

# **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


Support > WLAN > AP > AirEngine 5700   My Support  | Feedback  | Help


### AirEngine 5700 Series Access Points + Subscribe

AirEngine 5760-10	AirEngine 5760-11DH	AirEngine 5760-22W	AirEngine 5760-22WD
AirEngine 5760-51	AirEngine 5761-10W	AirEngine 5761-10WD	AirEngine 5761-11
AirEngine 5761-11EI	AirEngine 5761-11W	AirEngine 5761-11WD	AirEngine 5761-12
AirEngine 5761-12W	AirEngine 5761-21	AirEngine 5761R-11	<b>All Models</b>

Next-generation high-performance Wi-Fi 6 (802.11ax) access point (AP), ideal for coverage scenarios such as small and midsize enterprise offices, retail outlets, and education institutions.


[Expand](#) 


[Specifications](#) 

Documentation
Knowledge Base
Software Download
Bulletins
Tools
Video
Forum
Enter keyword 

Search by:

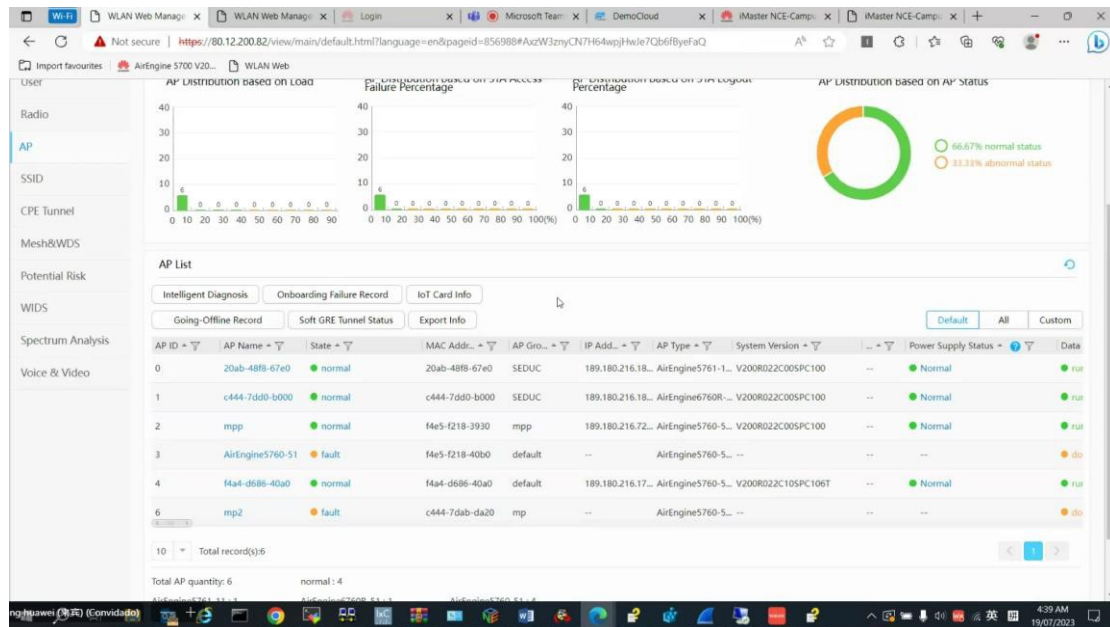
Select Version:

 Version and Patch

Version and Patch Number	Status	Publication Date
AirEngine 5700 V200R022C00SPC100 	Valid	2022-11-11

### 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

Support > WLAN > AP > AirEngine 6700

AirEngine 6700 Series Access Points [+ Subscribe](#)

AirEngine 6760-51E1	AirEngine 6760-X1	AirEngine 6760-X1E	AirEngine 6760R-51
AirEngine 6760R-51E	AirEngine 6761-21	AirEngine 6761-21E	AirEngine 6761-21T
AirEngine 6761-22T	AirEngine 6761S-21	AirEngine 6761S-21T	

Next-generation ultra-high-performance Wi-Fi 6 (802.11ax) access point (AP). Indoor APs ideal for high-density scenarios such as midsize and large enterprise offices, education institutions, and business spaces. Outdoor APs

Specifications

Documentation | Knowledge Base | **Software Download** | Bulletins | Tools | Video | Forum

Search by:

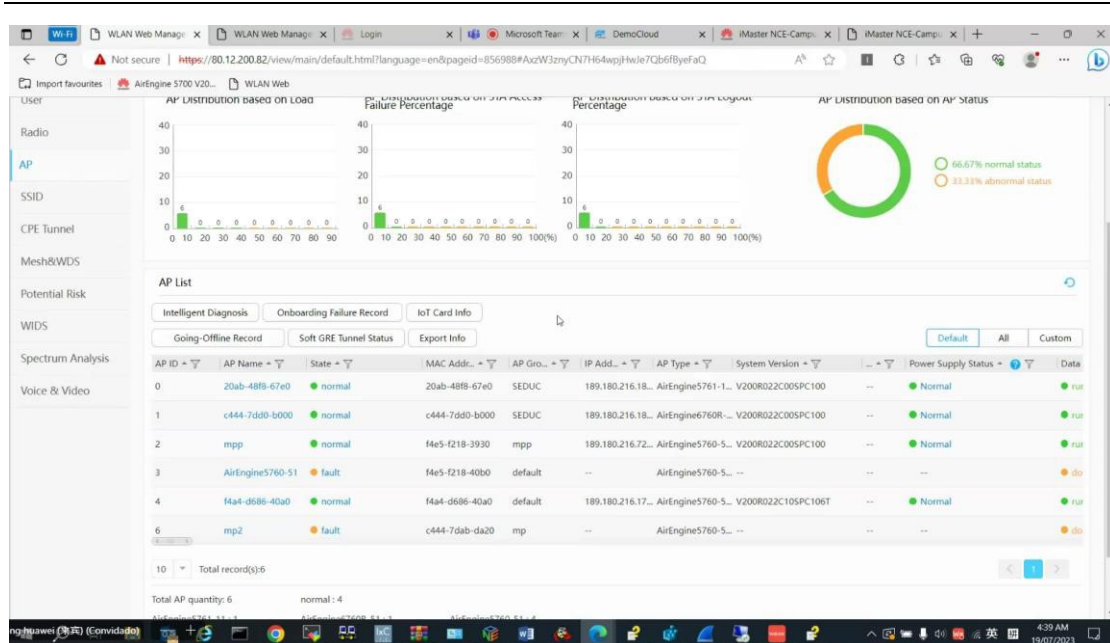
Select Version:

Version and Patch

Version and Patch Number	Status	Publication Date
AirEngine 6700 V200R022C00SPC100	Valid	2022-11-11

## 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**

Support > Switches > Campus Switch > S3700&S5700&S6700 Series > CloudEngine S5735-L-V2

My Support | Feedback | Help

### CloudEngine S5735-L-V2

Series: S3700&S5700&S6700 Series  
Classification: S5735-L-V2 Switches

Documentation Knowledge Base **Software Download** Bulletins Tools Video Forum

Search by: All All

Select Version: S3700&S5700&S6700 V600R022 All

Version and Patch

Version and Patch Number	Status	Publication Date
S3700&S5700&S6700 V600R022C00SPC500	Valid	2022-11-11

