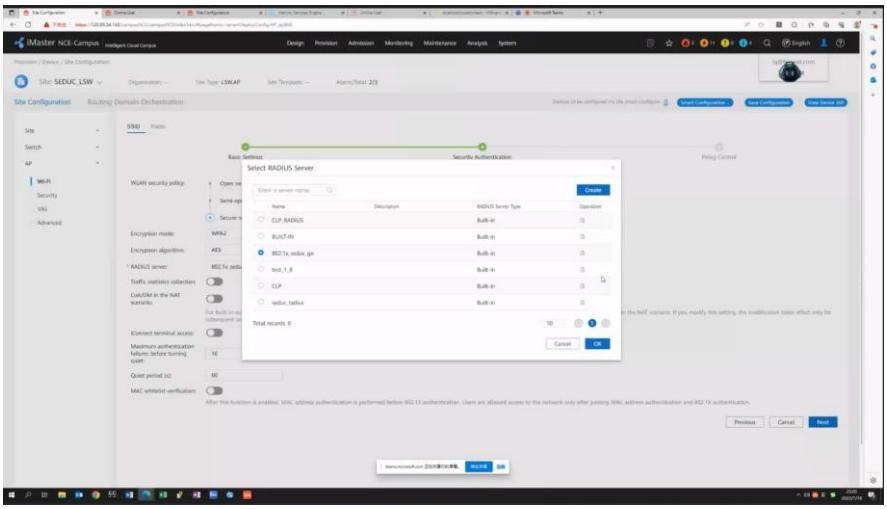


Figura 3 – Dentro do SSID seduc, foi configurado que a VLAN de serviço será a VLAN ID 10.





Figuras 4 e 5 – Novamente, foi e idenciado que a autenticação utilizada neste SSID, será 802.1x e está sendo utilizado um servidor Radius, já configurado na plataforma iMaster NCE Campus.

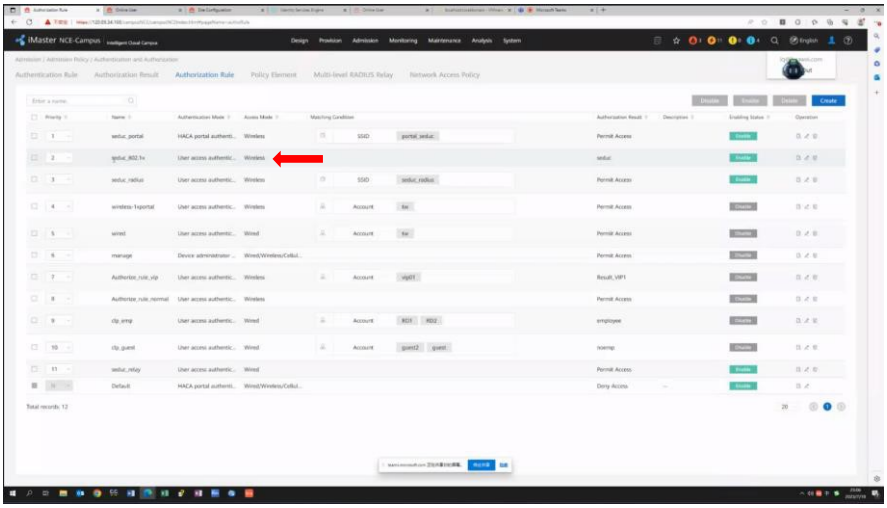
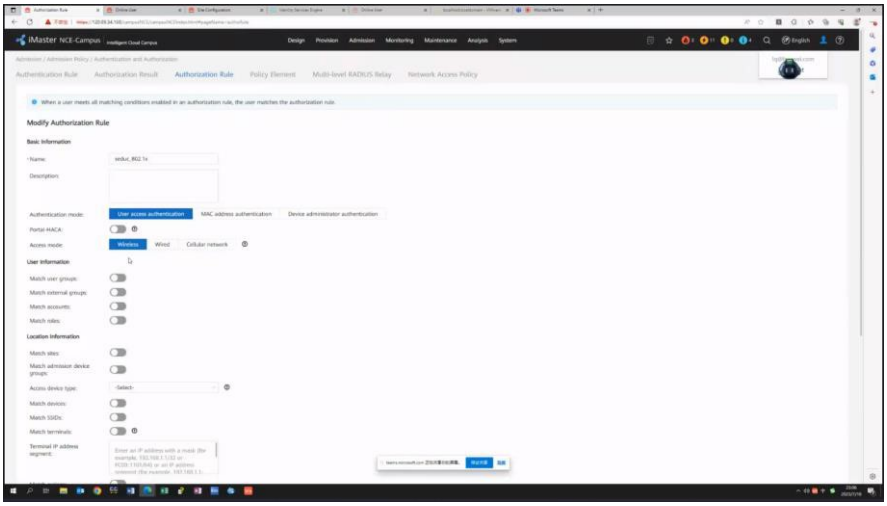


Figura 6 – Nas configurações de AAA, utilizamos a regra “seduc_802.1x”



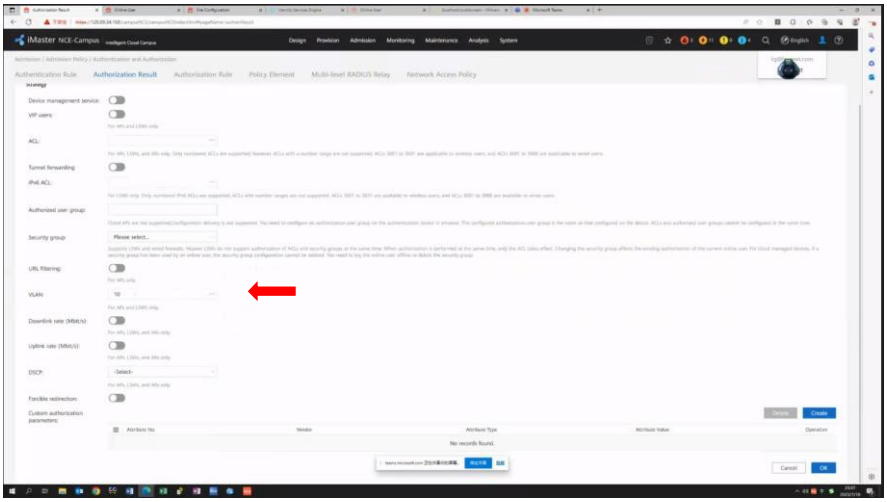


Figura 7 – Na tela de edição da regra, foi configurado a condição de entregar a VLAN 10 aos equipamentos.

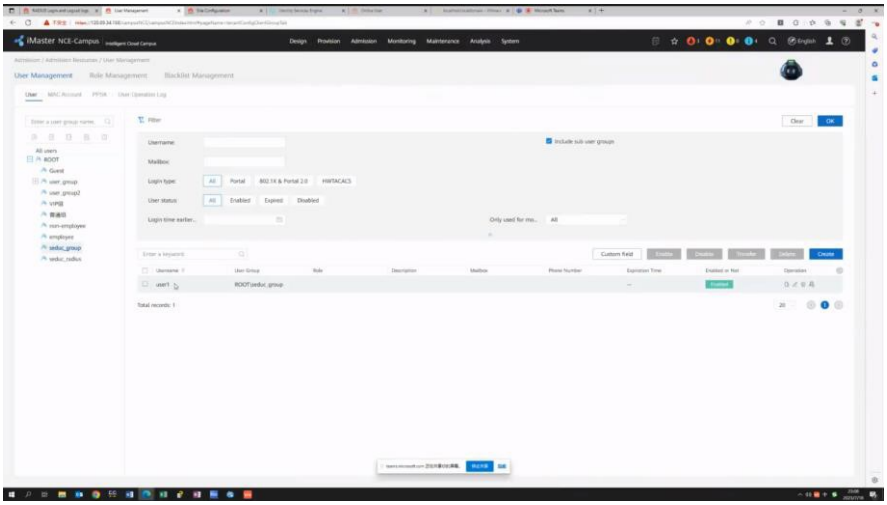
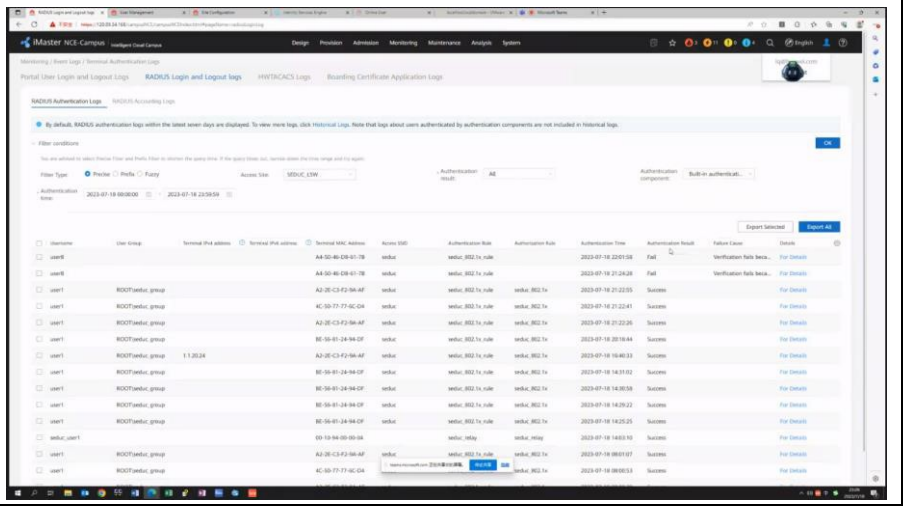
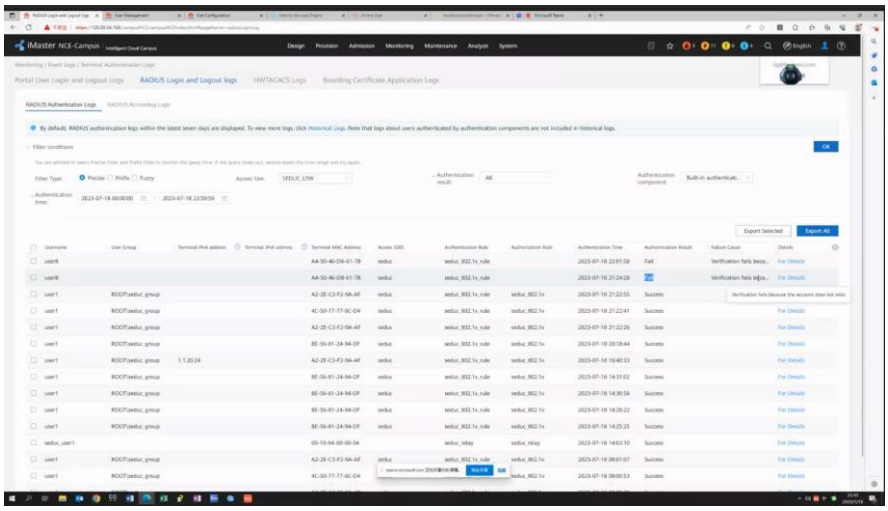


Figura 8 – Na plataforma iMaster NCE Campus, foi criado um grupo de usuários chamado “seduc_group”, e dentro do grupo um usuário chamado “user1”.





Figuras 8 e 9 – Na listagem dos logs de autenticação via RADIUS, evidenciamos testes com o usuário não existente na base, chamado “user8”, com status de falha. Nestes logs, também são mostrados as autenticações realizadas com o usuários “user1”, que está na base de dados.

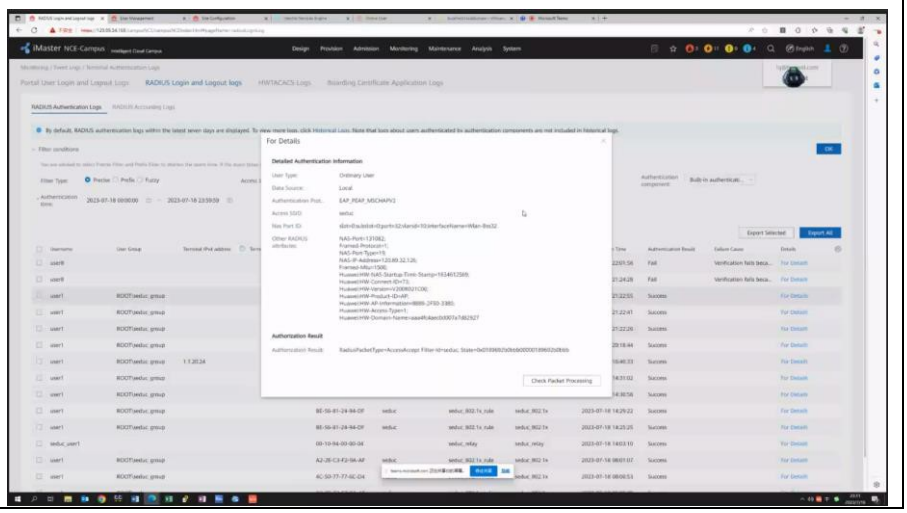


Figura 10 – Nos detalhes do log, podemos ver todo o pacote da autenticação via Radius, e nela são mostradas todas as informações enviadas, dentre elas que a autenticação foi realizada com sucesso e o ID de VLAN numero 10, foi entregue ao dispositivo.

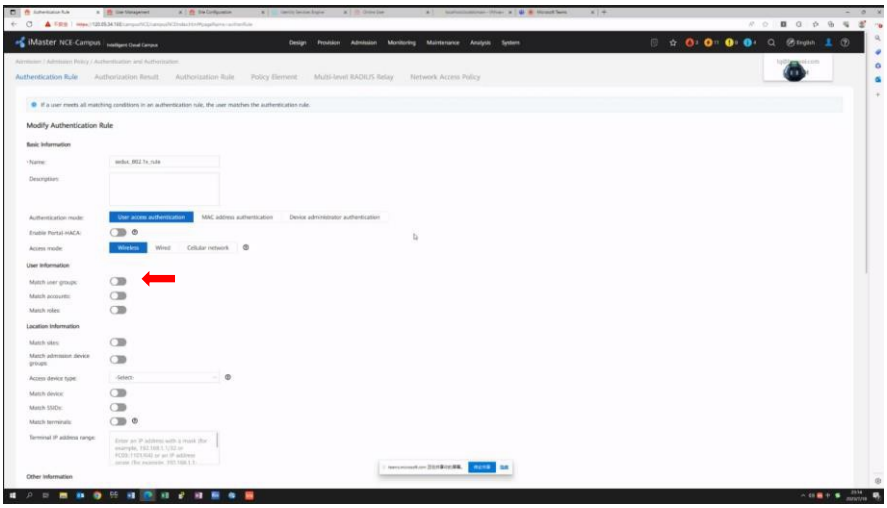


Figura 11 – Retornando a regra, foi evidenciado que não haviam condições especificando o grupo de usuários.

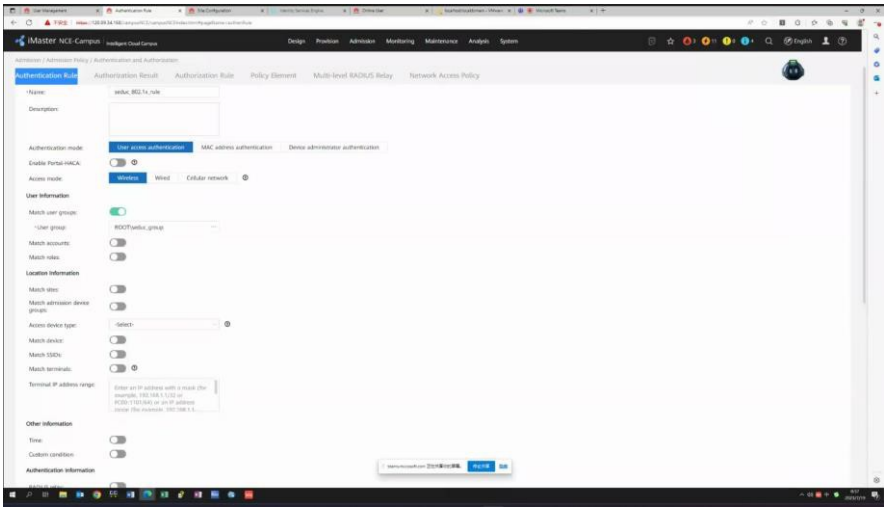
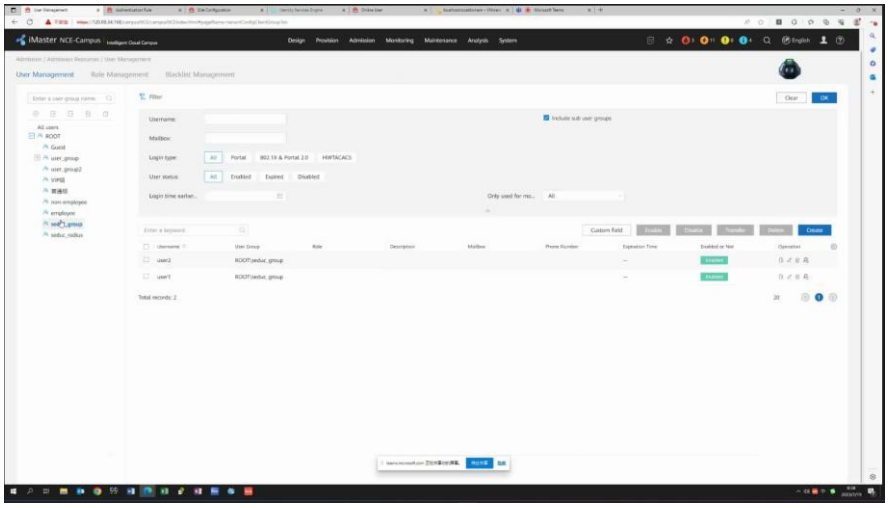
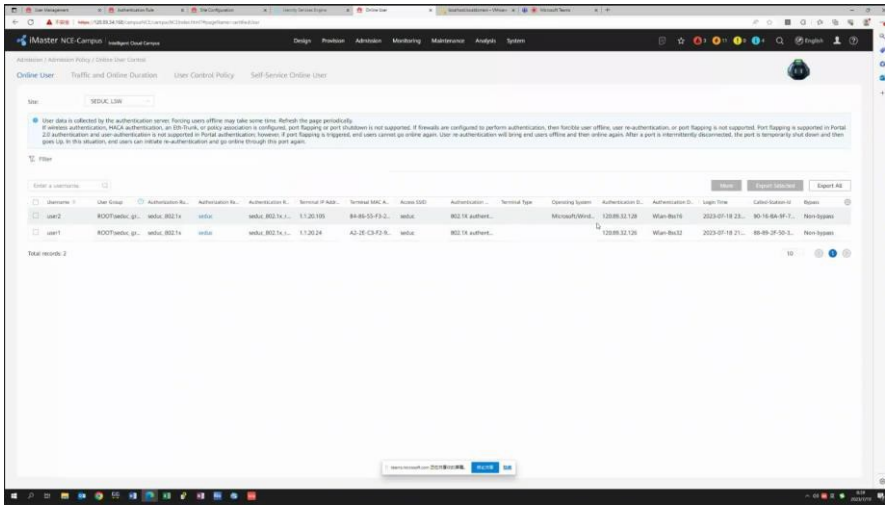


Figura 12 – Em seguida, habilitamos a condição. Onde apenas usuários do grupo “seduc_group”, podem dar “match” nas condições da regra.





Figuras 13 e 14 – Mais um usuário foi criado, “user2”, e foi feita sua autenticação com sucesso.

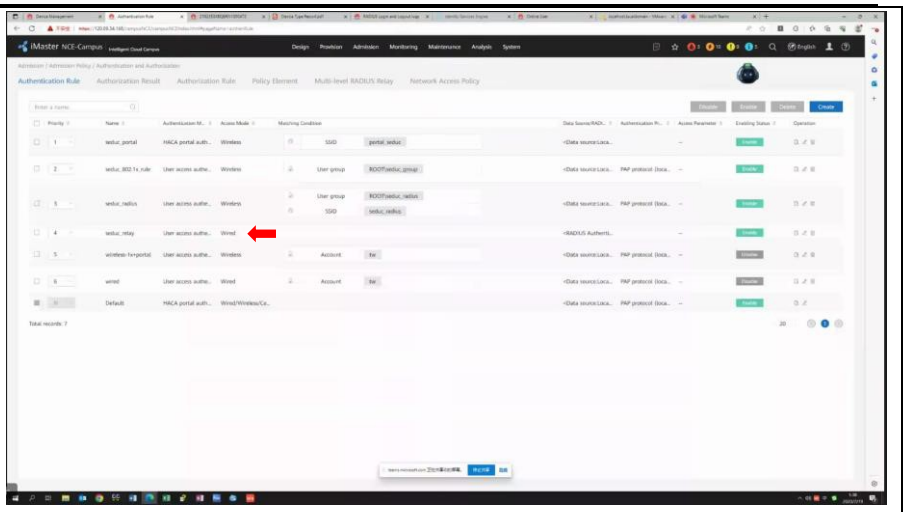


Figura 15 – Novamente, nas configurações de AAA, foi inserida uma nova regra, agora para autenticação 802.1x, em rede cabeada.

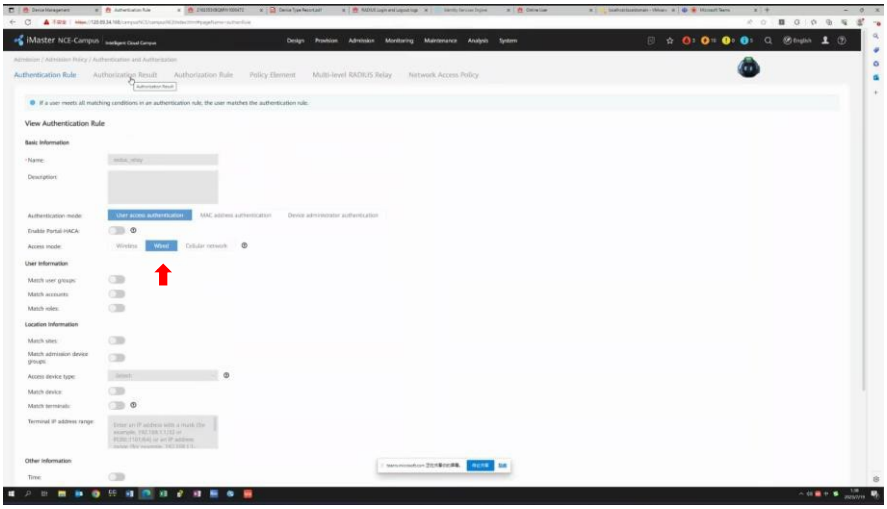
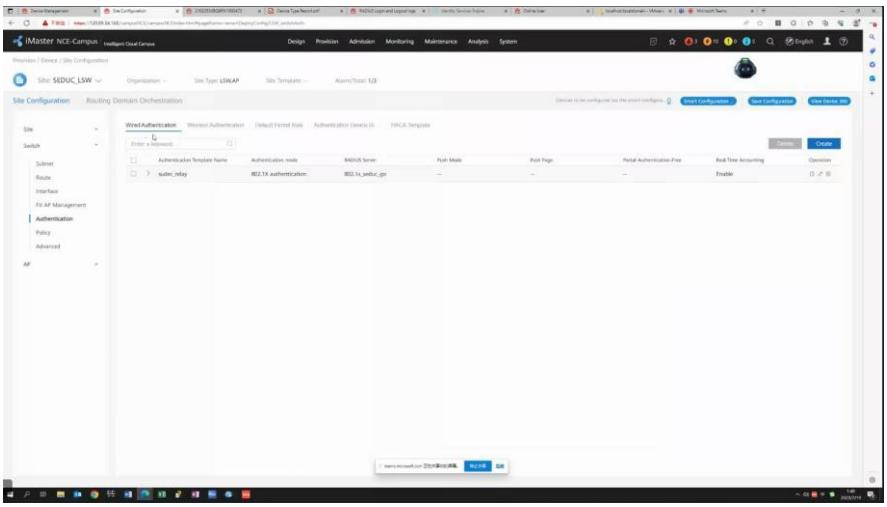
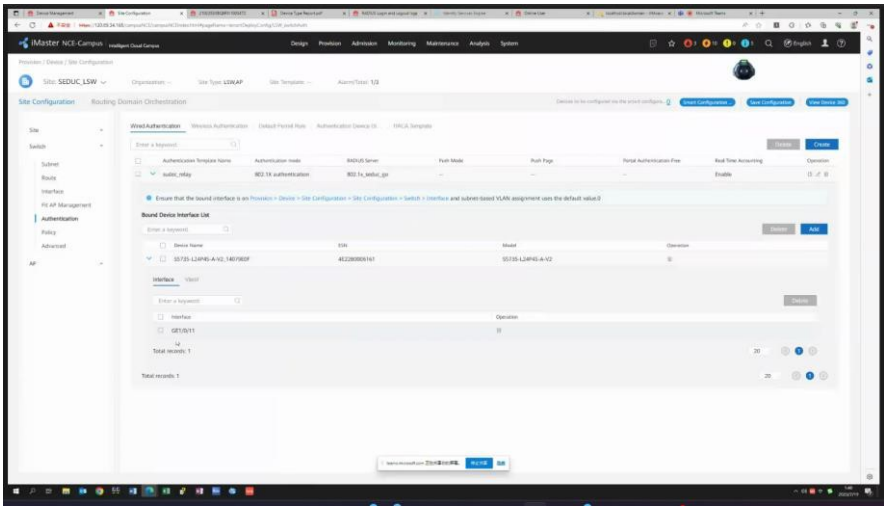


Figura 16 – Na edição da regra, podemos evidenciar o modo de acesso, como “Wired”





Figuras 17 e 18 – Nas configurações de autenticação do switch, associamos o servidor Radius externo e a porta do switch para receber a autenticação.

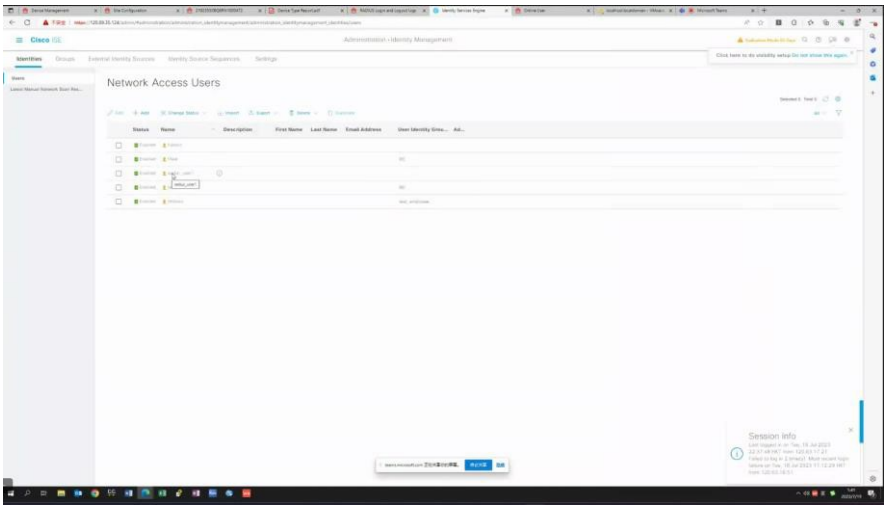
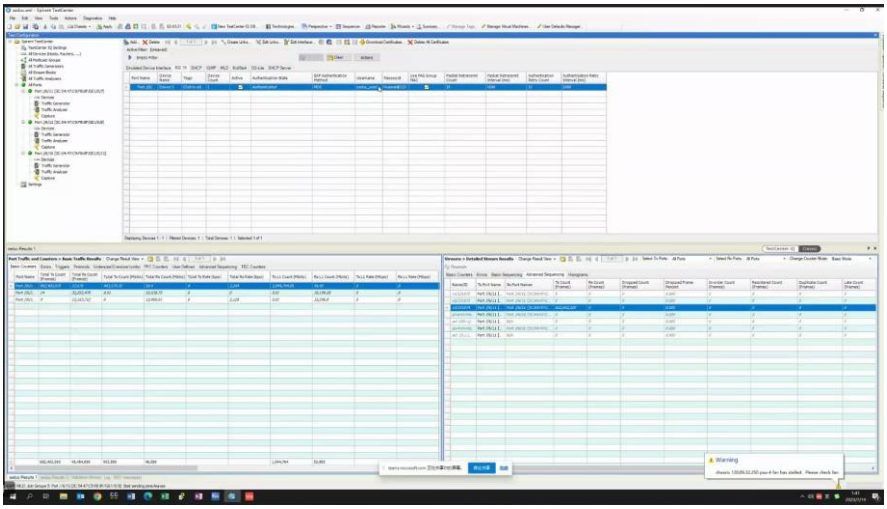
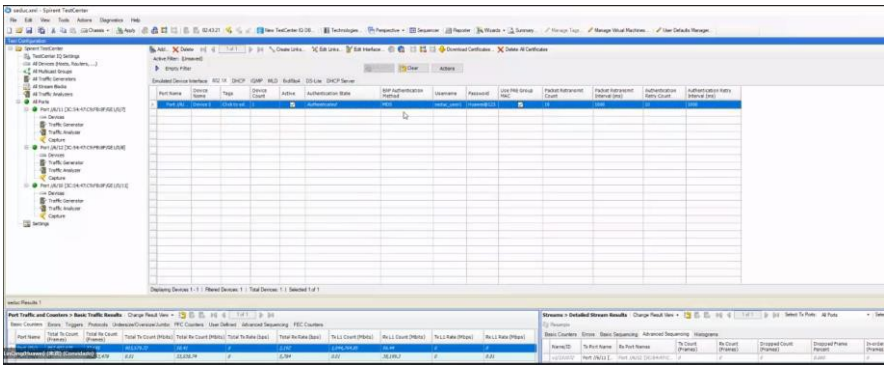


Figura 19 – No servidor de Radius externo, utilizamos o usuário destacado para a autenticação.





Figuras 20 e 21 – No gerador de tráfego, simulamos a autenticação com o usuário criado no servidor de Radius externo. O status da autenticação pode ser visto no gerador, como “authenticated”

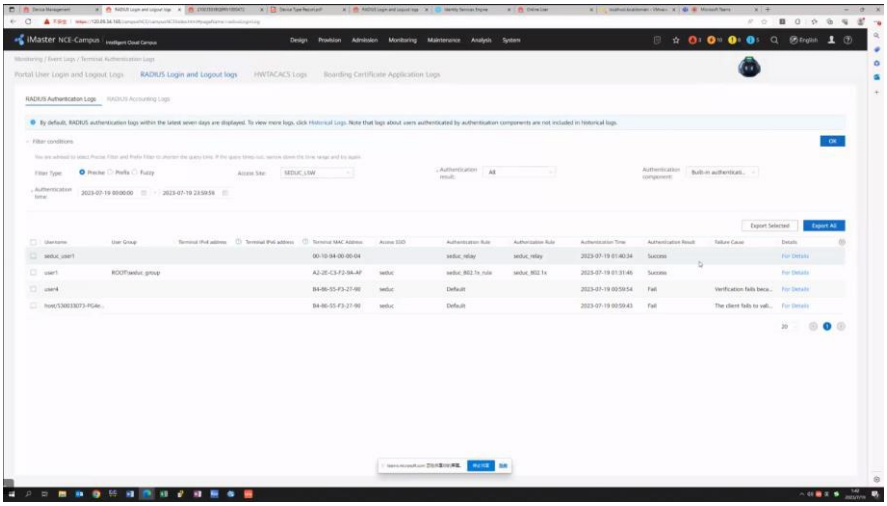


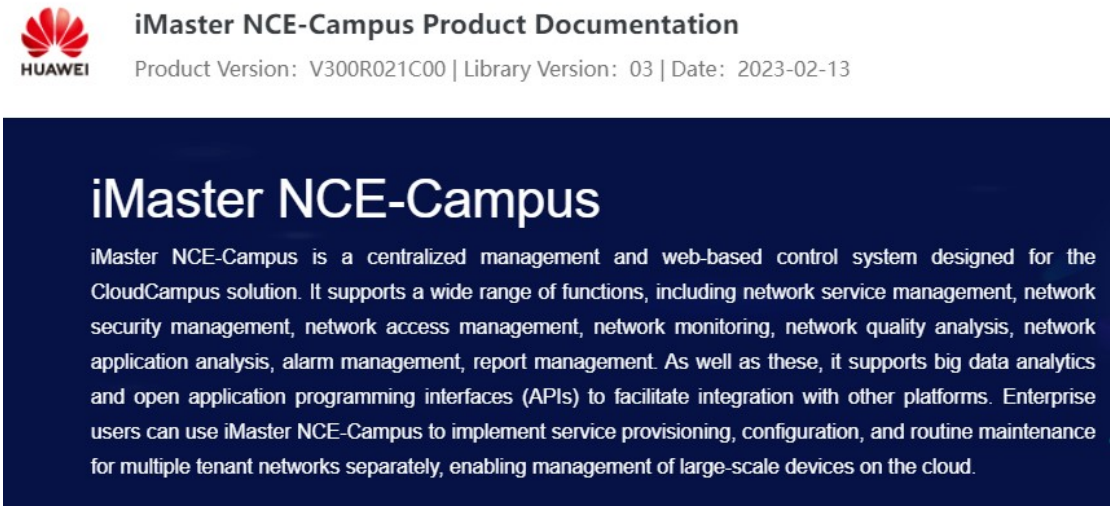
Figura 22 – Nos logs de autenticação da ferramenta iMaster NCE Campus, também foi possível identificar a autenticação realizada com sucesso.

Solução de Gerenciamento e Controle dos APs e Switches

Comprovações sem configuração:

5.10.2 A solução deve ser do mesmo fabricante dos demais itens ofertados no Lote 02;

Comprovação visual - Documentação complementar



5.10.9. A solução deverá ser compatível com VMware 6.7;

https://support.huawei.com/hedex/hdx.do?docid=EDOC1100211132&id=EN-US_TOPIC_0000001089252652

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Configuration Requirements (OS+Product, Virtual Machine)

Software Requirements

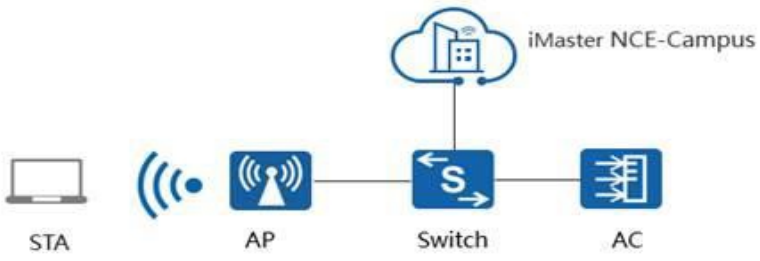
Table 1 Software requirements

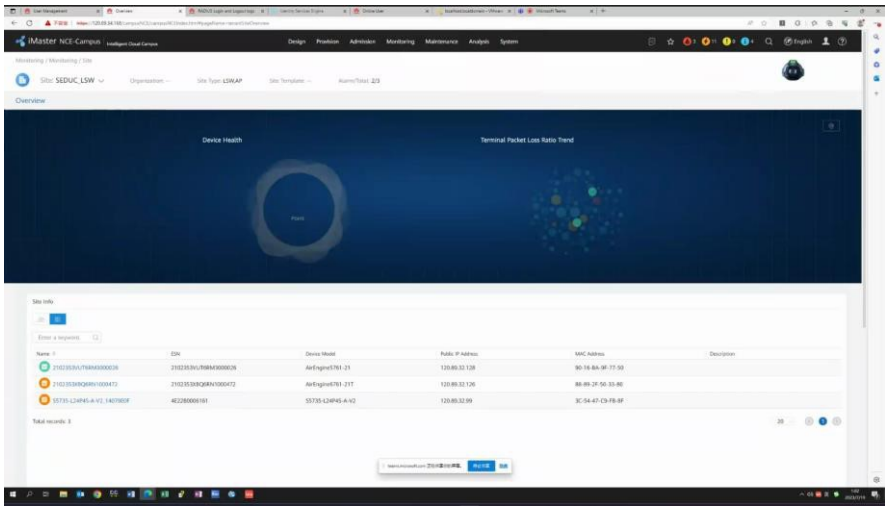
Virtualization Solution	VMWare vSphere 6.5/6.7
Operating System	SUSE Linux Enterprise 12 SP4 (English) SUSE Linux Enterprise 12 SP5 (English)

Comprovações com configurações:

Monitoramento e geração de relatórios

5.10.4 A solução deve ser capaz de centralizar o monitoramento e relatórios de todo o parque de dispositivos, através de console única;
5.10.17 Monitorar o desempenho da rede wireless;

Item de teste	**Monitoramento e geração de relatórios e desempenho da rede**
Objetivo do teste	**A solução deve ser capaz de centralizar o monitoramento e relatórios de todo o parque de dispositivos, através de console única.**
Configuração de teste	Topologia da rede: 

	Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Exibir as dashboards disponiveis na ferramenta
Resultado esperado	1) Monitorar todo o parque de dispositivos, através de console única; 2) Gerar relatórios de todo o parque de dispositivos, através de console única;
Resultado	 Figura 1 – Na ferramenta iMaster NCE Campus, foram exibidas de forma geral as informações dos dispositivos.

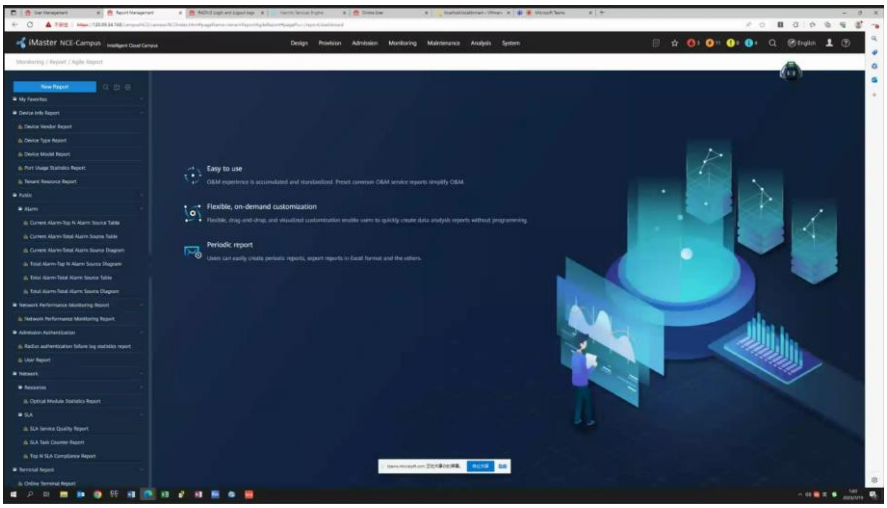


Figura 2 – Foi evidenciado também toda a gama de opções de relatórios e dashboards, disponiveis para a visualização.

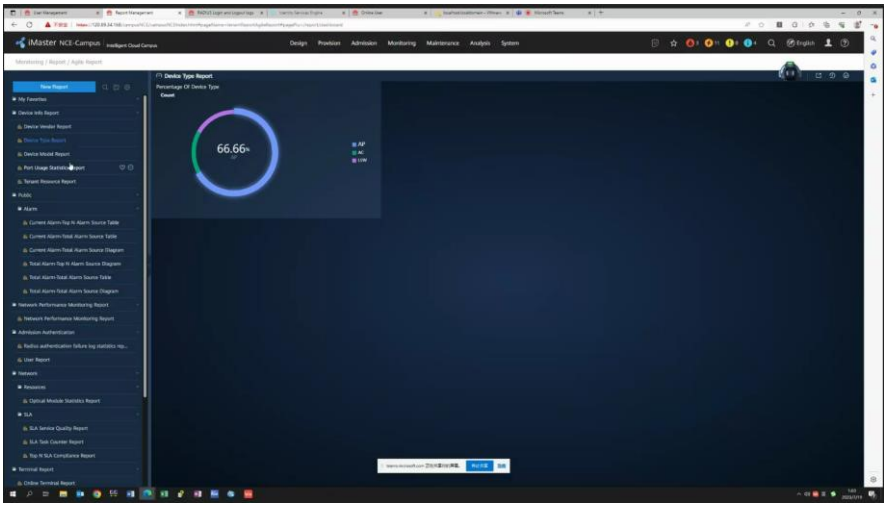
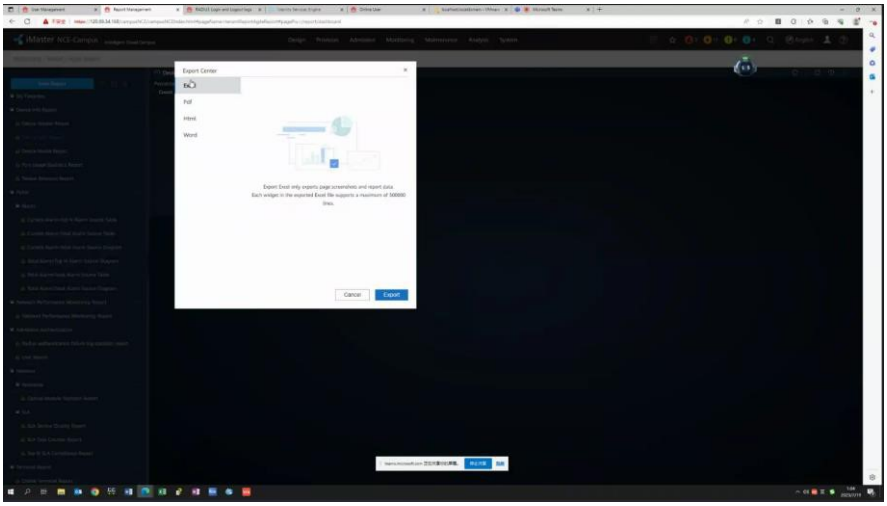
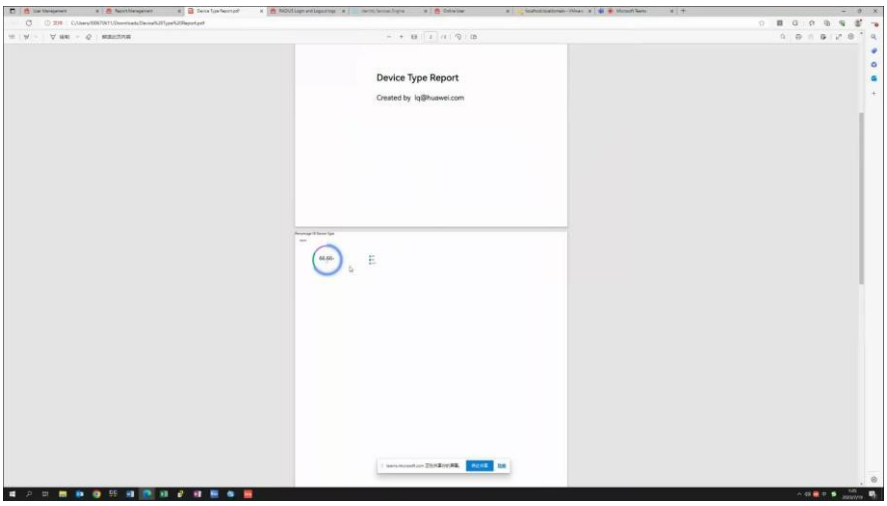
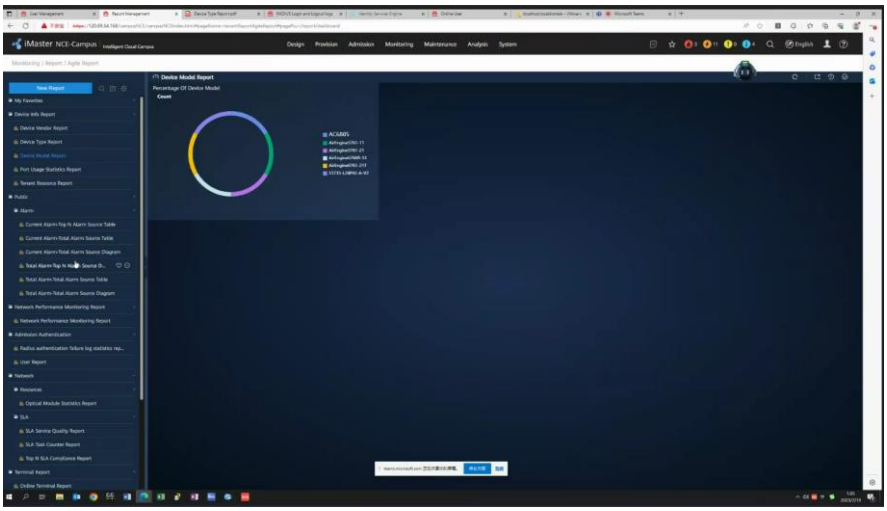


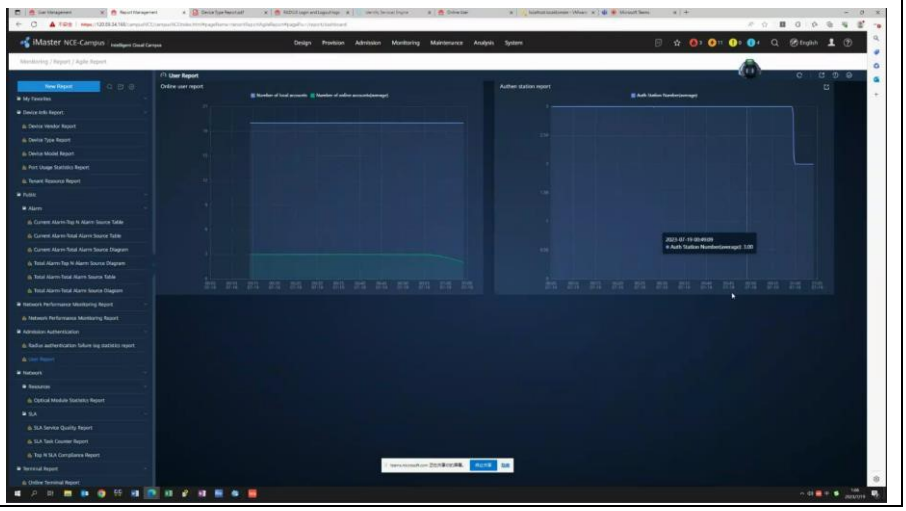
Figura 3 – Das opções disponiveis, foi exibido o relatorio que mostra a porcentagem de equipamentos, por dispositivo.

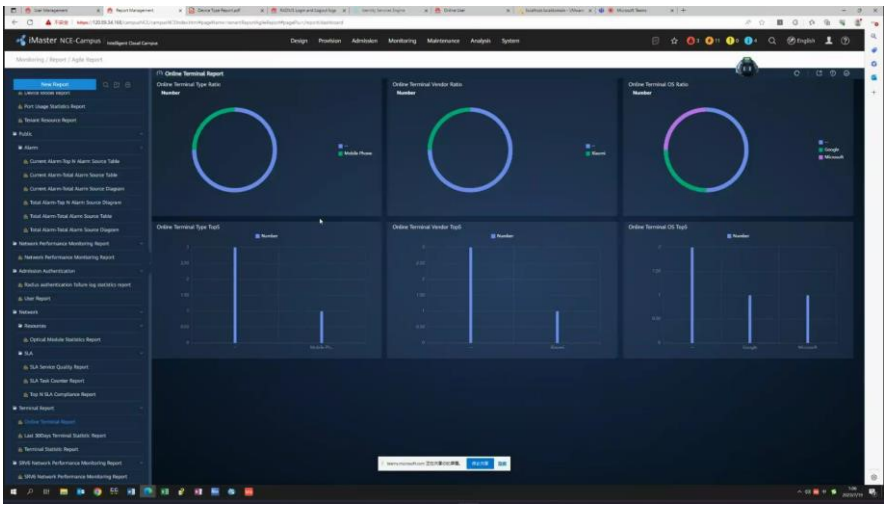


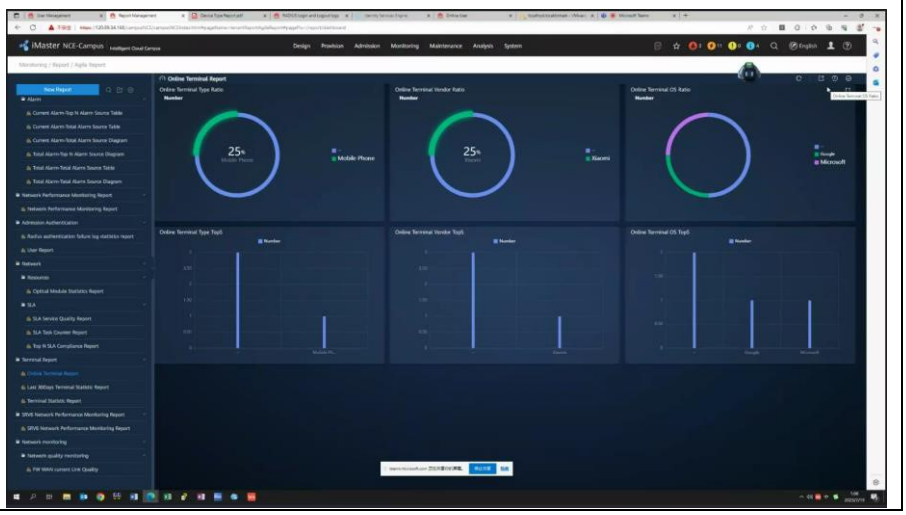


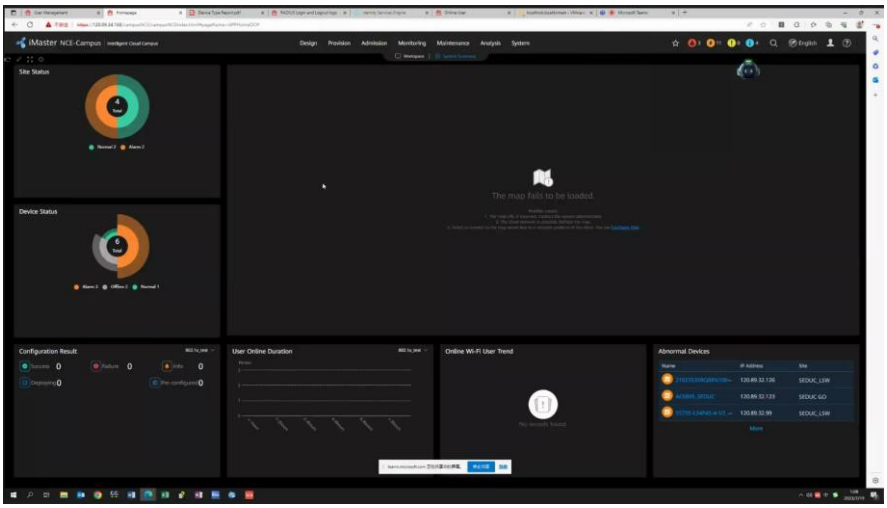
Figuras 4 e 5 – O mesmo relatório visto graficamente, também pode ser exportado para um relatório em arquivo PDF.



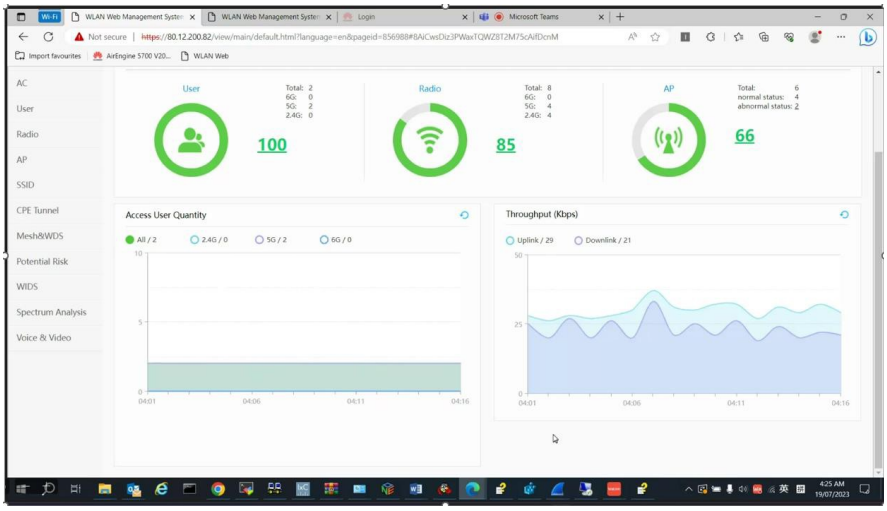




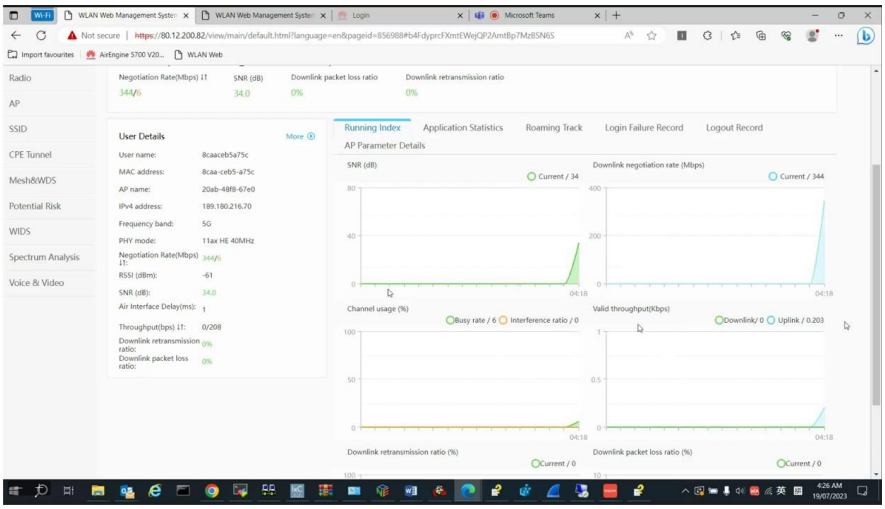


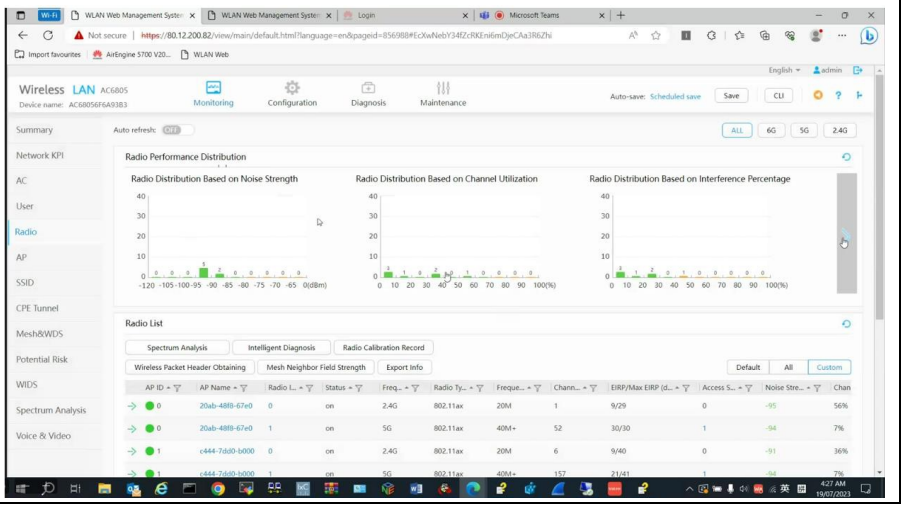


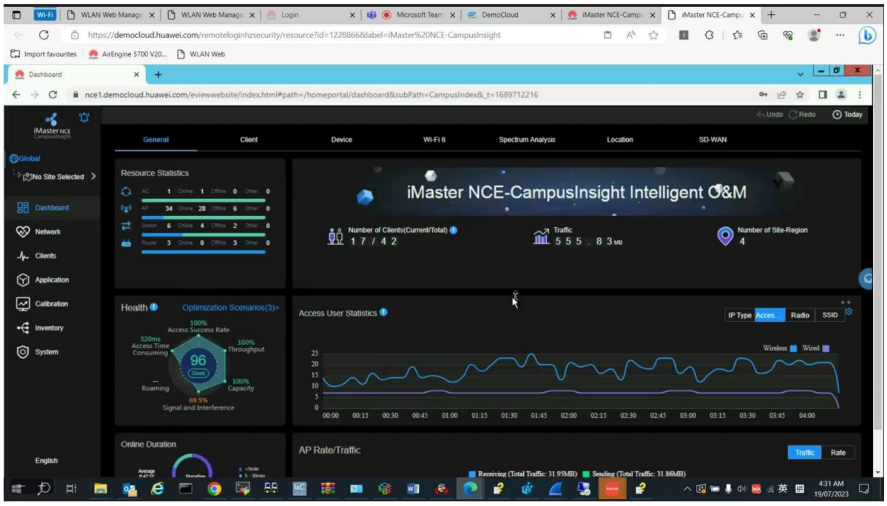
Figuras 6 a 10 – Exibição de várias opções de relatorios disponiveis na ferramenta.



PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES





	 Figura 11 a 14 – Na controladora e na plataforma de gerenciamento, foi possível validar de várias maneiras, a saúde e desempenho da rede.

Gerenciamento de permissões e domínio

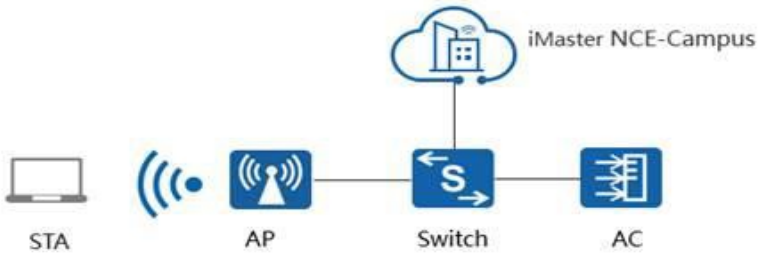
5.10.15 Permitir a customização do a acesso administrativo através de atribuição de grupo de função do usuário administrador.

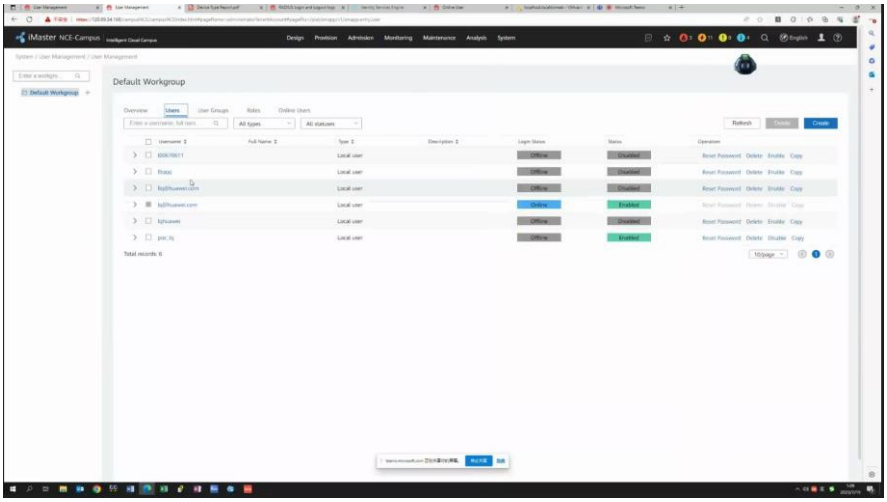
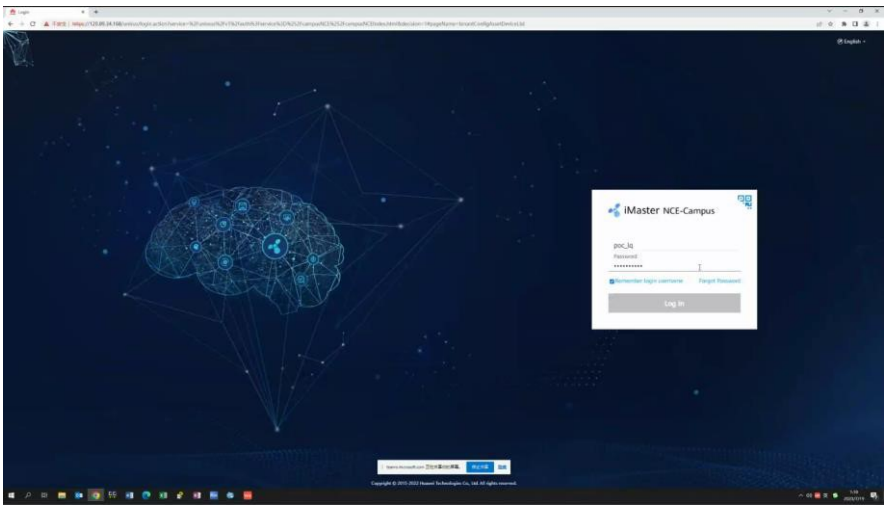
5.10.27 Implementar controle de a acesso de usuário administrativo por HTTPS. Deve ainda implementar perfis de a acesso diferenciados por usuário ou grupo de usuários;

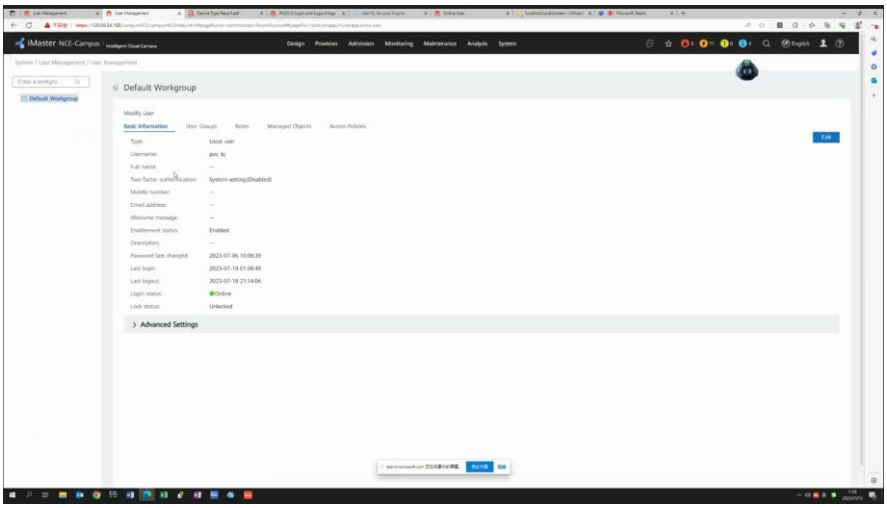
5.10.28 Gerenciar de forma centralizada a autenticação de usuários;

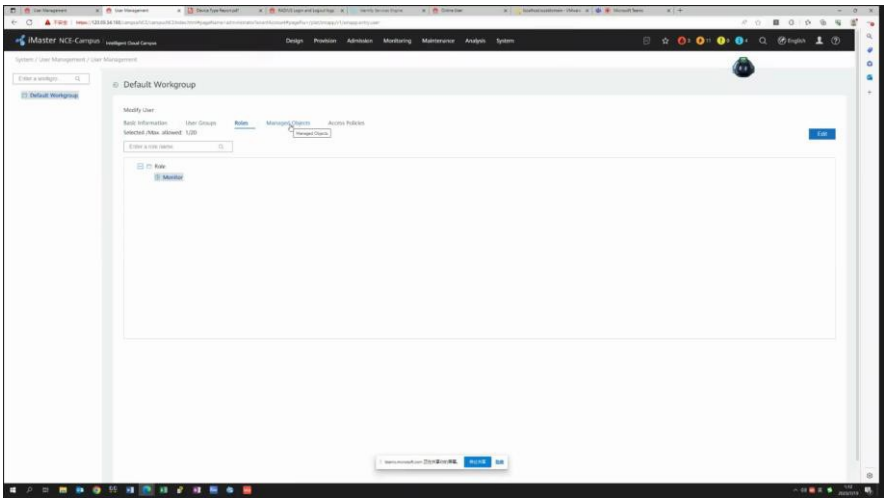
Item de teste	**Gerenciamento de permissões e domínio**
Objetivo do teste	Permite a administração de acessos baseado em atribuição de grupos de usuários administradores

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Adicionar usuários administrativos a ferramenta, e atribuir suas permissões.
Resultado esperado	1) Usuários adicionados, com opções de customização de permissões e objetos/sites utilizados.

Resultado	 Figura 1 – Na base de dados da ferramenta iMaster NCE Campus, foi evidenciado os usuários criados.  Figura 2 – Utilizamos o usuário “poc_lq”, para efetuar o login administrativo ao sistema.





Figuras 3 e 4 – Dentro da ferramenta é possível validar o status do usuário, e editar permissões como nivel de administração e quais os objetos serão gerenciados por ele.

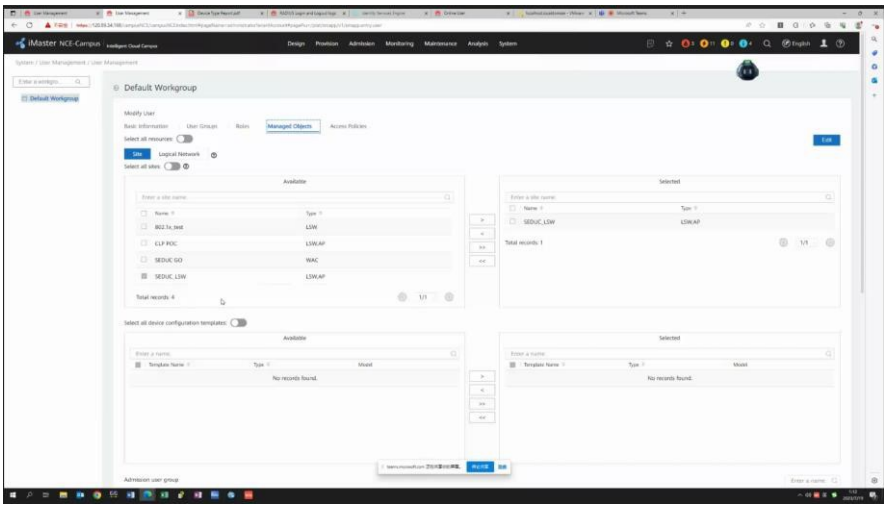
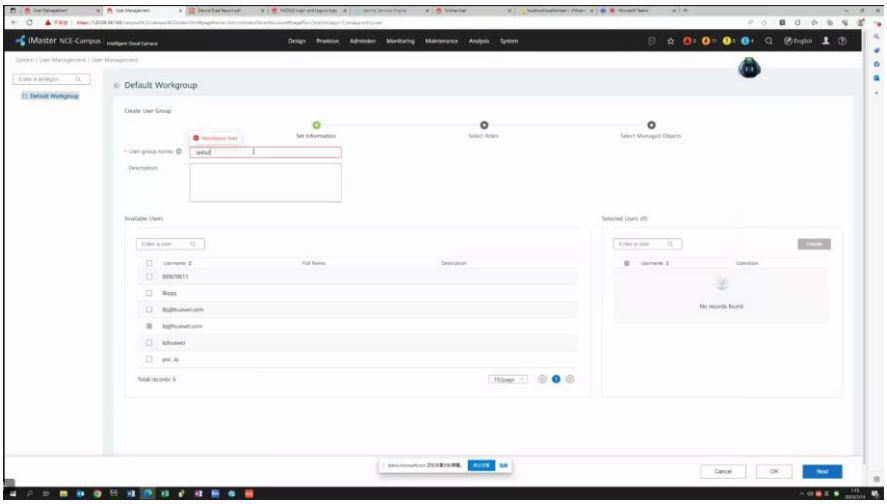
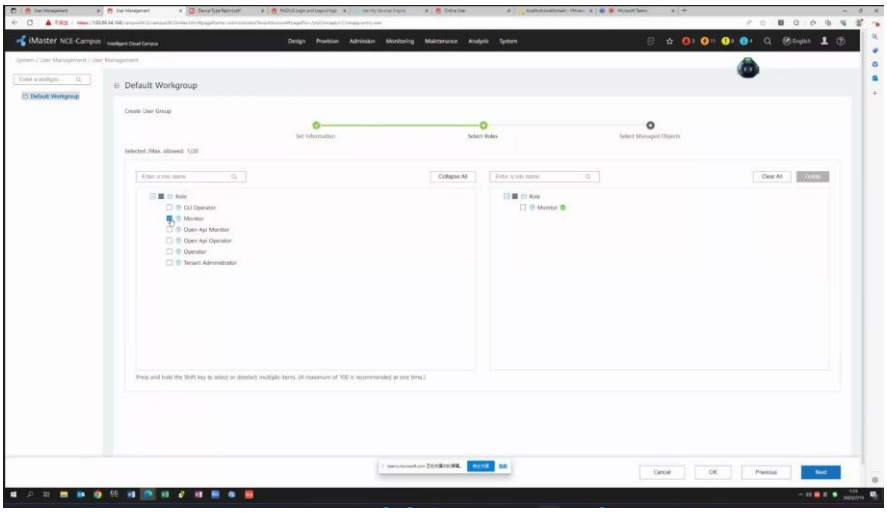
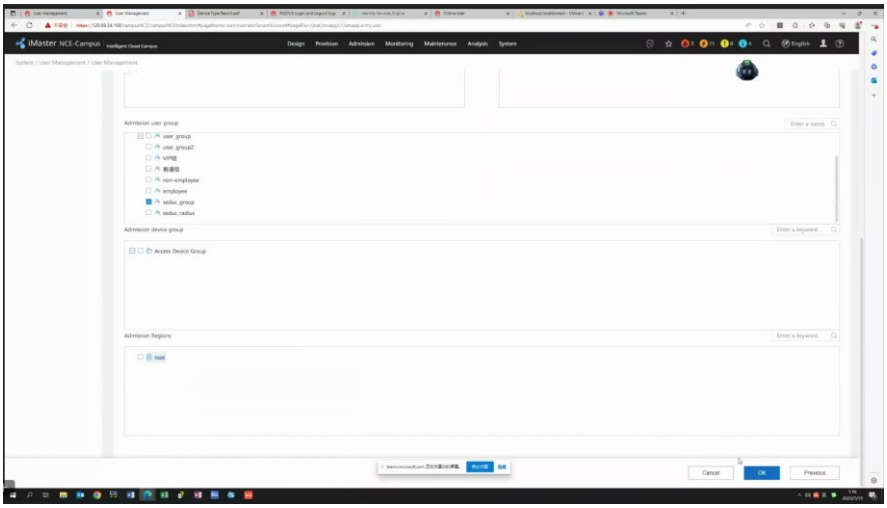


Figura 5 – Nas edições do usuário, os objetos gerenciados, podem ser incluidos ao usuário de forma categorizada por site (ou localidade).