**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
```

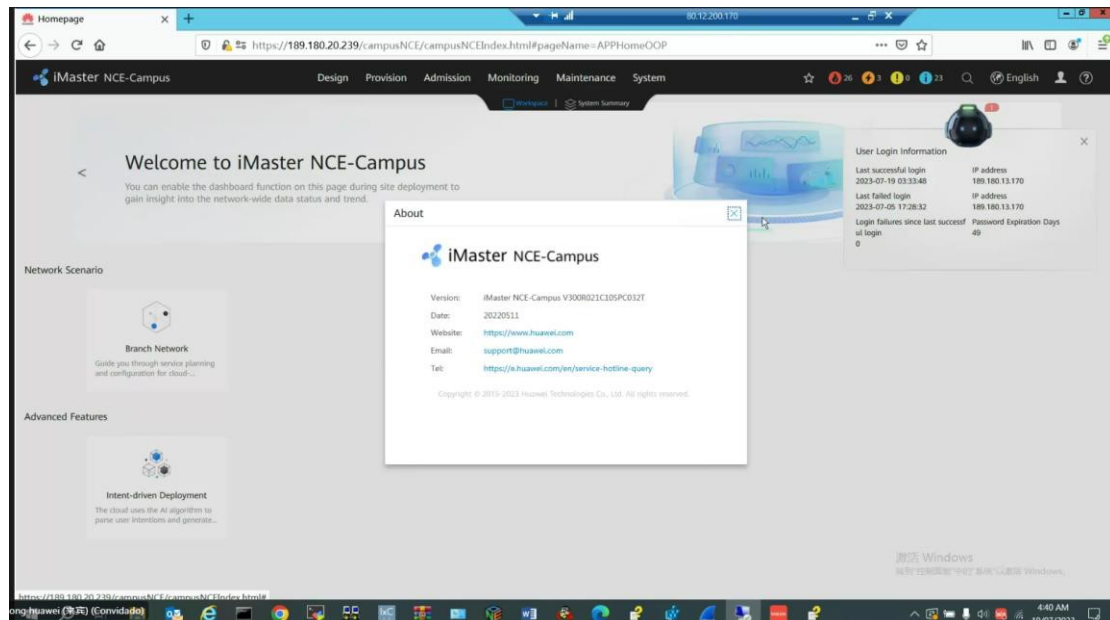
**Solução de gerenciamento e controle de Switches e APs**

**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**

[Support](#) > [WLAN](#) > [AC](#) > [AC6000](#)
My Support | Feedback | Help

## AC6000 Series WLAN Access Controllers + Subscribe

AC6003	AC6005	AC6507S	AC6508
AC6605	AC6800V	AC6805	

This Access Controller (AC), when used in conjunction with Huawei Access Points (APs), is ideal for constructing campus networks, enterprise office networks, wireless Metropolitan Area Networks (MANs), and hotspot coverage.
   
[Expand](#)

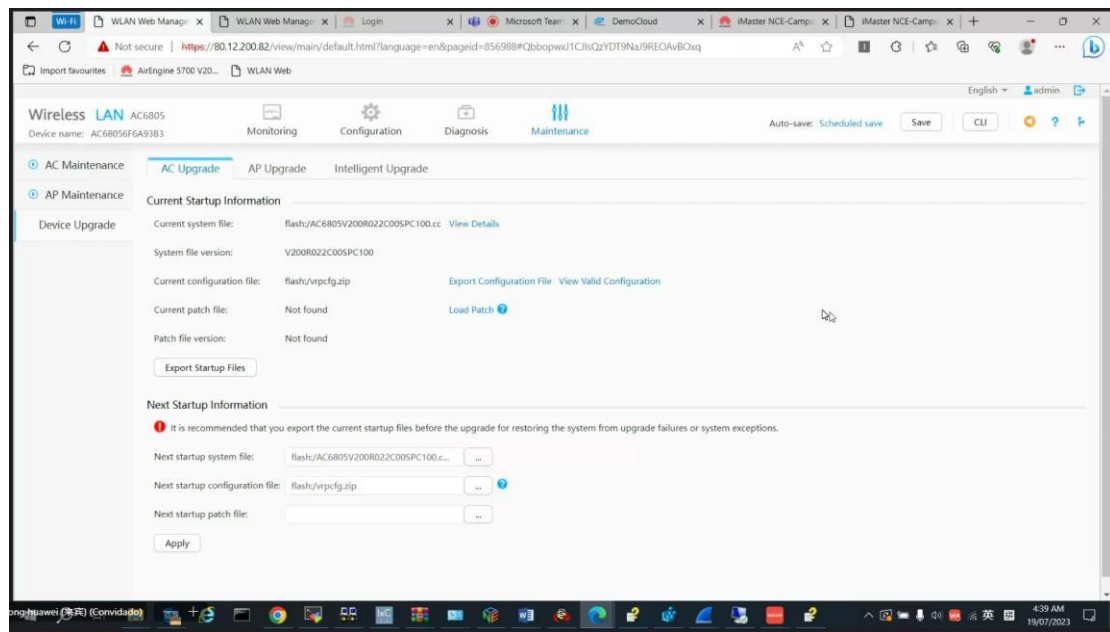
[Documentation](#) | [Knowledge Base](#) | **[Software Download](#)** | [Bulletins](#) | [Tools](#) | [Video](#) | [Forum](#)
Enter keyword

Search by: 
  
 Select Version:

Version and Patch

Version and Patch Number	Status	Publication Date
AC6000 V200R022C00SPC100	Valid	2022-11-11

### Evidência:



The screenshot shows the 'AC Upgrade' page in the Huawei AC6805 Web Management Interface. The device name is AC6805FA9383. The page is divided into 'Current Startup Information' and 'Next Startup Information' sections.

**Current Startup Information:**

- Current system file: flash:/AC6805V200R022C00SPC100.cc
- System file version: V200R022C00SPC100
- Current configuration file: flash/vrpcfg.zip
- Current patch file: Not found
- Patch file version: Not found

**Next Startup Information:**

- Next startup system file: flash:/AC6805V200R022C00SPC100.c...
- Next startup configuration file: flash/vrpcfg.zip
- Next startup patch file: (empty)

A warning message states: "It is recommended that you export the current startup files before the upgrade for restoring the system from upgrade failures or system exceptions."

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](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](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](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](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](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](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](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](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

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

---

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](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](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;


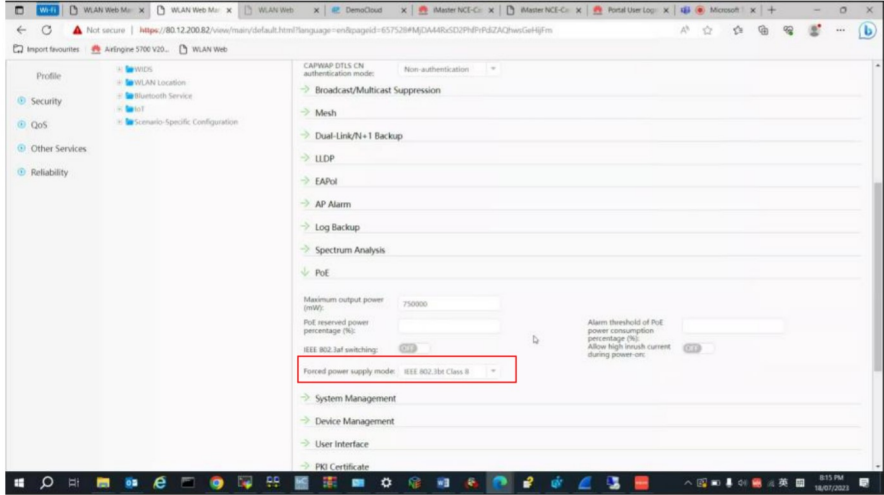
5.7.2.5 Possuir capacidade de alimentação PoE 802.3af, 802.3at ou 802.3bt;

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;

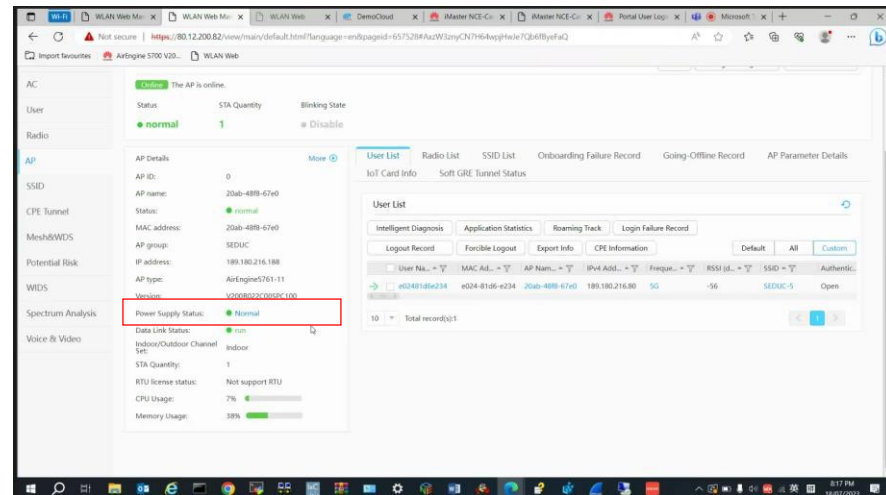
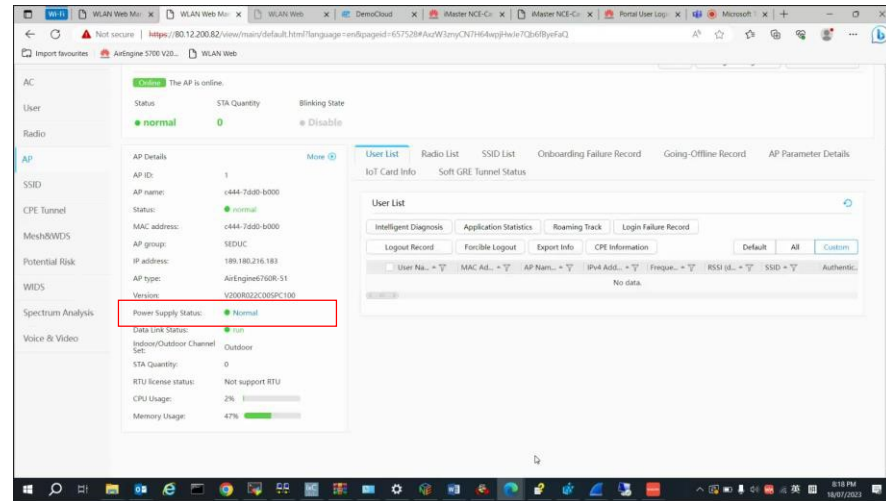
5.8.3 O Switch deve ser capaz de alimentar os Access Points Tipo 1 sem a necessidade de componentes adicionais;

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

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

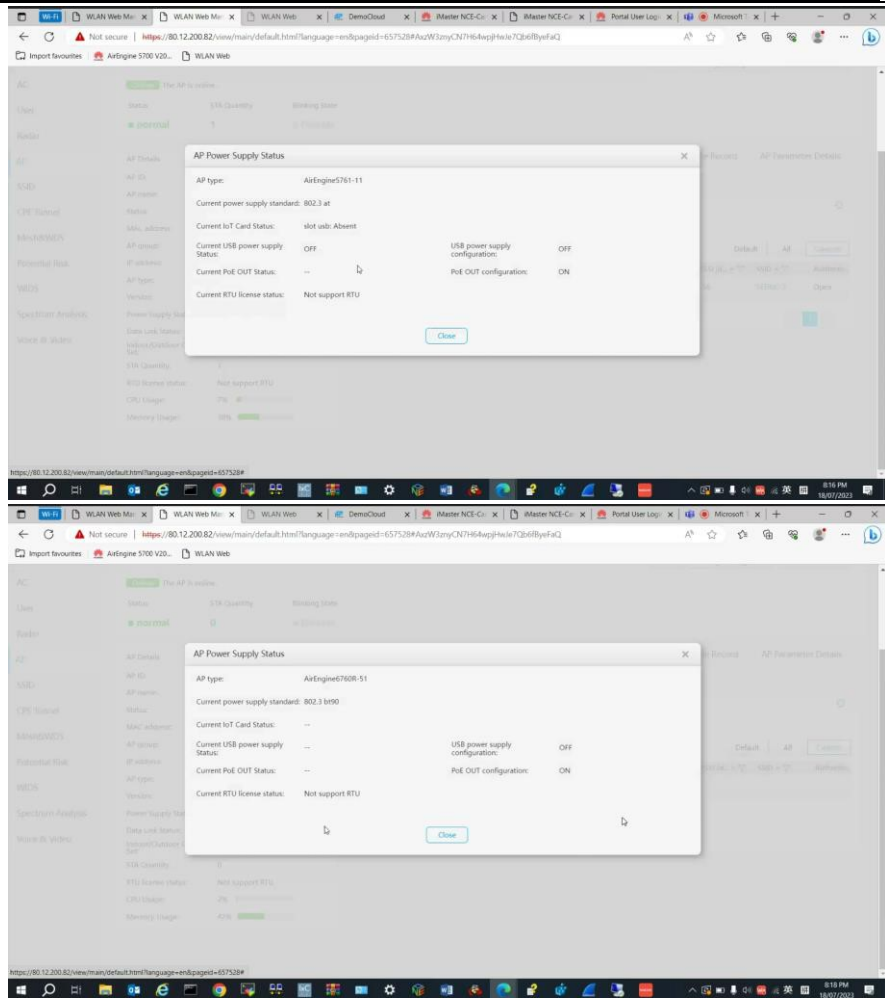
**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

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”.

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



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.

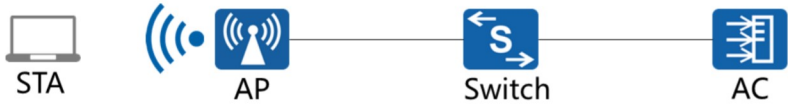
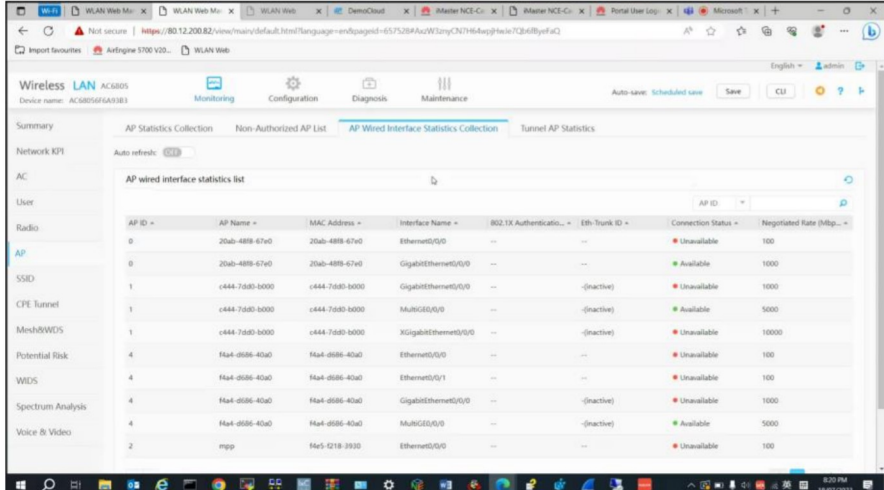
Para o modelo AirEngine 5761-11, 802.3at  
 Para o modelo AirEngine 6760R-51, 802.3bt

## 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;

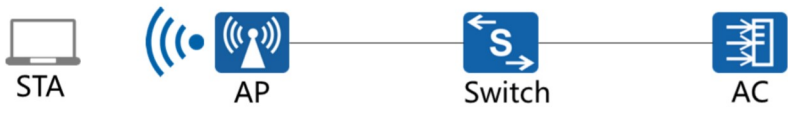
<b>Item de teste</b>	<b>Negociação de portas</b>
<b>Objetivo do teste</b>	Validar que o access point sem fio tenha pelo menos 1 interface 10/100/1000 Base-T ou acima;
<b>Configuração de teste</b>	Topologia da rede: <div style="text-align: center;">  </div> Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
<b>Procedimento de teste</b>	1) Verifique a velocidade da porta cabeada no AP.
<b>Resultado esperado</b>	1) O AP está operacional; a velocidade da porta é mostrada.
<b>Resultado</b>	<div style="border: 1px solid black; padding: 5px;">  <p>Figura 1 – Na controladora, é possível checar a listagem de interfaces dos pontos de acesso, bem como a negociação dessas interfaces.</p> </div>

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 conforme o padrão IEEE 802.1Q;

<b>Item de teste</b>	<b>Múltiplas VLANs</b>
<b>Objetivo do teste</b>	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;
<b>Configuração de teste</b>	Topologia da rede: <div style="text-align: center; margin: 10px 0;">  </div> Condições iniciais: <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Após as configurações de SSID da AC, realize uma captura de pacotes na;</li> <li>2) Crie 16 VLANs e add use them as service vlan for SSIDs.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) O pacote mostra a marcação de vlan 802.1q.</li> <li>2) 16 VLANs estão disponíveis no AP.</li> </ol>

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

**Resultado**

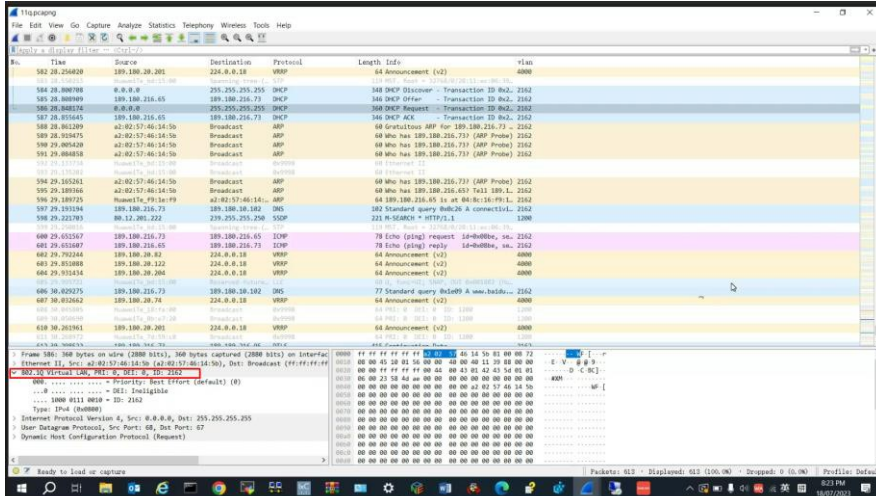
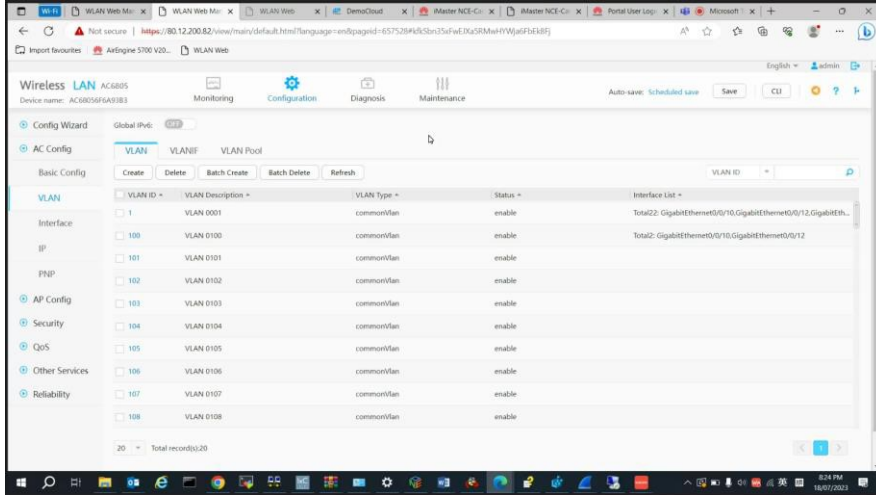