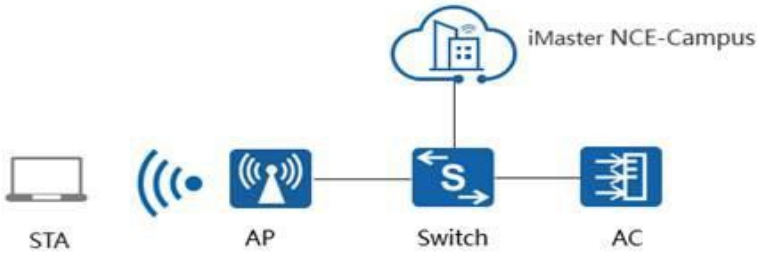


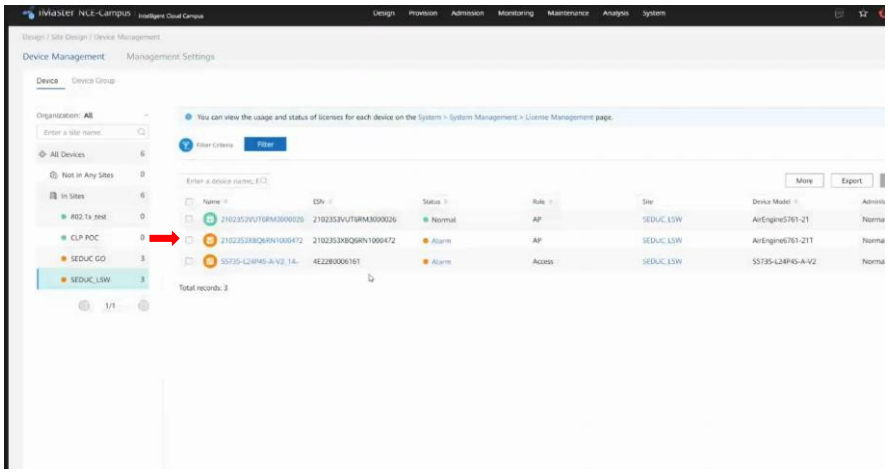
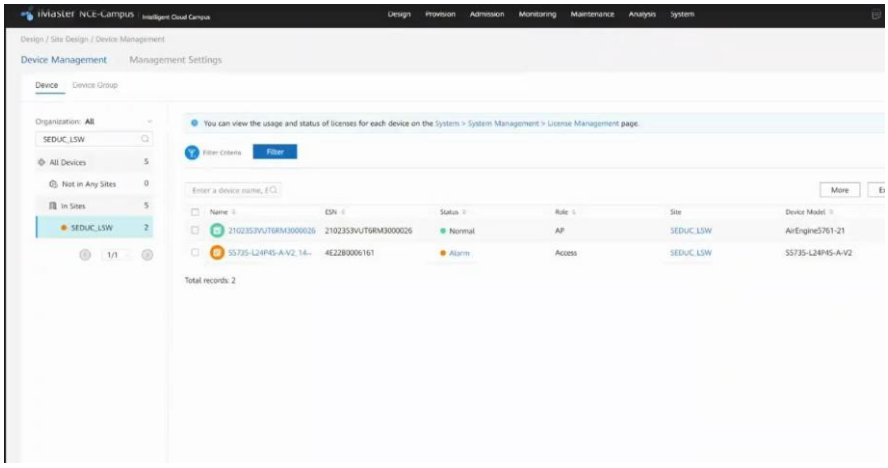
Figuras 6 a 8 – Os usuários administrativos, também podem ser organizados através de grupos de trabalho (workgroups), onde as permissões podem ser editadas a nivel do grupo como um todo.

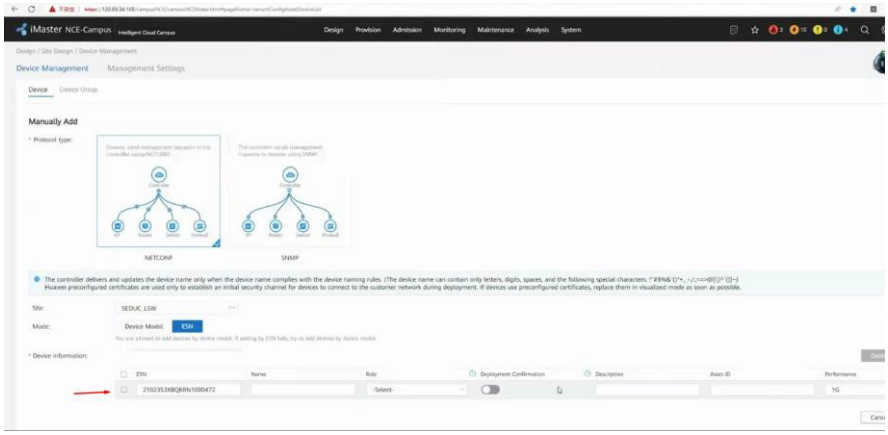
	Essas permissões, podem ser de nivel de configuração dos equipamentos, visualização dos recursos, criar novos usuários ou grupos e etc.

Restauração de configurações de provisionamento

5.10.25 Deverá ser capaz de provisionar remotamente novos dispositivos em estado padrão de fábrica para estado totalmente provisionado;

Item de teste	**Restauração de configurações de provisionamento**
Objetivo do teste	Deve ser capaz de provisionar novos dispositivos em estado de padrão de fábrica para estado totalmente provisionado
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente

	2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Provisionar novos equipamentos e restaurar as configurações de fábrica dos dispositivos já gerenciados
Resultado esperado	1) Novos dispositivos em estado padrão de fábrica são remotamente provisionados para um estado totalmente provisionado
Resultado	 

	Figuras 1 e 2 – Na ferramenta iMaster NCE Campus, foi identificado todos os equipamentos gerenciados, operando de formal normal. Em seguida, foi efetuado um reset no equipamento, para as configurações padrão de fábrica e em seguida, removido da lista de equipamentos gerenciados.  Figura 3 – Em seguida, novamente esse equipamento foi adicionado a ferramenta, inserindo apenas seu ESN (numero de série), para ser gerenciado.

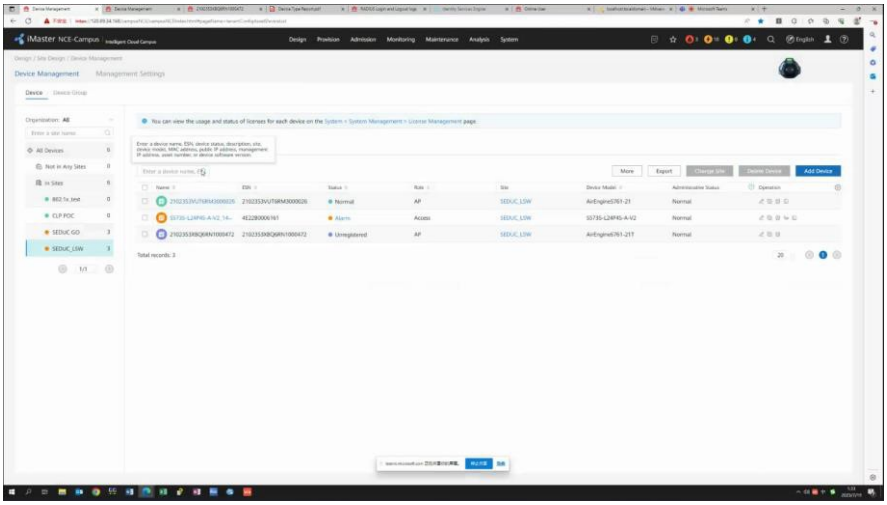
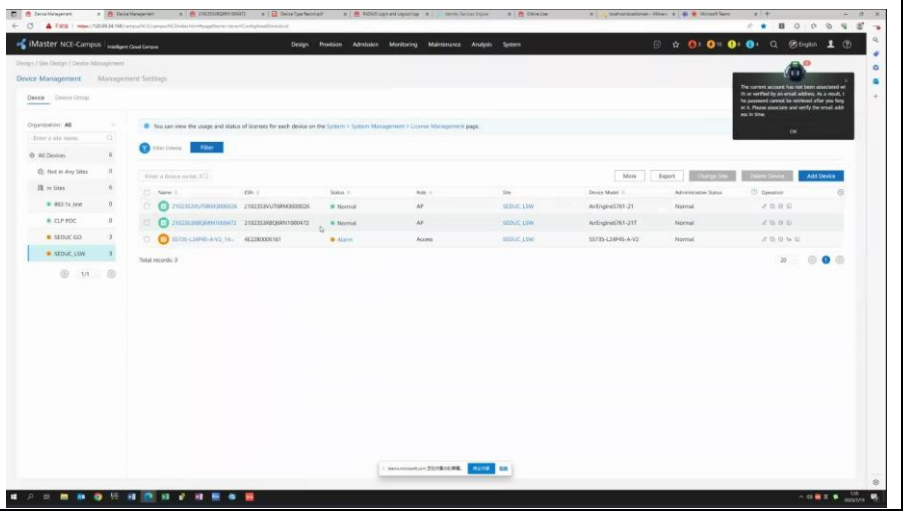
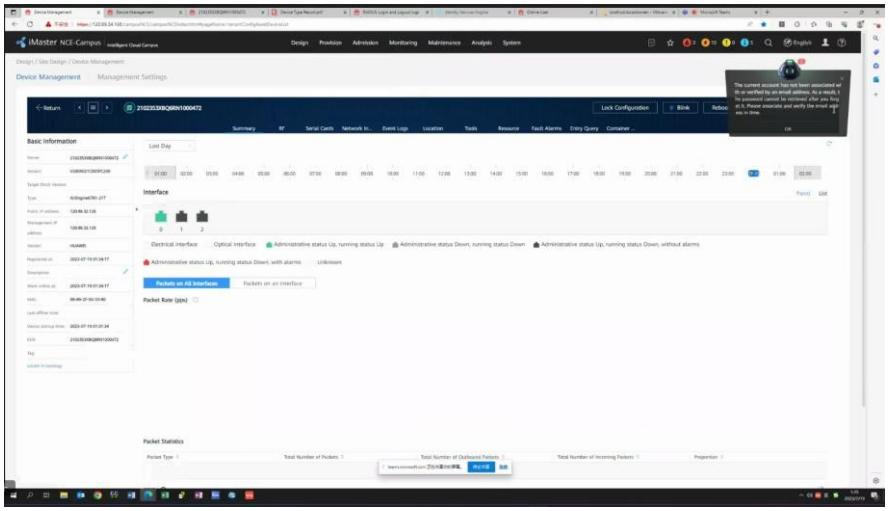


Figura 4 – Feita a adição do equipamento, como ele está em estado padrão de fábrica, o seu status aparece como “unregistred”, ou seja, ele nunca foi gerenciado pela ferramenta e não possui configuração alguma.

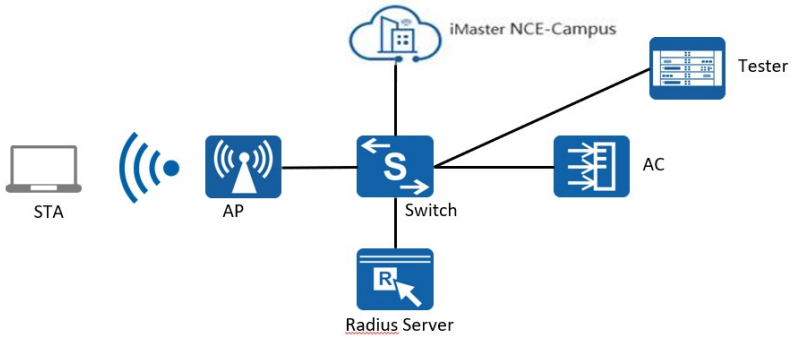


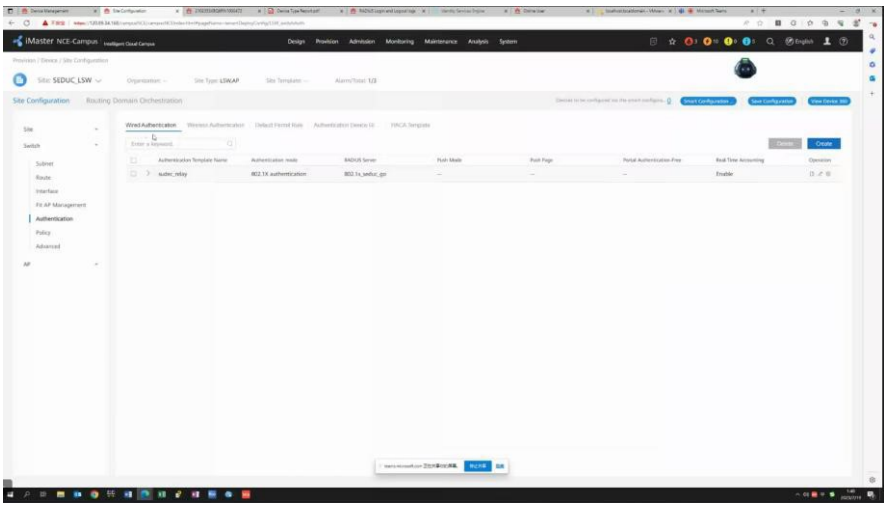
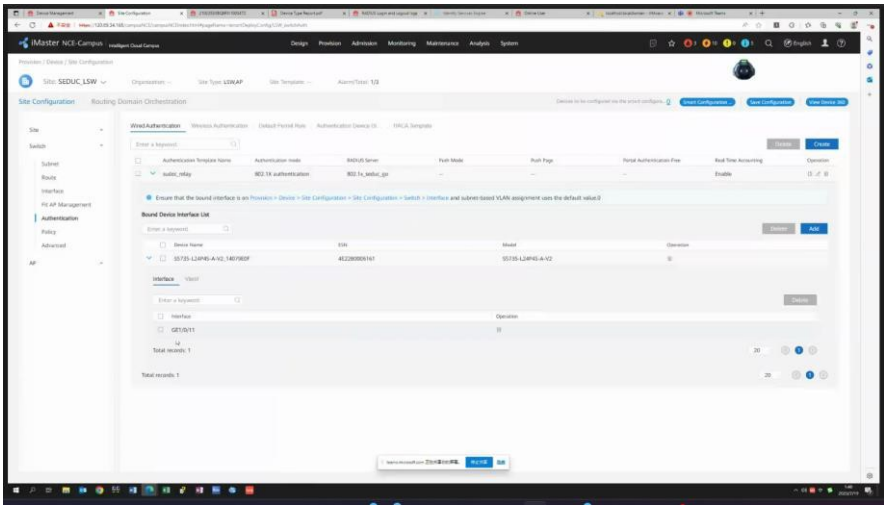
	 Figuras 5 e 6 – Alguns poucos minutos depois, o equipamento está com o status “normal” e gerenciado pela ferramenta.

Radius relay

5.10.32 Implementar Radius relay, de forma a permitir integração com servidor Radius externos;

Item de teste	**Radius relay**
Objetivo do teste	Implementar Radius relay, a fim de permitir a integração com servidores RADIUS externos;
Configuração de teste	Topologia da rede:

	 Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Selecione “Designn > Network Design > Template Management” a partir do menu principal. Clique em criar.Resultado esperado 1 é obtido.
Resultado esperado	1) Servidor RADIUS relay created com sucesso

Resultado	 Figura 1 – Nas configurações do switch, através da plataforma iMaster NCE Campus, foi atrelado um servidor de Radius (externo), para a autenticação de usuários na rede cabeada.  Figura 2 – Em seguida, foi feita associação da interface GE1/0/11, ao servidor.

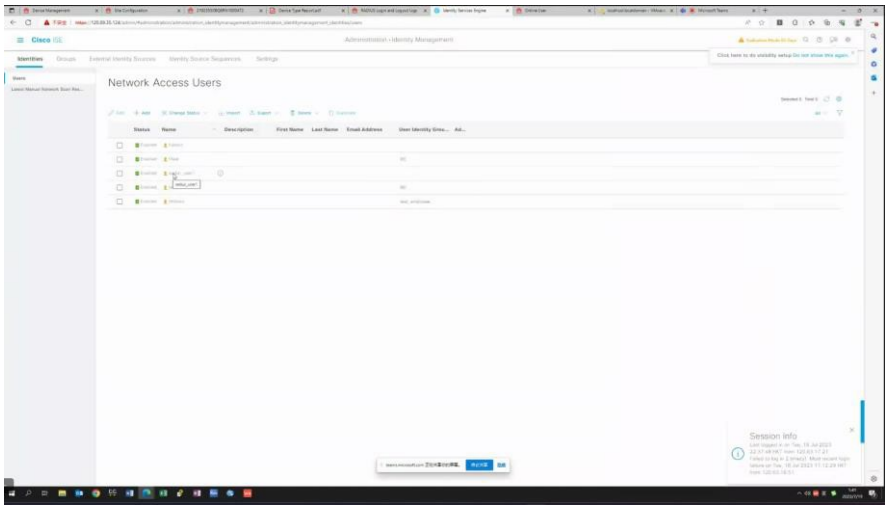
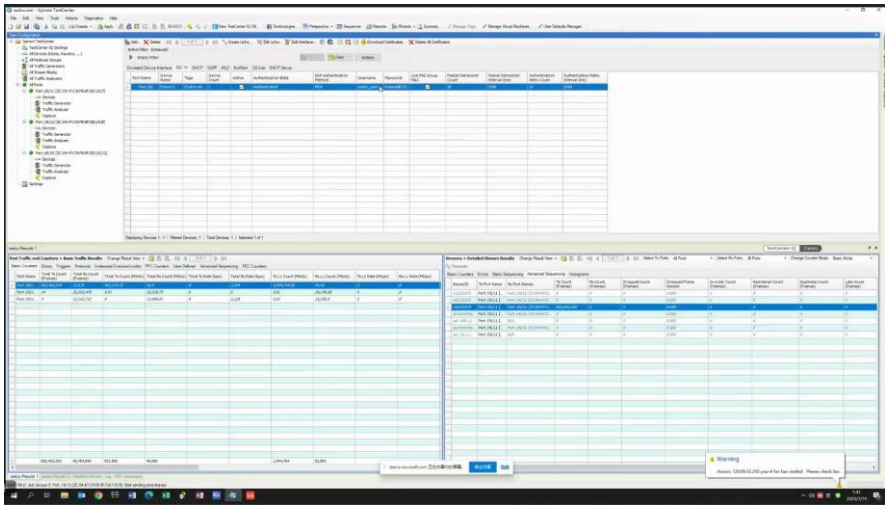


Figura 3 – No servidor de Radius (nos testes, utilizamos o software Cisco ISE), foi criado o usuário seduc_user1.



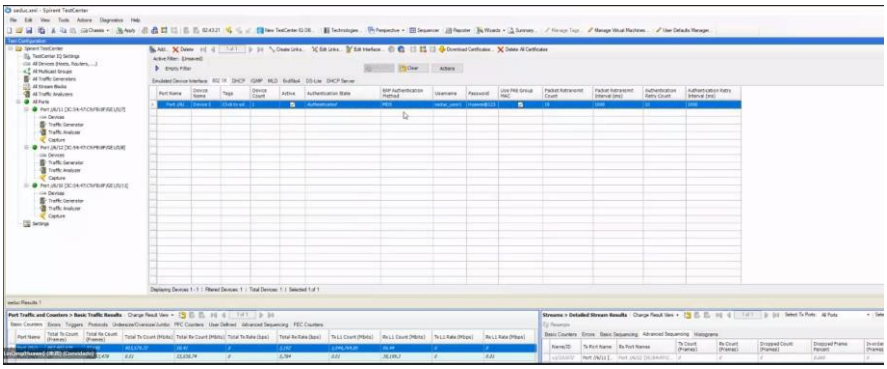


Figura 4 e 5 – Com o auxilio de um gerador de tráfego, foi simulada uma autenticação, utilizando o mesmo usuário criado no passo anterior.

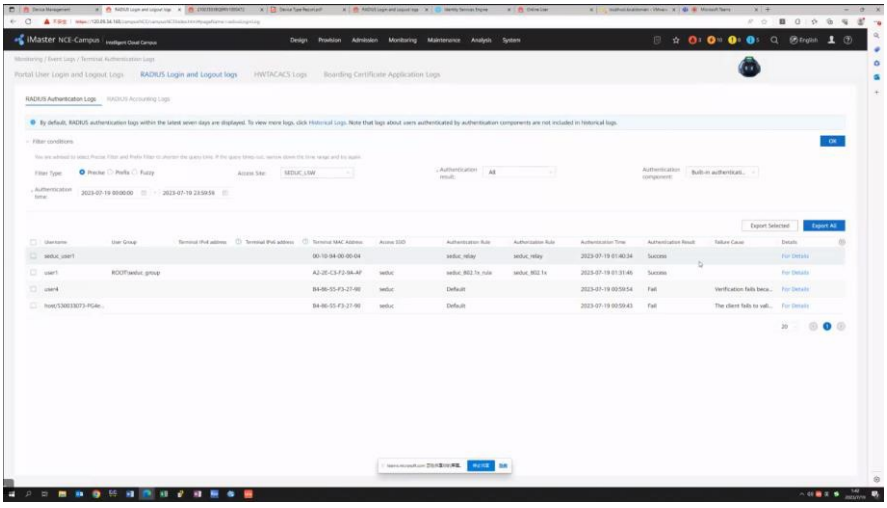
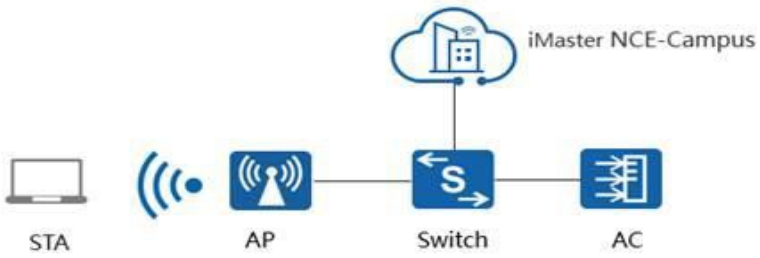


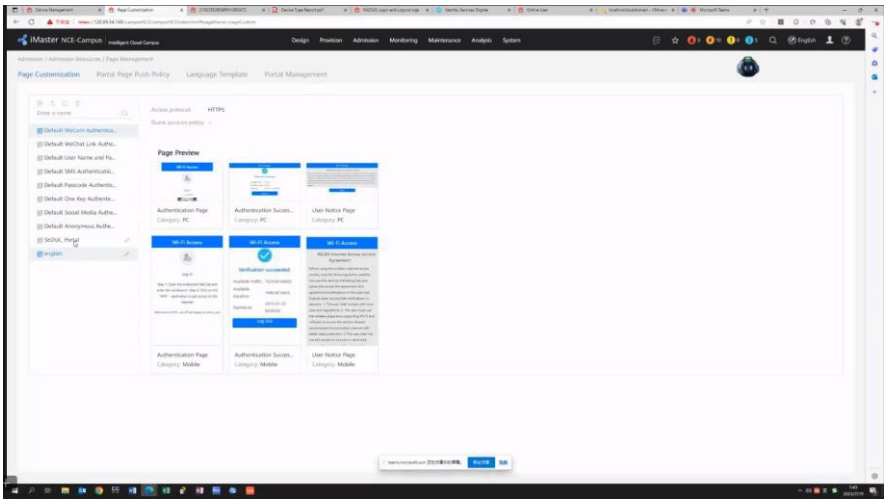
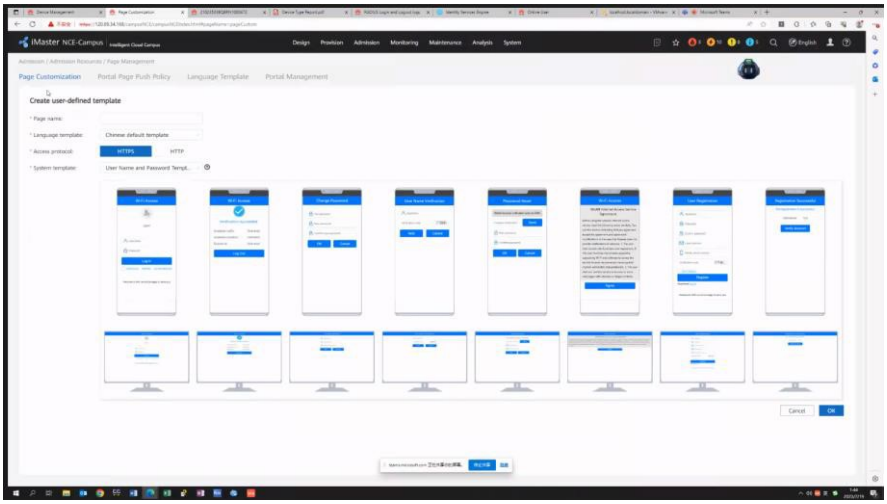
Figura 6 – Na plataforma iMaster NCE Campus, conseguimos listar os usuários conectados e autenticados via 802.1x. O usuário em destaque é o mesmo utilizado, com o nome seduc_user1.

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Permitir autenticação de usuário em página customizada

5.10.33 Permitir a customização de página de autenticação de usuários, com inclusão de textos e logotipo;

Item de teste	Permitir autenticação de usuário via portal customizado (5.10.33)
Objetivo do teste	Permitir a customização da página de autenticação do usuário, com inclusão de texto e logo;
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Customizar as páginas utilizadas para autenticação

Resultado esperado	**1) Permitir a customização da página de autenticação do usuário, com inclusão de texto e logo;**
Resultado	 Figura 1 – Foi evidenciada a possibilidade de criação e edição das páginas web utilizadas nas autenticações.  Figura 2 – Criação de templates de página

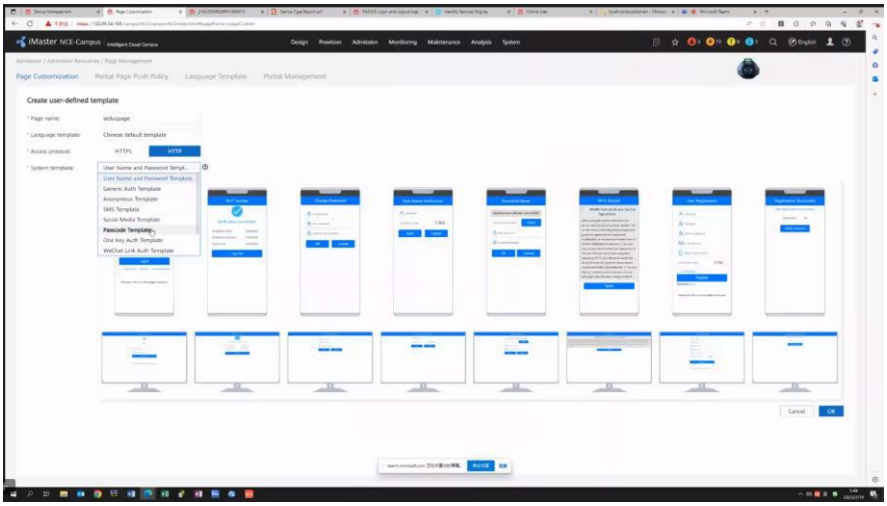
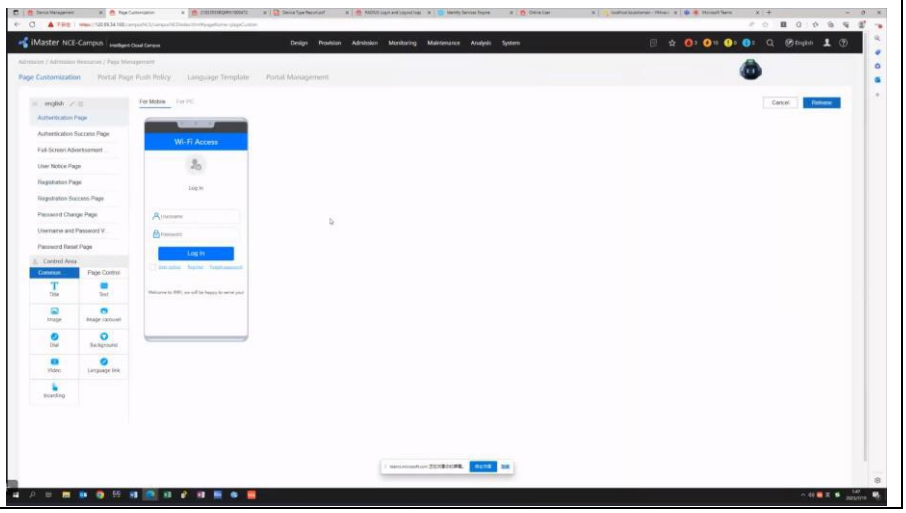
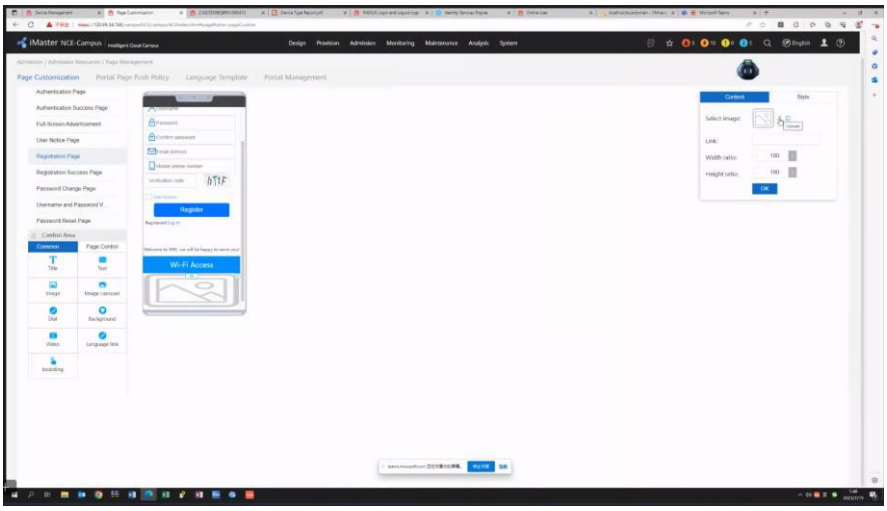
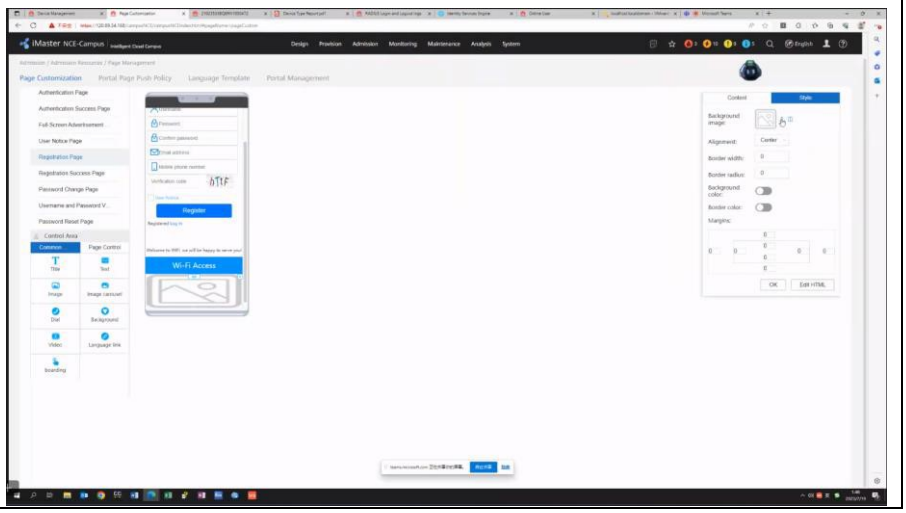
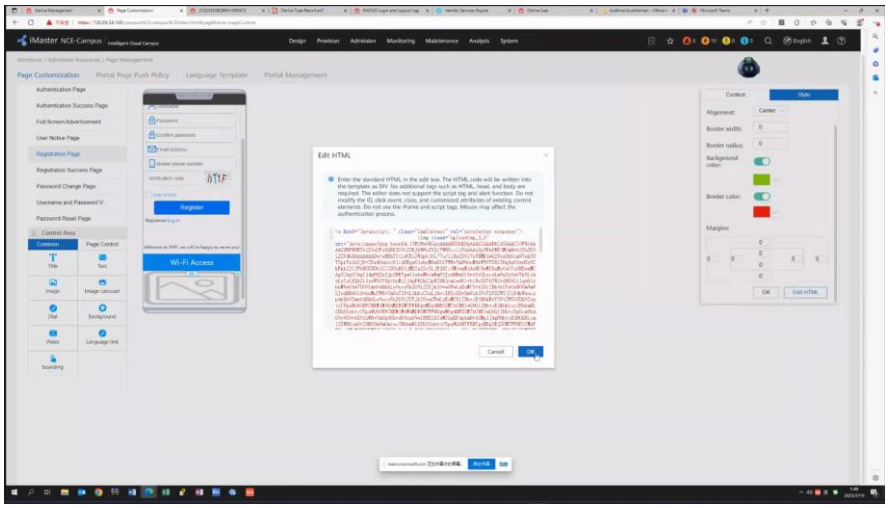


Figura 3 – Customização do template, com o uso de senha, redes sociais, SMS e etc.





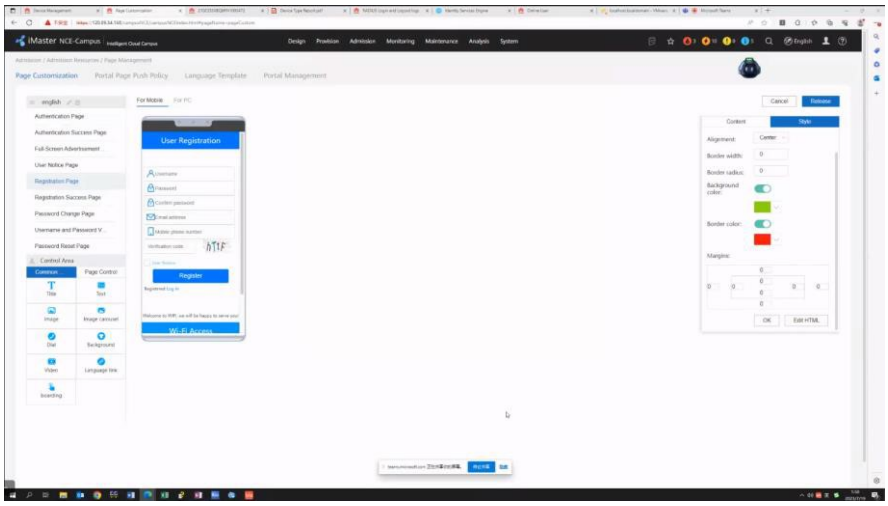


Figura 4 a 8 – Customizações de texto, logotipo, HTML e etc também foram evidenciadas.

Identificar usuários conectados e informação de dispositivos

5.10.36 Identificar usuários e dispositivo conectados e permitir a visualização de, no mínimo:

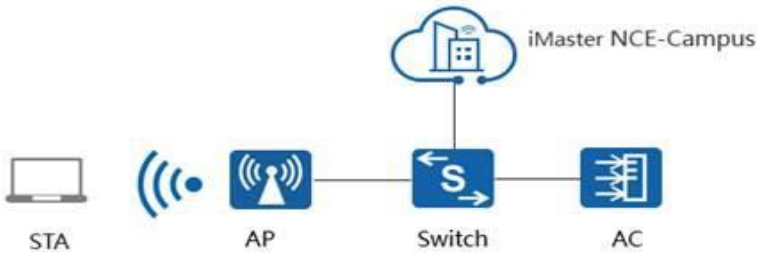
5.10.36.1 Nome usuário conectado;

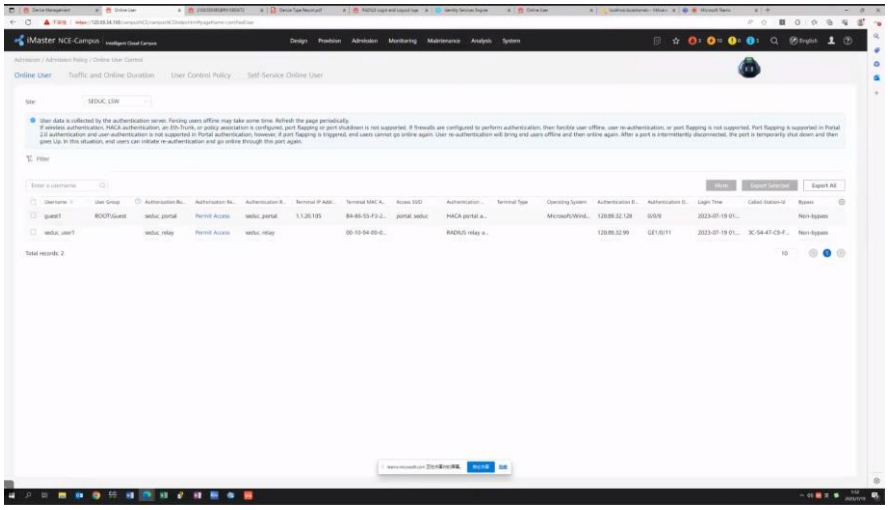
5.10.36.2 Endereço MAC;

5.10.36.3 Status da autenticação;

5.10.36.4 Horário de início da sessão ou Tempo de conexão;

5.10.36.5 Sistema Operacional do dispositivo a qual está associado;

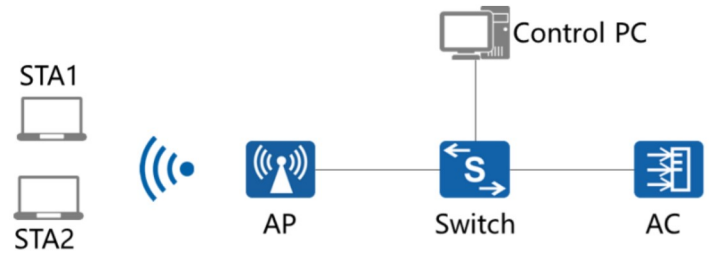
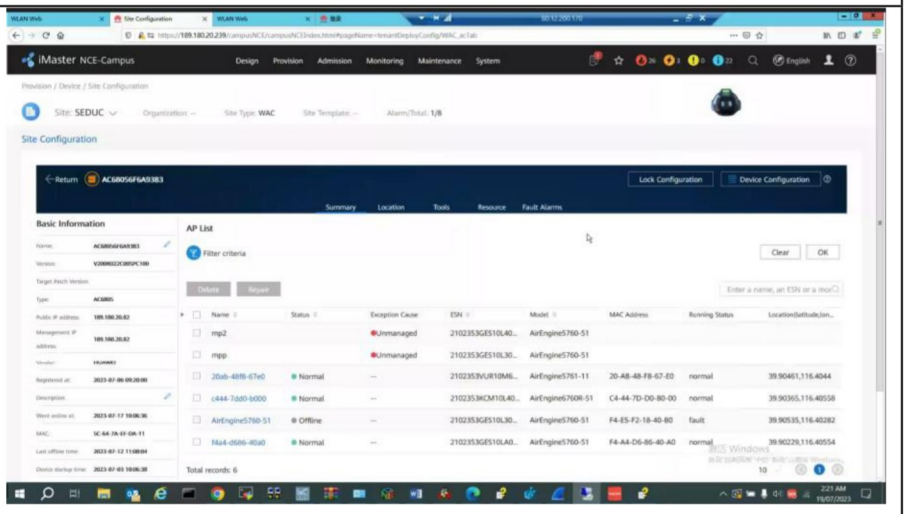
Item de teste	**Identificação de informações de dispositivos de usuário.**
Objetivo do teste	Identificação de dispositivos de usuários conectados, com a visão de Login de usuário. MAC address; Status de Autenticação; Horário de início da sessão ou Tempo de conexão; Sistema Operacional do dispositivo a qual está associado;
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Selecione “Admission > Admission Policy > Online User Control > Online User > Site

Resultado esperado	1) Identificar usuários conectados e dispositivos, e visualizar login de usuário, endereço MAC, status autenticação, horário de inicio de sessão, ou tempo de conexão e sistema operacional.
Resultado	 Figura 1 – Listagem de usuários conectados com suas devidas informações.