Figure 1 shows a Wireshark capture of network traffic. A specific frame is highlighted in red, showing an Ethernet II frame with a source MAC of 08:00:27:14:00:00 and a destination MAC of 08:00:27:14:00:00. The frame is tagged with a VLAN ID of 2162. The packet details pane shows the Ethernet II frame structure, including the source and destination MAC addresses, the protocol type (0x0800), and the VLAN ID (2162). The packet bytes pane shows the raw hexadecimal and ASCII representation of the frame, with the VLAN tag clearly visible.

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



The screenshot shows the configuration interface for a WLAN device. The 'VLAN' tab is selected, and a table of configured VLANs is displayed. The table includes columns for VLAN ID, VLAN Name, VLAN Type, Status, and Interface List. The following table represents the data shown in the interface:

VLAN ID	VLAN Name	VLAN Type	Status	Interface List
1	VLAN 0001	commonVlan	enable	Total2: GigabitEthernet0/10,GigabitEthernet0/12,GigabitEthernet0/14
100	VLAN 0100	commonVlan	enable	Total2: GigabitEthernet0/10,GigabitEthernet0/12
101	VLAN 0101	commonVlan	enable	
102	VLAN 0102	commonVlan	enable	
103	VLAN 0103	commonVlan	enable	
104	VLAN 0104	commonVlan	enable	
105	VLAN 0105	commonVlan	enable	
106	VLAN 0106	commonVlan	enable	
107	VLAN 0107	commonVlan	enable	
108	VLAN 0108	commonVlan	enable	



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

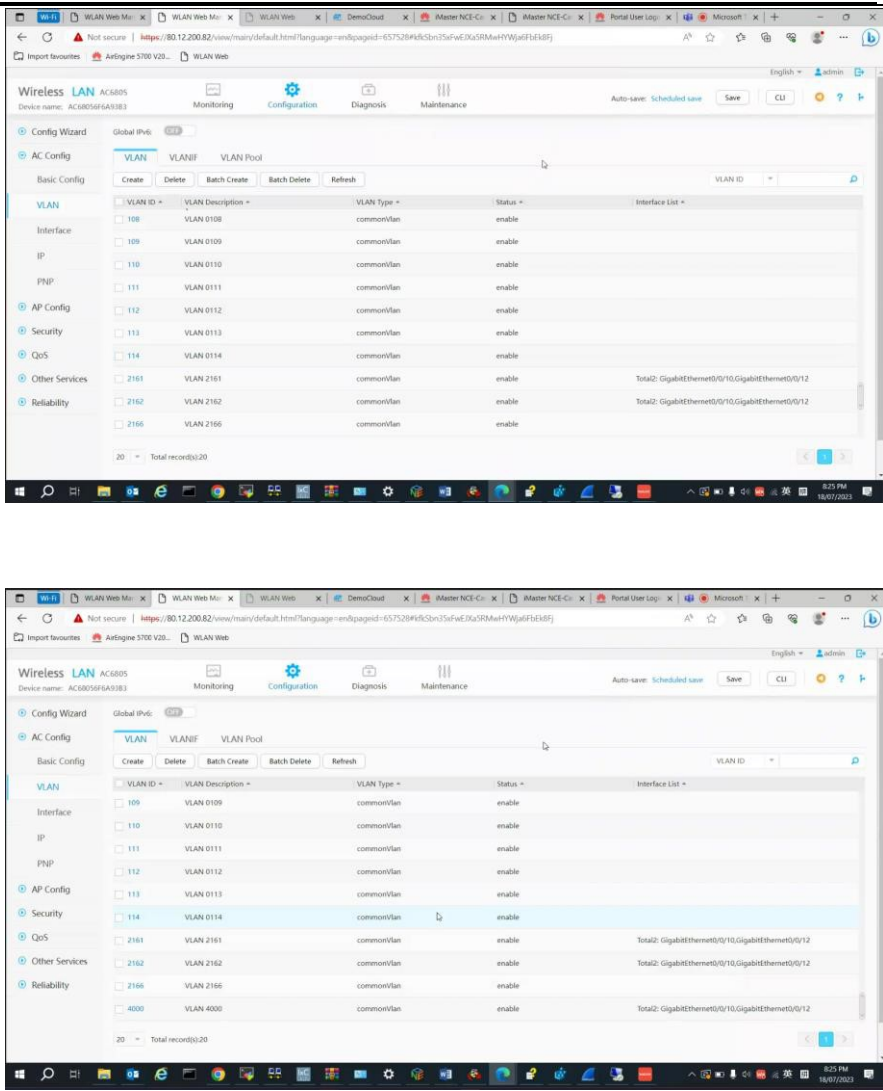
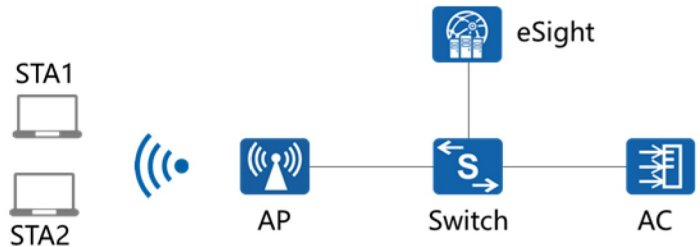
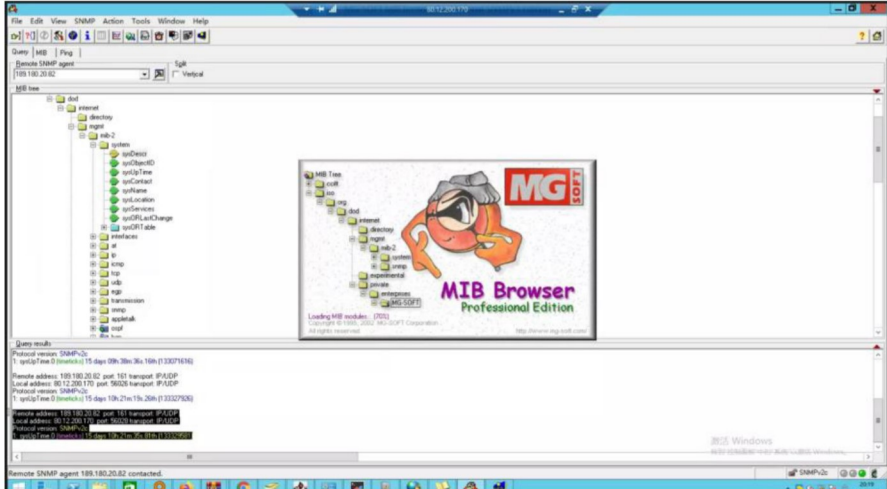


Figura 2, 3 e 4 – Na controladora, foram configuradas várias VLANs diferentes, contabilizando um total de 20 VLANs configuradas e aplicadas aos APs registrados.

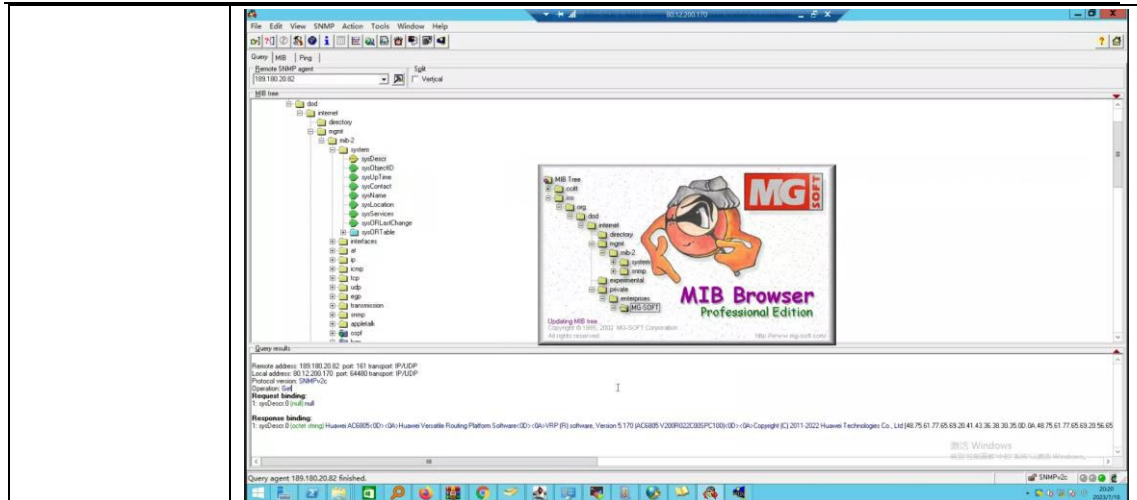
**Sistema de WLAN suporta a função de SNMP**

<p><b>Item de teste</b></p>	<p><b>Sistema de WLAN suporta a função de SNMP</b></p>
-----------------------------	--

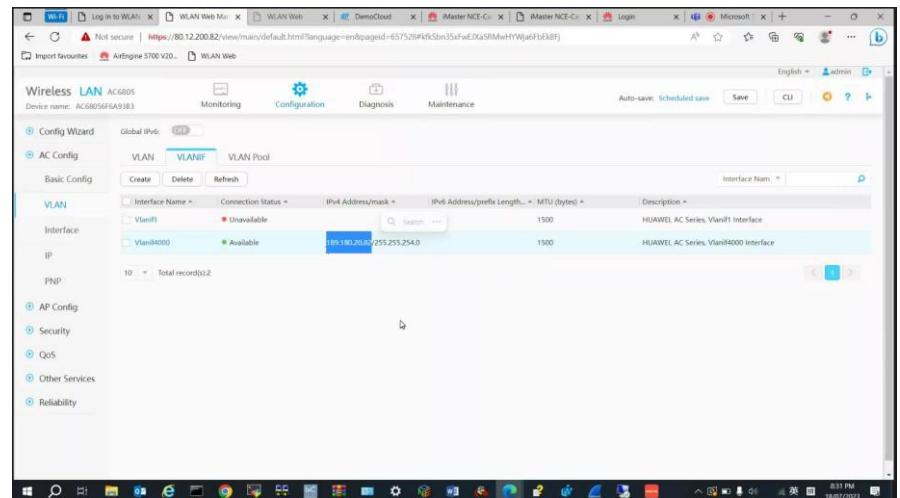
**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

<b>Objetivo do teste</b>	Validar que o sistema de WLAN suporta a função de SNMP
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Habilite a função SNMP na WAC,</li> <li>2) Configure NMS para gerenciar a WAC;</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) AC gerenciada via SNMP (NMS)</li> <li>2) Verifica-se informação de alarme no servidor SNMP (NMS)</li> </ol>
<b>Resultado</b>	

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


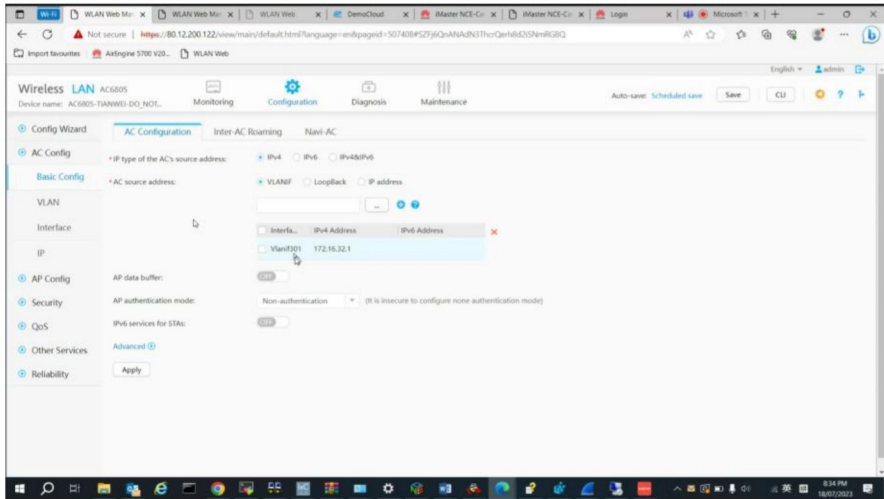


Figuras 1 e 2 – Visualização de todas as MIBs disponíveis na AC, através do protocolo SNMPv2c.





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

<b>Item de teste</b>	Layer 2 CAPWAP WAC Discovery
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta descoberta da AC por CAPWAP na camada 2
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure os parametros na AC: o AP obtem endereço IP do servidor DHCP.</li> <li>2) O AP e AC estão na mesma subrede;</li> <li>3) Verifique as configurações do AP.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) O AP aparece como online na AC, dentro da mesma faixa de rede;</li> </ol>
<b>Resultado</b>	 <p>Figura 1 – Os APs gerenciados pelo controlador AC podem aprender o endereço IP especificado ou o endereço IP da interface especificada para</p>

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

configurar um túnel CAPWAP com o AC. Essa configuração foi evidenciada alterando os parametros em “AC source address”, configurando o endereço para a formação do tunel CAPWAP.

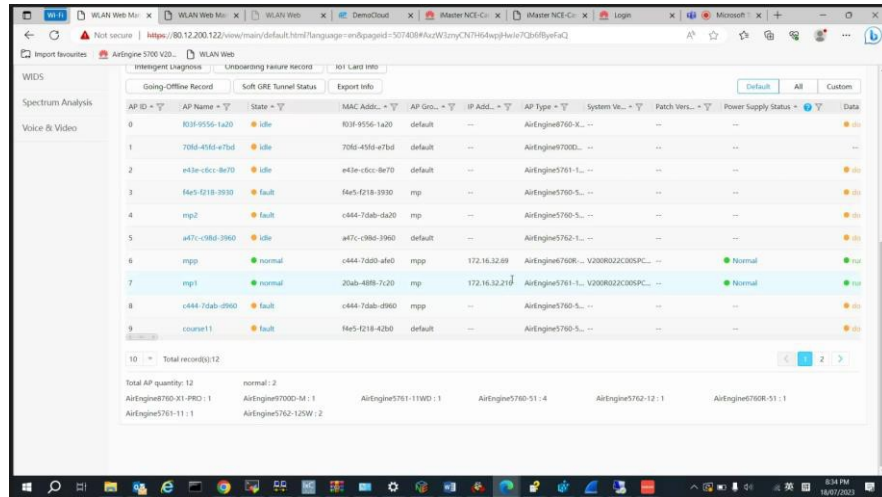


Figura 2 – Checando as informações dos APs descobertos, os APs com ID 6 e 7, receberam de forma automática, via protocolo DHCP, os endereços de IP da mesma faixa que foi configurada no “AC source address”.


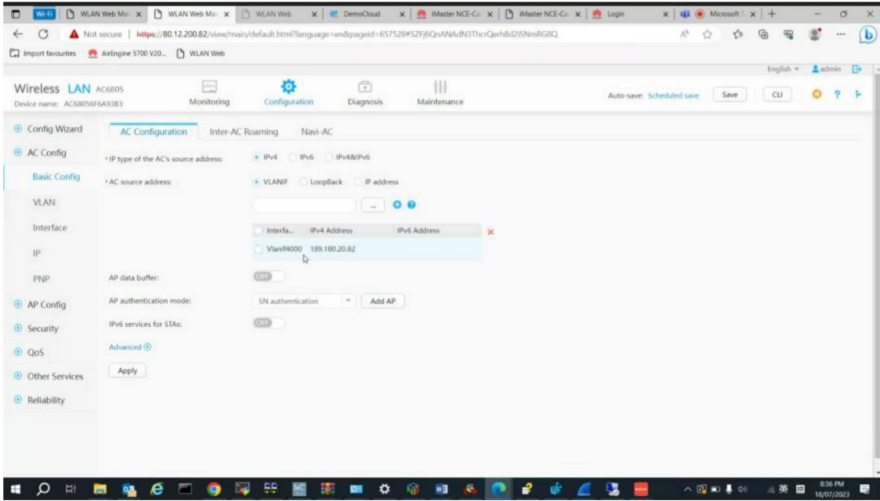
**Layer 3 CAPWAP ac Discovery (DHCP Option 43) | Descoberta de AC por CAPWAP na camada 3 usando DHCP Option 43**

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;

<b>Item de teste</b>	Descoberta de WAC por CAPWAP na camada 3 usando DHCP Option 43
<b>Objetivo do teste</b>	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**

<p align="center"><b>Configuração de teste</b></p>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p align="center"><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Configure os parâmetros na AC: o AP obtém endereço IP do servidor DHCP.</li> <li>2) O AP e AC estão em redes distintas;</li> <li>3) Verifique as configurações do AP.</li> </ol>
<p align="center"><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) O AP aparece como online na AC, dentro de uma faixa de rede diferente da AC;</li> </ol>
<p align="center"><b>Resultado</b></p>	 <p>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</p>

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

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

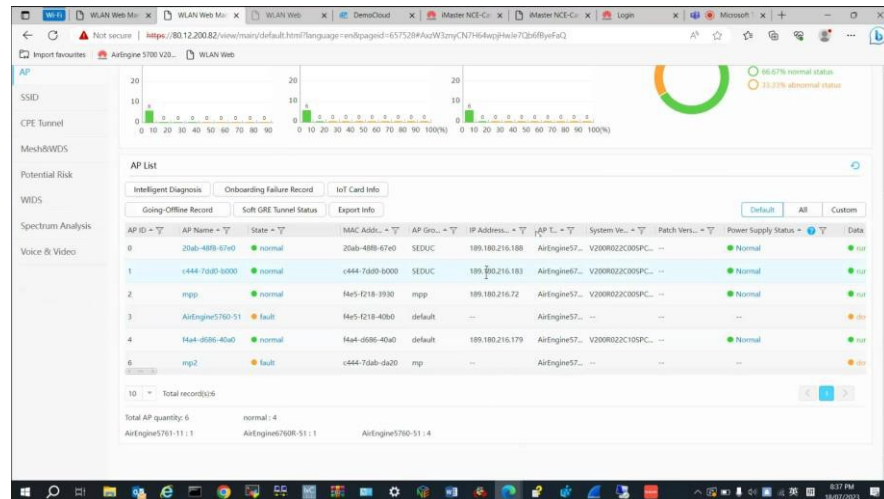


Figura 2 – Checando as informações dos APs descobertos, os APs com ID 0 e 1, receberam de forma automática, via protocolo DHCP, os endereços de IP, de uma VLAN diferente da que foi configurada no “AC source address”.

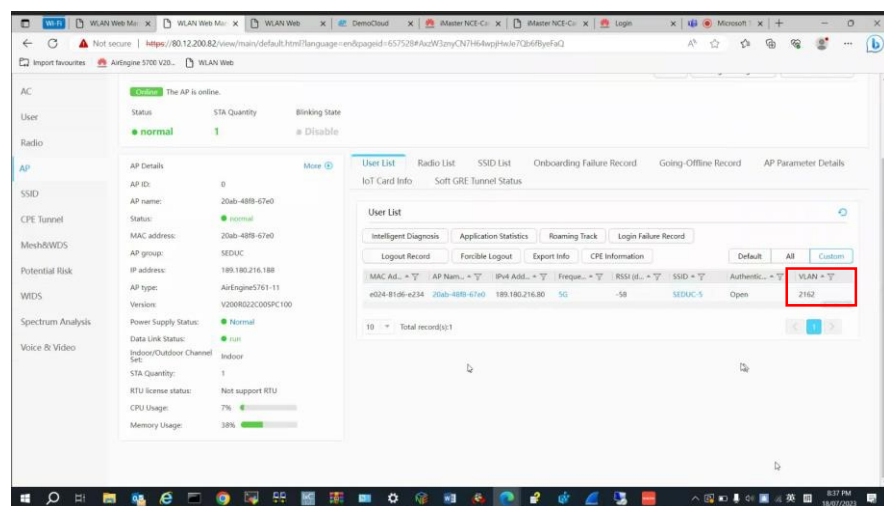
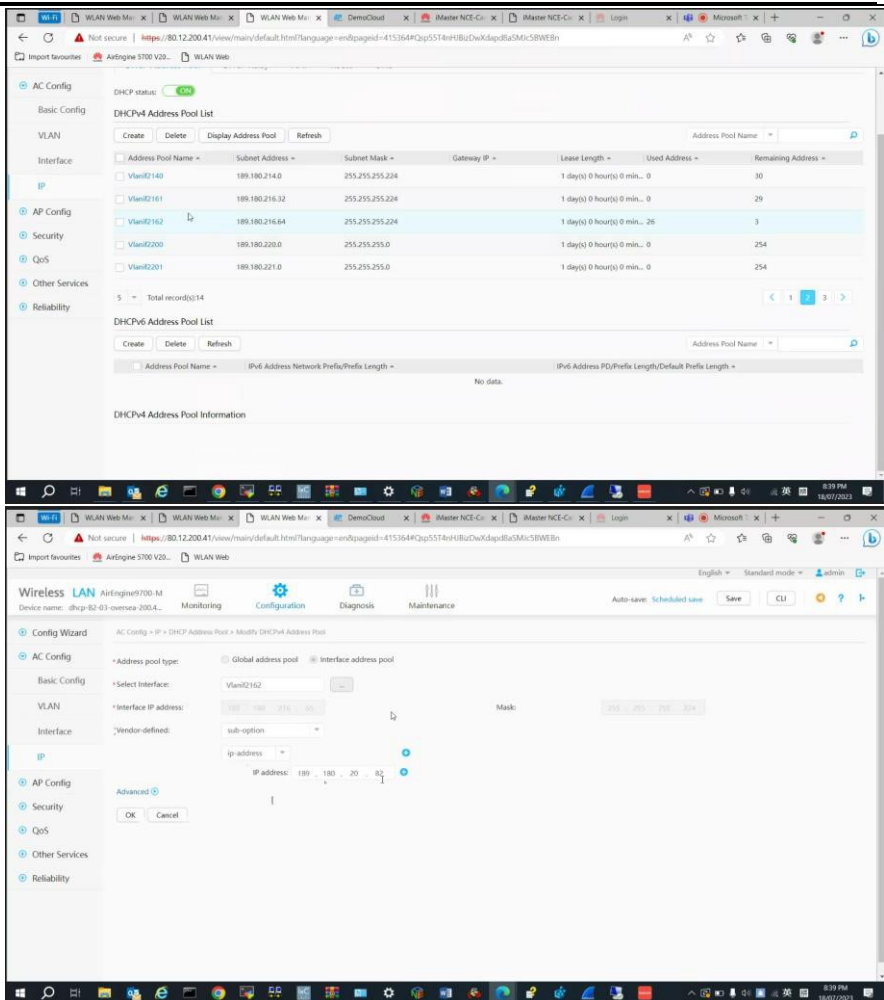


Figura 3 – Analisando as informações do AP ID 0, evidenciamos que seu funcionamento estava com o status de normal, e que a VLAN utilizada para a sua gerência, possui o ID 2162.