WLAN AC GUI

Item de teste	WLAN AC Web Management
Objetivo do teste	Validar que a WLAN AC suporta Web Management
Configuração de teste	Topologia da rede:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	 Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure Switch, AC e Control PC,Control PC pode acessar a AC; 2) Login à AC GUI por meio da controladora do iMaster NCE Campus. Resultado esperado 1.
Resultado esperado	1) Usuário pode logar na GUI com as credenciais de username e senha corretas. Usuário pode gerenciar a AC por meio da interface gráfica GUI.
Resultado	 Figura 1 – Gerenciamento via interface gráfica através da plataforma gerenciamento iMaster NCE Campus.

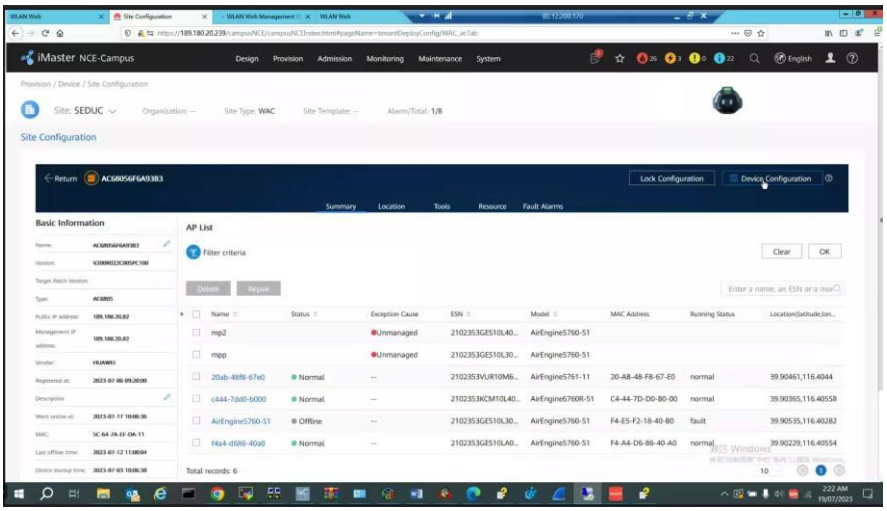
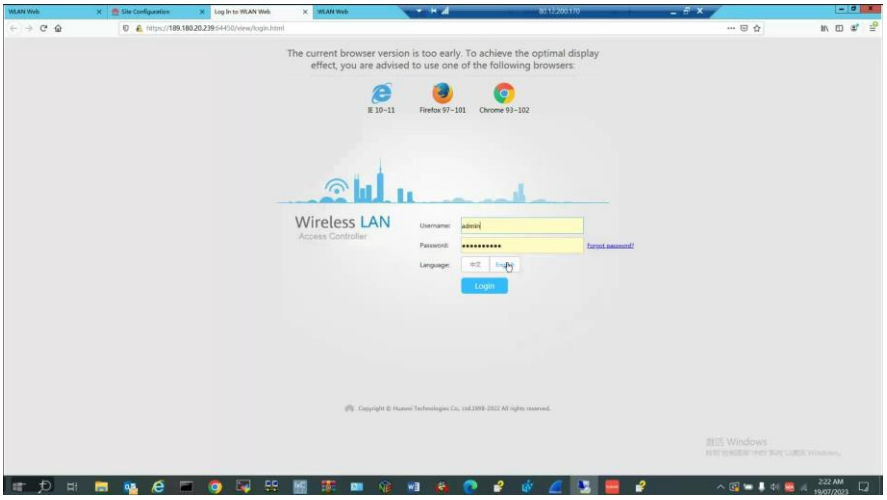
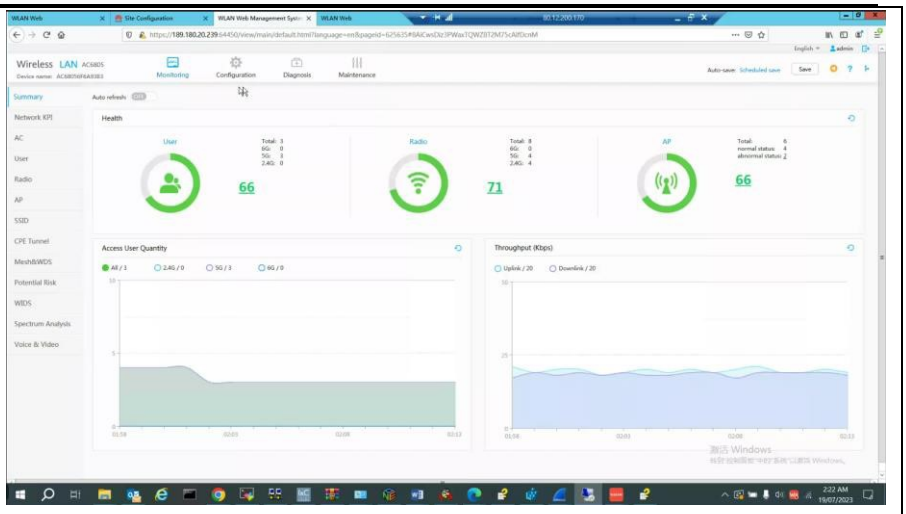
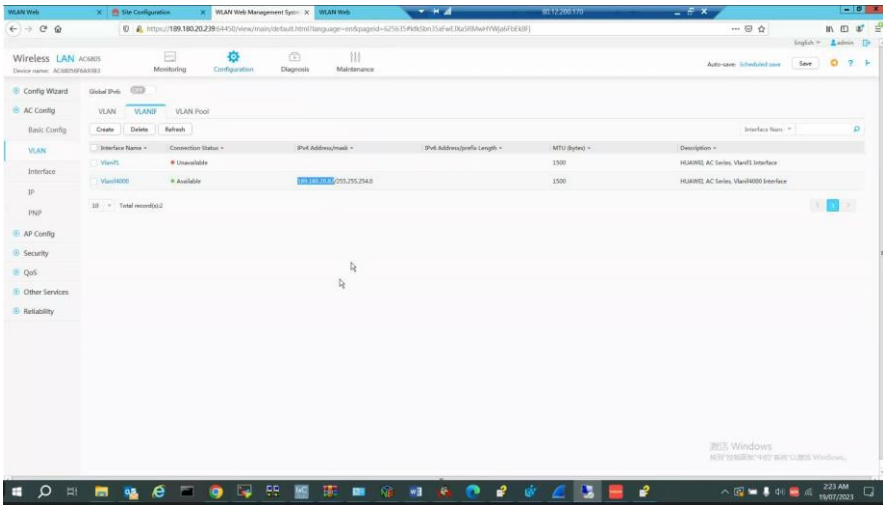


Figura 2 – Através do botão “Device Configuration”, é feito um direcionamento para a interface gráfica da controladora, diretamente da mesma console do iMaster NCE Campus.







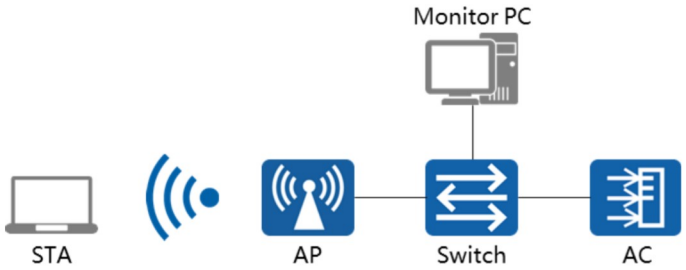
Figuras 3 a 5 – Diretamente do iMaster NCE Campus, uma vez direcionado a controladora.

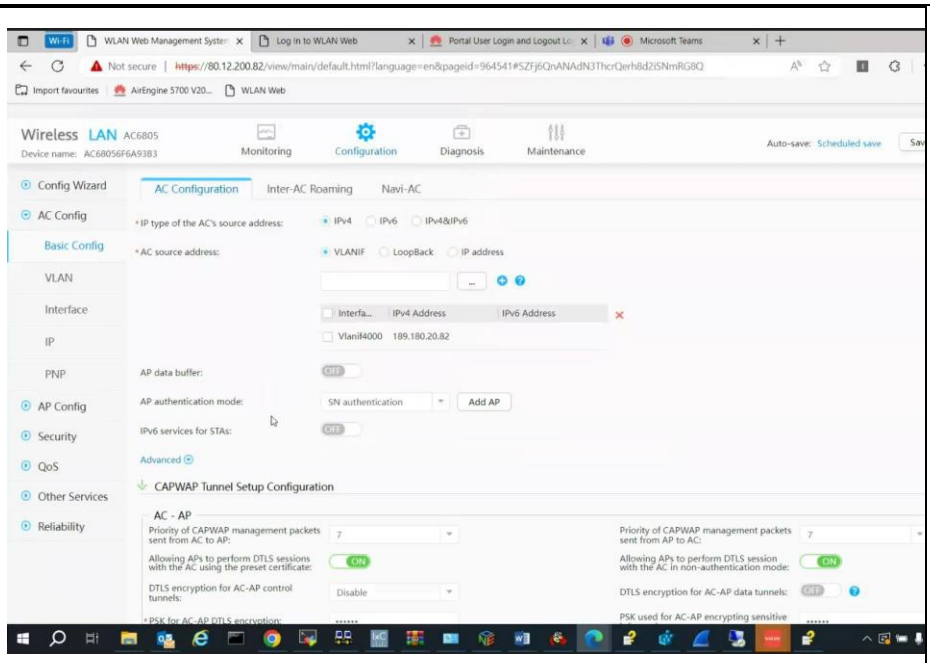
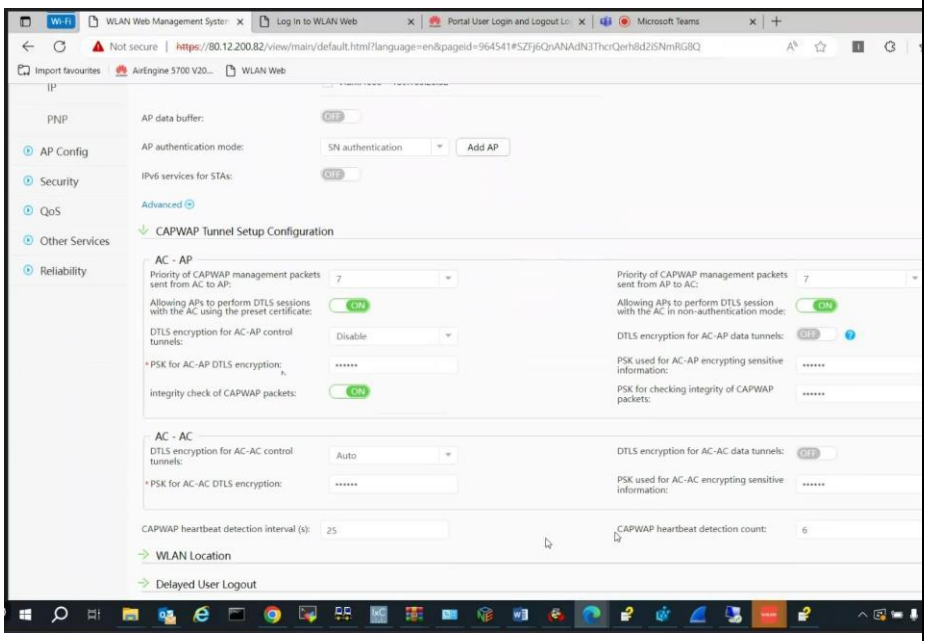
Obs. O endereço de IP é o mesmo em todas as imagens, mostrando a gerência unificada da ferramenta iMaster NCE Campus.

CAPWAP Control-link DTLS Encrypt by PSK

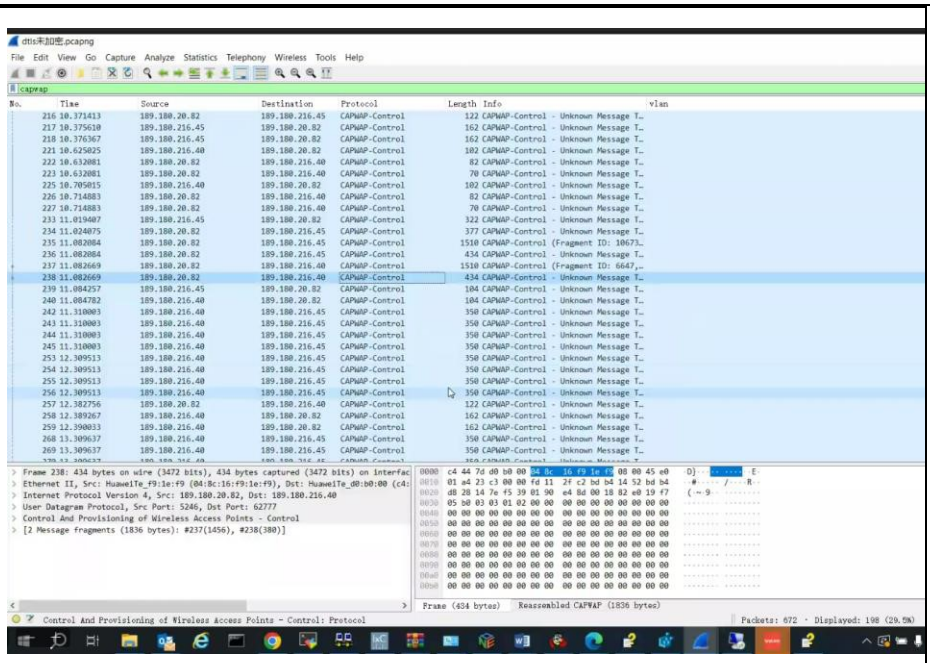
5.10.6 A comunicação entre a solução de Gerenciamento e os access Points/Switches deve ser criptografada;

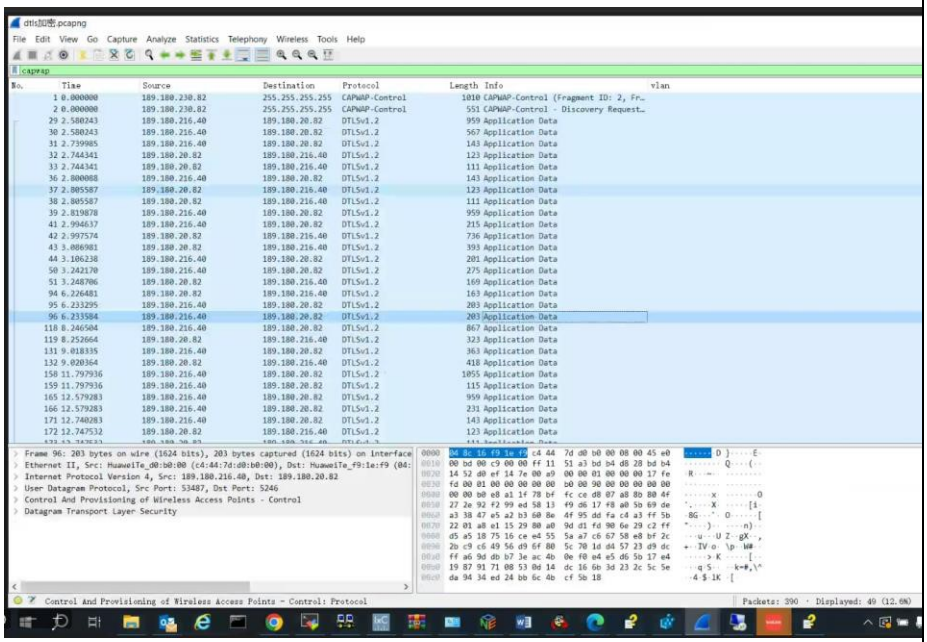
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Item de teste	CAPWAP Control-link DTLS Encrypt by PSK
Objetivo do teste	Validar que o Sistema WLAN suporta CAPWAP control-link DTLS encrypt via PSK
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos are funcionando normalmente. 2) Montar o ambiente de teste de acordo com a topologia acima.
Procedimento de teste	1) Configure os dispositivos de rede para que o AP possa comunicar com o AC. 2) Habilite autenticação CAPWAP DTLS
Resultado esperado	1) Pacotes trocados entre o AP e a AC mostram que o método de encriptação DTLS é PSK.

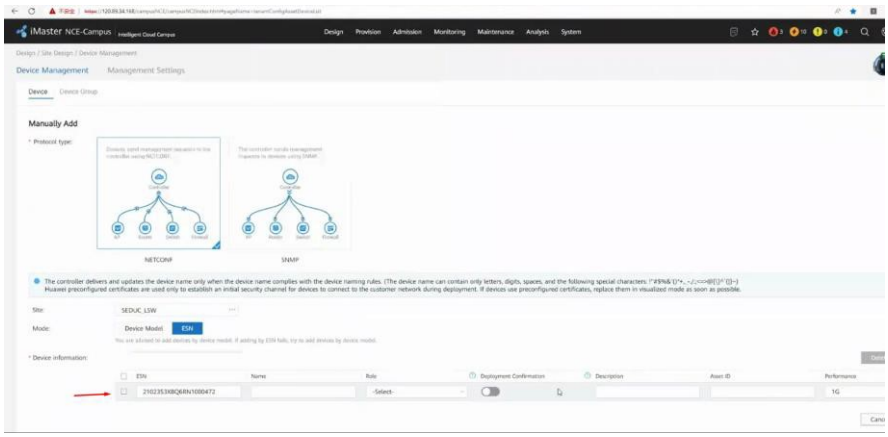
Resultado	  Figuras 1 e 2 – Na controladora, nas configurações de CAPWAP, foi habilitada a criptografia DTLS.

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES





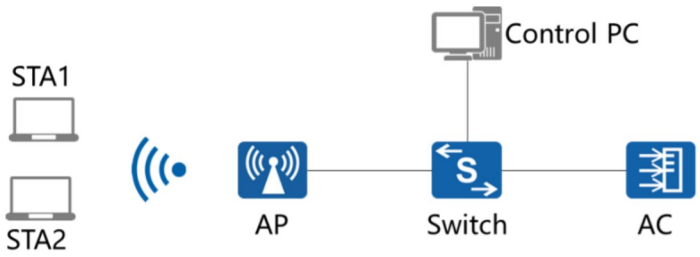
Figuras 3 e 4 – Evidenciamos através de duas capturas de pacotes, o trafego com a opção desabilitada, onde os pacotes CAPWAP são mostrados e outra, com o DTLS habilitado, onde os pacotes passam a ser capturados como DTLSv1.2

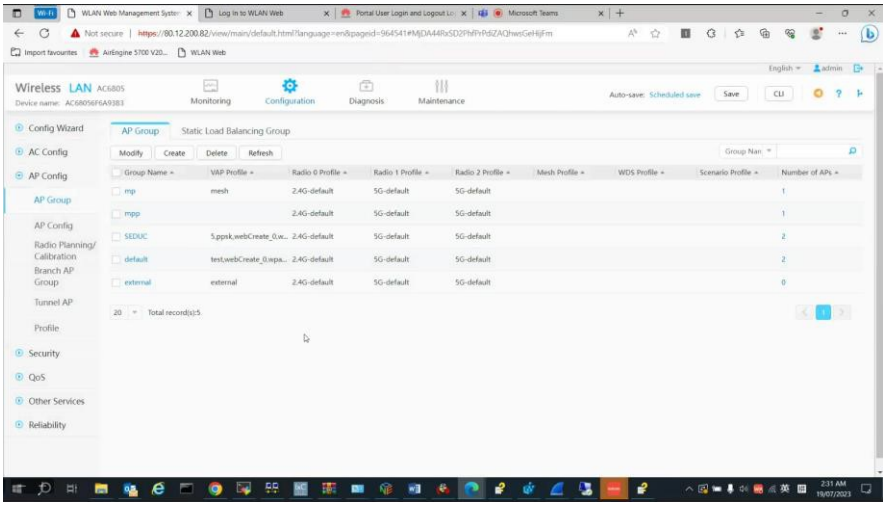
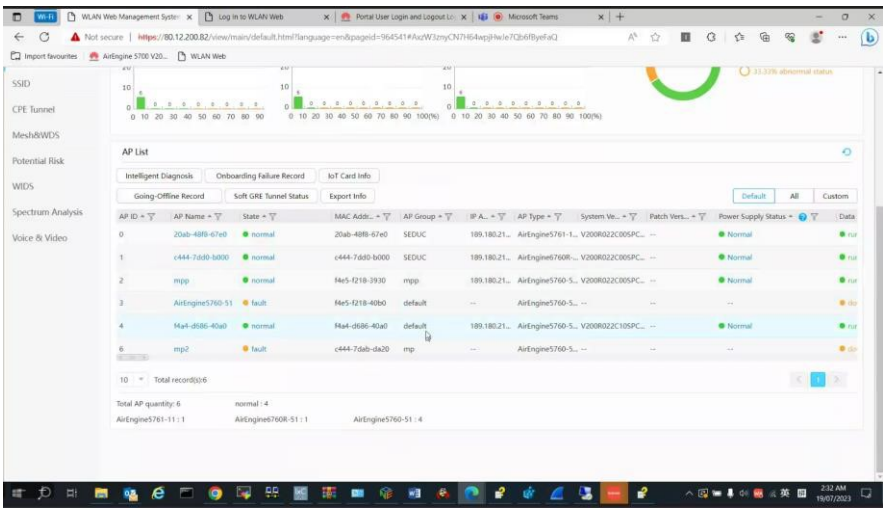
	Obs. Toda a comunicação entre dispositivos e iMaster NCE Campus, é feito via NETCONF, conforme evidenciado anteriormente. O protocolo, em conjunto com o protocolo SSH, criptografa toda a comunicação entre dispositivos (APs, switches, controladoras) e plataforma de gerenciamento.  Complemento: NETCONF Working Mechanism NETCONF Protocol Architecture Secure Transport SSH, SOAP, etc. The Secure Transport layer provides a communication path for interaction between the NMS and network devices. Em tradução livre: Mecanismo de funcionamento do NETCONF Arquitetura do protocolo NETCONF Transporte seguro SSH SOAP, etc. A camada de transporte seguro fornece um caminho de comunicação para a interação entre o Sistema de Gerenciamento de Rede (NMS) e os dispositivos de rede. Referência: iMaster NCE-Campus Product Documentation

	https://support.huawei.com/hedex/hdx.do?docid=EDOC1100211132&id=EN-US_CONCEPT_0000001172280645&lang=en

AP Group

5.10.12 Deve permitir que as configurações sejam aplicadas em vários pontos de a acesso selecionados simultaneamente, isto é, não será permitido soluções que necessitem configurar os pontos de a acesso individualmente.

Item de teste	WLAN AC Web Management
Objetivo do teste	Validar que a WLAN AC suporta gerenciamento via Web e é possível realizar configurações em grupos de AP
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configurar grupos de AP na controladora
Resultado esperado	1) AP gerenciados como grupos

Resultado	 Figura 1 – Na controladora, foi evidenciado a função de criar grupos para gerenciamento de APs. Nesta opção, a quantidade de APs em cada grupo é mostrada na coluna a direita.  Figura 2 – Na listagem de APs gerenciados, existe uma coluna especifica, identificando a qual grupo este AP pertence.

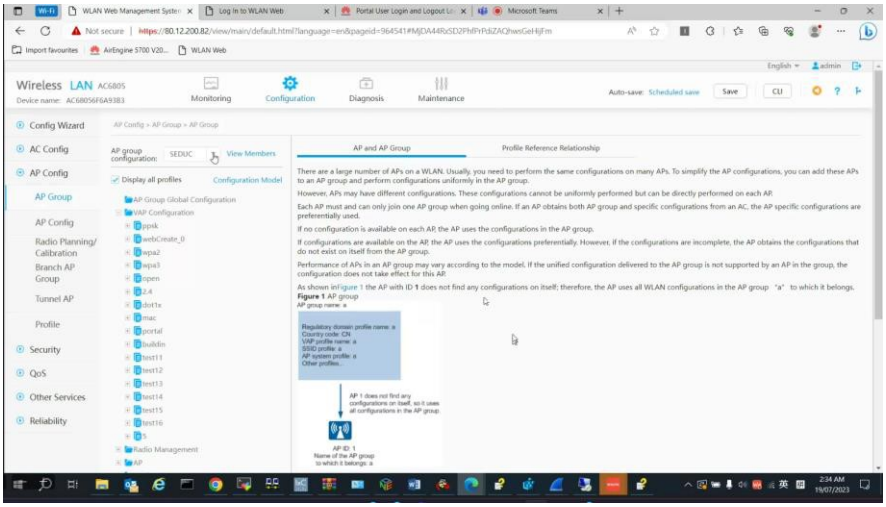


Figura 3 – Cada grupo de APs, tem o seu proprio VAP Configuration, onde cada parametro e configuração inserido, será aplicado apenas ao grupo. No exemplo, foi mostrado o grupo “SEDUC”.

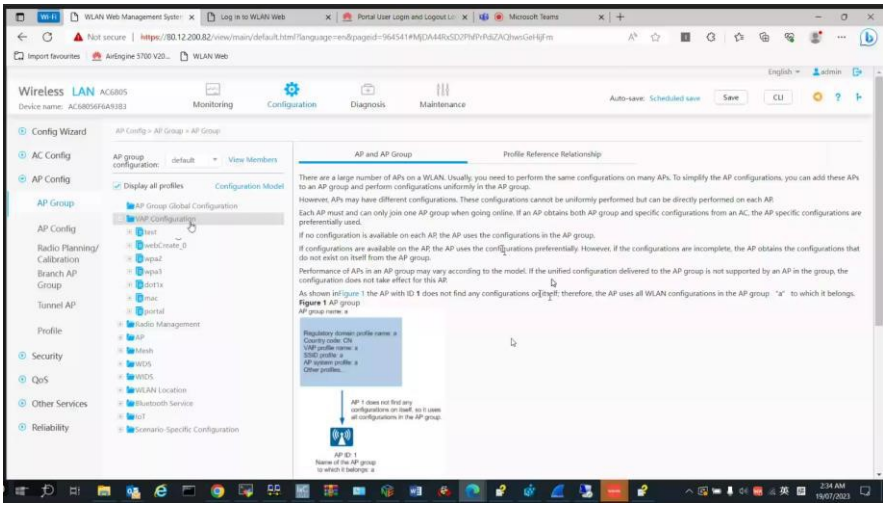


Figura 4 – Complementando a figura 3, agora foi mostrado o grupo “default”

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Auto-off radio

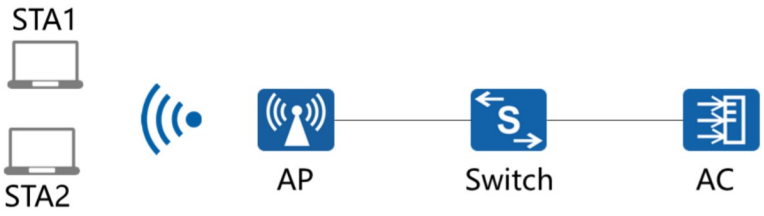
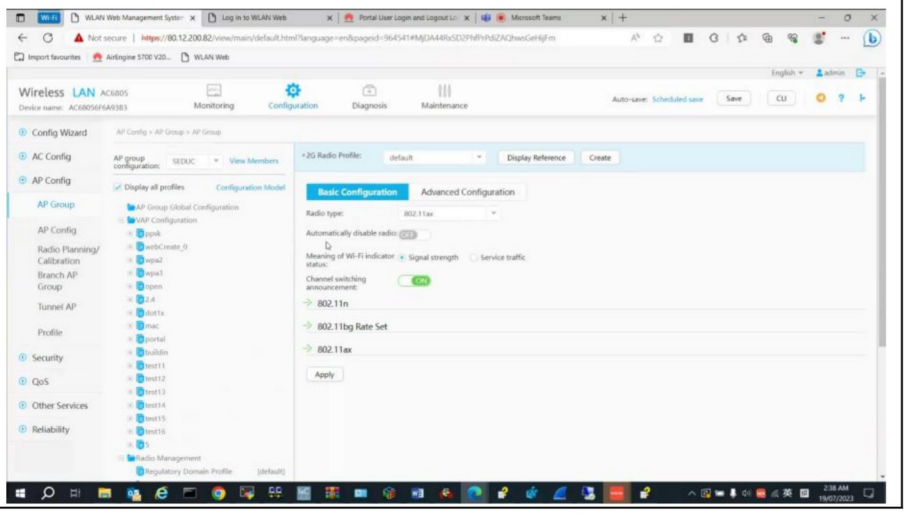
Item de teste	Auto-off radio
Objetivo do teste	Validar que o Sistema WLAN suporta shutdown em radios individuais de forma imediata ou agendada
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Desabilitar de forma automatica a operação dos radios de acordo com o agendamento.
Resultado esperado	1) Os radios param de funcionar no momento agendado
Resultado	

Figura 1 – Dentro do VAP Configuration, nas configurações de radio, foi evidenciada a opção “Automatically disable radio”

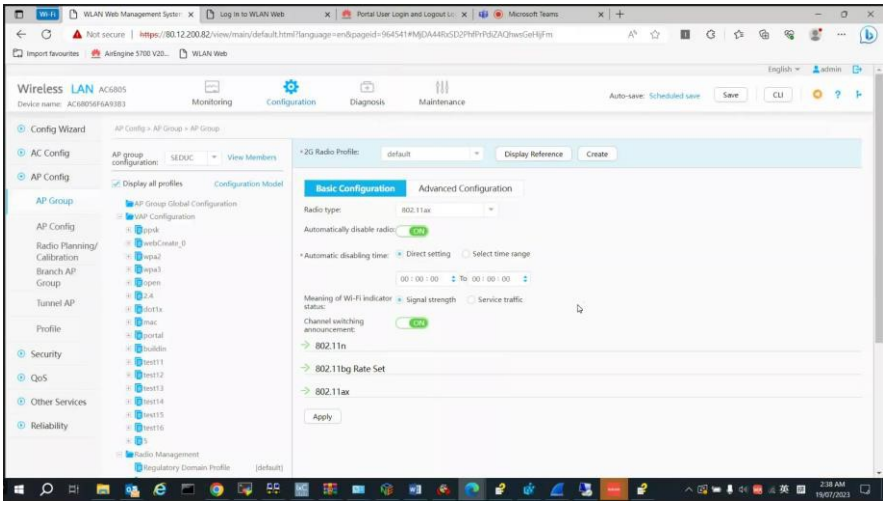


Figura 2 – Uma vez habilitada, podemos agendar o momento exato que este rádio deverá parar sua operação.

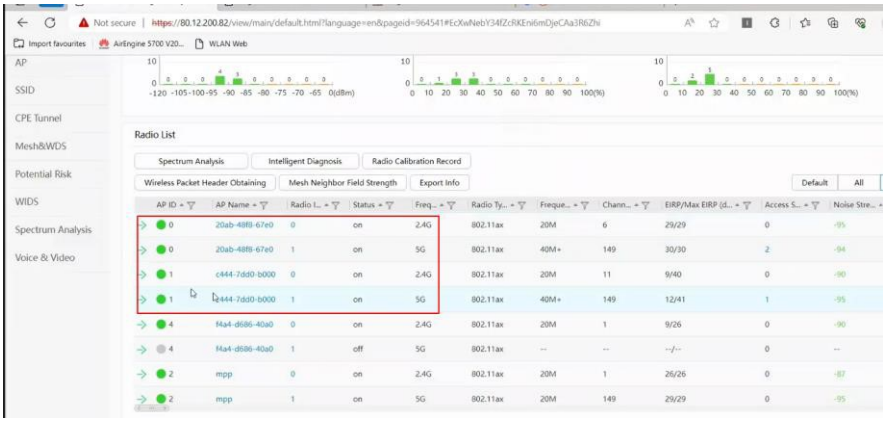


Figura 3 – Foi listado os rádios disponiveis de cada AP, e evidenciado que os APs sob teste, estão com os radios com status “on”.

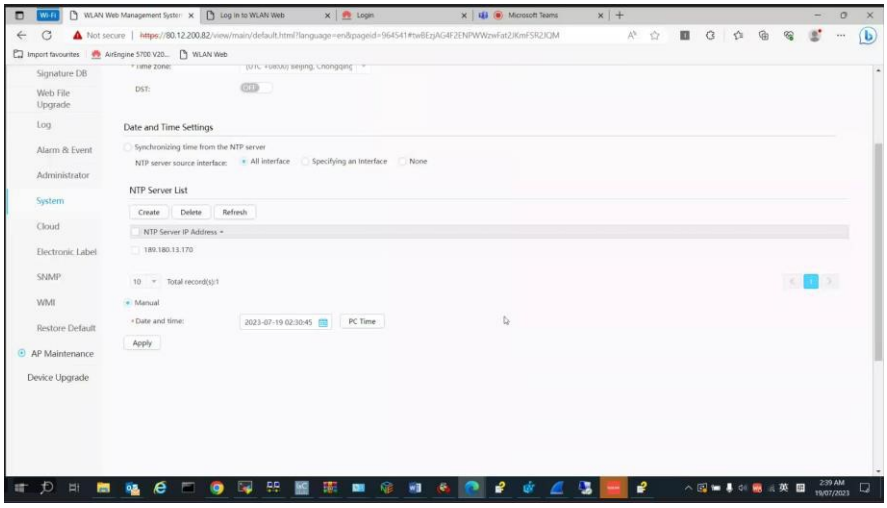


Figura 4 – Em seguida, foi mostrado o horário de operação da controladora, que no caso, é diferente do laptop, por estar sincronizado com o um servidor AD.

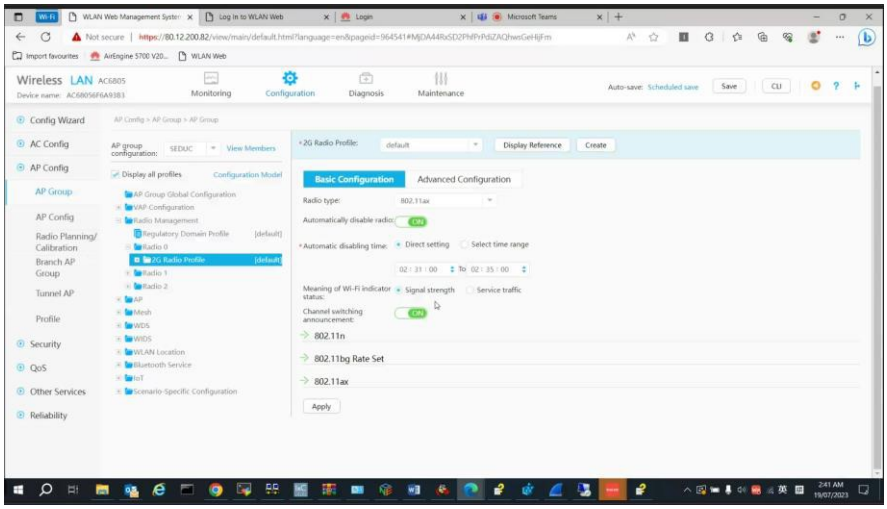


Figura 5 – Foi configurado o momento exato que este rádio (2.4Ghz) deverá parar com sua operação.

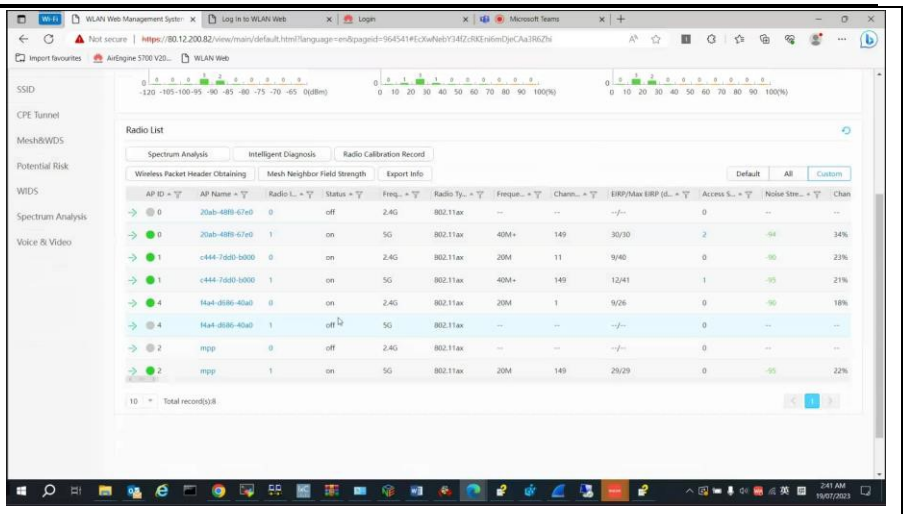


Figura 6 – Atingindo o tempo configurado, o radio 0, do AP ID 0, passou o status para “off”.

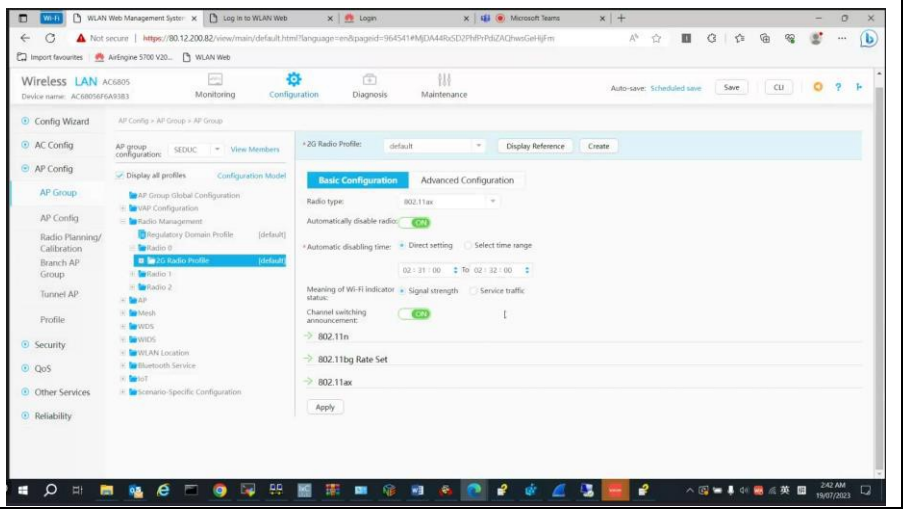


Figura 7 – O tempo de desativação deste rádio foi ajustado novamente para evitar que o teste se prolongasse demais.

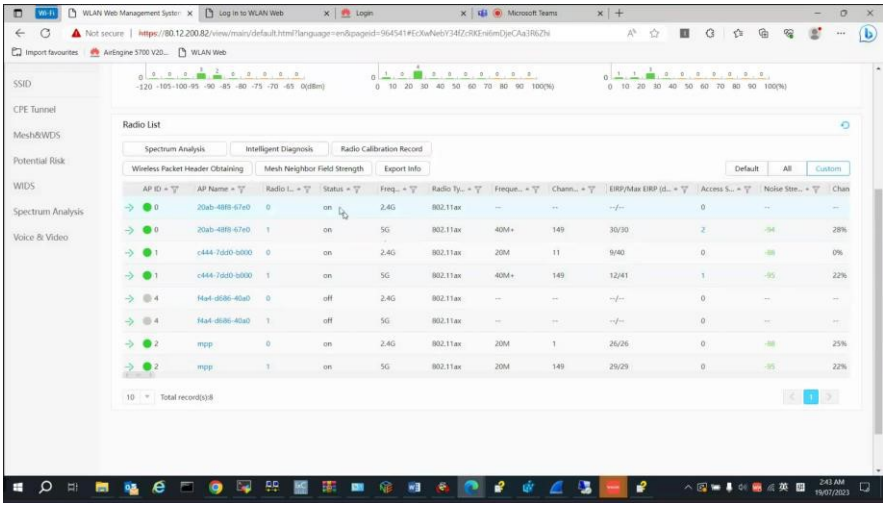


Figura 8 – Atingindo novamente o tempo estipulado, o radio passou seu status para “on”.

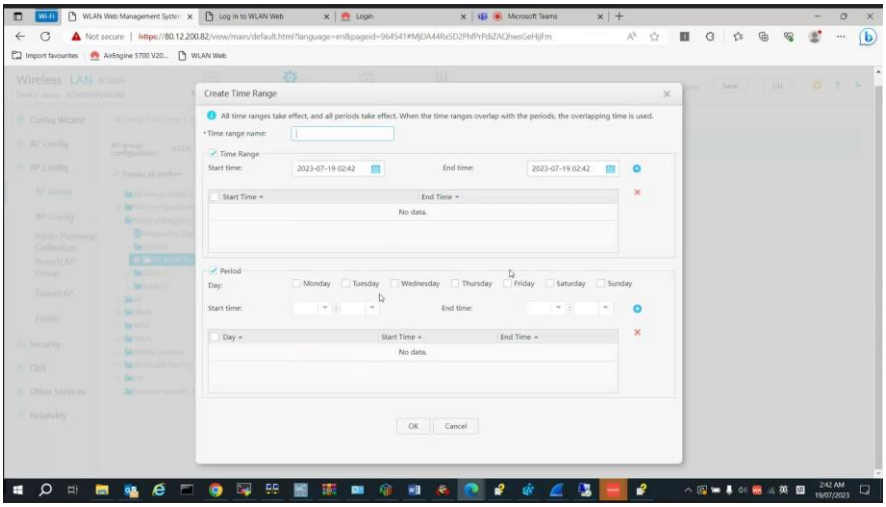


Figura 9 – Foi evidenciado também, a opção de agendamento, considerando periodos.

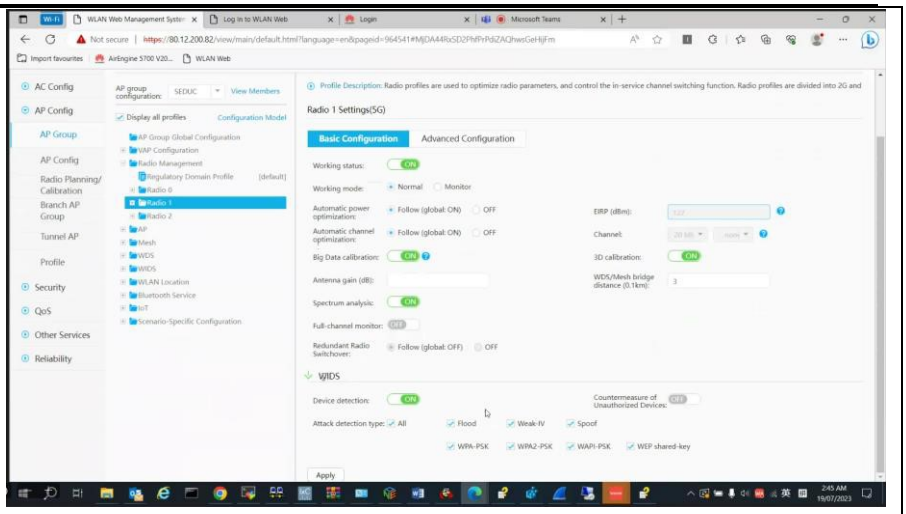
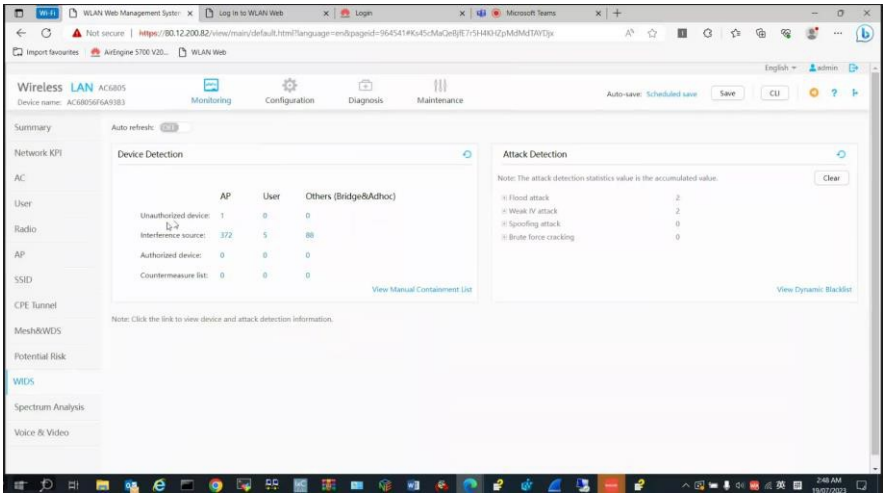
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Detecção de Rogue AP

5.10.13 Permitir a configuração total dos pontos de a acesso, assim como os aspectos de segurança da rede sem fio (WLAN) e Rádio Frequência (RF).

5.10.21 Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática; (Complementado pelo teste 5.10.20)

Item de teste	Detecção de Rogue AP
Objetivo do teste	Validar que o Sistema WLAN suporta Rogue AP Detection
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure Rogue AP to deliver SSID: “SSID-Temp”; 2) Configure a ac corretamente, AP deliver SSID: “SSID-Temp”; 1) Habilite Rogue AP detection function na AC. Resultado esperado 1.
Resultado esperado	1) Rogue AP será detectado pelo sistema WLAN.

Resultado	 Figura 1 – Nas configurações dentro de VAP Configuration, foi evidenciada a opção de WIDS, onde foi habilitada a opção “Device detections”, e as opções de ataques disponiveis para identificação.  Figura 2 – Na controlodora, foi mostrada todas as informações do WIDS, com a quantidade de origens com interferencia, APs não autorizados e etc.

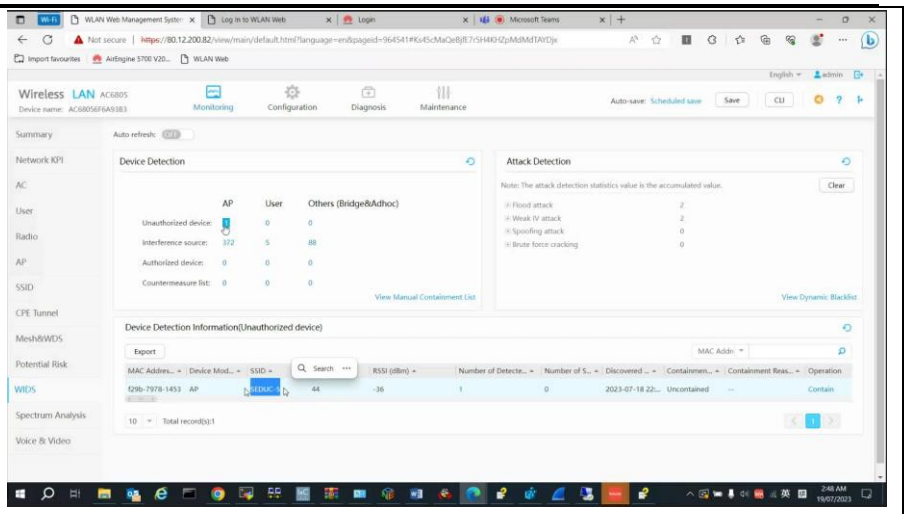
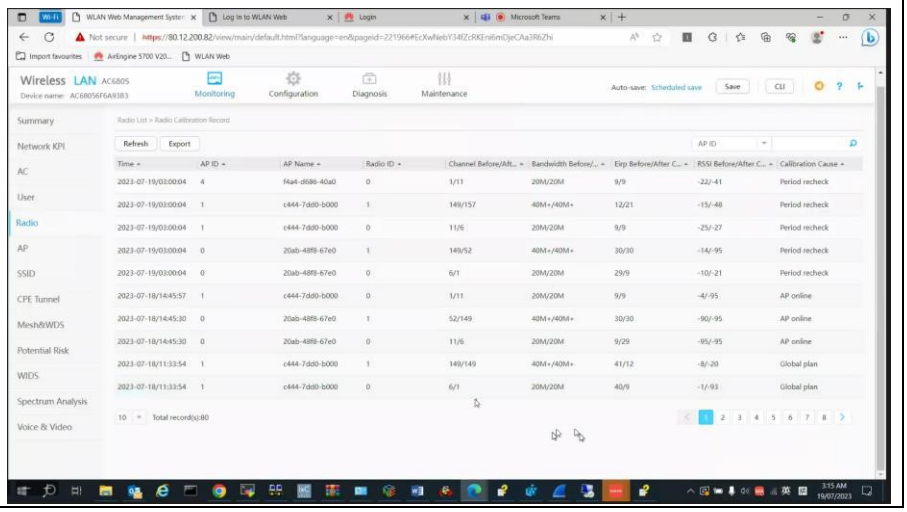


Figura 3 – Ao clicar em um AP não autorizado, identificamos o AP que haviamos simulado propagando o mesmo SSID configurado na controladora.

Obs.

O ajuste de radio frequencia, canais, potência e etc, foi evidenciado no item 5.10.20.

Ao executar a calibração de radio, todos os parametros, inclusive as detecções do WIDS são levadas em consideração.



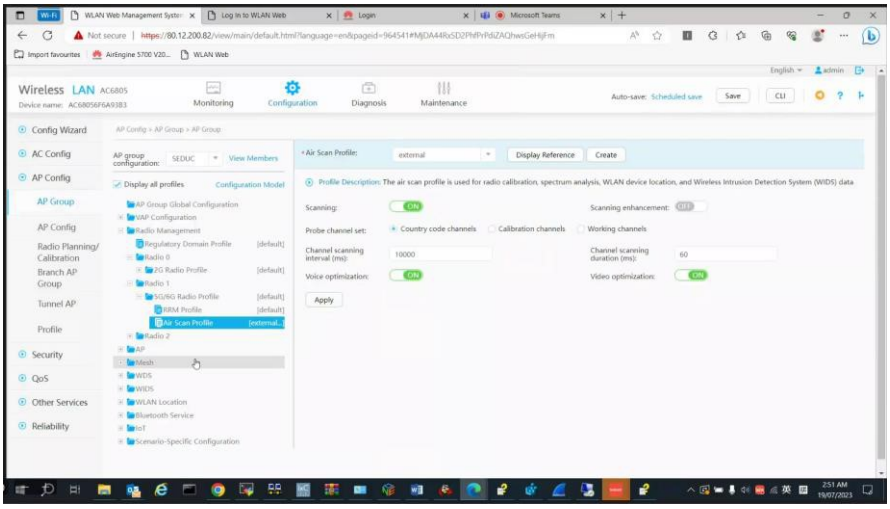
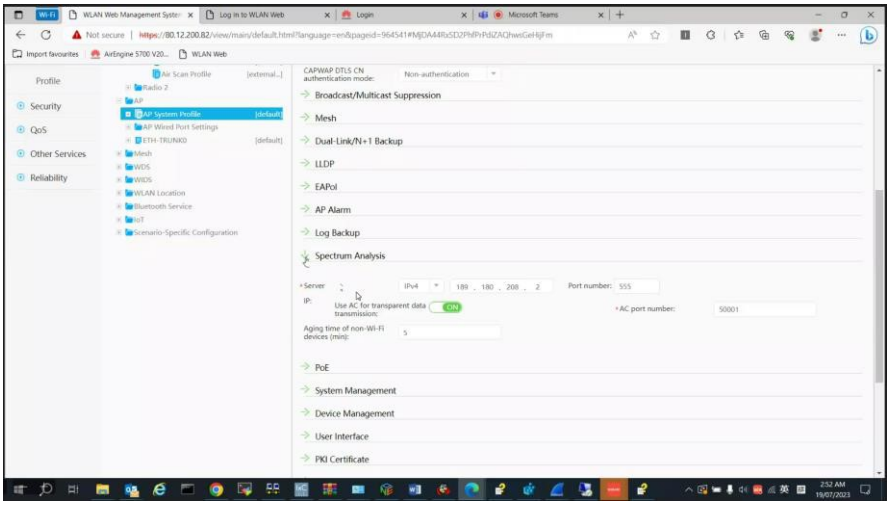
	Calibração de rádio – item 5.10.20

Detecção de dispositivos não Wi-Fi e Análise de espectro

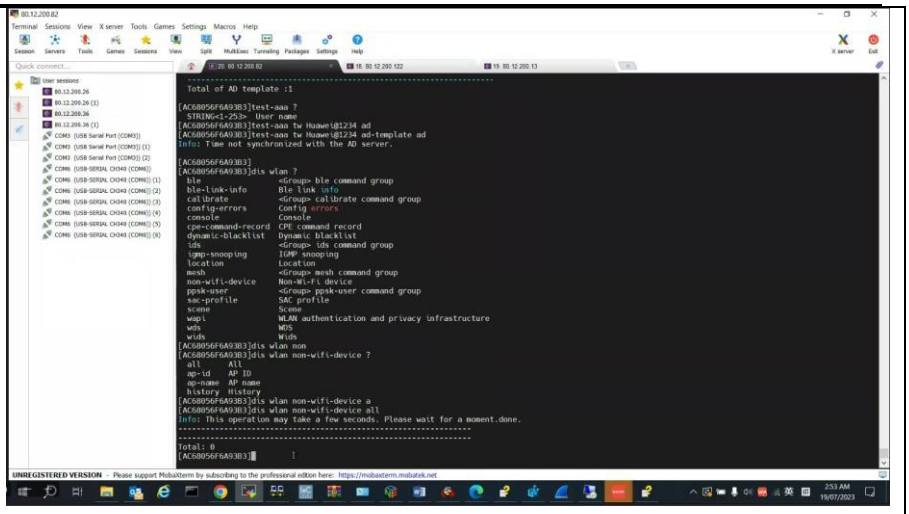
5.10.13 Permitir a configuração total dos pontos de a acesso, assim como os aspectos de segurança da rede sem fio (WLAN) e Rádio Frequência (RF).

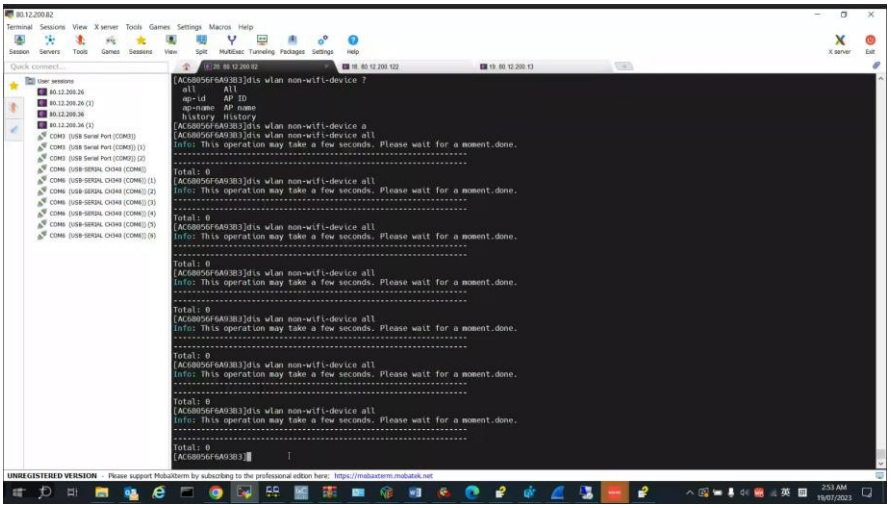
5.10.21 Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática; (Complementado pelo teste 5.10.20)

Item de teste	Detecção de dispositivos não Wi-Fi e Análise de espectro
Objetivo do teste	Validar que o Sistema WLAN suporta detecção de fontes de RF Non-Wi-Fi função de análise de espectro.
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Detectar dispositivos de radio frequencia não Wi-Fi no espectro da rede sem fio.
Resultado esperado	1) Dispositivos podem ser detectados na AC, e a informação sobre os dispositivos é listada pela AC.

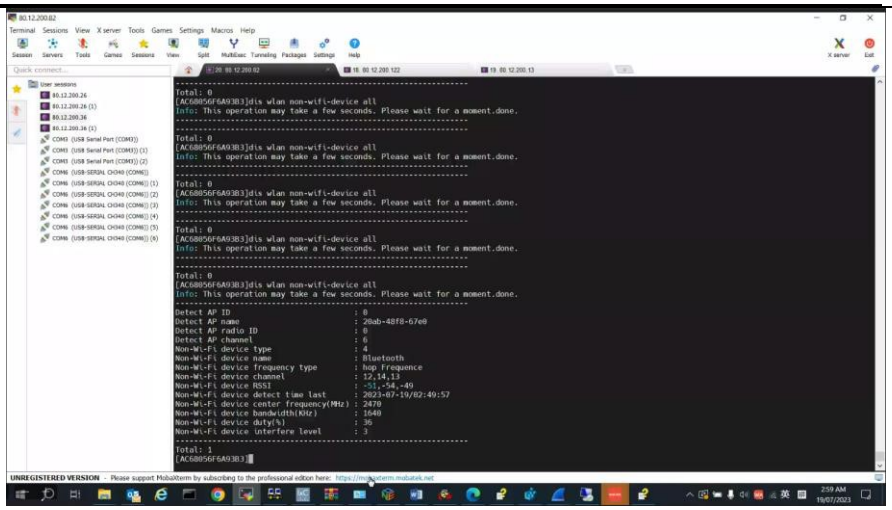
Resultado	  Figuras 1 e 2 – Nas configurações da controladora, habilitamos a opção “Scanning”, para que o AP seja utilizado com um sensor da rede sem fio. E também habilitamos a função de “Spectrum Analisys”.

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES





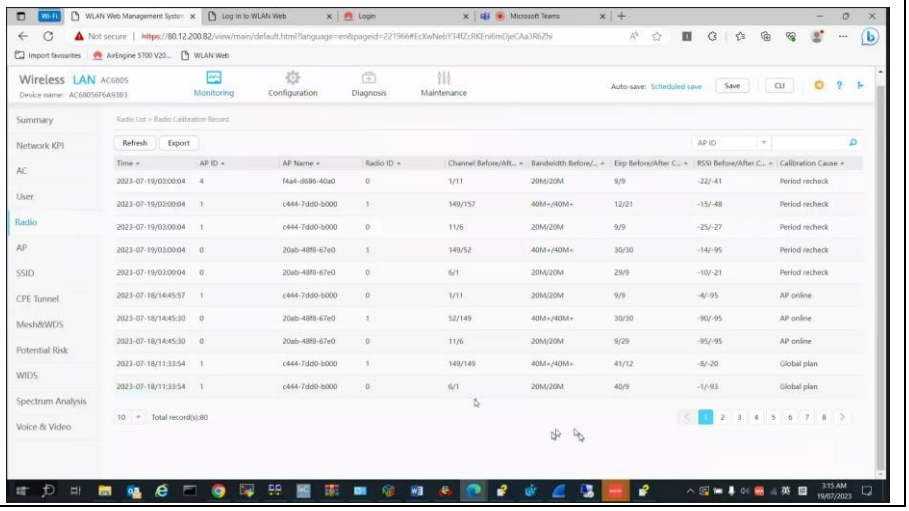
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES



Figuras 3 a 5 – Também foi evidenciada, diretamente na linha de comando da controladora, a detecção de dispositivos com interferencia. No caso simulamos uma transmissão de arquivos via Bluetooth, proxima ao AP.

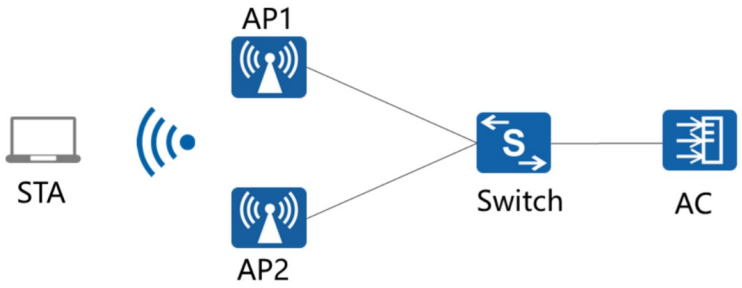
Obs.

O ajuste de radio frequencia, canais, potência e etc, foi evidenciado no item 5.10.20.



	Calibração de rádio – item 5.10.20

Balanceamento de carga dinâmico por sessão.

Item de teste	**Balanceamento de carga dinâmico por sessão.**
Objetivo do teste	Validar que o Sistema WLAN suporta session based dynamic load balancing – Balanceamento de carga dinâmico por sessão.
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure a ac corretamente, 2) Habilite Dynamic load balancing function na AC,
Resultado esperado	1) Balanceamento de dispositivos entre pontos de acesso

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Resultado

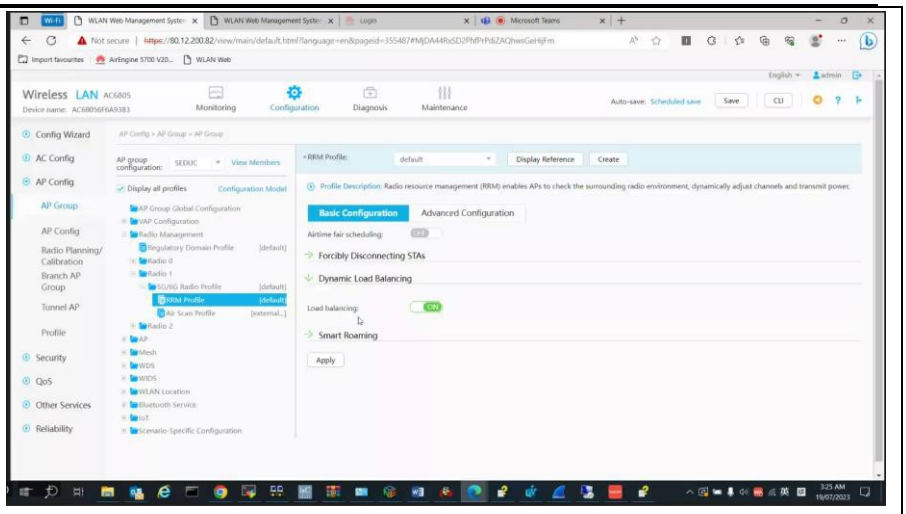


Figura 1 – Nas configurações da AC, outra opção habilitada foi a "Dynamic Load Balancing (balanceamento de carga dinâmico).

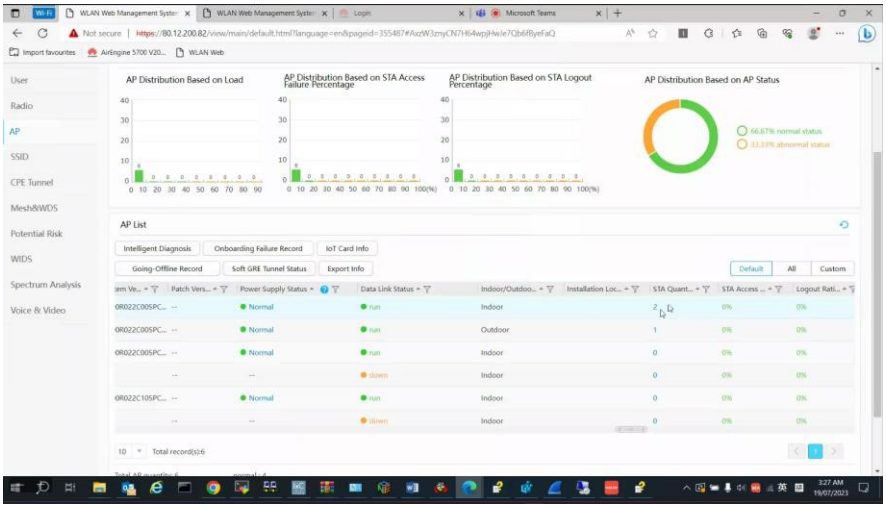


Figura 2 – Na listagem dos APs utilizados no ambiente de teste, podemos ver que existem 3 dispositivos sem fio conectados, sendo que 2 estão em um AP e 1 em outro AP.

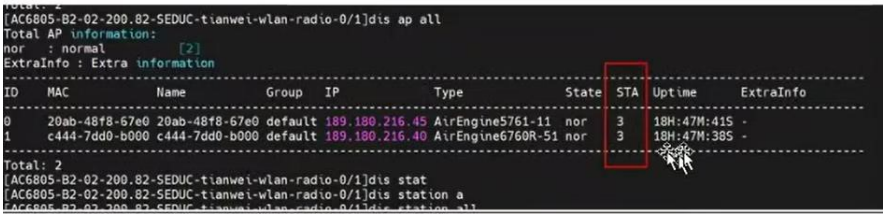
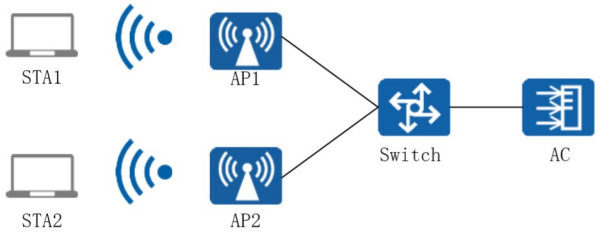


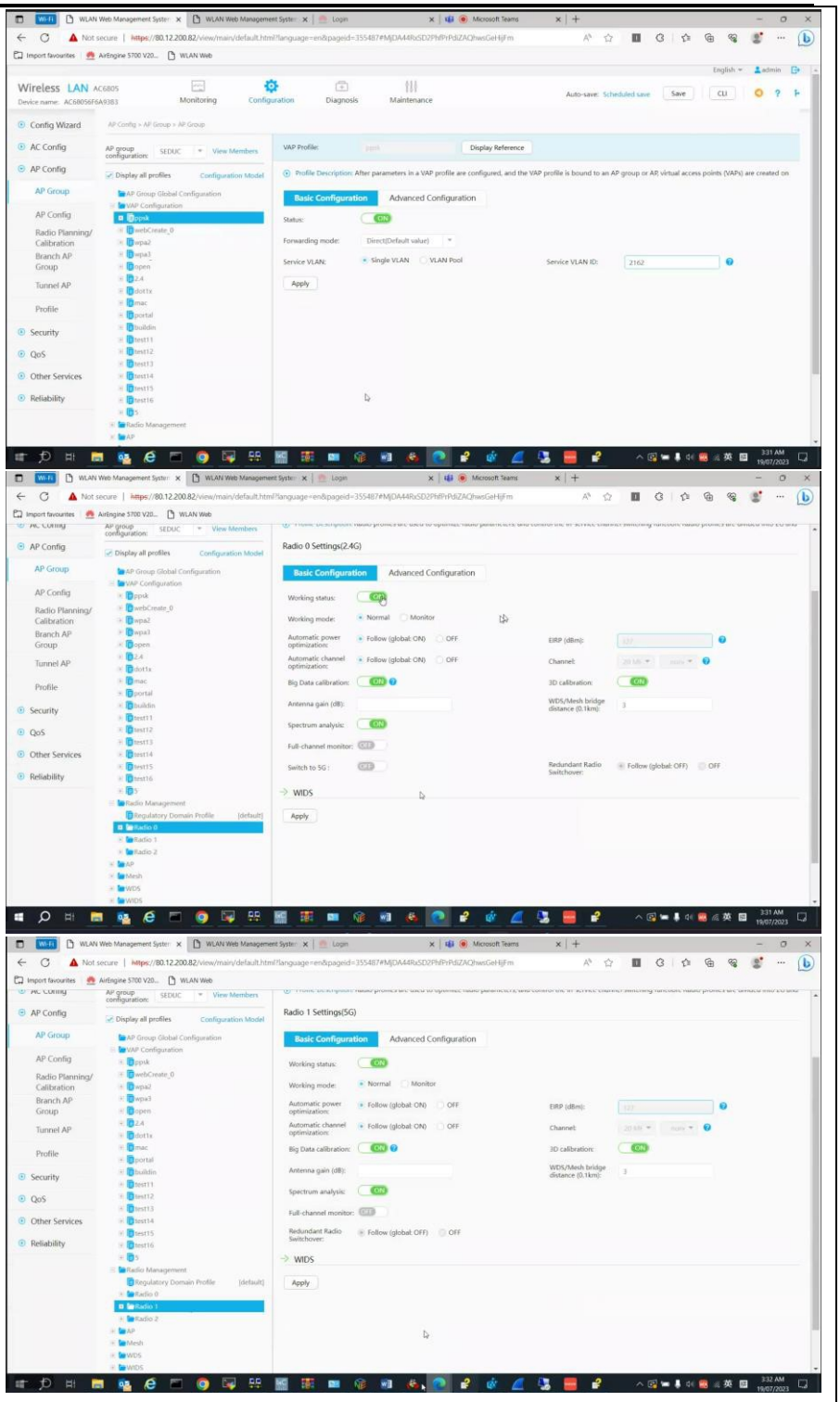
	Figura 3 – Foi mostrado também um balanceamento identico entre 6 dispositivos distribuidos igualmente entre 2 APs.

Desabilitando o serviço sem fio.

5.10.24 Permitir que o serviço sem fio seja desabilitado de determinado ponto de a acesso;

Item de teste	**Desabilitando o serviço sem fio.**
Objetivo do teste	Validar que o sistema suporta shutdown do serviço Wireless em um ou mais AP's
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure a AC corretamente, 2) Disabilitar todos os radios dos AP na AC.
Resultado esperado	1) O serviço WLAN do AP é desabilitado

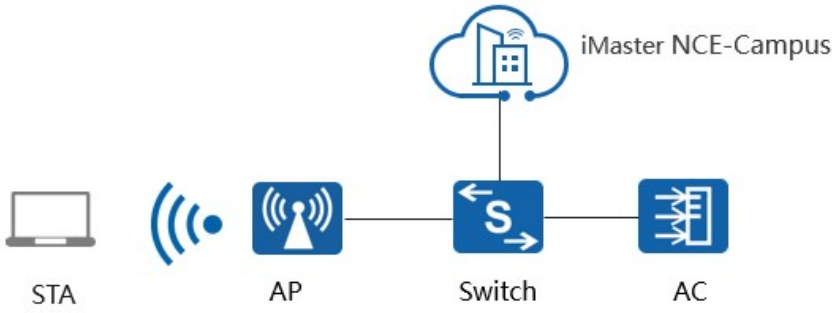
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Resultado	 Figuras 1 a 3 – Na controlodora, no VAP Configuration, podemos manter o AP operacional e desabilitar apenas o serviço do radio escolhido.