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



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

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

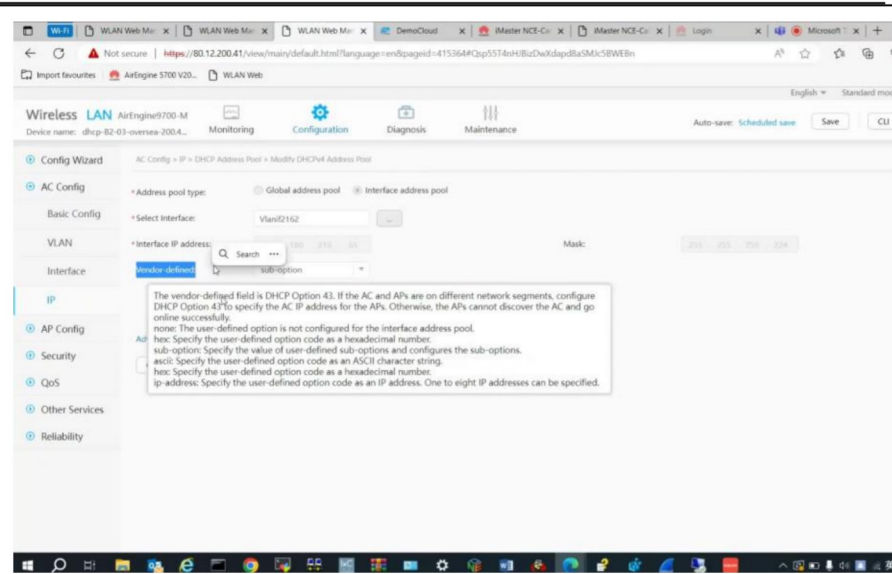

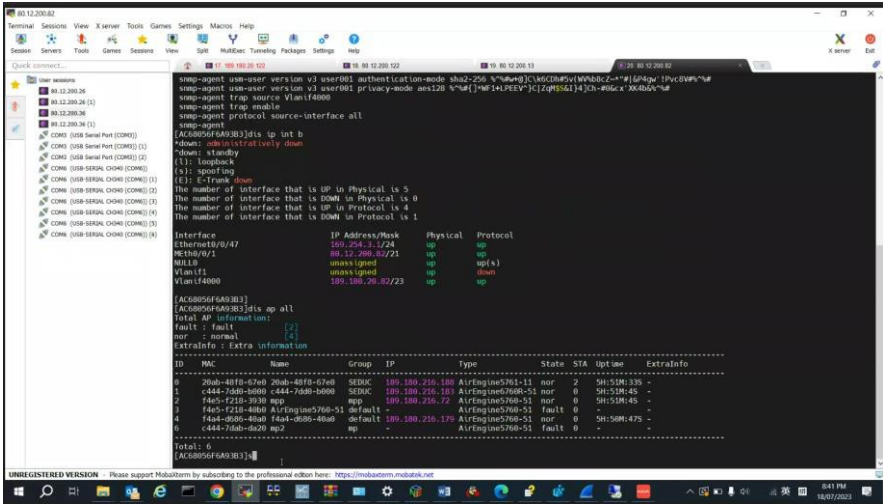
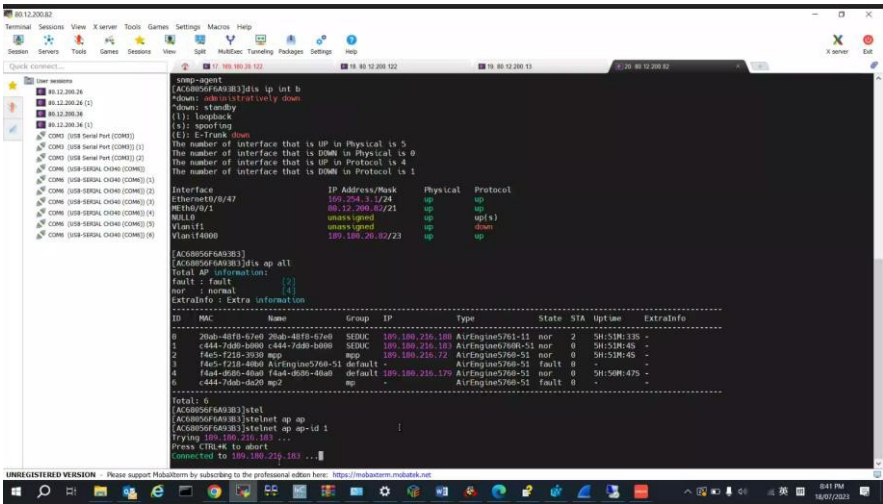


Figura 6 - Nas suas configurações, foi evidenciado a utilização do parametro “sub-options”, com a opção 43.

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

<b>Item de teste</b>	Layer 3 CAPWAP AC Discovery (static Endereço IP)
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta descoberta de AC por CAPWAP na camada 3 usando IP estático
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>

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

<p align="center"><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Configure o endereçamento IP do AP, de forma estática.</li> <li>2) O AP e AC estão em redes distintas;</li> <li>3) Verifique as configurações do AP.</li> </ol>
<p align="center"><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) O AP aparece como online na AC, dentro da uma faixa de rede diferente da AC;</li> </ol>
<p align="center"><b>Resultado</b></p>	 <p>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.</p> 

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

Figura 2 – Iniciamos um acesso via protocolo SSH, ao AP ID 1

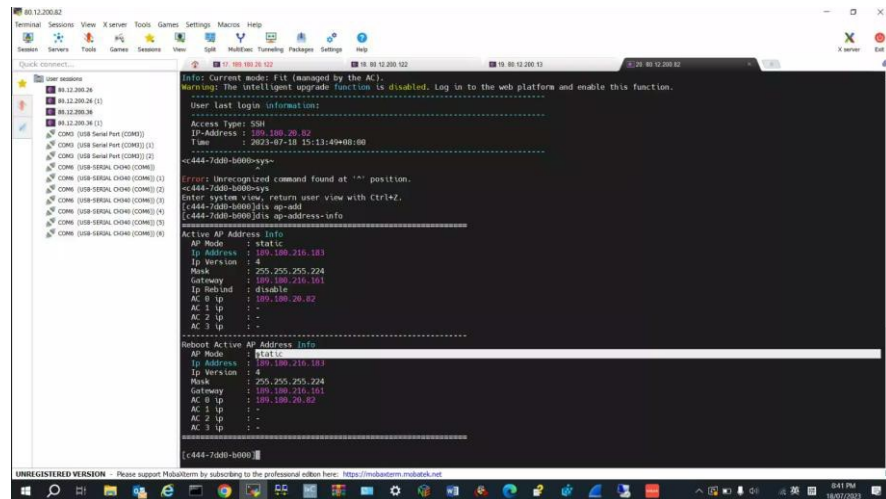


Figura 3 – Visualizando as informações de endereçamento IP do AP ID 0, atestamos que o IP utilizado foi configurado de forma estática, e que ainda sim foi possível formar o tunel CAPWAP, com a AC que está em outra rede.

## Segurança WLAN


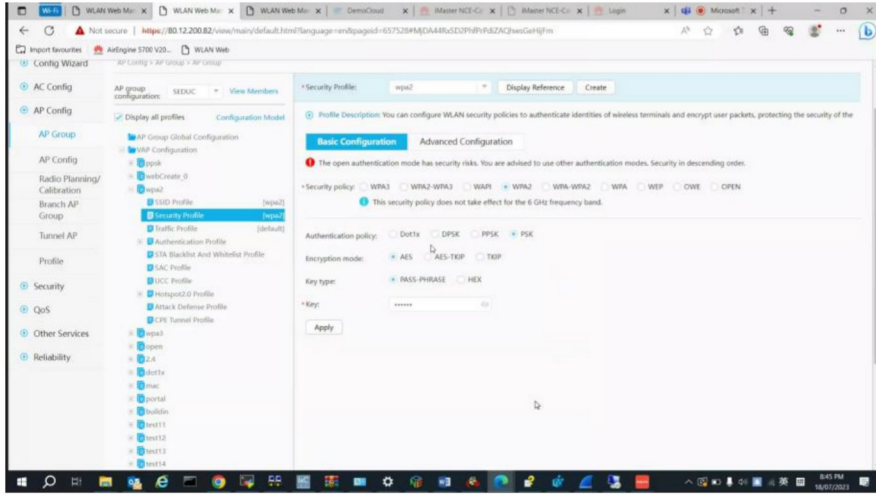
### Autenticação WPA2

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

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

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

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

	<div style="text-align: center;">  <p>STA      AP      Switch      AC</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Configuração de SSID, com a política de segurança definida para WPA2.</li> </ol>
<p><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) Divulgação de SSID onde a política de segurança com WPA2, foi configurada.</li> <li>2) Associação de dispositivo ao SSID criado</li> </ol>
<p><b>Resultado</b></p>	 <p>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)</p>

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

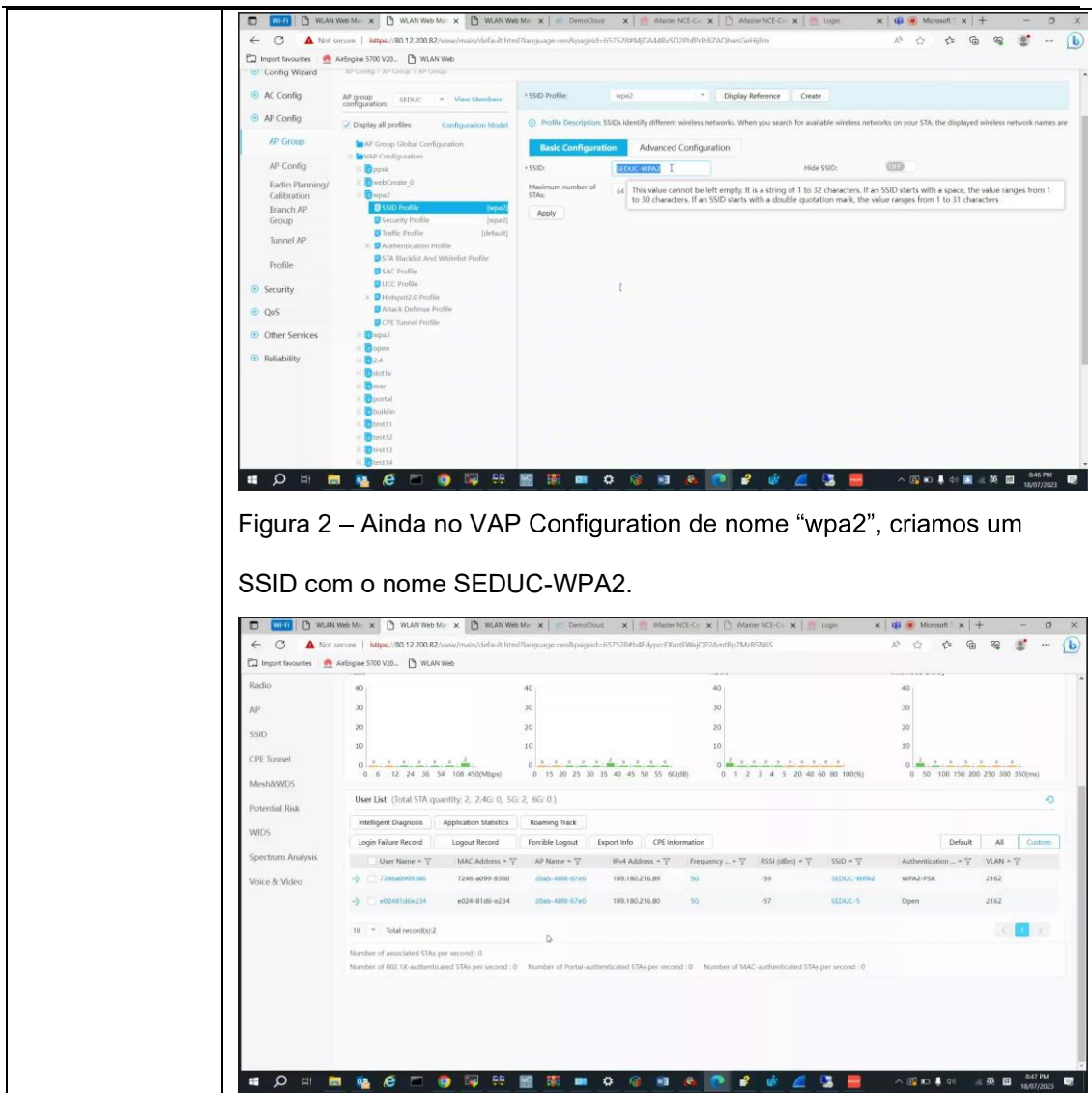


Figura 2 – Ainda no VAP Configuration de nome “wpa2”, criamos um SSID com o nome SEDUC-WPA2.

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

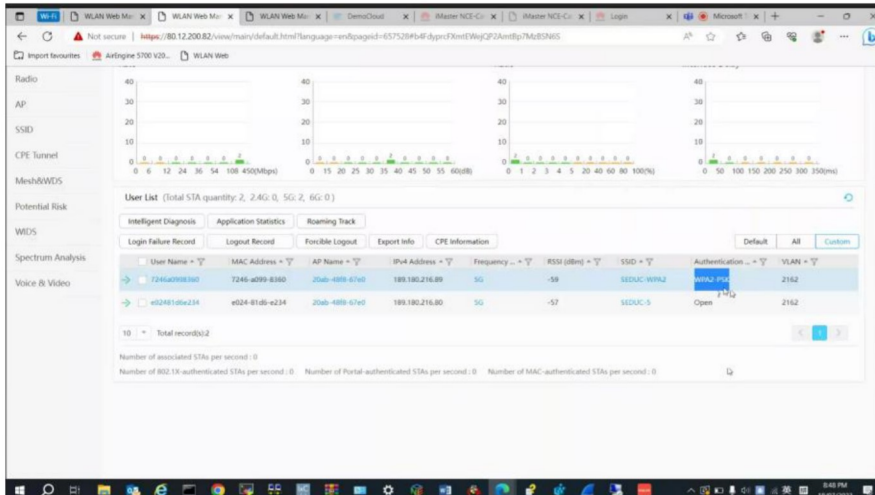



Figura 3 e 4 – Na listagem de dispositivos conectados (User list), podemos verificar um dispositivo associado ao SSID SEDUC-WPA2, e que o método de autenticação utilizado foi WPA2-PSK.

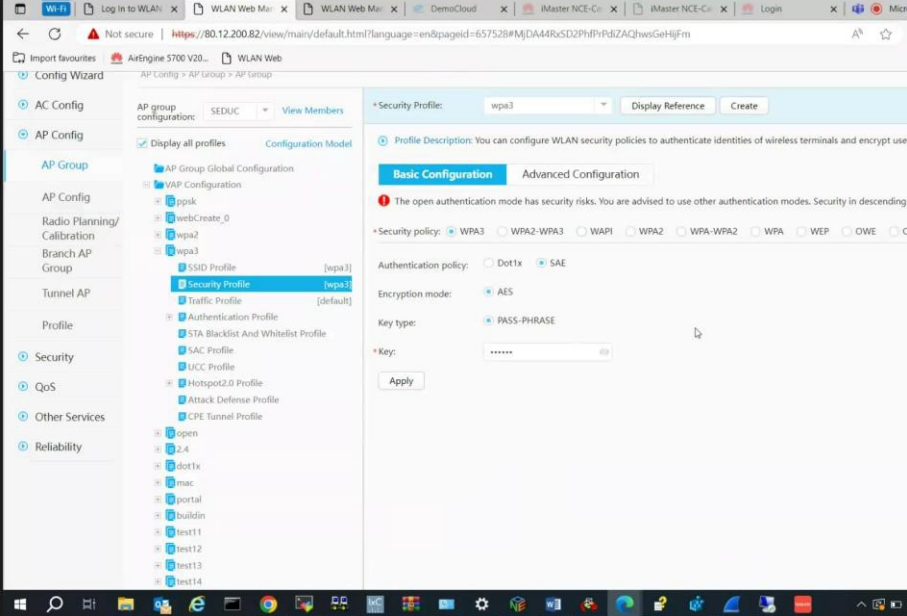
### Autenticação WPA3-SAE

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

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

<b>Item de teste</b>	Políticas de segurança da rede WLAN (WPA3)
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta autenticação WPA3-SAE
<b>Configuração de teste</b>	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 estão funcionando normalmente.  2) Montar o ambiente de teste de acordo com a topologia acima.  3) O dispositivo cliente (STA) suporta autenticação WPA3-SAE.
<b>Procedimento de teste</b>	1) Configuração de SSID, com a política de segurança definida para WP3-SAE.
<b>Resultado esperado</b>	1) Configuração de SSID onde a política de segurança com WPA3-SAE.
<b>Resultado</b>	 <p>                     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 política de autenticação SAE, criptografia AES e uma senha de acesso (PASS-PHRASE).                 </p>

### Autenticação 802.1x

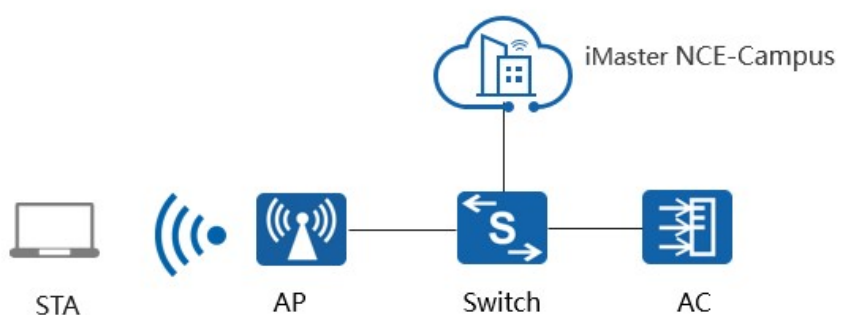
5.6.5 Implementar no mínimo as opções WPA2, WPA3, 802.1X;

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



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

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

<b>Item de teste</b>	Políticas de segurança da rede WLAN (802.1x)
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Autenticação 802.1x
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configuração de SSID, com a política de segurança definida para Dot1x (802.1x).</li> <li>2) Autenticar usuários através de 802.1x</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Configuração de SSID onde a política de segurança é 802.1x e autenticar usuários.</li> </ol>

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

Resultado

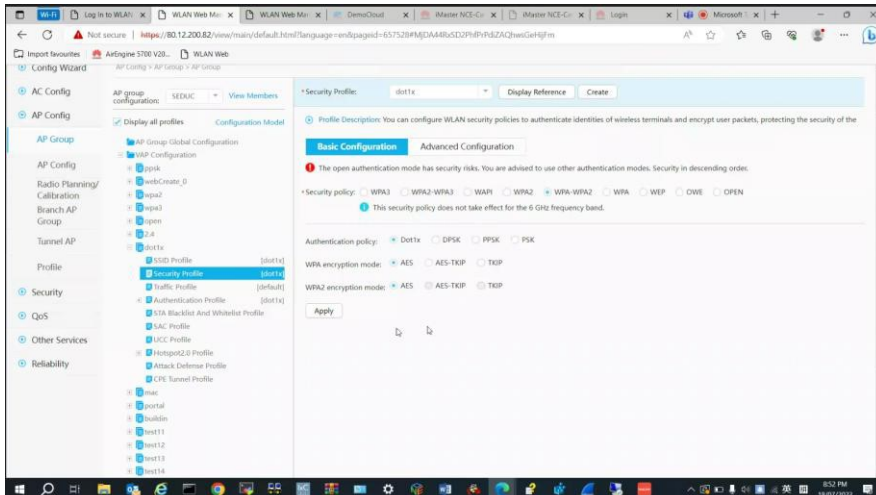


Figura 1 – Complementando o teste anterior, também foi criado um VAP Configuration, de nome “dot1x”, onde o perfil de segurança utilizado foi o WPA-WPA2, com a política de autenticação Dot1x (802.1x) e criptografia AES.

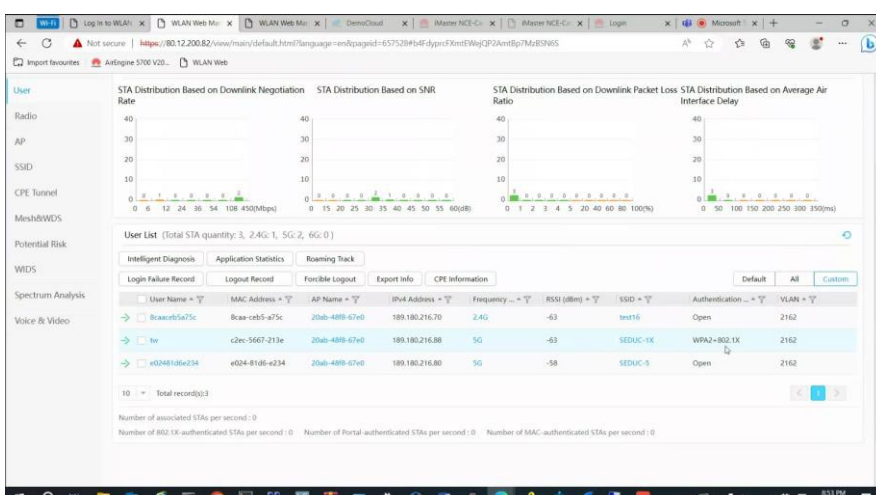


Figura 2 – Foi evidenciado, na listagem de usuários conectados, o usuário “tw”, autenticado via 802.1x pelo SSID SEDUC-1X.

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