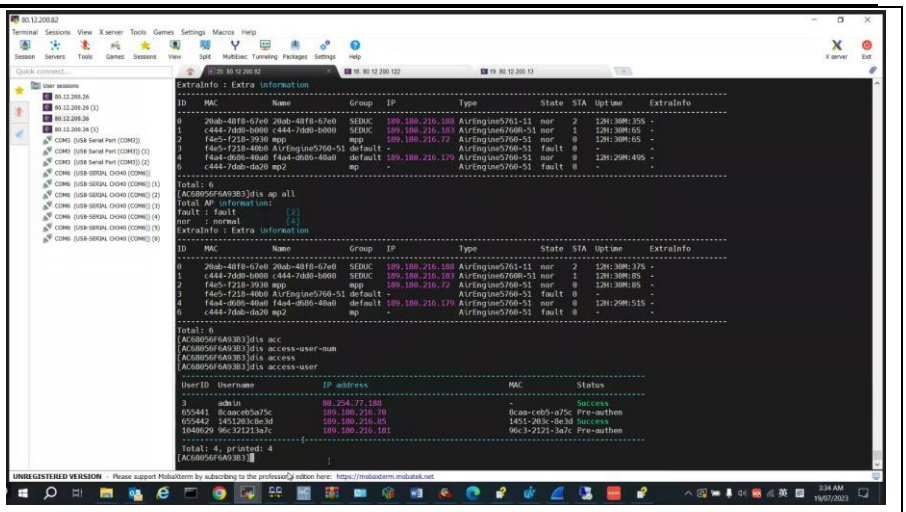
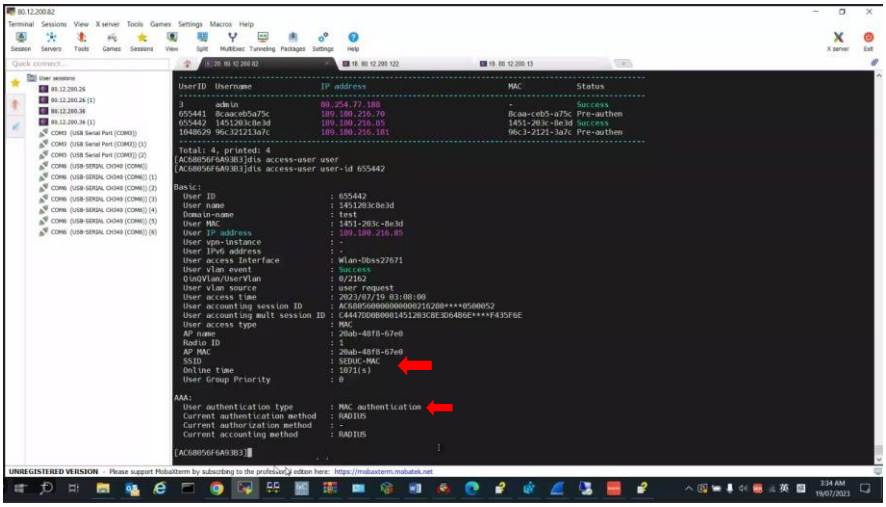
	Basta habilitar ou desabilitar a o botão “Working status”

Autenticação MAC

5.10.26 Implantar autenticação de dispositivos e usuários via 802.1x, Web Portal e endereço MAC na rede sem fio;

Item de teste	Autenticação via MAC
Objetivo do teste	Validar que o Sistema WLAN suporta Autenticação via MAC
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure a autenticação via MAC para a rede WLAN
Resultado esperado	1) O dispositivo cliente (STA1) se conecta e se autentica via MAC Authentication.

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Resultado	 Figura 1 – Na controladora, foi listado todos os dispositivos autenticados a rede através do comando “display access-user”  Figura 2 – Filtrando um pouco mais a lista de usuários, inserindo o ID do usuário, temos as informações completas do dispositivo. O comando completo foi “display access-user user-id 655442”. O resultado do comando podemos ver que é um dispositivo autenticado por MAC, no SSID SEDUC-MAC.

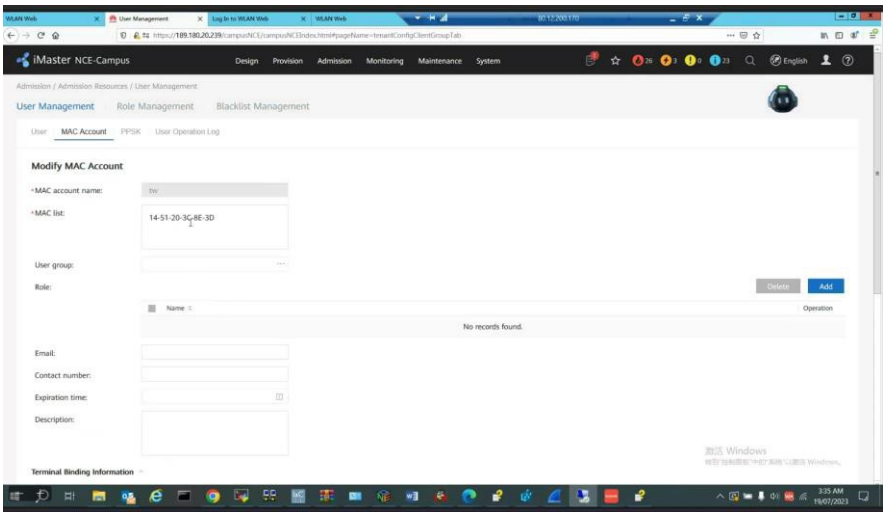
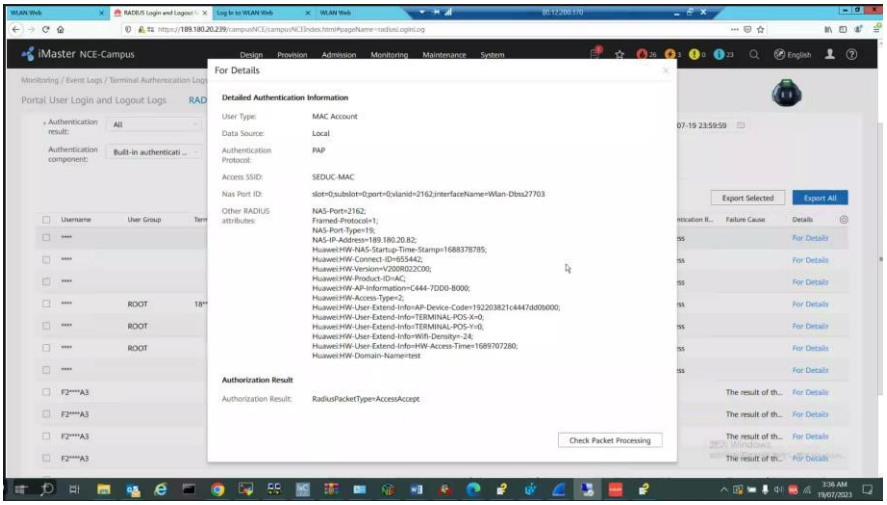
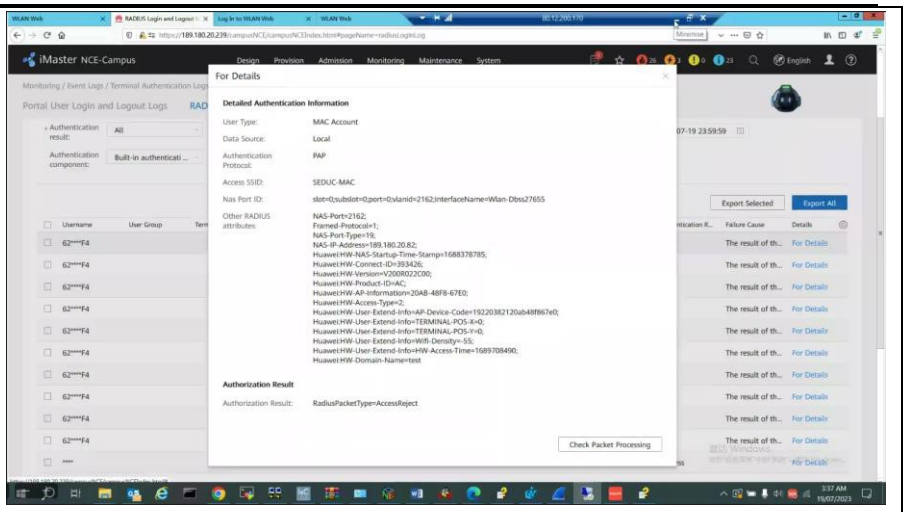


Figura 3 – Na plataforma iMaster NCE Campus, conseguimos ver as informações do usuário MAC criado. Com o mesmo endereço MAC mostrado na figura 2.



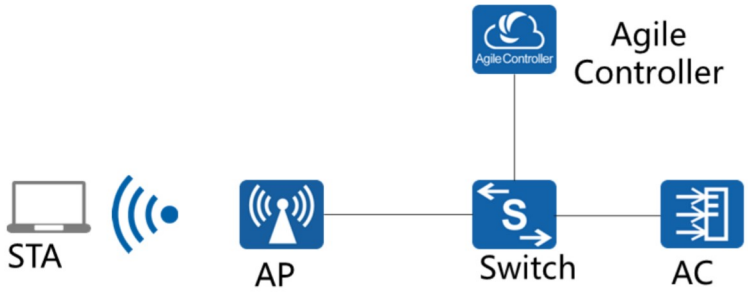
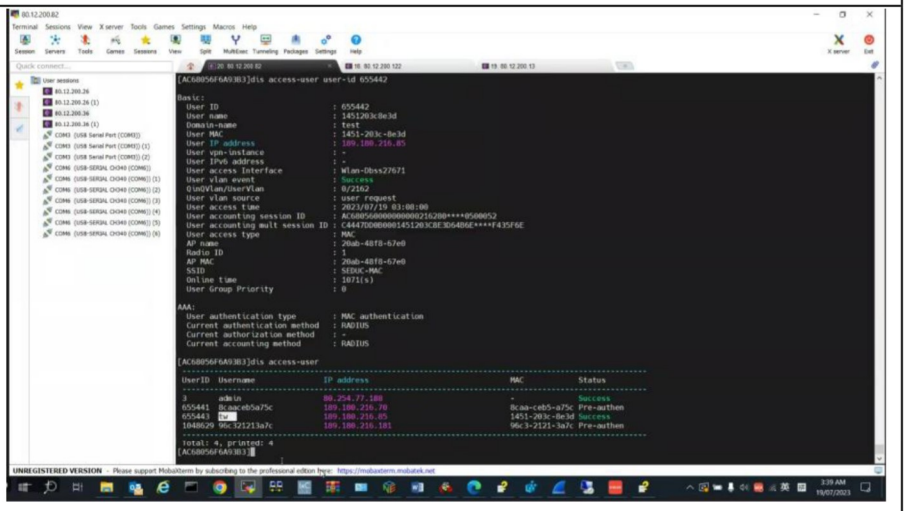
	 Figura 4 e 5 – Nos logs de autenticação Radius, também conseguimos validar todo o pacote com as informações da autenticação via MAC.

Autenticação via Portal (iMaster NCE-Campus como servidor de Portal)

5.10.26 Implantar autenticação de dispositivos e usuários via 802.1x, Web Portal e endereço MAC na rede sem fio;

Item de teste	Portal Autenticação
Objetivo do teste	Validar que o Sistema WLAN suporta Portal Autenticação
Configuração de teste	Topologia da rede:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	 Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configure a autenticação via Portal para a rede WLAN
Resultado esperado	1) O dispositivo cliente (STA1) se conecta e se autentica via Portal Authentication.
Resultado	 Figura 1 – Listando novamente os usuários autenticados na controladora, temos o usuário “tw”, que foi utilizado para o teste.

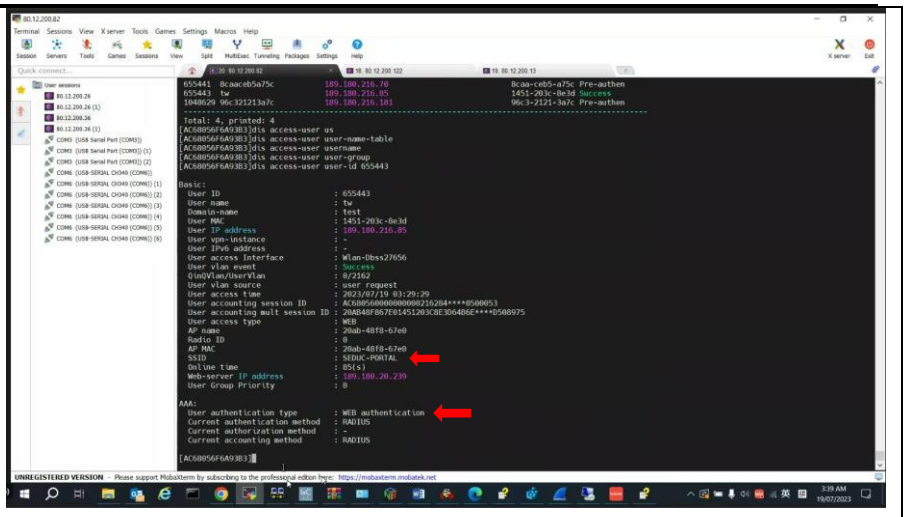


Figura 2 – Com o comando “display access-user user-id 655443”, listamos todos os detalhes desta autenticação. É possivel ver que foi realizada por “WEB Authentication” no SSID SEDUC PORTAL.

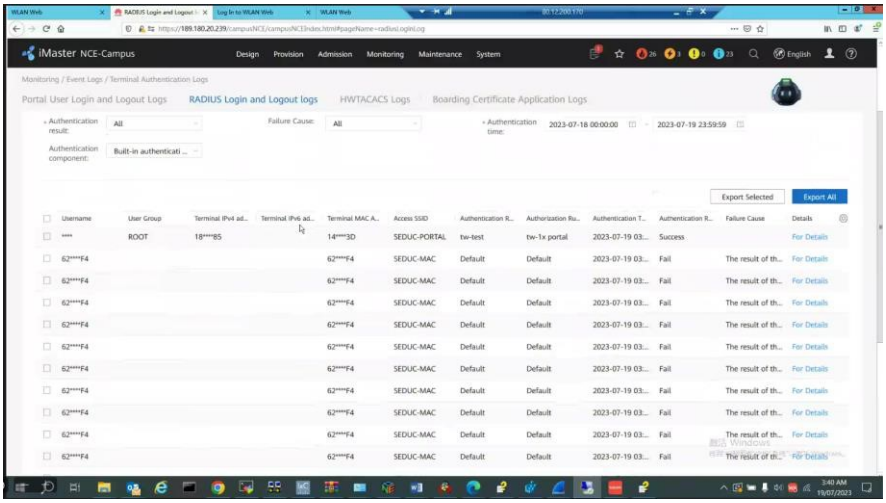


Figura 3 – Na plataforma iMaster NCE Campus, listando os logs das autenticações Radius, vemos o usuário autenticado no SSID SEDUC-PORTAL

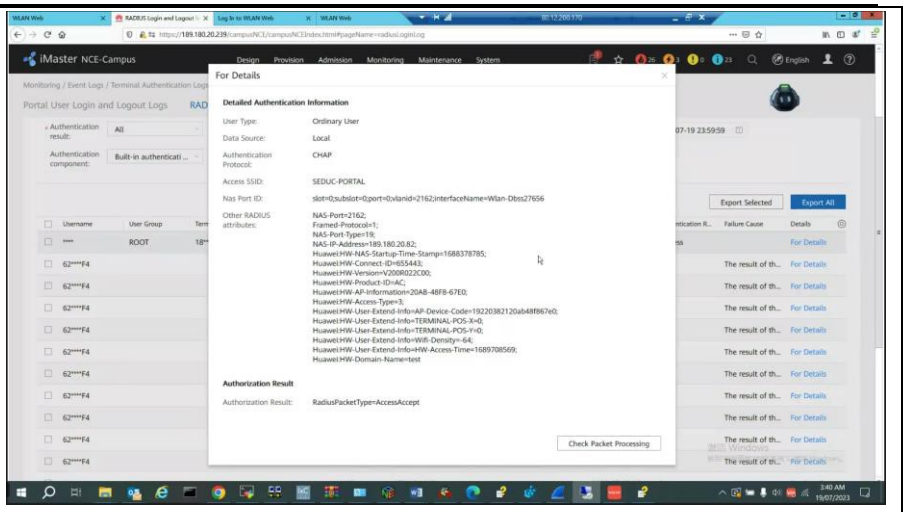


Figura 3 – Detalhando o pacote da autenticação Radius, também vemos todas as informações da autenticação realizada com sucesso.

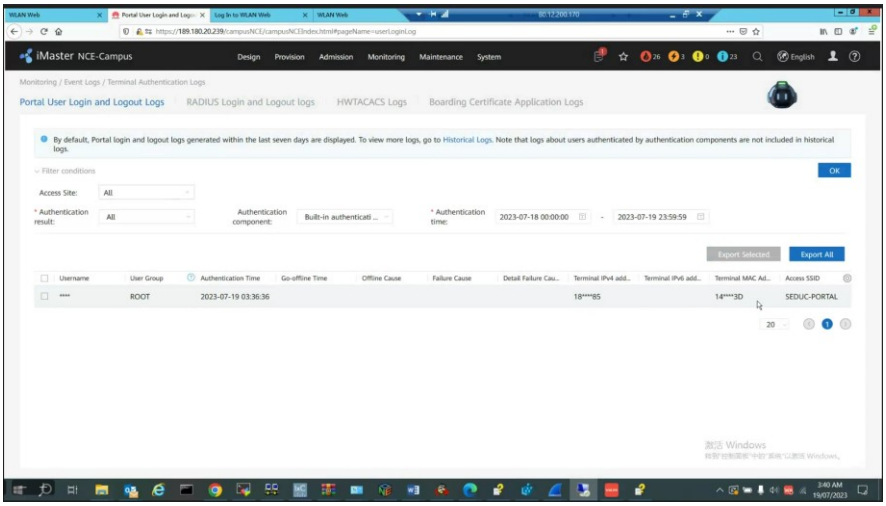


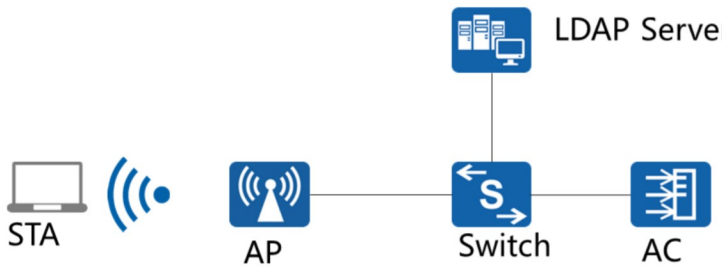
Figura 4 – Também é possivel validar na aba “Portal User Login and Logouts Logs” que a autenticação foi bem sucedida.

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Autenticação de usuários em redes sem fio

Built-in Portal-Authentication (LDAP)

5.10.26 Implantar autenticação de dispositivos e usuários via 802.1x, Web Portal e endereço MAC na rede sem fio;

Item de teste	Built-in Portal Authentication
Objetivo do teste	Validar que o Sistema WLAN suporta Autenticação e autorização via LDAP
Configuração de teste	Topologia da rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configura a autenticação WEB com usuários de uma base LDAP
Resultado esperado	1) O dispositivo cliente (STA1) se conecta e se autentica via Portal Authentication.
Resultado	

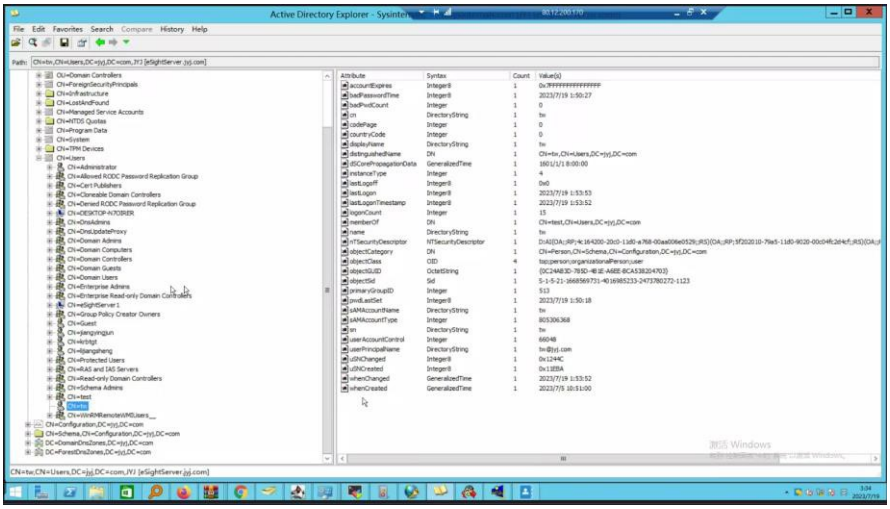


Figura 1 – Em um Active Directory do Windows Server, foi criado o usuário "tw"

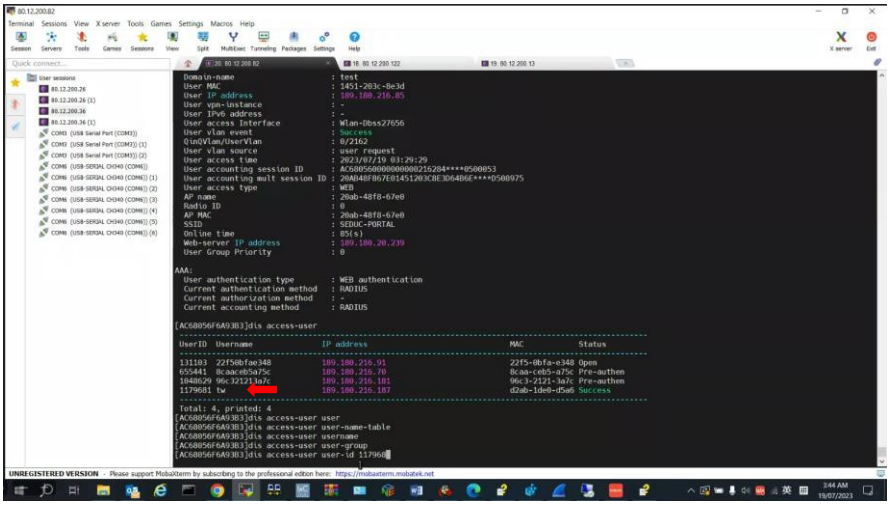


Figura 2 – Listando os usuários autenticados na controladora.

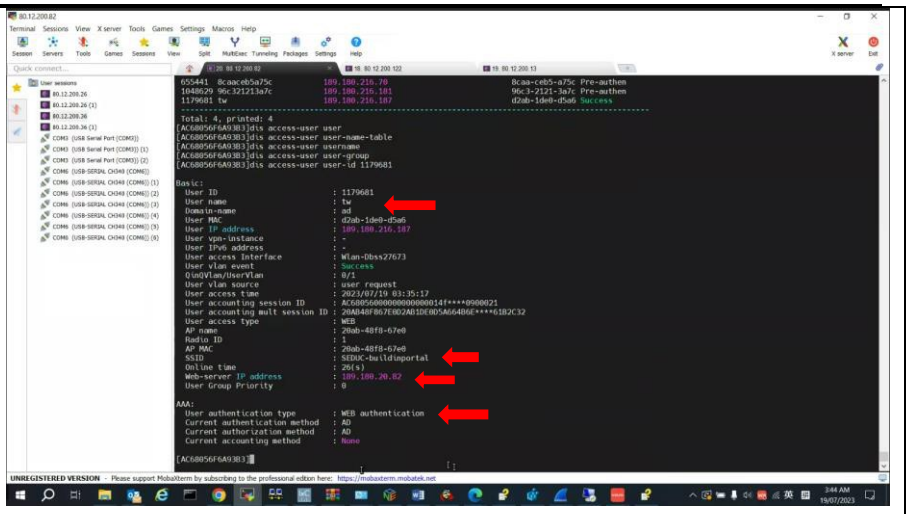


Figura 3 – Detalhando a autenticação do usuário “tw”, via comando “display access-user user-id 1179681”, conseguimos verificar que a autenticação foi feita via WEB Authentication, o usuário está no domínio “ad” e o endereço IP do portal utilizado.

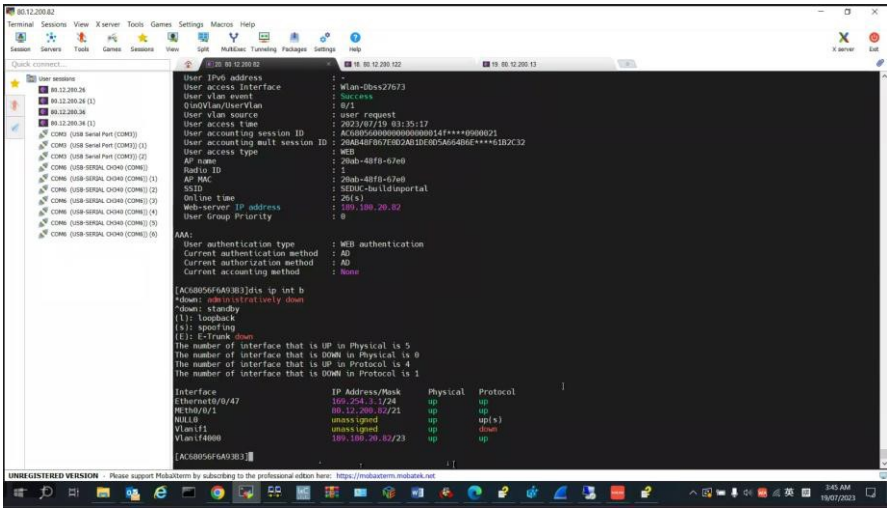
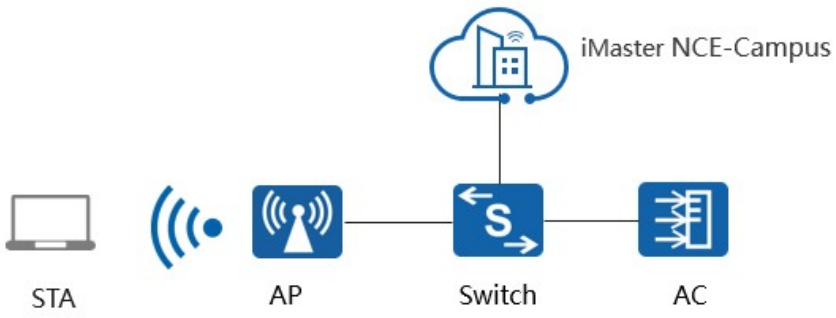


Figura 4 – O endereço do portal utilizado, é o mesmo da controladora.

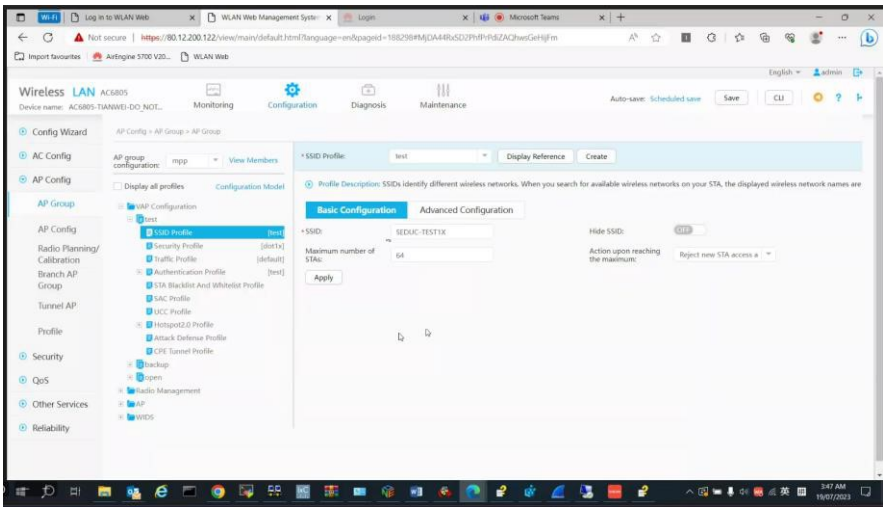
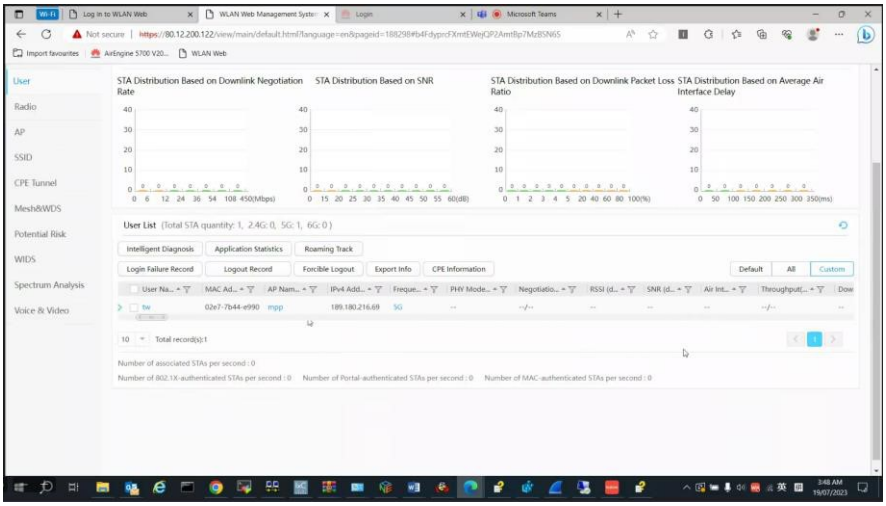
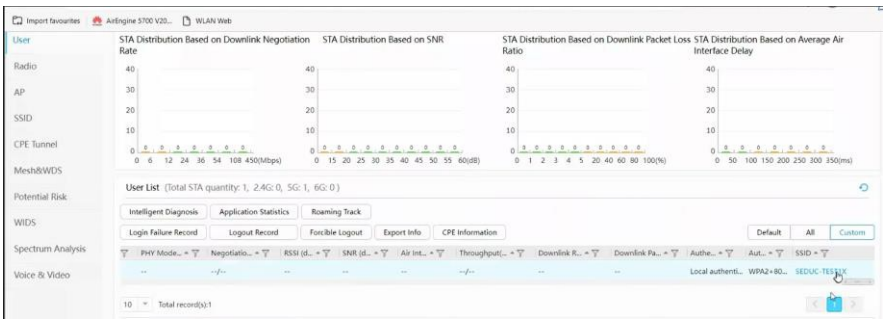
802.1x Authentication Escape

5.10.18 A falha de comunicação entre o sistema de Gerenciamento e os Pontos de Acesso não devem interferir na operação dos Pontos de Acesso;

5.10.8 A alta disponibilidade da rede sem fio será mantida pela arquitetura definida, não permitindo que a rede sem fio se torne inoperante em caso de falha na solução de gerenciamento;

Item de teste	802.1x Authentication Escape
Objetivo do teste	Valida que o sistema WLAN suporta a função de Radius server backup
Configuração de teste	Topologia da Rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Configurar as politicas de “escape” na controladora
Resultado esperado	1) Propagação de SSIDs de backup quando os eventos ocorrerem

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

Resultado	   Figuras 1 a 3 – Na controladora, temos um SSID SEDUC-TEST1X, configurado e operando normalmente.

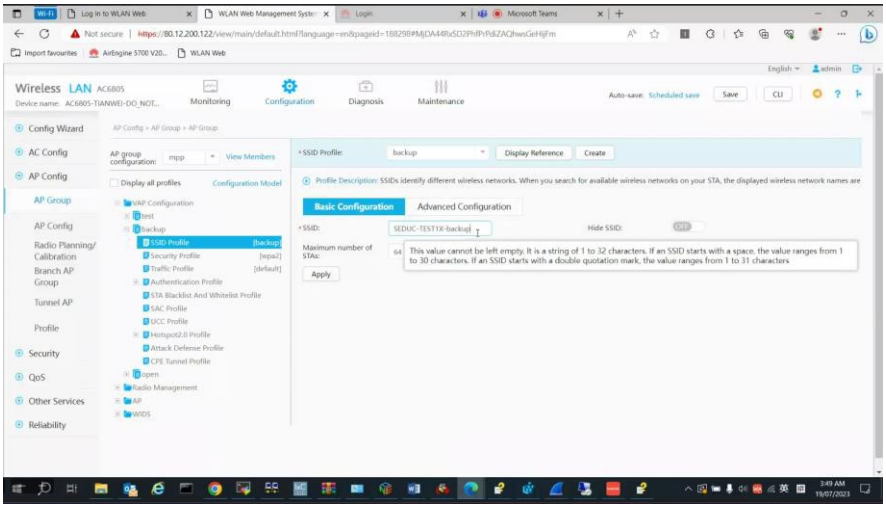


Figura 4 – Foi configurado também um SSID, chamado SEDUC-TEST1X-backup o qual iremos utilizar na nossa politica de “escape”.