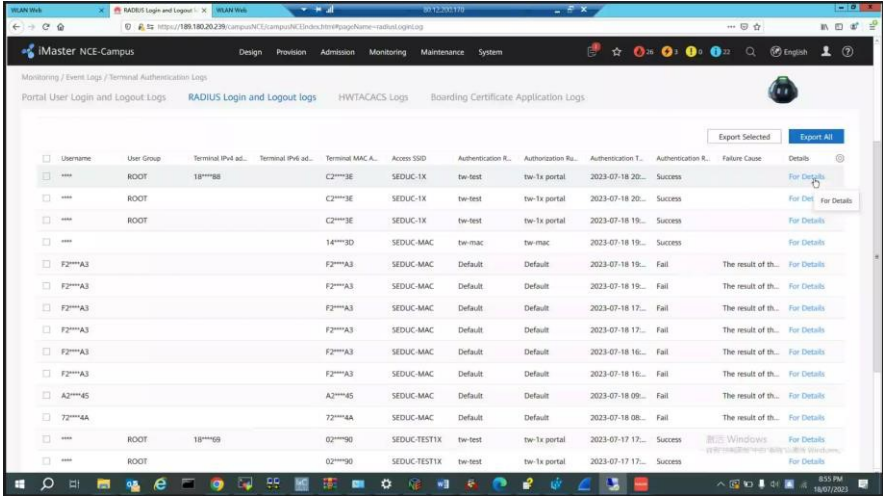


Figura 3 – Na plataforma iMaster NCE Campus, também é listado a autenticação com sucesso no SSID SEDUC-1X.

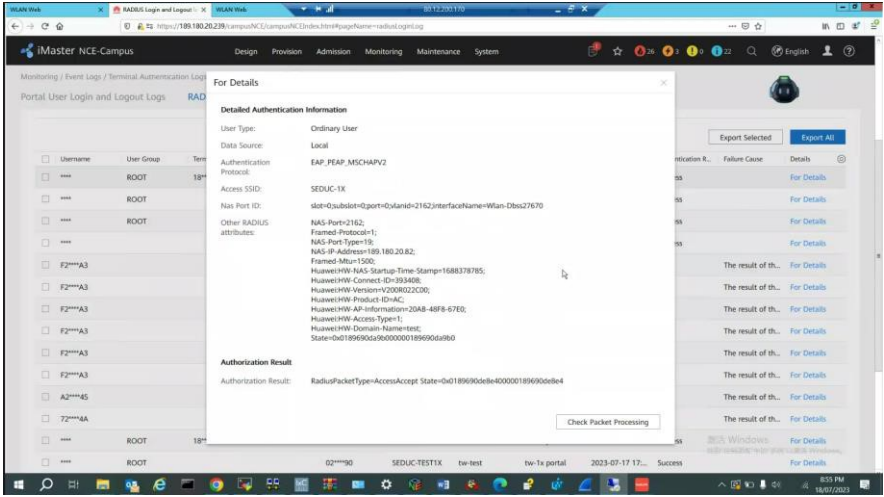
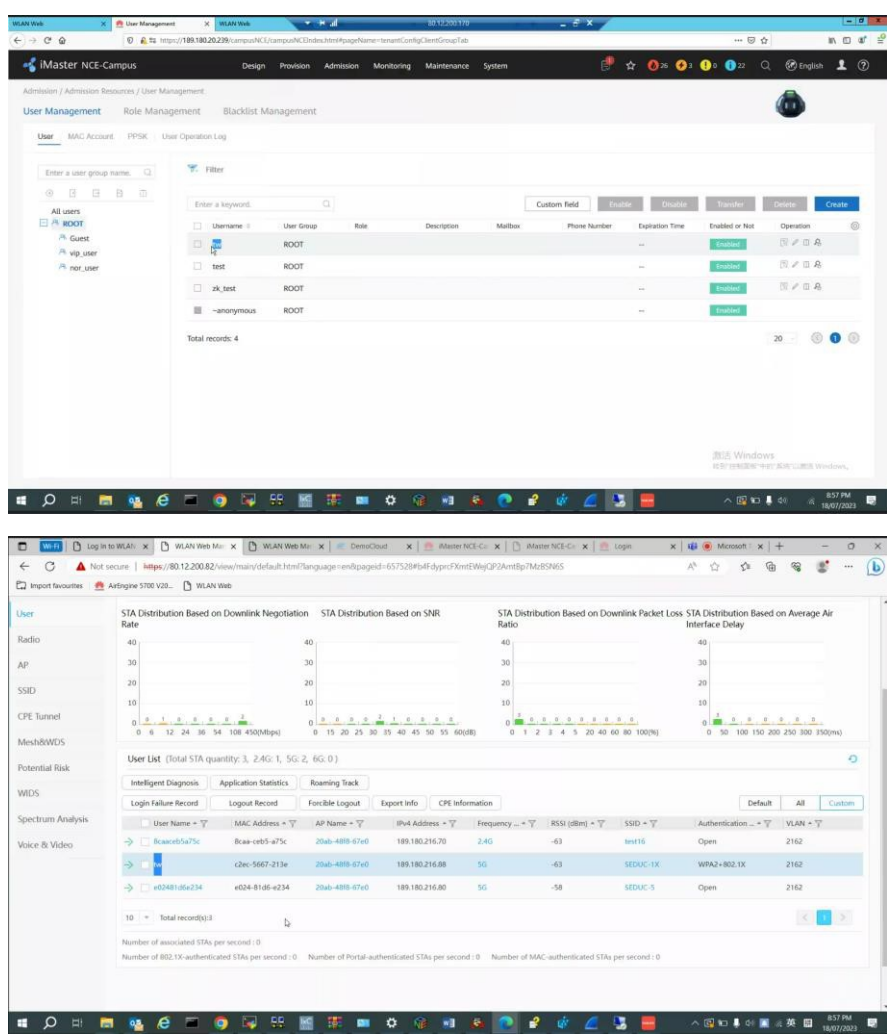


Figura 4 – Também foi evidenciado os logs do protocolo RADIUS, dentro da plataforma iMaster NCE, mostrando todo o processo de autenticação realizado com sucesso.

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



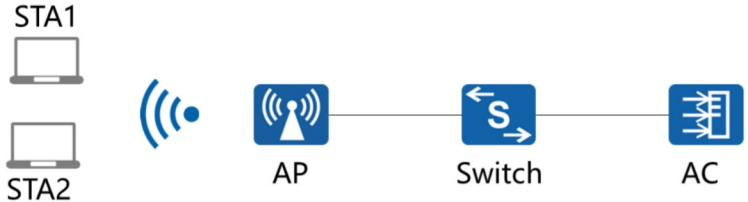
Figuras 5 e 6 – Por último, finalizando o teste, foi evidenciado o mesmo usuário “tw”, utilizado para a autenticação, na base de dados da plataforma iMaster NCE Campus, e na listagem de usuários conectados da controladora.

### Autenticação WPA/WPA2-PPSK

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

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

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

<b>Item de teste</b>	Autenticação WPA/WPA2-PPSK
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Autenticação WPA/WPA2-PPSK
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configuração de SSID, com a política de segurança definida para WPA2-PPSK.</li> <li>2) Autenticar usuários através de WPA2-PPSK</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Configuração de SSID onde a política de segurança é WPA2-PPSK e autenticar usuários.</li> </ol>

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

**Resultado**

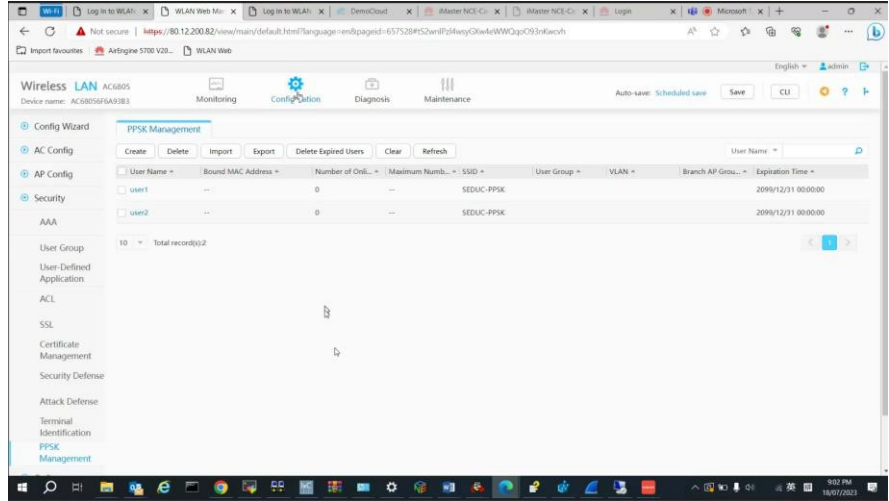


Figura 1 – Na controladora, foram criados dois usuários com diferentes PPSK (Private Pre-Shared Key), que são chaves de acesso privadas ou individuais.

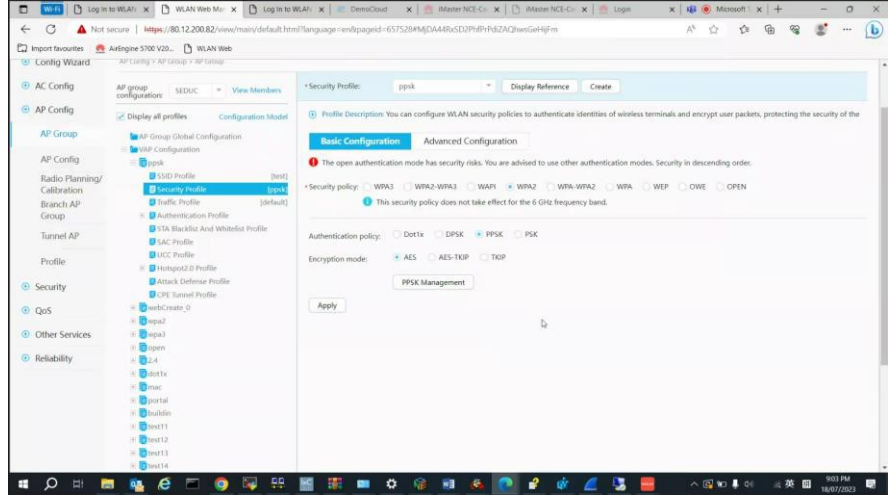


Figura 2 – Em seguida, também foi criado um VAP Configuration, de nome “ppsk”, onde o perfil de segurança utilizado foi o WPA2, com a política de autenticação PPSK e criptografia AES.

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

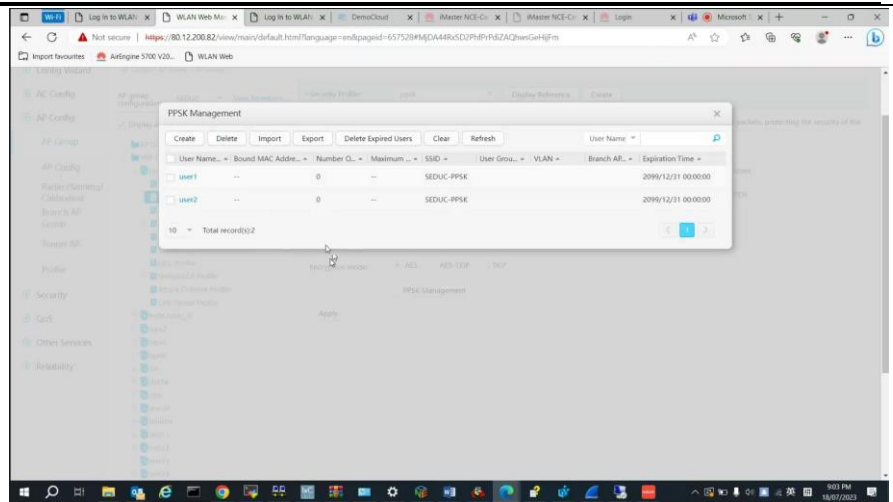


Figura 3 – Nesta mesma tela de configuração, também foi evidenciado o gerenciamento dos usuários e senhas tipo PPSK.

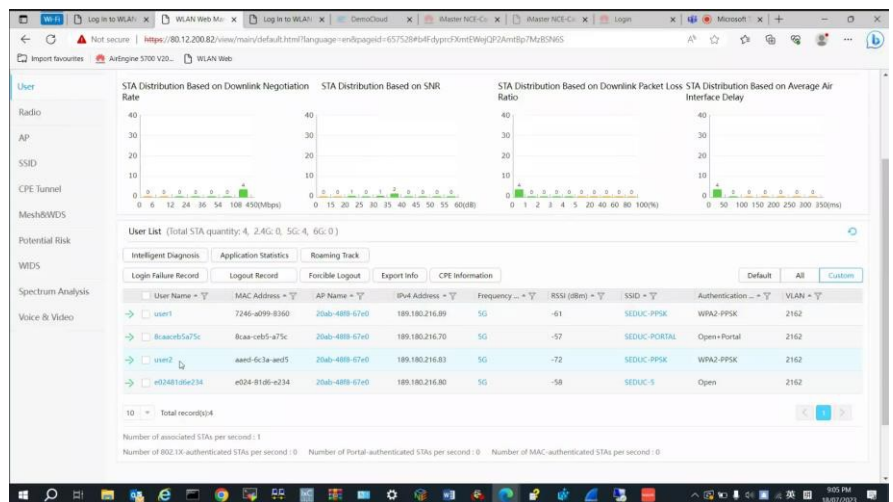


Figura 4 – Na listagem de dispositivos conectados, temos os dois usuários criados com a política PPSK, associados ao SSID SEDUC-PPSK.

## Radio

### Fluxo 2.4Ghz e 5Ghz

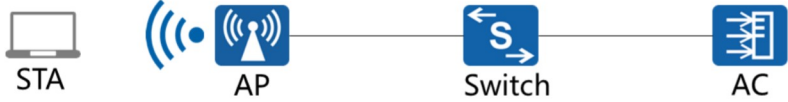
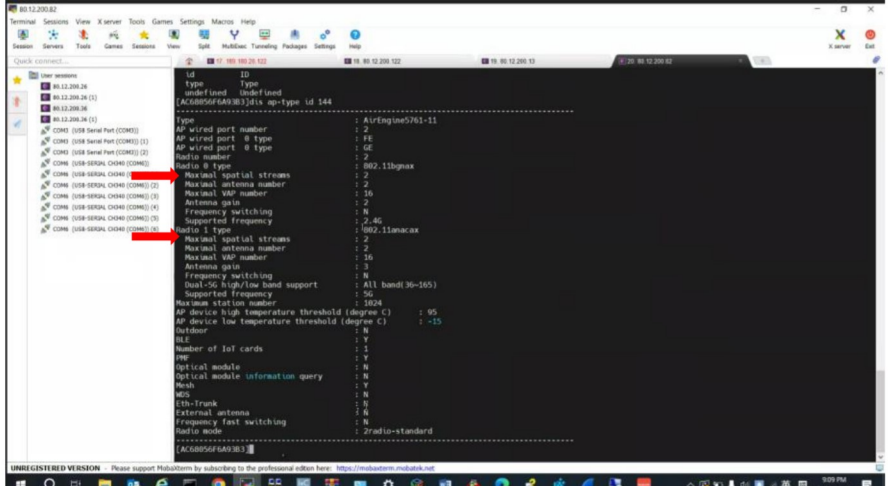
#### 5.6.7.1 Fluxo 2.4Ghz e 5Ghz: no mínimo 2x2

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

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;

<b>Item de teste</b>	<b>Fluxo 2.4Ghz e 5Ghz</b>
<b>Objetivo do teste</b>	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
<b>Configuração de teste</b>	Topologia da rede: <div style="text-align: center;">  </div> Condições iniciais: 1) Todos os dispositivos funcionando normalmente 2) Montar o ambiente de teste de acordo com a topologia acima
<b>Procedimento de teste</b>	1) Verifique os spatial streams no AP.
<b>Resultado esperado</b>	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
<b>Resultado</b>	



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

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.

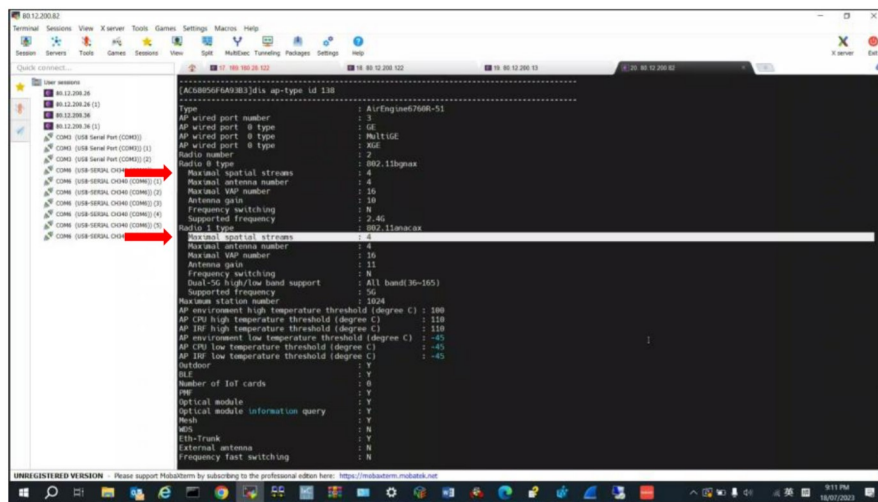

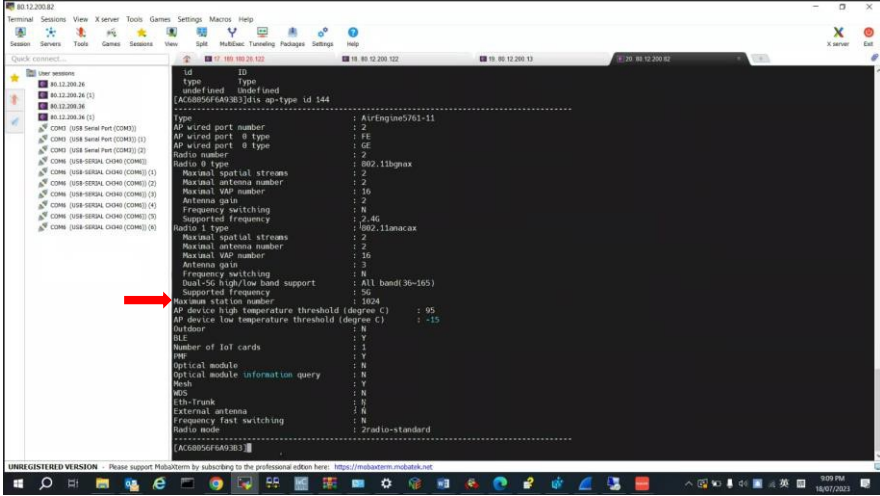
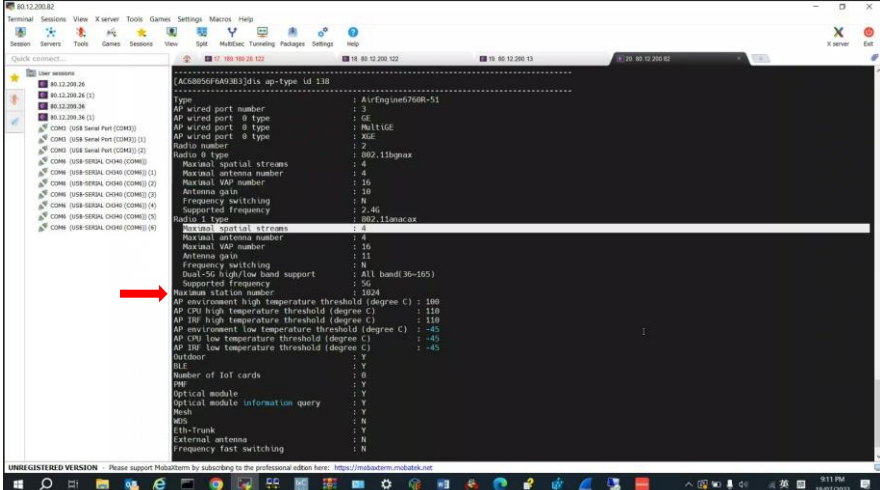


Figura 2 – Via CLI, foi listada todas as informações do AP modelo AirEngine 6760R-51. Nestas informações, é possível checar a quantidade de spatial streams suportada por rádio.

**Maximum access user | Máximo de usuários simultâneos**

<b>Item de teste</b>	<b>Máximo de usuários simultâneos</b>
<b>Objetivo do teste</b>	Validar que o access point sem fio suporta pelo menos 512 clientes por unidade de AP.
<b>Configuração de teste</b>	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
<b>Procedimento de teste</b>	1) Verifique a quantidade máxima de terminais suportados por AP.
<b>Resultado esperado</b>	2) O AP mostra a informação que suporta mais de 512 terminais.
<b>Resultado</b>	 <p>                     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).                 </p> 

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

	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)**

<b>Item de teste</b>	<b>Bluetooth Low-Energy (BLE) radio   Rádio Bluetooth de baixo consumo energético</b>
<b>Objetivo do teste</b>	<b>Validar que o a access point sem fio suporte rádio Bluetooth de baixo consumo energético (BLE)</b>
<b>Configuração de teste</b>	Topologia da rede:  Condições iniciais: <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	1) Verifique o suporte a BLE.
<b>Resultado esperado</b>	1) O AP mostra a informação que suporta radio do tipo Bluetooth Low-Energy.

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

**Resultado**

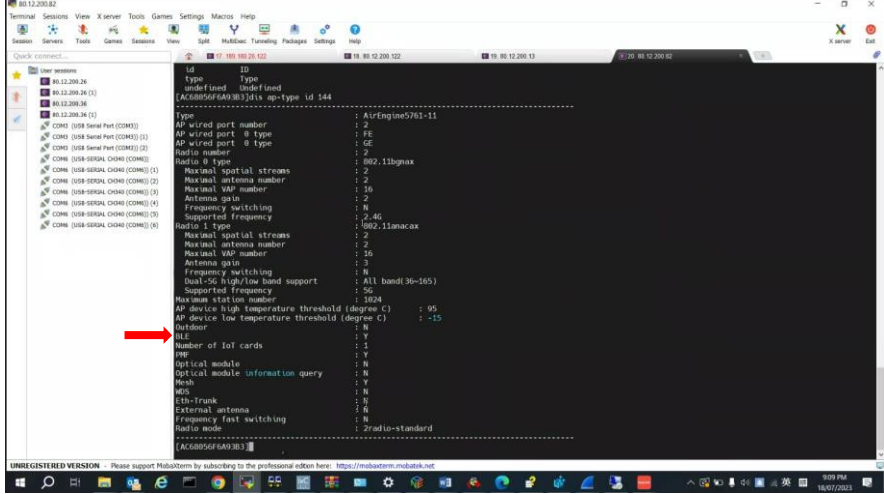


Figura 1 – Via CLI, foi listada todas as informações do AP modelo AirEngine 5761-11. Nestas informações, é possível checar o suporte a tecnologia BLE.

**Resultado**

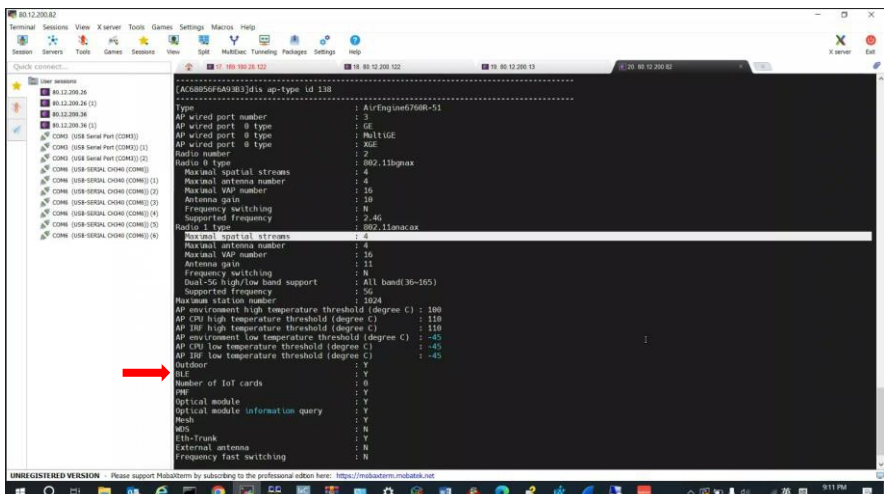



Figura 2 – Via CLI, foi listada todas as informações do AP modelo AirEngine 6760R-51. Nestas informações, é possível checar o suporte a tecnologia BLE.

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;

<b>Item de teste</b>	<b>Funcionamento simultâneo em 2.4GHz e 5GHz;</b>
<b>Objetivo do teste</b>	<b>Validar que o Sistema WLAN suporta funcionamento simultâneo em 2,4GHz e 5GHz</b>
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p style="text-align: center;"> <span>STA</span>      <span>AP</span>      <span>Switch</span>      <span>AC</span> </p> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>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.</li> <li>2) Conecte o os dispositivos em cada SSID.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>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);</li> <li>2) Os dispositivos clientes (STAs) conectam-se SSIDs respectivamente</li> </ol>

**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 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

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

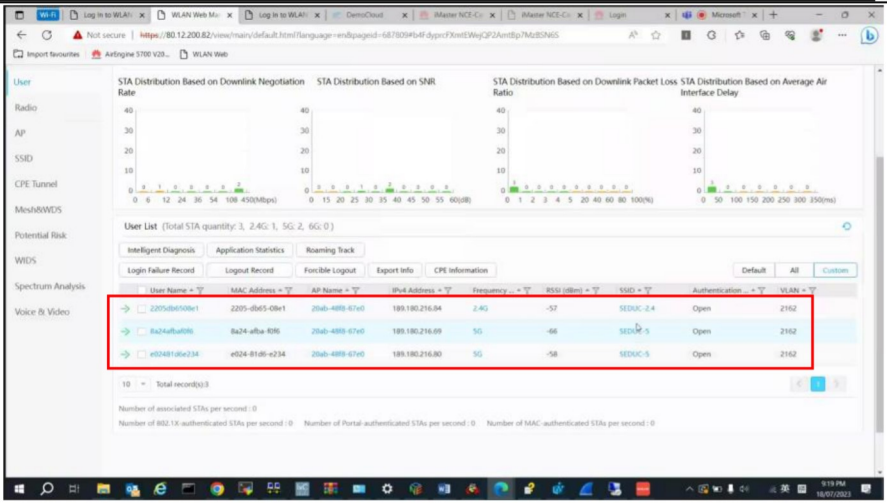

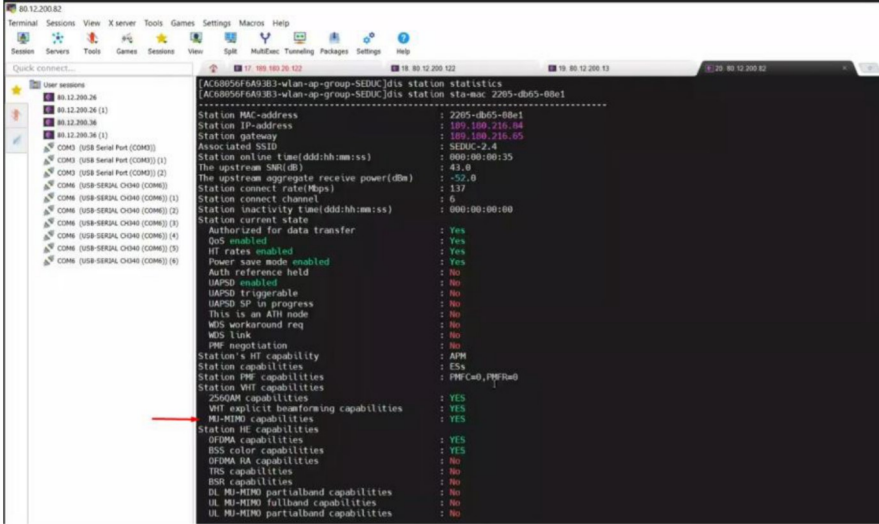


Figura 3 – Na listagem de usuários associados, foi possível atestar que existem dispositivos conectados ao mesmo AP (chegar o MAC ADDRESS), nos dois SSIDs criados, e suas respectivas frequências.


### Suporte MU-MIMO

<b>Item de teste</b>	Teste de suporte a MU-MIMO
<b>Objetivo do teste</b>	Validar o suporte a MU-MIMO
<b>Configuração de teste</b>	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
<b>Procedimento de teste</b>	1) Configure a AC corretamente, e propague associe um dispositivo ao SSID.

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

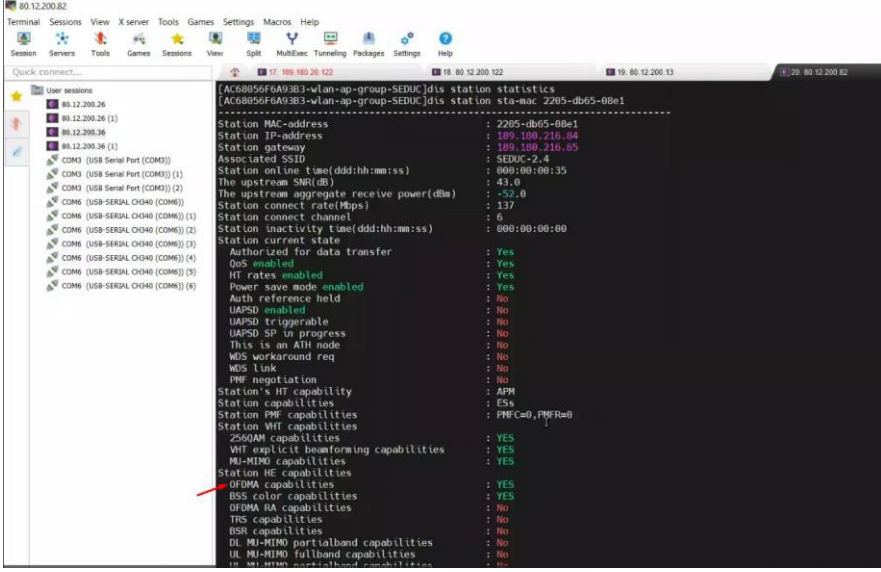
<b>Resultado esperado</b>	1) Listar as informações do dispositivo associado ao SSID
<b>Resultado</b>	 <p>                     Figura 1 – Via CLI, foi listada através do comando “display station sta-mac 2205-db-65-08e1”, todas as informações de um dispositivo conectado ao SSID SEDUC-2.4, criado no procedimento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

**OFDMA**

<b>Item de teste</b>	Teste de suporte a OFDMA
<b>Objetivo do teste</b>	Validar o suporte a OFDMA
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>                     Condições iniciais:                 </p>




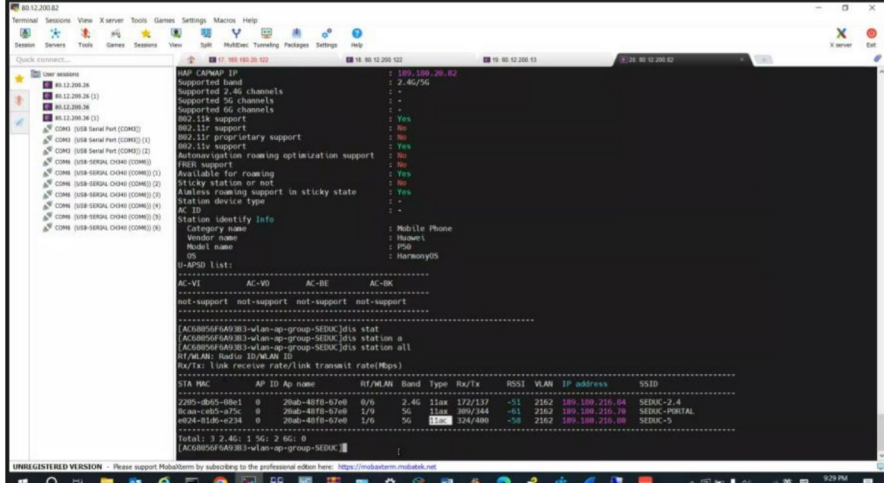
**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

	3) Todos os dispositivos clientes devem suportar 802.11ax 4) Montar o ambiente de teste de acordo com a topologia acima
<b>Procedimento de teste</b>	1) Configure a AC corretamente, e propague associe um dispositivo ao SSID.
<b>Resultado esperado</b>	2) Listar as informações do dispositivo associado ao SSID
<b>Resultado</b>	 <p>                     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.                 </p> <p>                     Na saída deste comando é possível atestar o suporte a tecnologia OFDMA.                 </p>

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

<b>Item de teste</b>	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**


<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta os padrões 802.11a/b/g/n/ac/ax
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure a AC corretamente, e propague associe um dispositivo ao SSID.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Listar as informações do dispositivo associado ao SSID</li> </ol>
<b>Resultado</b>	 <p>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.</p>

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

---

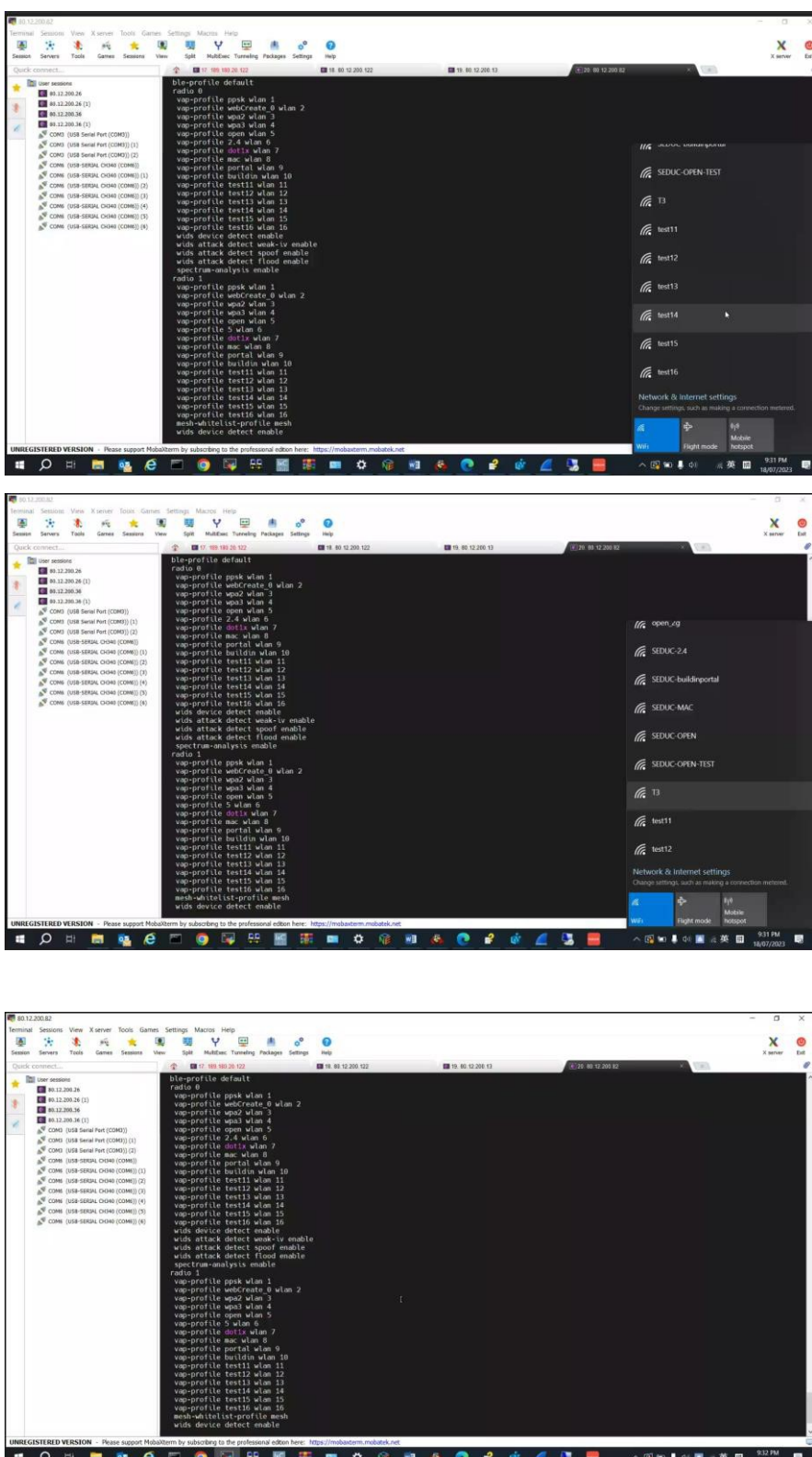
**Multiplas SSIDs**

5.6.7.8 Capacidade de implementar no mínimo 16 SSID;

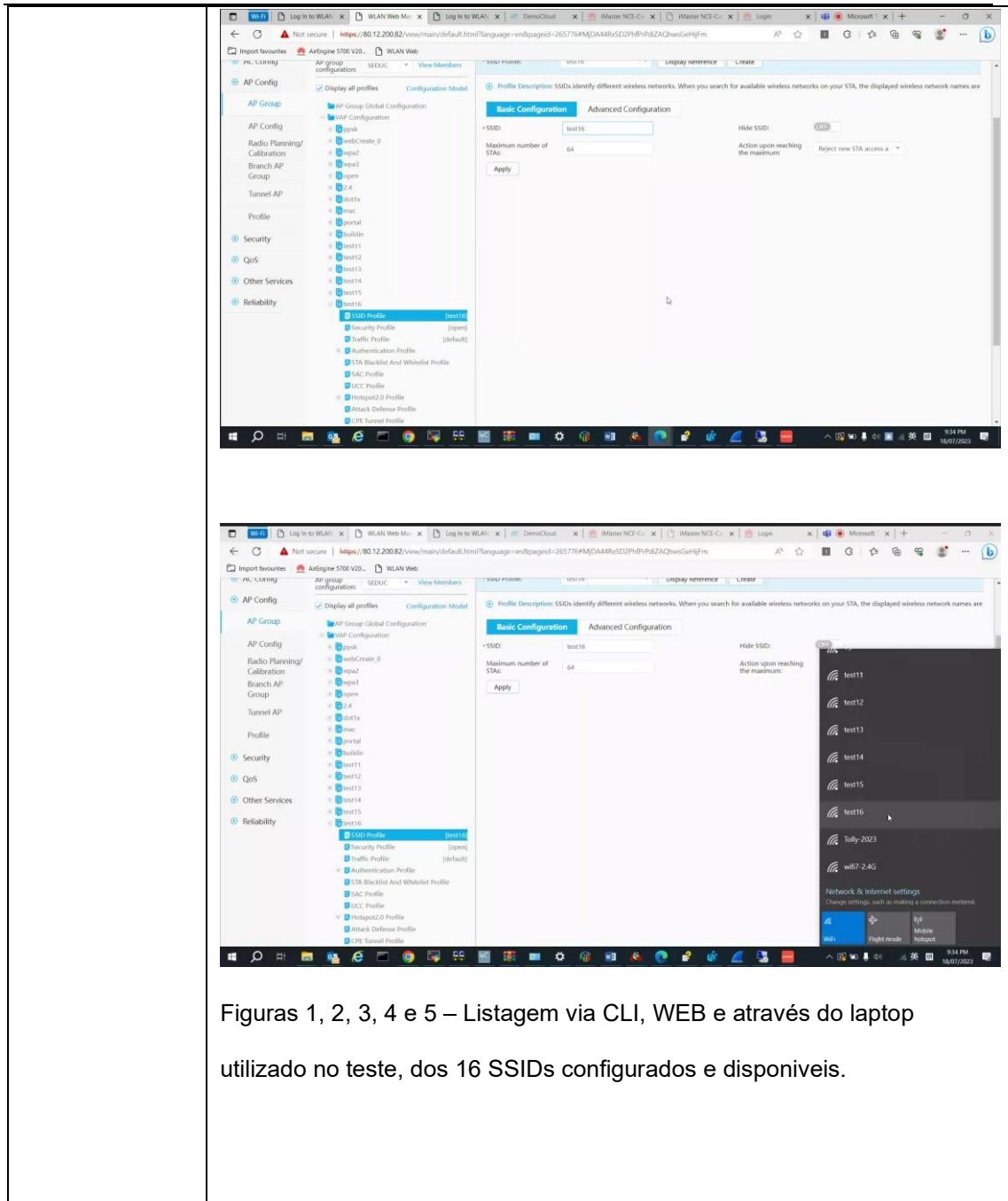
<b>Item de teste</b>	Multi-SSIDs
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta pelo menos 16 SSIDs
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configurar corretamente a AC e propagar 16 SSIDs diferentes através dos pontos de acesso.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Os 16 sinais diferentes podem ser detectados.</li> </ol>

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

Resultado



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


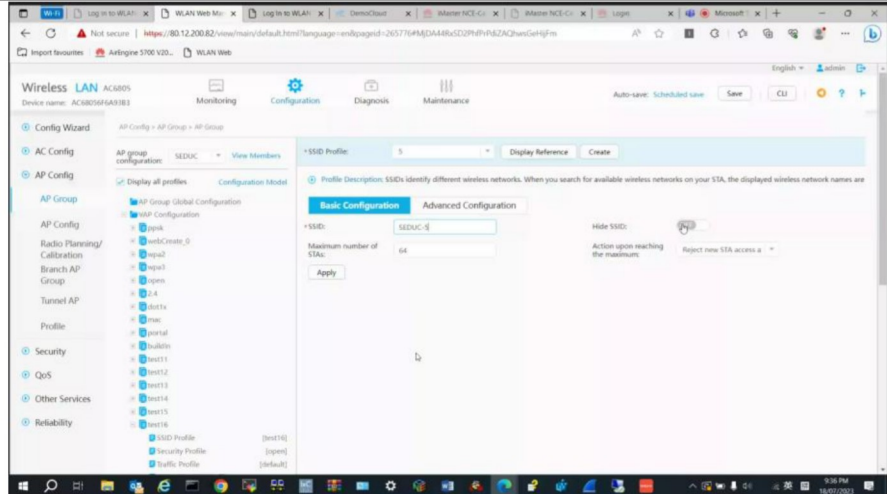


### SSID oculto

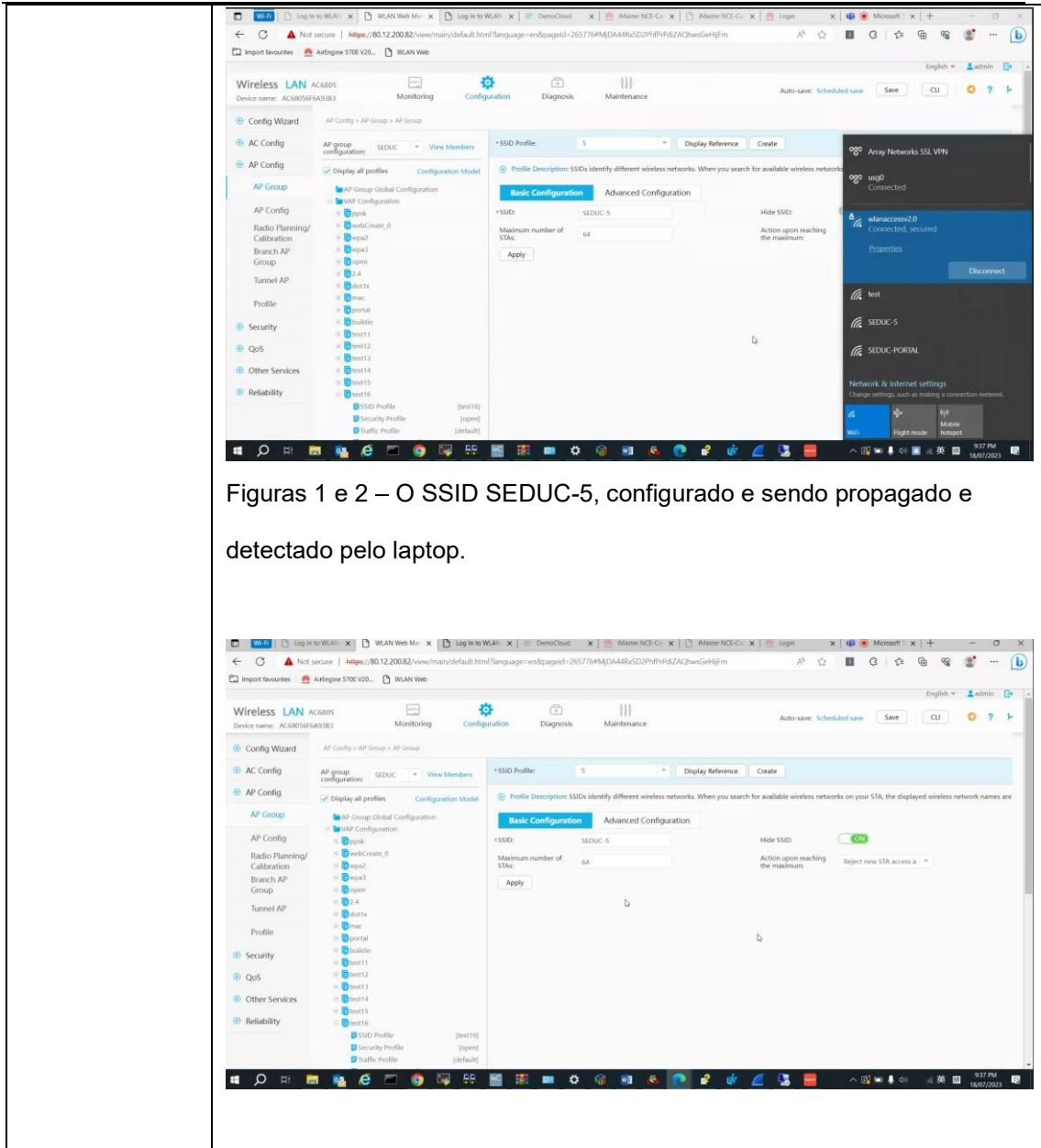
5.6.7.9 Deve permitir habilitar e desabilitar a divulgação do SSID;

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

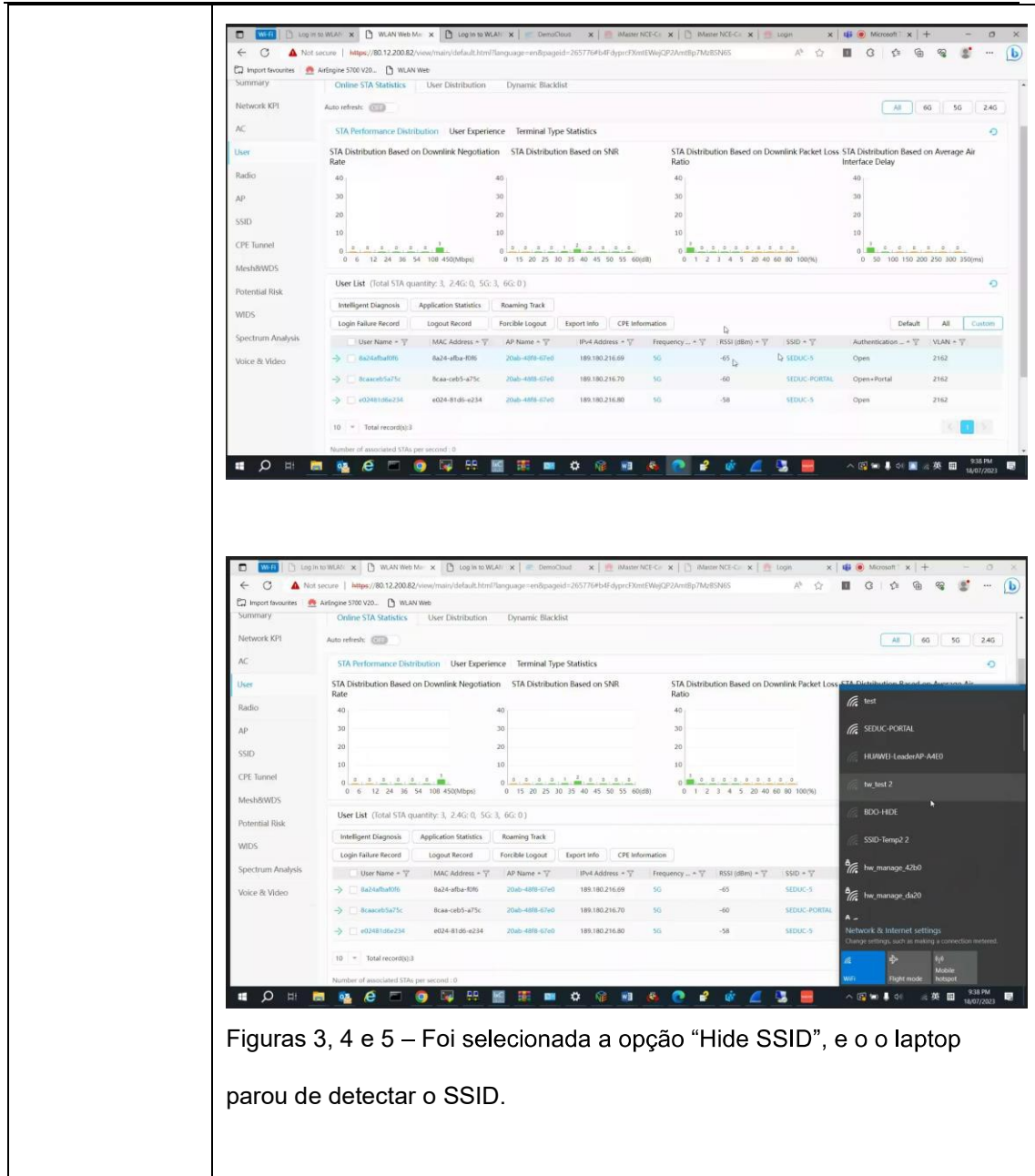
5.7.7.9 Deve permitir habilitar e desabilitar a divulgação do SSID;

<b>Item de teste</b>	SSID oculto
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta SSID função oculto.
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configurar corretamente a AC para propagar um SSID oculto através dos pontos de acesso</li> <li>2) Desabilitar a propagação de SSID</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) O SSID oculto pode ser descoberto pelo STA;</li> <li>2) Após desabilitar os radios, os SSIDs não serão mais detectados</li> </ol>
<b>Resultado</b>	

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



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

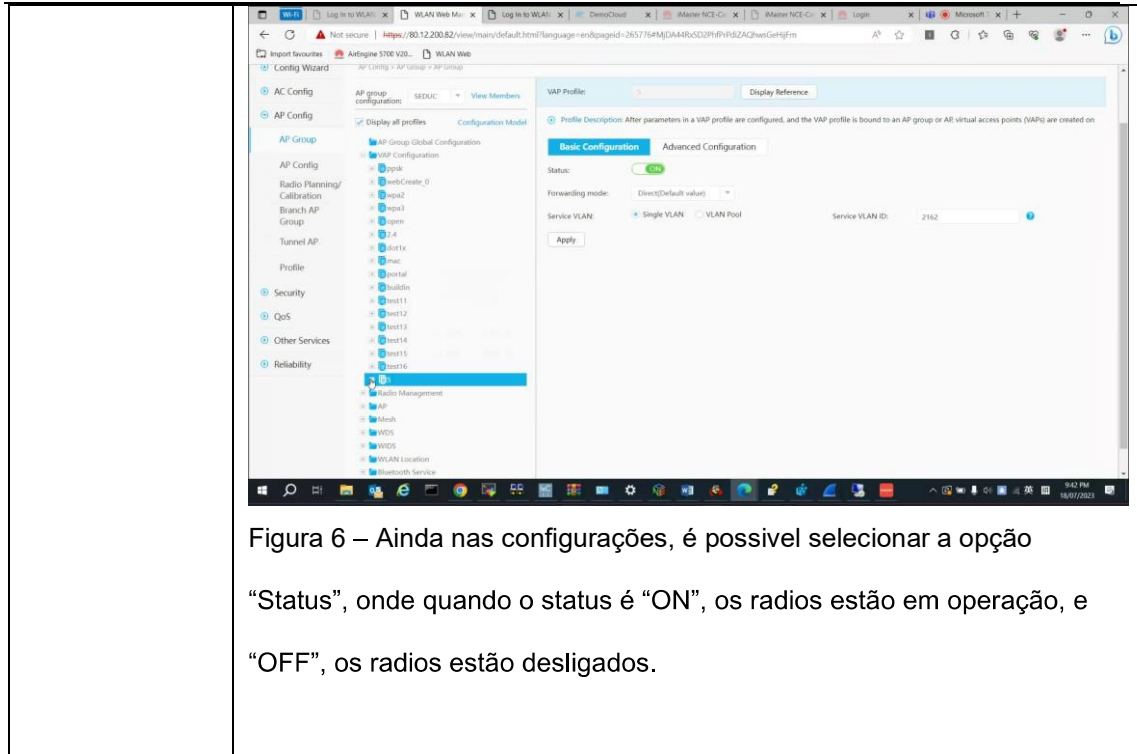


Figura 6 – Ainda nas configurações, é possível selecionar a opção “Status”, onde quando o status é “ON”, os radios estão em operação, e “OFF”, os radios estão desligados.

### 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;

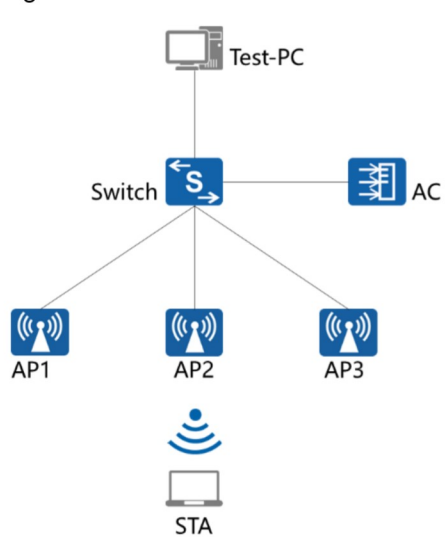