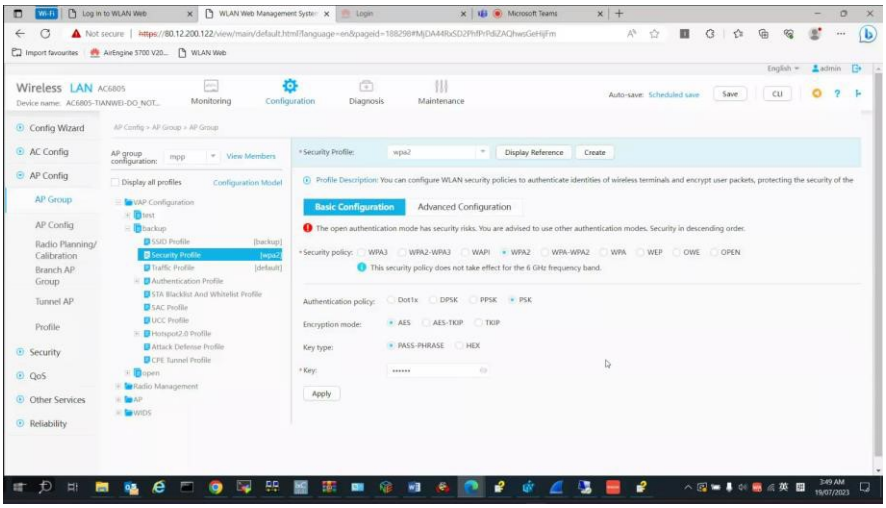
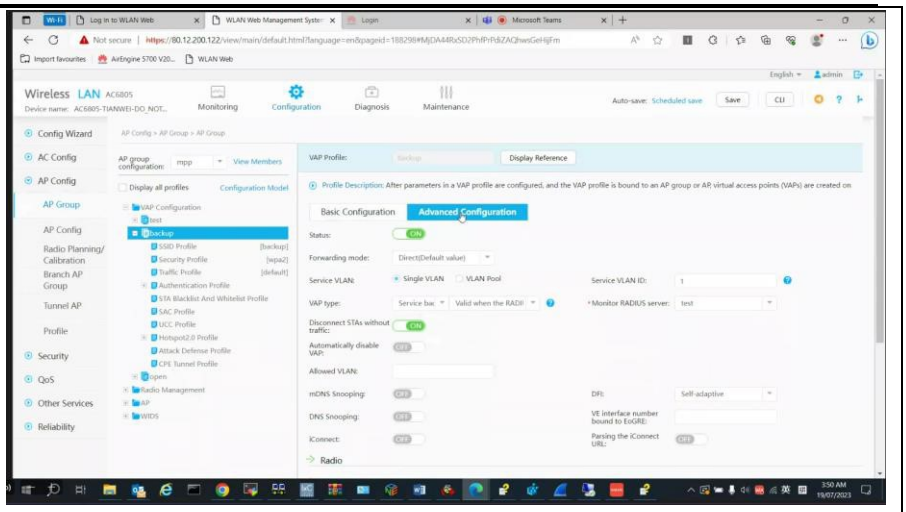
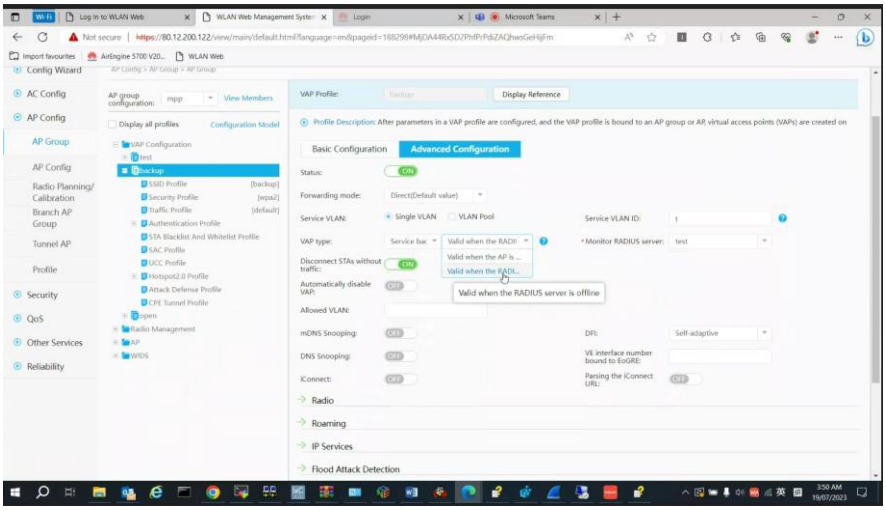
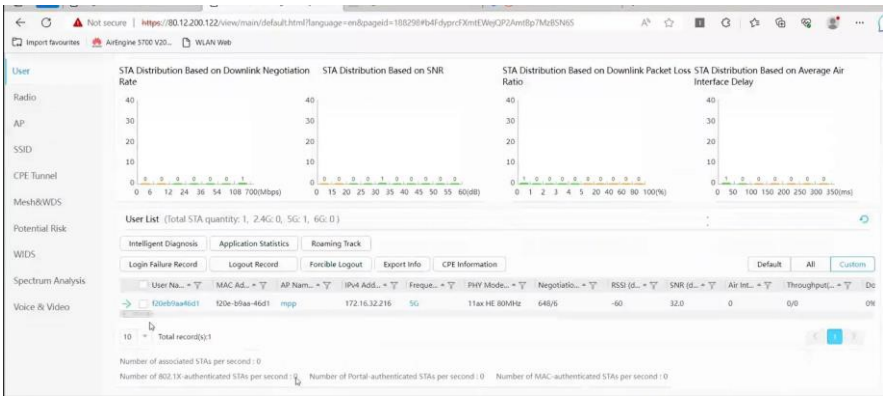


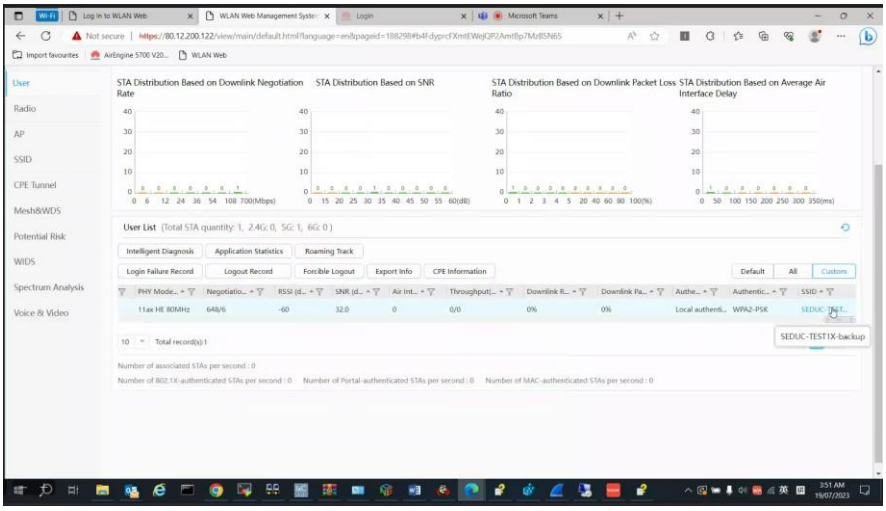
Figura 5 – No “Security Profile” deste novo SSID, nas configurações básicas foram configuradas as politicas de segurança como WPA2, e uma senha padrão (PASS-PHRASE)





Figuras 6 e 7 – Nas configurações avançadas, escolhemos a opção de quando este SSID de backup, irá ser propagado pelos APs. Nesta primeira etapa, utilizamos como opção “Valid when the RADIUS server is offline”, ou seja, quando não houver conexão com o servidor RADIUS.





Figuras 8 e 9 – Simulamos uma queda do servidor RADIUS, e o AP começou a ser propagado de forma automatica.

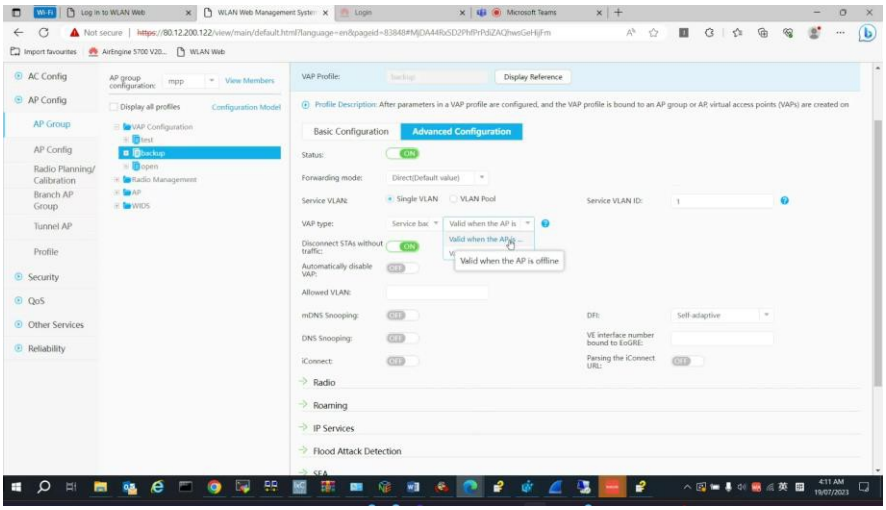


Figura 10 – Na segunda etapa, trocamos a condição de quando este SSID ficará operacional. Agora escolhemos a opção “Valid when the AP is offline”, ou seja, quando não houver conectividade entre controladora e AP.

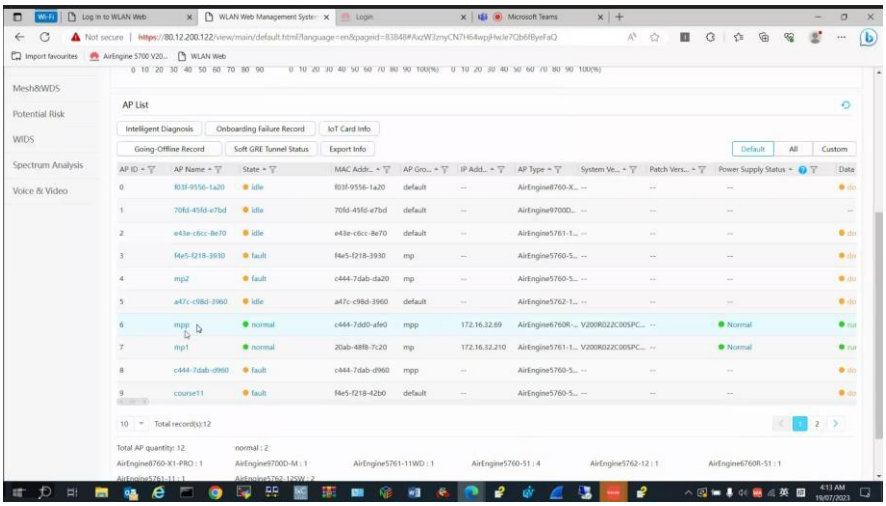


Figura 11 – Antes de simular o ambiente, validamos que existe sim conectividade entre a controlodora e o AP ID 6 (status normal).

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

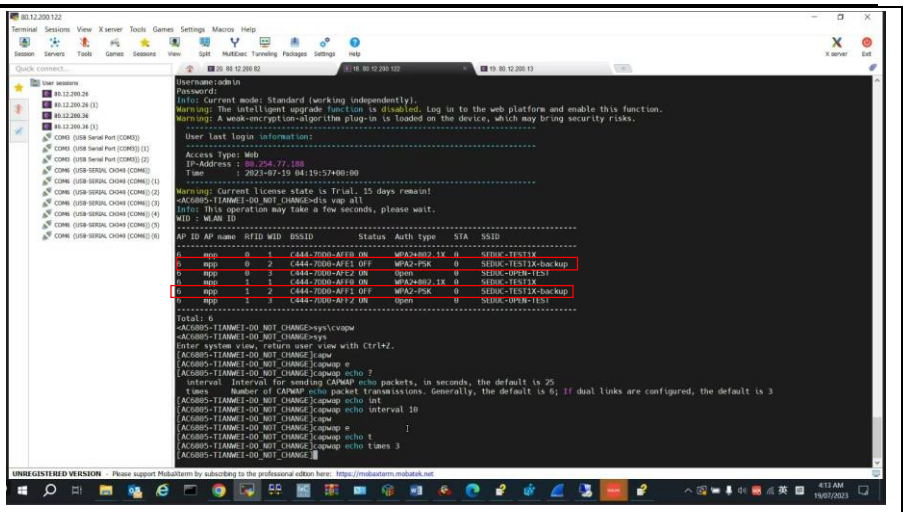


Figura 12 – Listando os SSIDs, disponiveis na controladora, vemos que o SSID SEDUC-TEST1X-backup, está com o status “OFF”.

Em seguida, foi configurado um intervalo baixo de verificação do tunel CAPWAP, com os comandos “capwap echo interval 10” e “capwap echo times 3”, em seguida o AP foi desconectado da controladora.

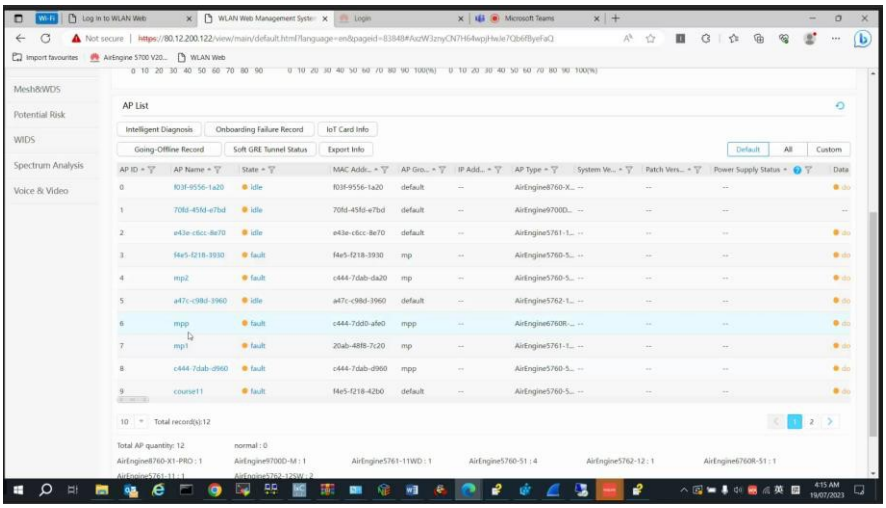


Figura 13 – Retornando a lista de APs disponiveis, verificamos que o AP ID 6, está com o status “fault”, ou seja, está offiline.

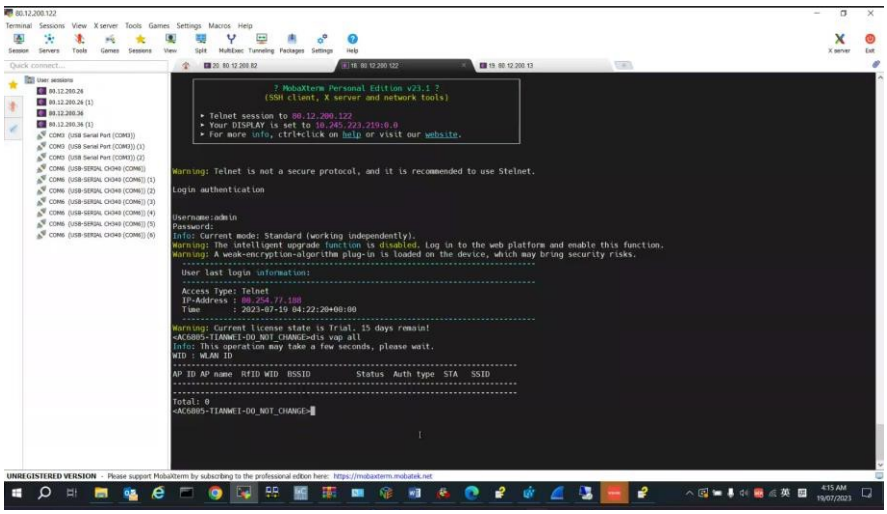
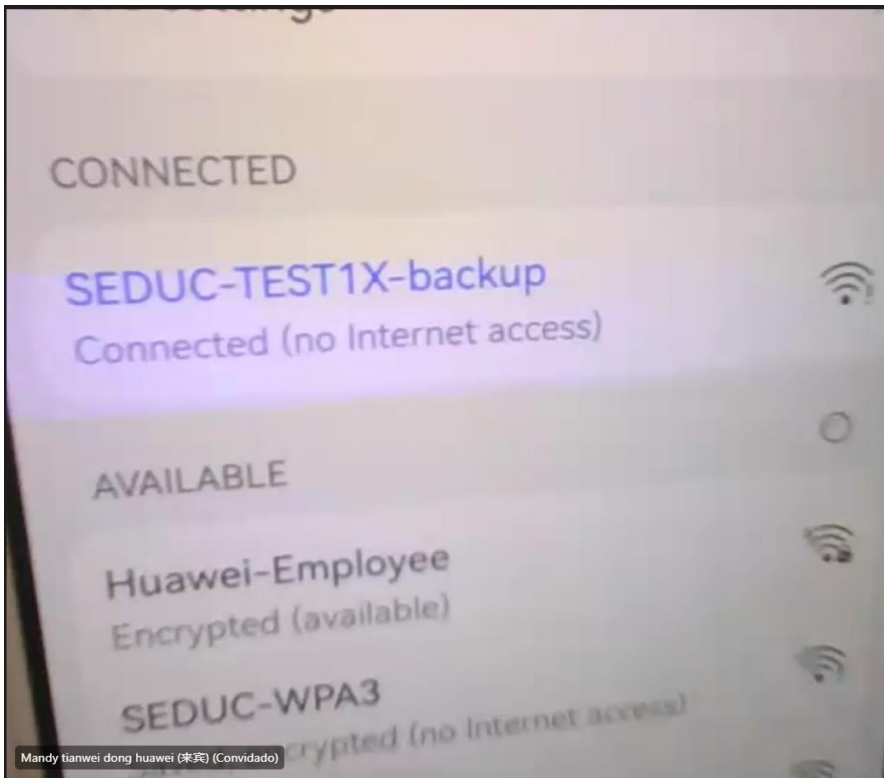
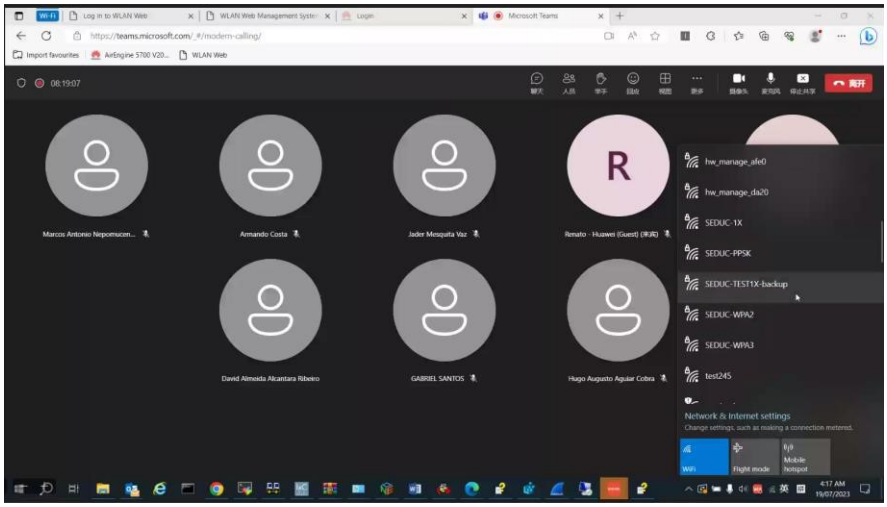


Figura 14 – O AP e seus SSIDs, não é mais listado na controladora via CLI.



	 Figura 15 e 16 – Em dispositivo movel localmente no mesmo ambiente dos testes, e no laptop, foi possível atestar que o SSID SEDUC-TEST1X-backup, estava sendo propagado.

Integração com domínio AD/LDAP para Autenticação

5.10.30 Implantar autenticação de usuários nas redes wireless por:

5.10.30.2 LDAP;

Item de teste	Integração com domínio AD/LDAP para Autenticação
Objetivo do teste	Verificar que o CloudCampus da Huawei oferece suporte à integração com o domínio AD/LDAP para autenticação
Configuração de teste	Topologia da Rede:

PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

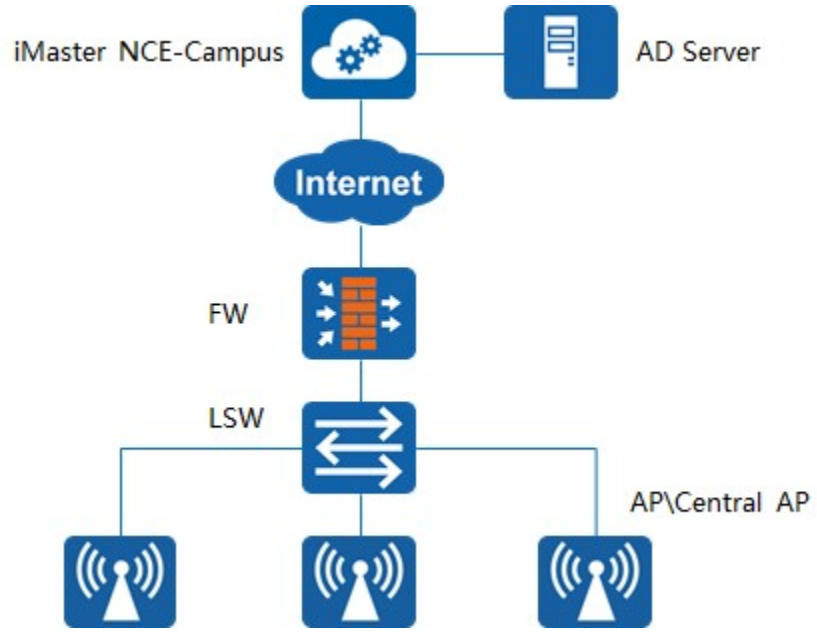
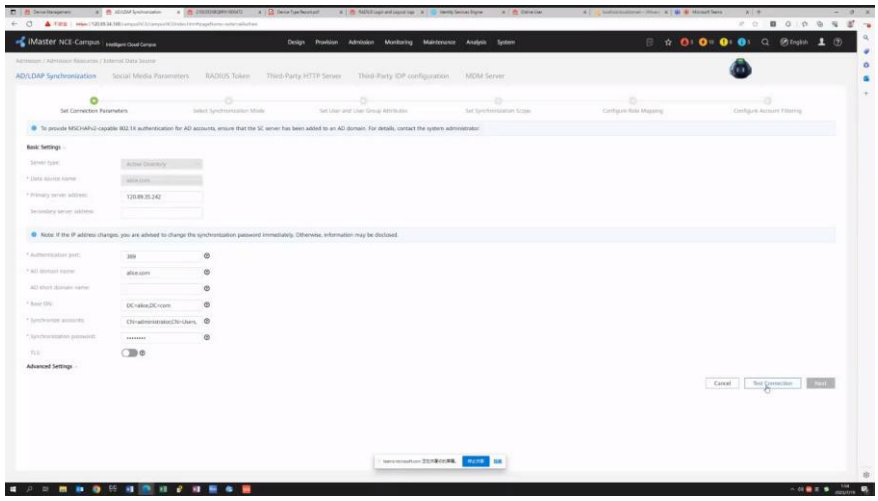
	 Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
Procedimento de teste	1) Integrar o AD/LDAP a plataforma iMaster NCE Campus
Resultado esperado	1) Sincronizar a base de usuários do AD/LDAP com o iMaster NCE Campus
Resultado	

Figura 1 – Na plataforma iMaster NCE Campus, foi configurado um servidor AD/LDAP, para o início da sincronização da base de usuários.

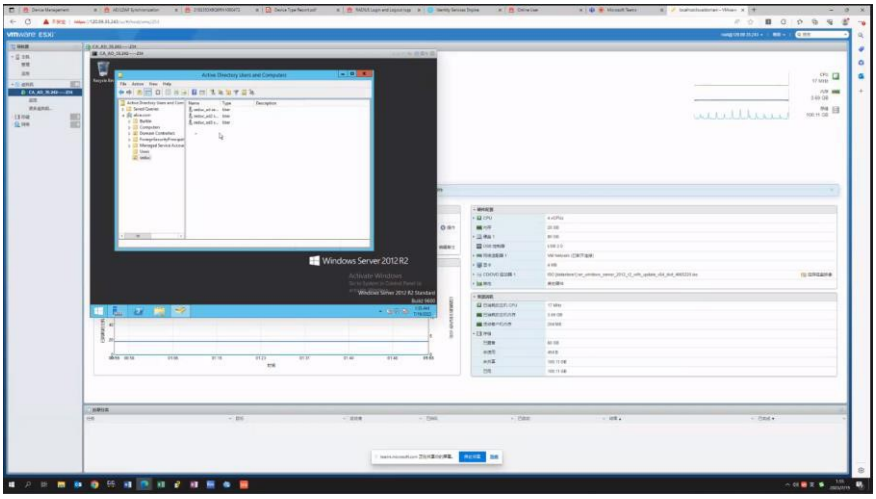
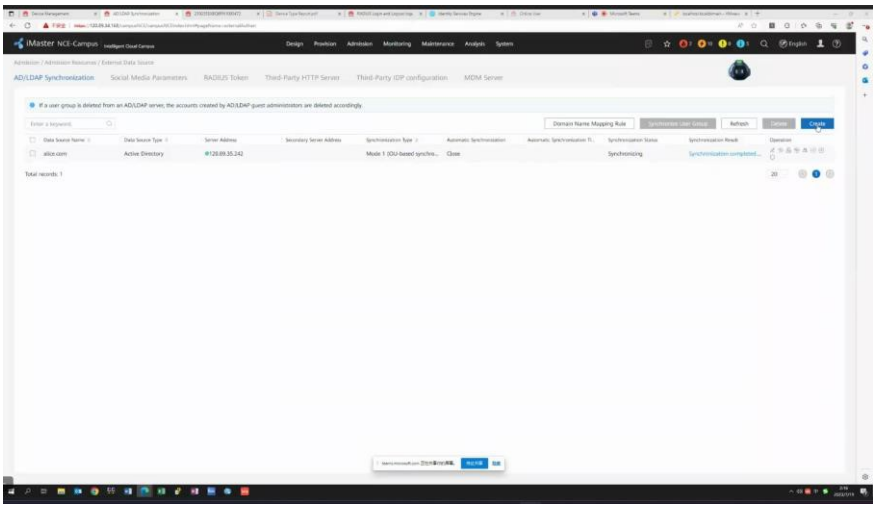
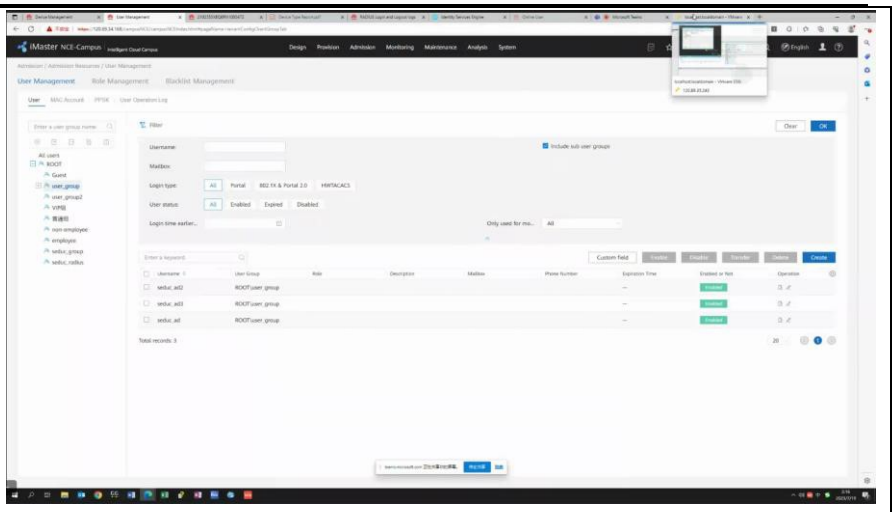
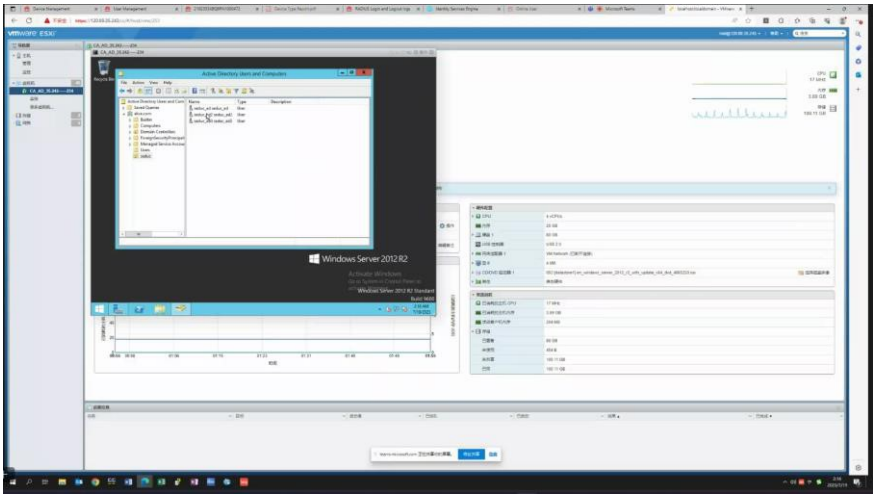


Figura 2 – No AD, são listados alguns usuários já criados.

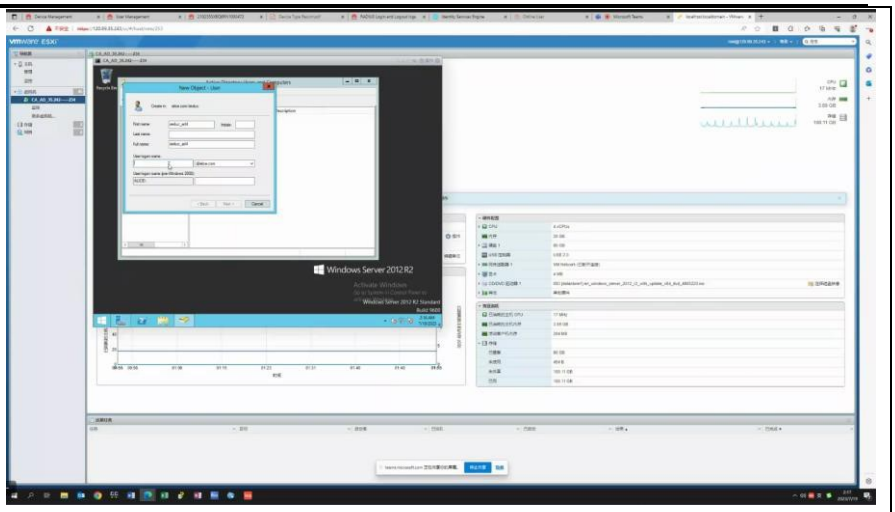


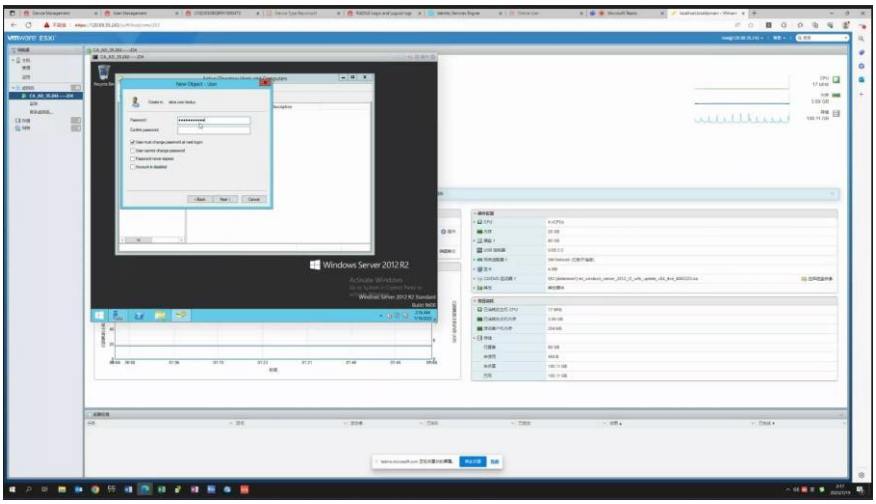


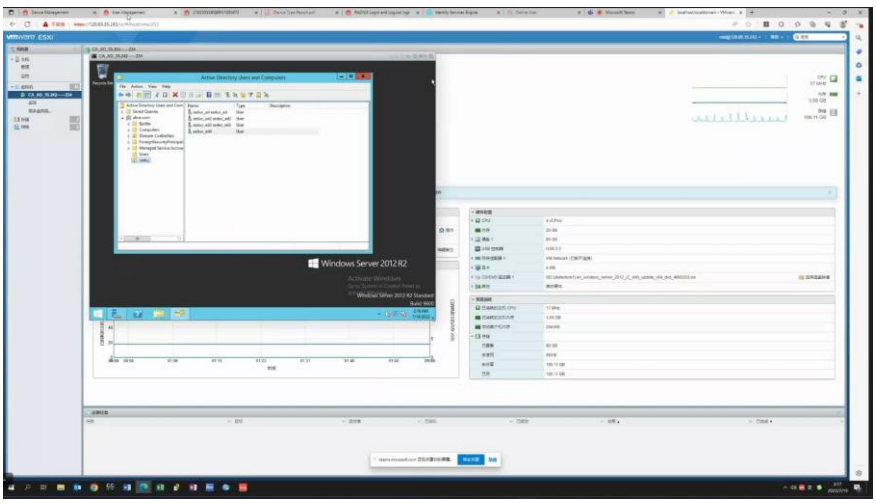
Figuras 3 e 4 – Após a primeira sincronização entre base de usuários, é possível ver que os mesmos são vistos via iMaster NCE Campus.

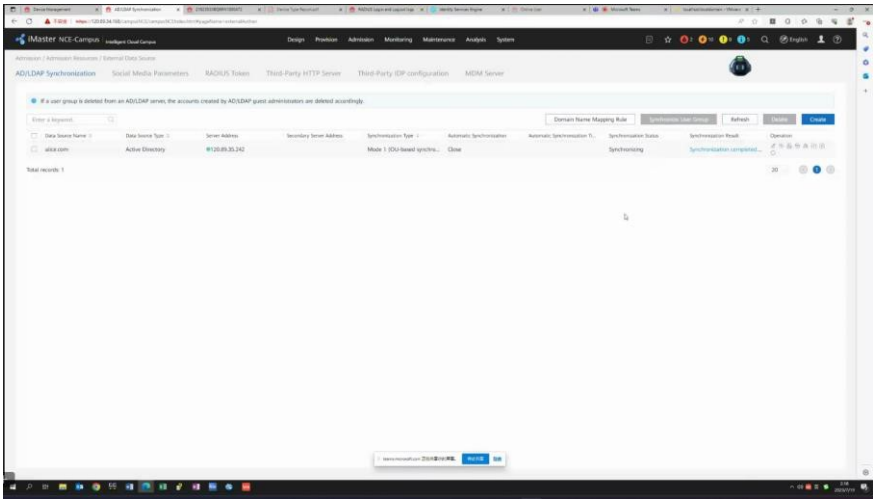
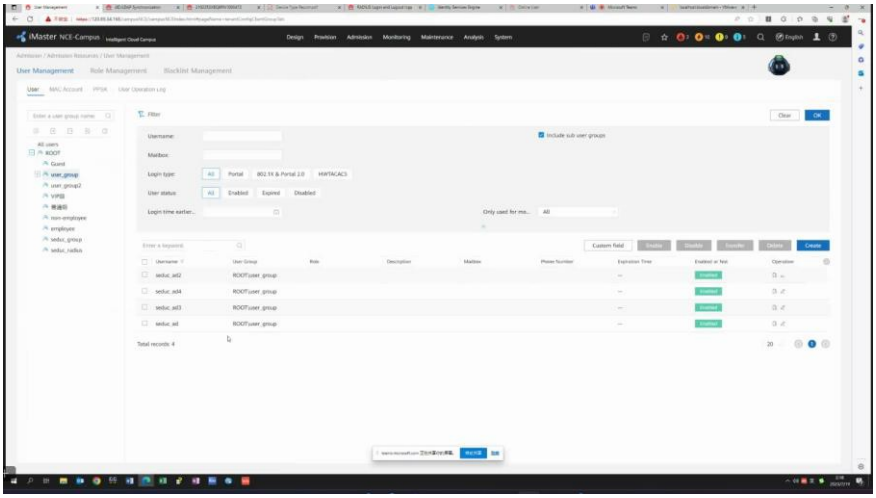


PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO
PROCESSO Nº 2020.0000.604.5301
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES





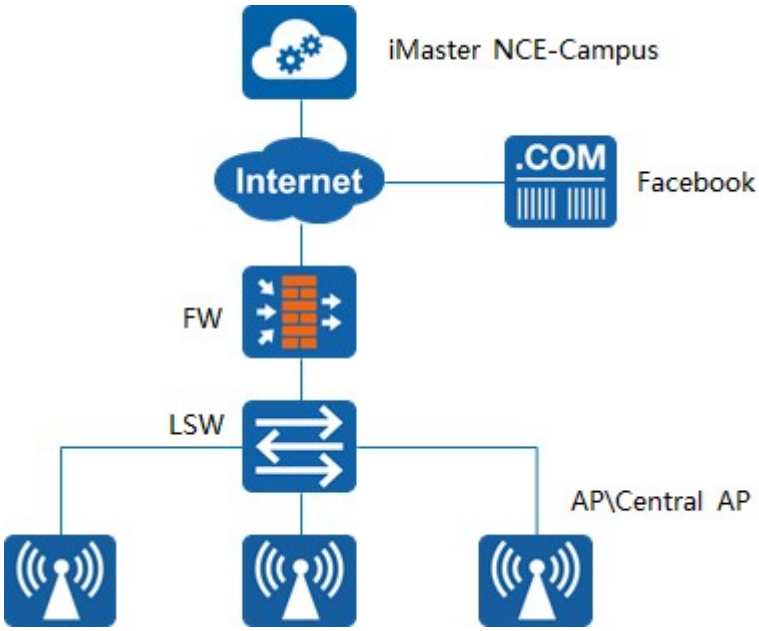


	Figuras 5 a 8 – Foi criado mais um usuário no AD/LDAP. O nome do usuário é “seduc_ad4”
	
	Figura 9 – Foi feita uma nova sincronização entre as bases de usuários.
	
	Figura 10 – O usuário “seduc_ad4” passa a ser listado no iMaster NCE Campus.