5.10.19 Na ocorrência de inoperância de um Ponto de Acesso, a solução deverá ajustar

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

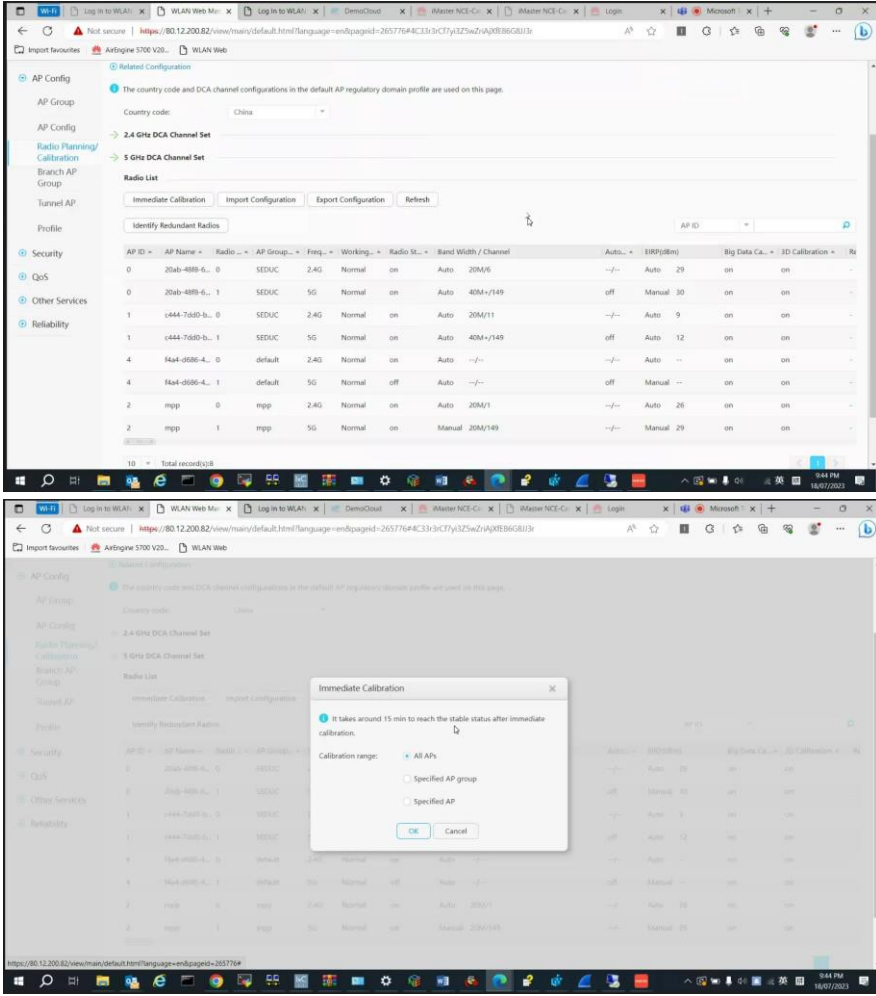
automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;

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

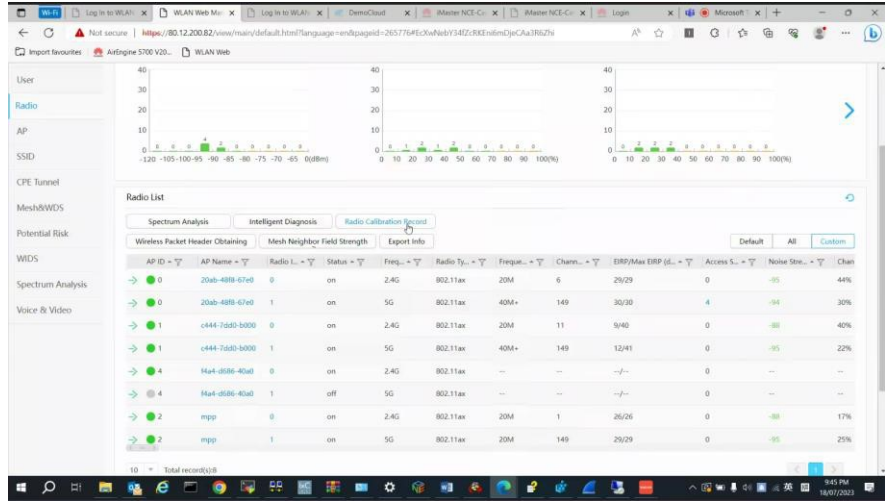
5.10.21 Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática;

<b>Item de teste</b>	Calibração de Rádio
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta calibração de rádio
<b>Teste environment</b>	<p>Topologia da rede:</p>  <pre>             graph TD                 Test-PC --- Switch                 Switch --- AC                 Switch --- AP1                 Switch --- AP2                 Switch --- AP3                 STA --- AP1                 STA --- AP2                 STA --- AP3             </pre> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure a AC corretamente</li> <li>2) Habilite a função Radio Calibration;</li> </ol>

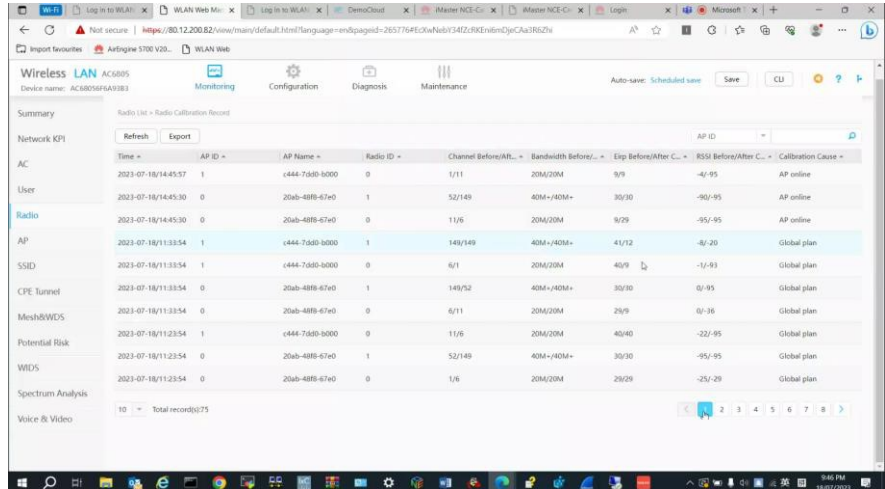
**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

<p><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) Registrar informações de rádio sobre todos os APs;</li> <li>2) O canal AP e a potência de trânsito foram ajustados de forma dinâmica.</li> </ol>
<p><b>Resultado</b></p>	 <p>The screenshot displays the WLAN Web interface. The top part shows the 'Radio List' table with columns for AP ID, AP Name, Radio, AP Group, Freq., Working, Radio St., Band Width / Channel, Auto., ERP(dBm), Big Data Ca., and 3D Calibration. The table contains several rows of data for different APs and radio configurations. Below the table, an 'Immediate Calibration' dialog box is open, showing a message: 'It takes around 15 min to reach the stable status after immediate calibration.' The dialog has radio buttons for 'All APs', 'Specified AP group', and 'Specified AP', with 'All APs' selected. 'OK' and 'Cancel' buttons are at the bottom.</p>

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



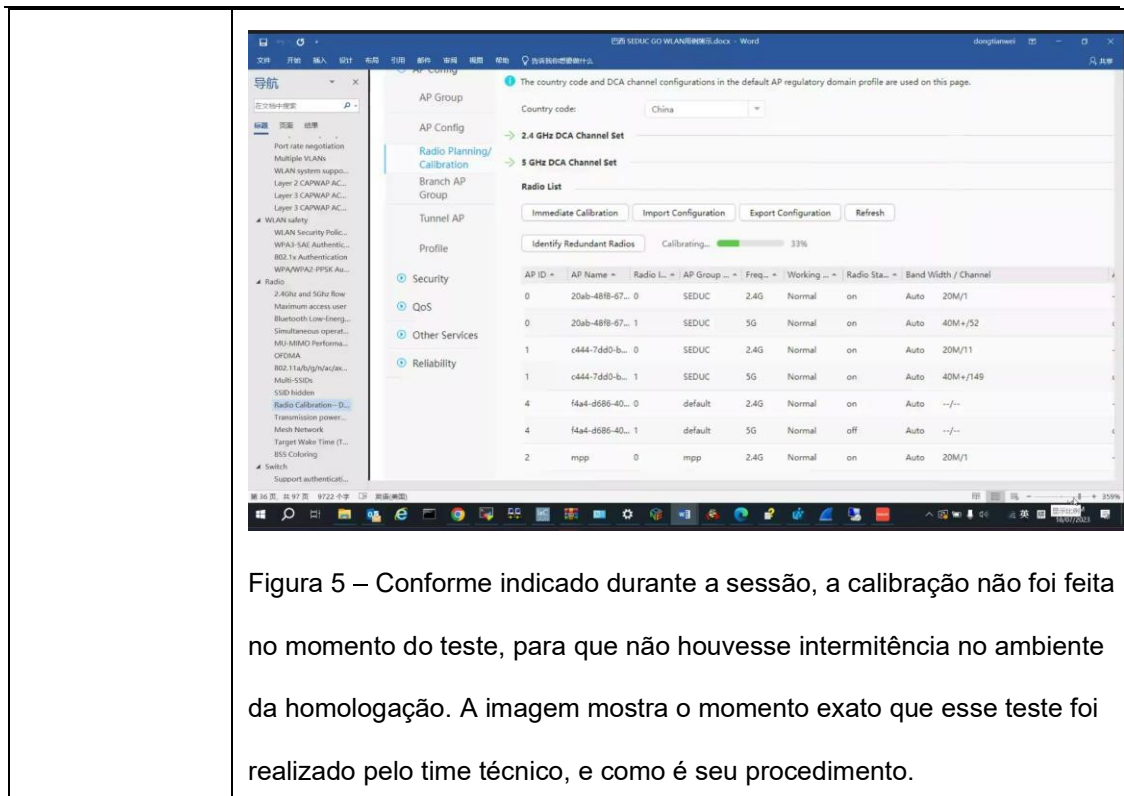
The screenshot shows the 'Radio Calibration Record' page in the WLAN Web interface. The page includes a 'Radio List' table with the following columns: AP ID, AP Name, Radio ID, Status, Freq., Radio Type, Channel, ERP/Max ERP (dBm), Access, Noise, and Chain. The table contains several rows of data, including records for APs 20ab-488b-67e0, c444-7d50-b000, and mpp, with various radio types and channels.



The screenshot shows the 'Radio Calibration Record' page in the Wireless LAN AC6805 interface. The page includes a 'Radio List' table with the following columns: Time, AP ID, AP Name, Radio ID, Channel Before/After, Bandwidth Before/After, ERP Before/After, RSSI Before/After, and Calibration Cause. The table contains several rows of data, including records for APs 20ab-488b-67e0, c444-7d50-b000, and mpp, with various radio types and channels.

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.

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




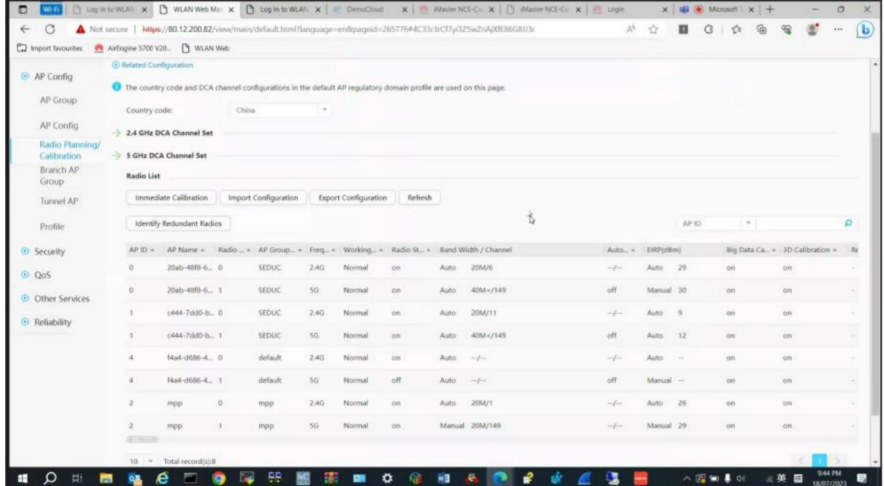
### Alteração da potência de transmissão

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;

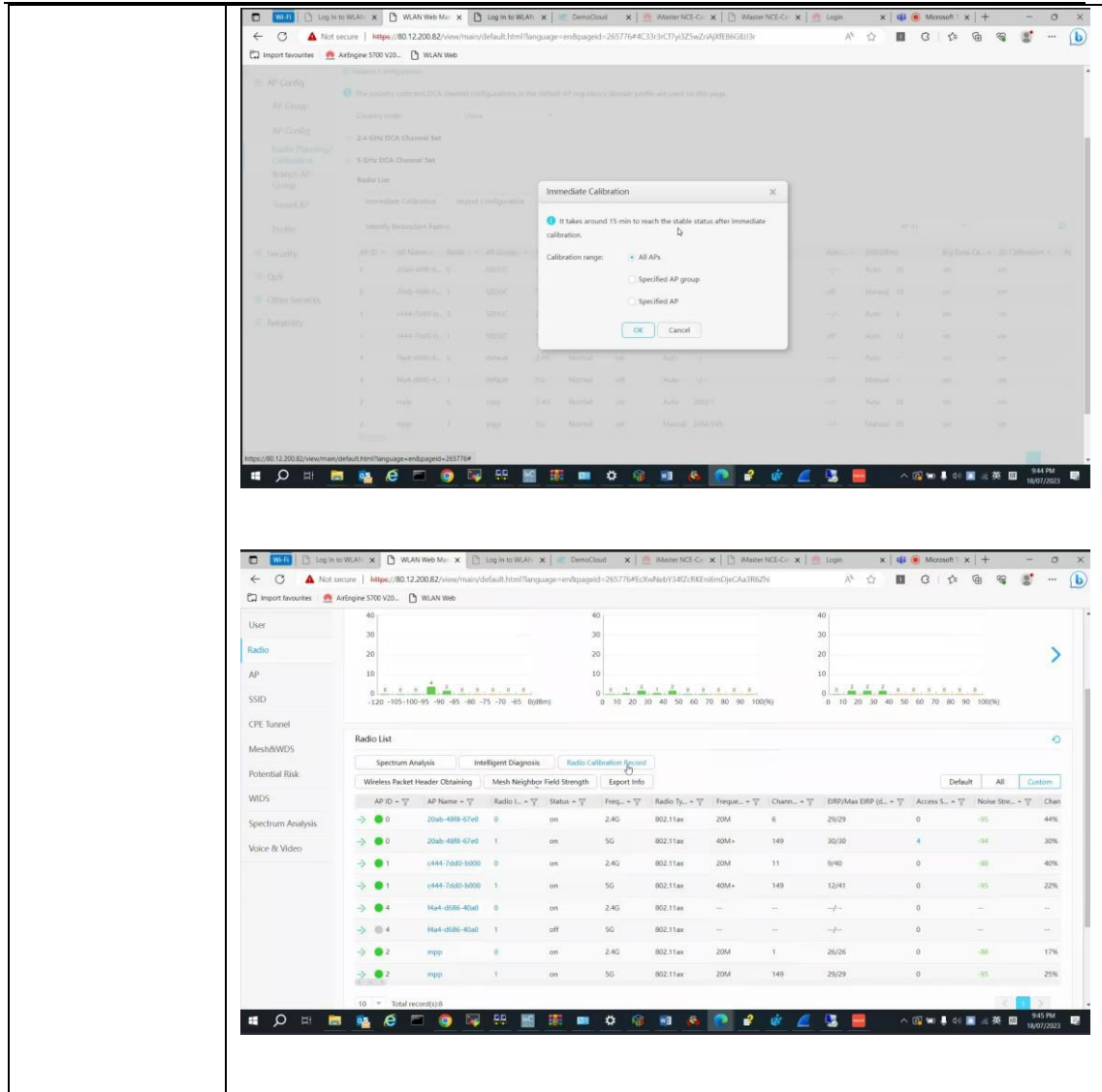
5.7.7.11 Deve permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF (rádio frequência) conforme as características do ambiente, evitando intervenção manual;

<b>Item de teste</b>	Alteração da potência de transmissão
----------------------	--------------------------------------

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

<b>Objetivo do teste</b>	Validar se a potência de transmissão do AP pode ser modificada e se o intervalo de potência está dentro da legislação local.																																																																																																																					
<b>Configuração de teste</b>	<p>Topologia da rede:</p> <div style="text-align: center;">  <p>STA      AP      Switch      AC</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>																																																																																																																					
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure a AC corretamente</li> <li>2) Habilite a função Radio Calibration;</li> </ol>																																																																																																																					
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Registrar informações de rádio sobre todos os APs;</li> <li>2) O canal AP e a potência de trânsito foram ajustados de forma dinâmica.</li> </ol>																																																																																																																					