Facebook Authentication

5.10.30 Implantar autenticação de usuários nas redes wireless por:

5.10.30.3 Implementar pelo menos duas formas de autenticação que permita que o usuário obtenha acesso a rede sem a necessidade de usuário ou senha previamente cadastrados. Exemplo: Google, Office365, Facebook, Instagram, Linkedin, Twitter;

Item de teste	Autenticação via Facebook e Google
Objetivo do teste	Verificar se o CloudCampus da Huawei suporta funcionar como servidor de portal para fornecer autenticação do Facebook e Google para usuários Guest
Configuração de teste	Topologia da Rede:  Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima 3) Os parâmetros da conta facebook estão configurados corretamente.
Procedimento de teste	1) Configurar os parâmetros de autenticação via mídia social
Resultado esperado	1) O terminal móvel pode acessar a rede através de autenticação via Facebook e Google;
Resultado	

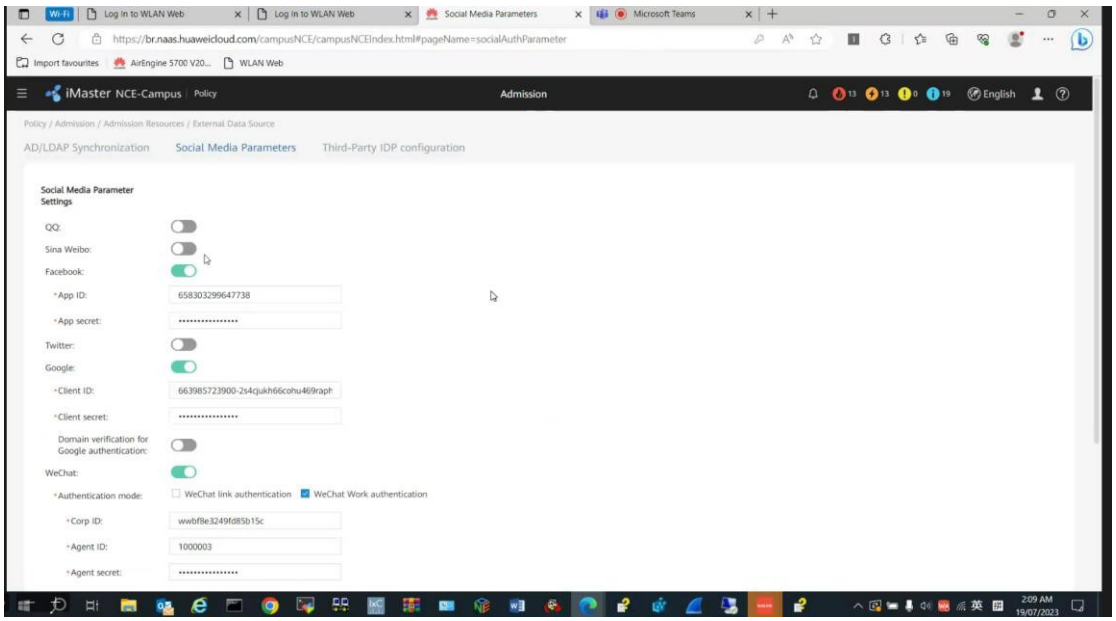


Figura 1 – Configurações para autenticação via redes sociais, onde estão configurados os dados para Facebook e Google.

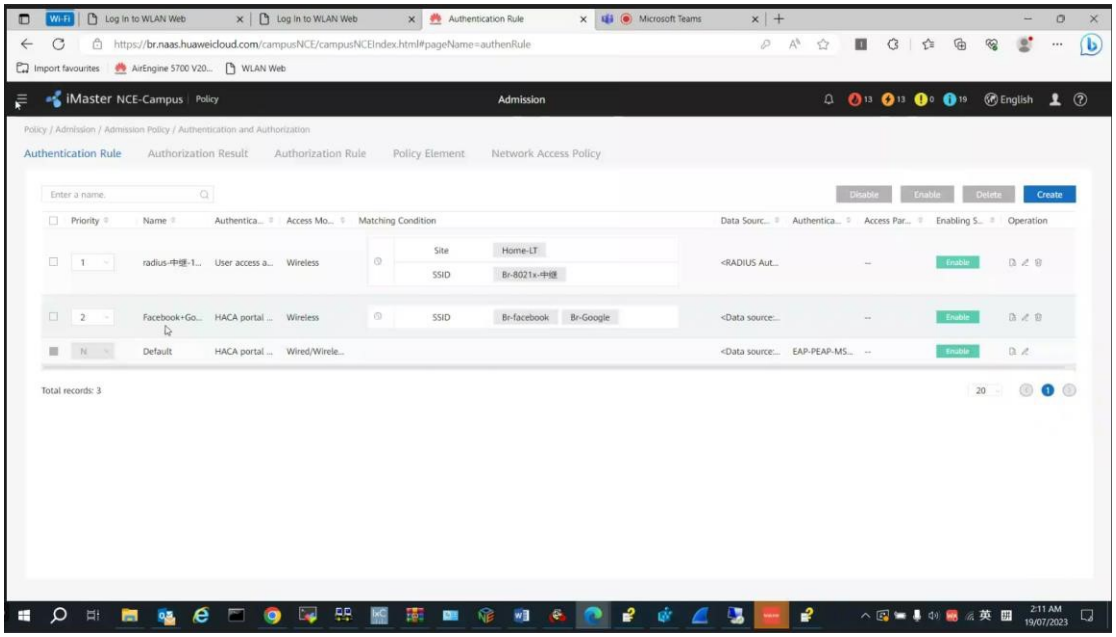
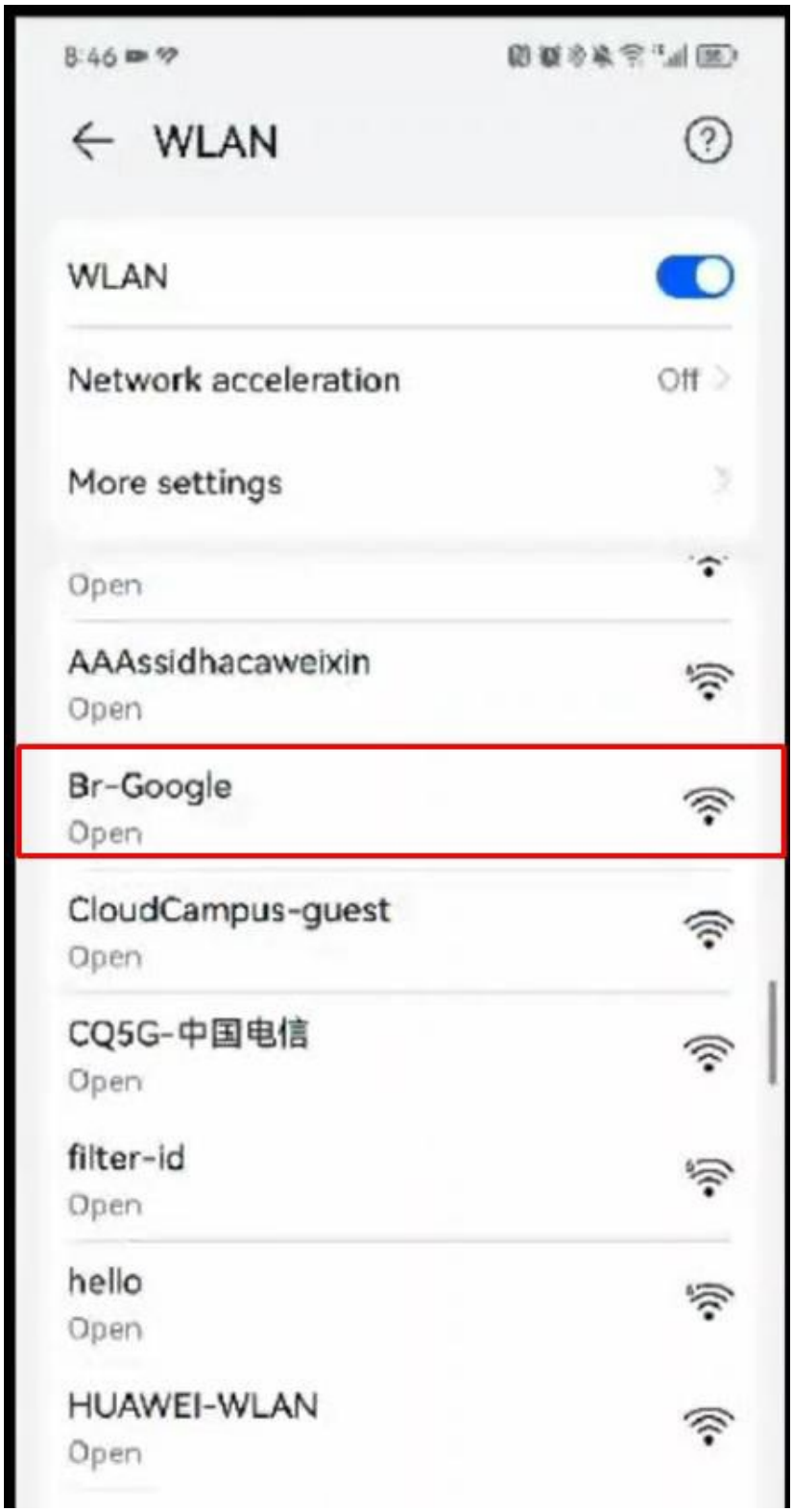
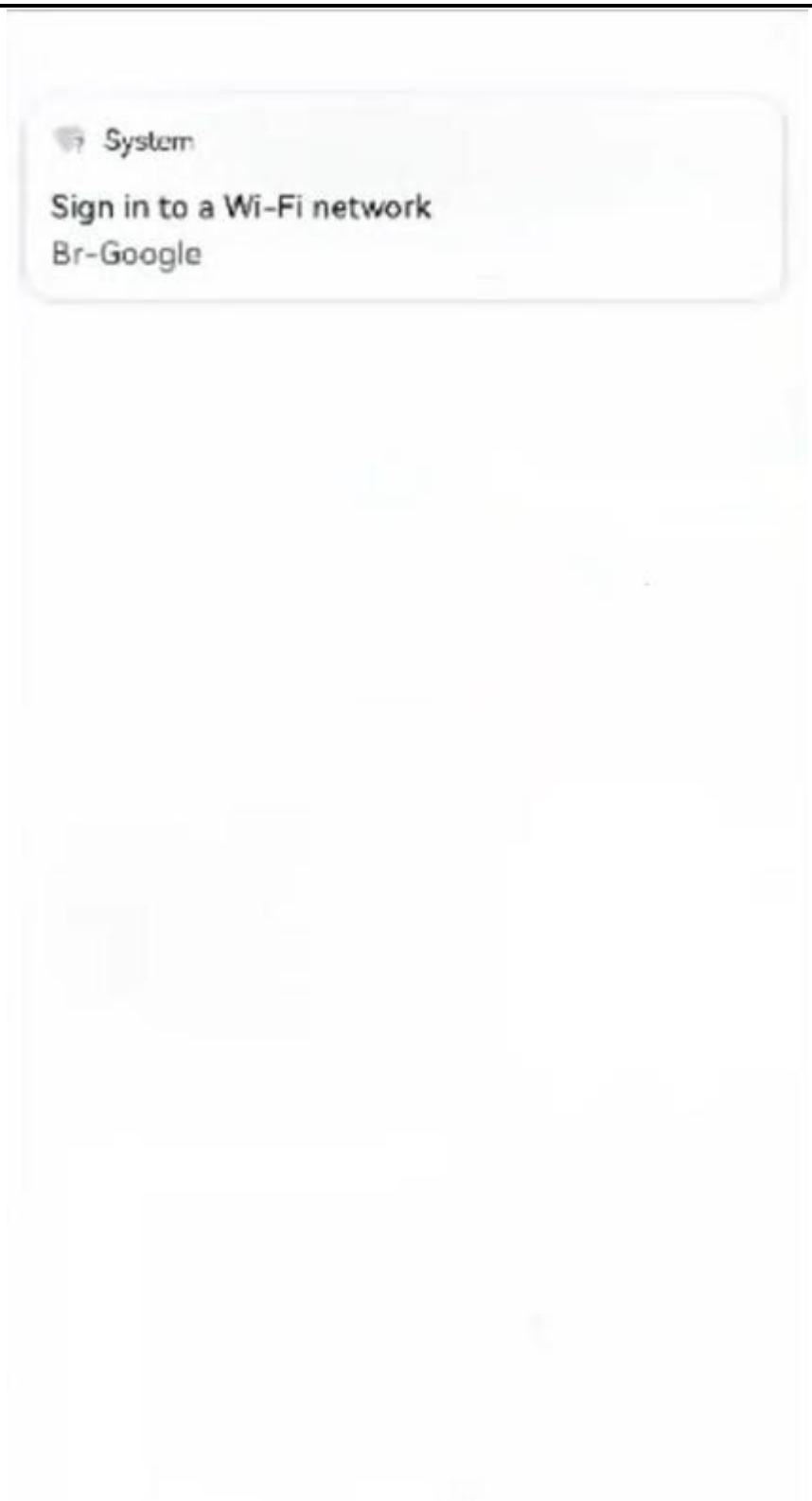


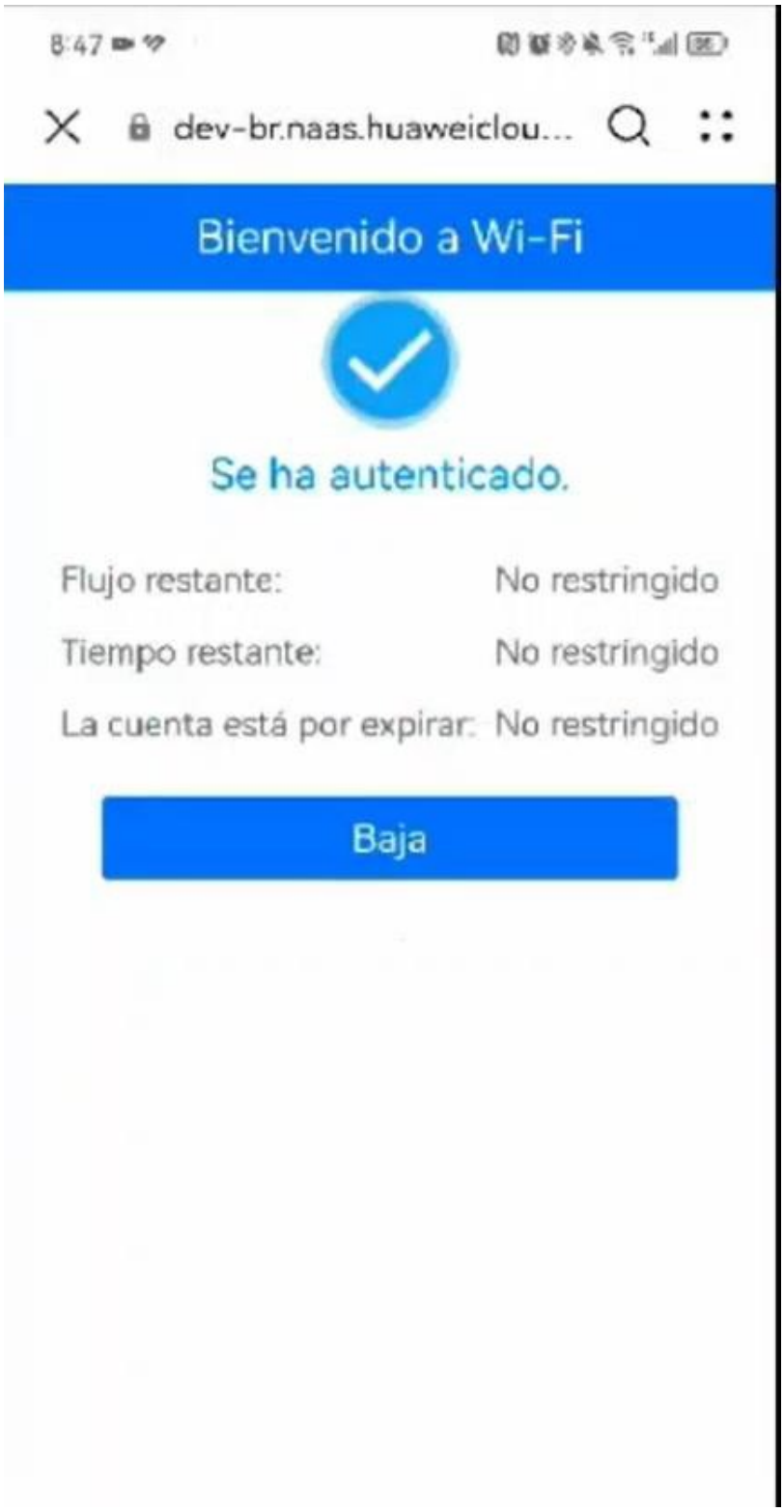
Figura 2 – Dentros das configurações de AAA, vemos as regras de autenticação tanto para Facebook quanto para Google, com os SSIDS Br-facebook e Br-Google


8:46
WLAN
WLAN
Network acceleration
Off
More settings
Open
AAAssidhacaweixin
Open
Br-Google
Open
CloudCampus-guest
Open
CQ5G-中国电信
Open
filter-id
Open
hello
Open
HUAWEI-WLAN
Open

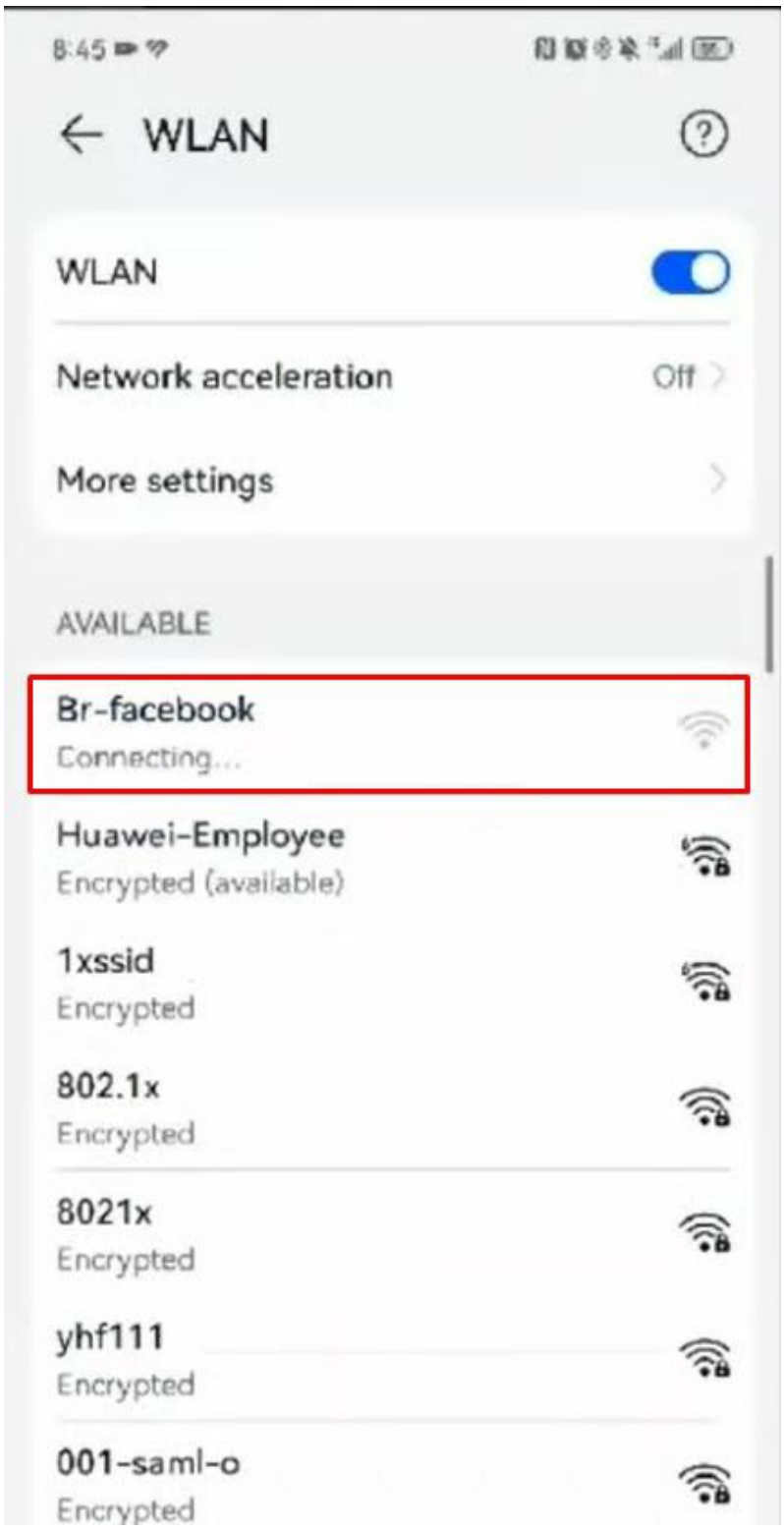

System
Sign in to a Wi-Fi network
Br-Google

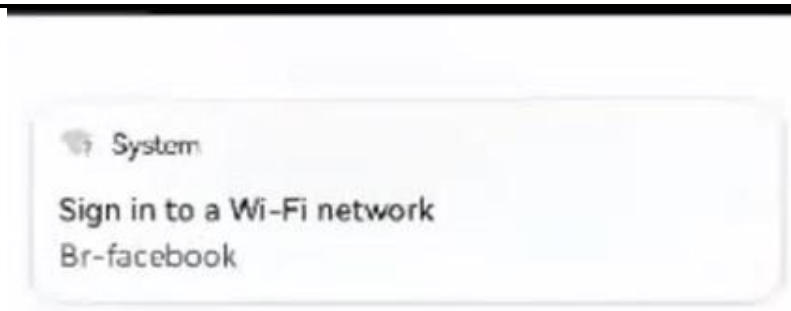

8:47
dev-br.naas.huaweiclou...
Bienvenido a Wi-Fi
Inicio de sesión
Google Auth
Instrucciones del usuario
Otros métodos de inicio de sesión
Bienvenido a WIFI, estaremos encantados de atenderte!

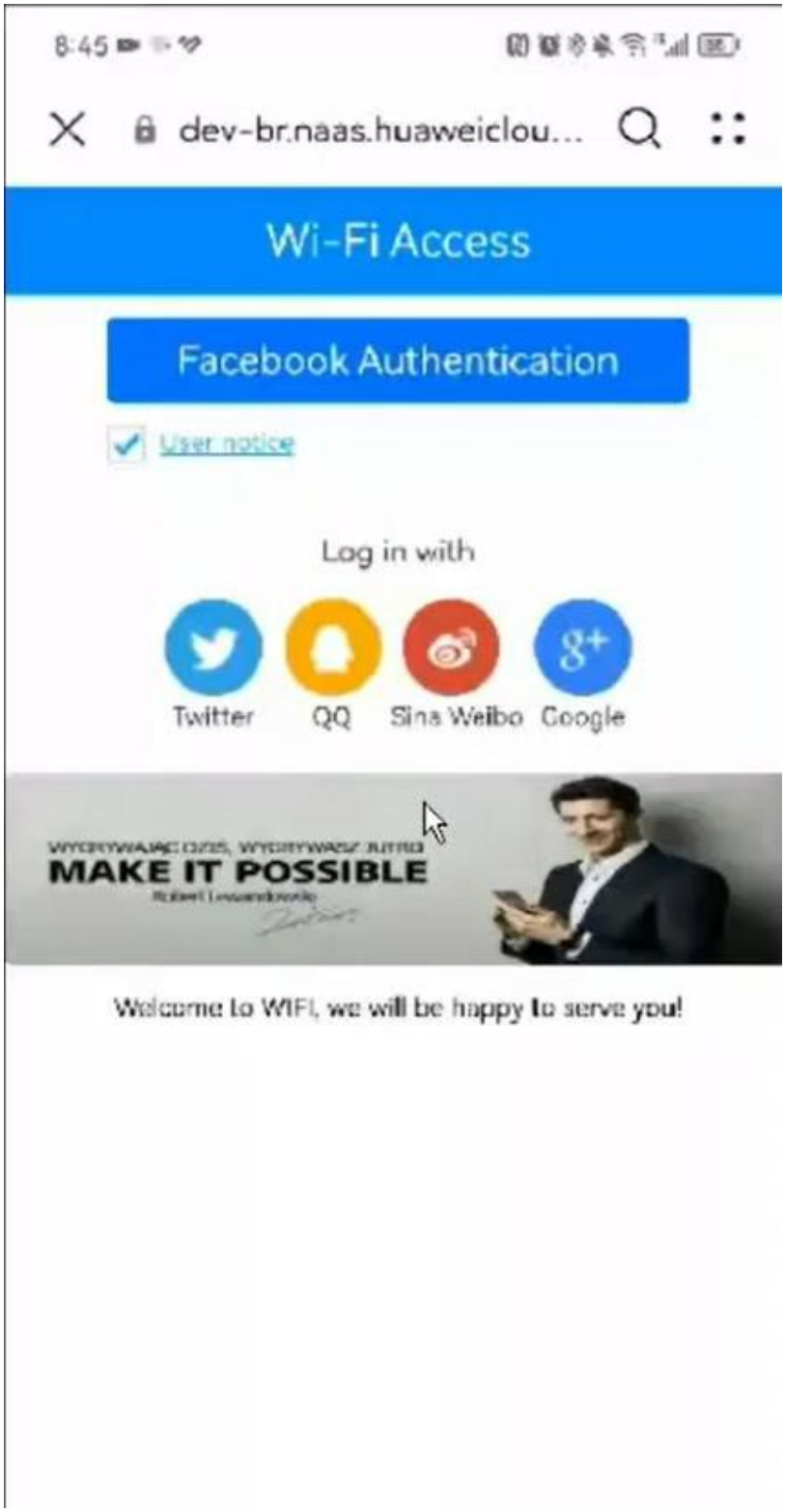

8:47
accounts.google.com
Google
选择帐号
mex alarm
alarm_mex@163.com
添加帐号

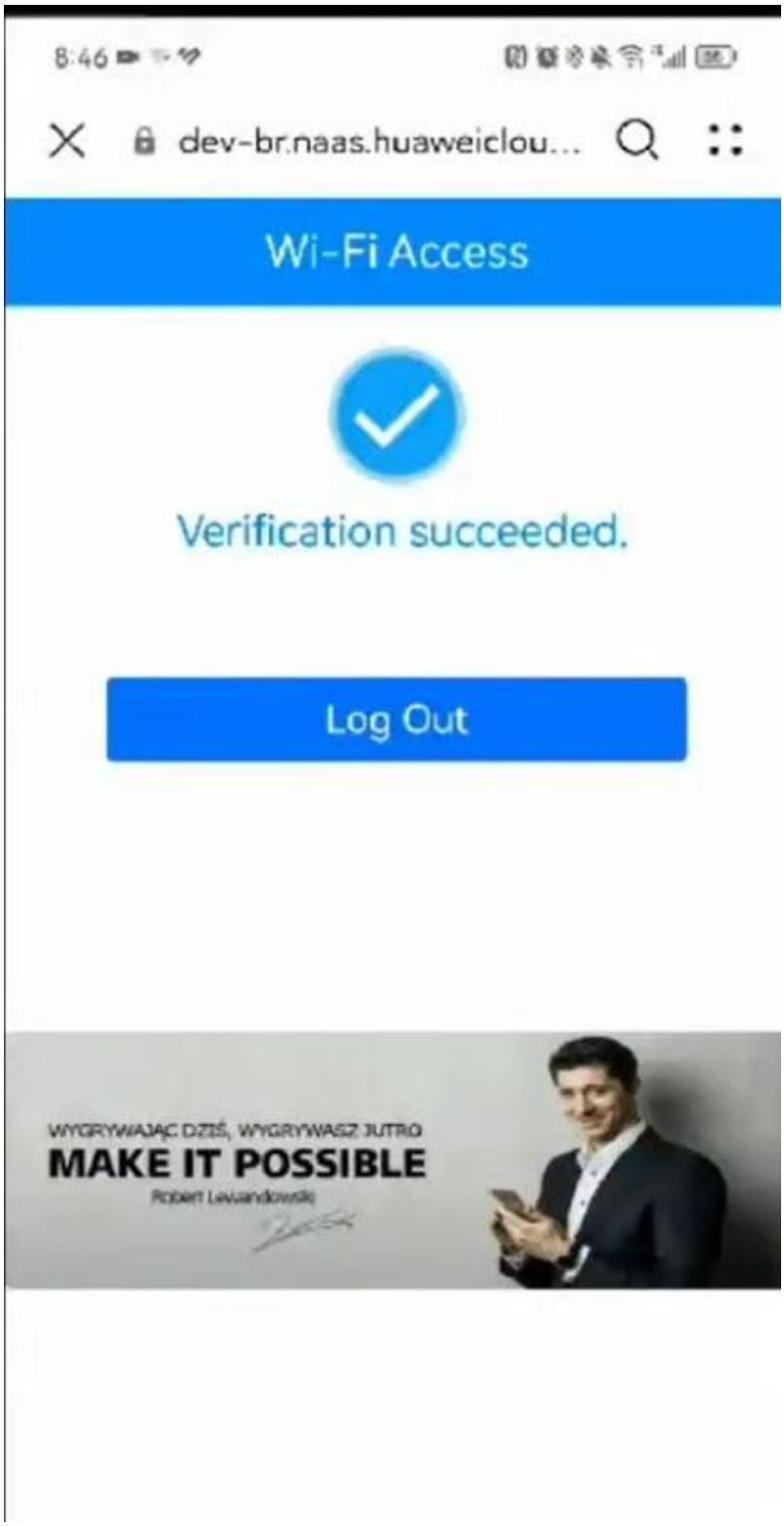

8:47
dev-br.naas.huaweiclou...
Bienvenido a Wi-Fi
Se ha autenticado.
Flujo restante: No restringido
Tiempo restante: No restringido
La cuenta está por expirar: No restringido
Baja

	Figuras 3 a 7 – Passo a passo de uma autenticação via mídias sociais, utilizando o Google como exemplo.


8:45
WLAN
WLAN
Network acceleration
Off
More settings
AVAILABLE
Br-facebook
Connecting...
Huawei-Employee
Encrypted (available)
1xssid
Encrypted
802.1x
Encrypted
8021x
Encrypted
yhf111
Encrypted
001-saml-o
Encrypted


System
Sign in to a Wi-Fi network
Br-facebook


8:45
dev-br.naas.huaweiclou...
Wi-Fi Access
Facebook Authentication
User notice
Log in with
Twitter
QQ
Sina Weibo
Google
MAKE IT POSSIBLE
Welcome to WIFI, we will be happy to serve you!


8:46
dev-br.naas.huaweiclou...
Wi-Fi Access
Verification succeeded.
Log Out
WYGRYWAJĄC DZIŚ, WYGRYWASZ JUTRO
MAKE IT POSSIBLE

Figuras 8 a 11 – Passo a passo de uma autenticação via mídias sociais, utilizando o Facebook como exemplo.

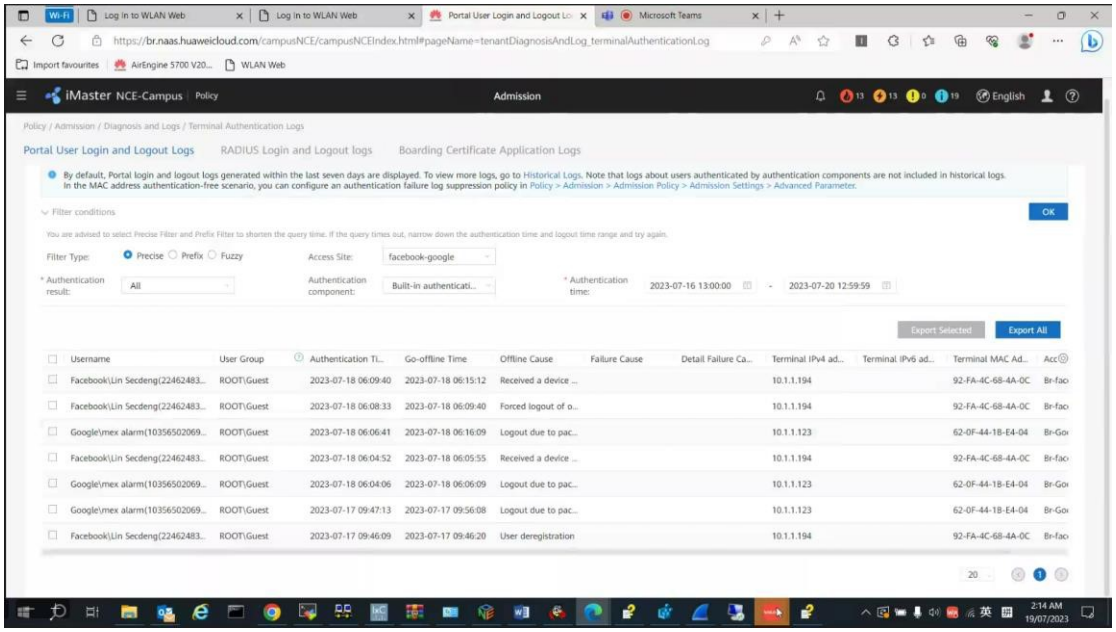
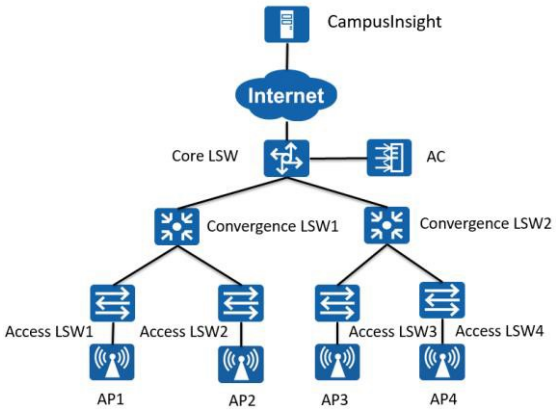


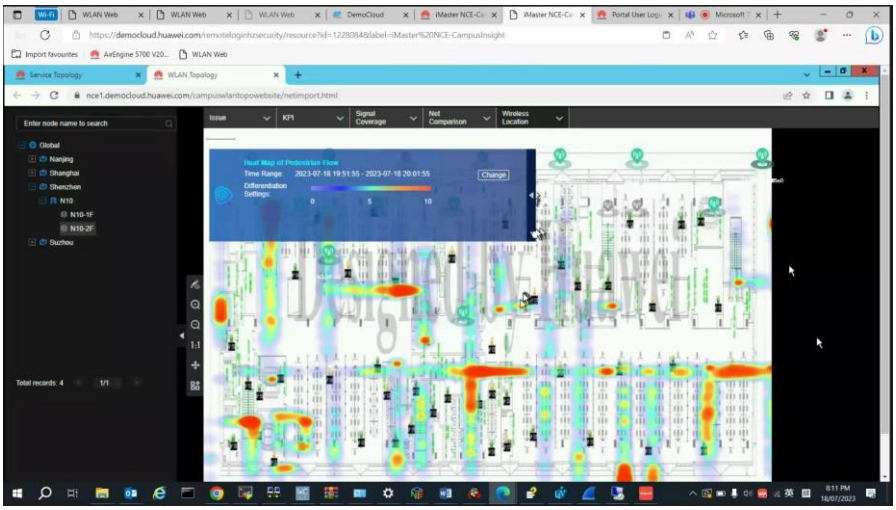
Figura 12 – Na plataforma iMaster NCE Campus, estão os registros das autenticações com mídias sociais.

Wireless Location and Heatmap

5.10.22 Deve permitir ao administrador visualizar e monitorar o mapa de cobertura da rede sem fio;

Item de	Wireless Location and Heatmap

teste	
Objetivo do teste	Para verificar a função de localizar terminais sem fio na topologia WLAN..
Topologia da Rede:	 Prerequisites: 1. O CampusInsight e o pacote de patch de localização sem fio foram instalados e o sistema está funcionando corretamente. 2. A AC e os APs foram configurados para relatar toda a telemetria necessária.
Procedimento de teste	1. Realizar login no CampusInsight e selecionar **Inventory** > **Service Topology** do menu principal. Clique no icone **Enter WLAN Topology** na esquerda. Na página de topologia de WLAN exibida, selecione um piso planejado no painel de navegação e clique **Wireless Location** no canto superior direito. Resultado esperado 1. 2. Selecione o **Heat Map of Pedestrian Flow** e clique **OK**. Resultado esperado 3. 3. Selecionar **Wi-Fi Interference** e clique **OK**. Resultado esperado 4.
Resultado esperado	1. Na topologia, um mapa de calor baseado no tráfego do cliente detectado é exibido no caminho percorrido, e o tráfego do cliente pode ser distinguido por cores diferentes.

Resultado	 Figura 1 – O mapa de calor é mostrado na plataforma iMaster NCE CampusInsight.