<b>Resultado</b>	 <table border="1"> <thead> <tr> <th>AP ID</th> <th>AP Name</th> <th>Radio</th> <th>AP Group</th> <th>Freq.</th> <th>Working</th> <th>Radio St.</th> <th>Band Width / Channel</th> <th>Auto</th> <th>1920MHz</th> <th>Big Data CA</th> <th>3D Calibration</th> <th>Rs</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>20ab-489b-4...</td> <td>0</td> <td>SEUDC</td> <td>2.4G</td> <td>Normal</td> <td>on</td> <td>Auto 20M/6</td> <td>off</td> <td>Auto 29</td> <td>on</td> <td>on</td> <td>-</td> </tr> <tr> <td>0</td> <td>20ab-489b-4...</td> <td>1</td> <td>SEUDC</td> <td>5G</td> <td>Normal</td> <td>on</td> <td>Auto 40M+/149</td> <td>off</td> <td>Manual 30</td> <td>on</td> <td>on</td> <td>-</td> </tr> <tr> <td>1</td> <td>c444-7680-b...</td> <td>0</td> <td>SEUDC</td> <td>2.4G</td> <td>Normal</td> <td>on</td> <td>Auto 20M/11</td> <td>off</td> <td>Auto 9</td> <td>on</td> <td>on</td> <td>-</td> </tr> <tr> <td>1</td> <td>c444-7680-b...</td> <td>1</td> <td>SEUDC</td> <td>5G</td> <td>Normal</td> <td>on</td> <td>Auto 40M+/149</td> <td>off</td> <td>Auto 12</td> <td>on</td> <td>on</td> <td>-</td> </tr> <tr> <td>4</td> <td>444-d586-4...</td> <td>0</td> <td>default</td> <td>2.4G</td> <td>Normal</td> <td>on</td> <td>Auto</td> <td>off</td> <td>Auto</td> <td>on</td> <td>on</td> <td>-</td> </tr> <tr> <td>4</td> <td>444-d586-4...</td> <td>1</td> <td>default</td> <td>5G</td> <td>Normal</td> <td>off</td> <td>Auto</td> <td>off</td> <td>Manual</td> <td>on</td> <td>on</td> <td>-</td> </tr> <tr> <td>2</td> <td>mpp</td> <td>0</td> <td>mpp</td> <td>2.4G</td> <td>Normal</td> <td>on</td> <td>Auto 20M/1</td> <td>off</td> <td>Auto 26</td> <td>on</td> <td>on</td> <td>-</td> </tr> <tr> <td>2</td> <td>mpp</td> <td>1</td> <td>mpp</td> <td>5G</td> <td>Normal</td> <td>on</td> <td>Manual 20M/149</td> <td>off</td> <td>Manual 29</td> <td>on</td> <td>on</td> <td>-</td> </tr> </tbody> </table>	AP ID	AP Name	Radio	AP Group	Freq.	Working	Radio St.	Band Width / Channel	Auto	1920MHz	Big Data CA	3D Calibration	Rs	0	20ab-489b-4...	0	SEUDC	2.4G	Normal	on	Auto 20M/6	off	Auto 29	on	on	-	0	20ab-489b-4...	1	SEUDC	5G	Normal	on	Auto 40M+/149	off	Manual 30	on	on	-	1	c444-7680-b...	0	SEUDC	2.4G	Normal	on	Auto 20M/11	off	Auto 9	on	on	-	1	c444-7680-b...	1	SEUDC	5G	Normal	on	Auto 40M+/149	off	Auto 12	on	on	-	4	444-d586-4...	0	default	2.4G	Normal	on	Auto	off	Auto	on	on	-	4	444-d586-4...	1	default	5G	Normal	off	Auto	off	Manual	on	on	-	2	mpp	0	mpp	2.4G	Normal	on	Auto 20M/1	off	Auto 26	on	on	-	2	mpp	1	mpp	5G	Normal	on	Manual 20M/149	off	Manual 29	on	on	-
AP ID	AP Name	Radio	AP Group	Freq.	Working	Radio St.	Band Width / Channel	Auto	1920MHz	Big Data CA	3D Calibration	Rs																																																																																																										
0	20ab-489b-4...	0	SEUDC	2.4G	Normal	on	Auto 20M/6	off	Auto 29	on	on	-																																																																																																										
0	20ab-489b-4...	1	SEUDC	5G	Normal	on	Auto 40M+/149	off	Manual 30	on	on	-																																																																																																										
1	c444-7680-b...	0	SEUDC	2.4G	Normal	on	Auto 20M/11	off	Auto 9	on	on	-																																																																																																										
1	c444-7680-b...	1	SEUDC	5G	Normal	on	Auto 40M+/149	off	Auto 12	on	on	-																																																																																																										
4	444-d586-4...	0	default	2.4G	Normal	on	Auto	off	Auto	on	on	-																																																																																																										
4	444-d586-4...	1	default	5G	Normal	off	Auto	off	Manual	on	on	-																																																																																																										
2	mpp	0	mpp	2.4G	Normal	on	Auto 20M/1	off	Auto 26	on	on	-																																																																																																										
2	mpp	1	mpp	5G	Normal	on	Manual 20M/149	off	Manual 29	on	on	-																																																																																																										

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



The image displays two screenshots of the Aruba WLAN Web management interface. The top screenshot shows the 'Immediate Calibration' dialog box, which prompts the user to select a calibration range. The bottom screenshot shows the 'Radio List' table, which provides detailed information about the network's radio resources.

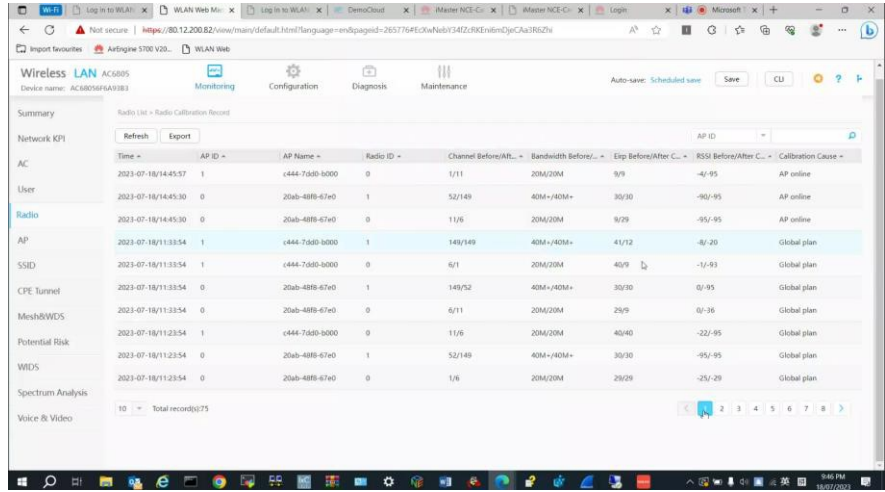
**Immediate Calibration Dialog:**

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

**Radio List Table:**

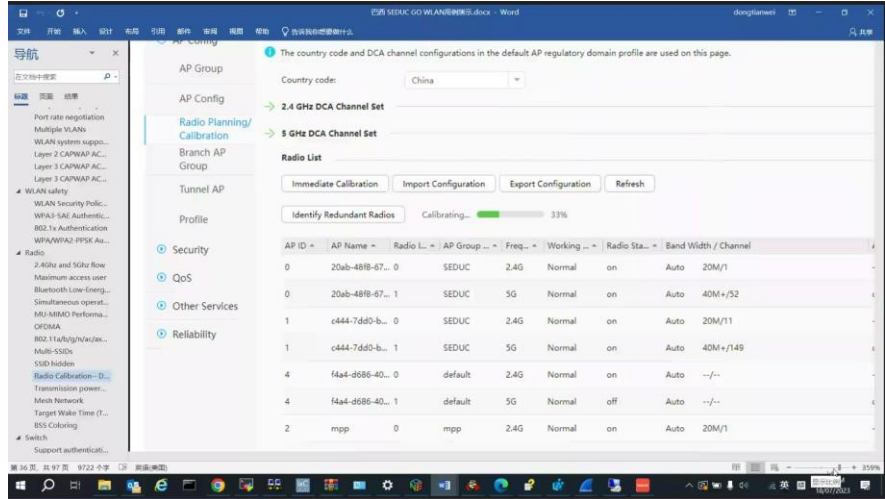
AP ID	AP Name	Radio L.	Status	Freq.	Radio Ty.	Frequ.	Chan.	ERP/Max ERP (dL)	Access S.	Noise Ste.	Chan
0	20ab-4889-67e0	0	on	2.4G	802.11ax	20M	6	29/29	0	95	44%
0	20ab-4889-67e0	1	on	5G	802.11ax	40M+	149	30/30	4	94	30%
1	c444-7d80-5000	0	on	2.4G	802.11ax	20M	11	9/40	0	88	40%
1	c444-7d80-5000	1	on	5G	802.11ax	40M+	149	12/41	0	95	22%
4	M44-d586-40a0	0	on	2.4G	802.11ax	--	--	--	0	--	--
4	M44-d586-40a0	1	off	5G	802.11ax	--	--	--	0	--	--
2	mpp	0	on	2.4G	802.11ax	20M	1	26/26	0	88	17%
2	mpp	1	on	5G	802.11ax	20M	149	29/29	0	95	25%

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



Time	AP ID	AP Name	Radio ID	Channel Before/After	Bandwidth Before/After	Exp. Before/After C.	RSSI Before/After C.	Calibration Cause
2023-07-18/14:45:57	1	c444-7d60-6000	0	1/11	20M/20M	9/9	-4/-95	AP online
2023-07-18/14:45:30	0	20ab-48f8-67d0	1	52/149	40M+/40M+	30/30	-90/-95	AP online
2023-07-18/14:45:30	0	20ab-48f8-67d0	0	11/6	20M/20M	9/29	-95/-95	AP online
2023-07-18/11:33:54	1	c444-7d60-6000	1	149/149	40M+/40M+	41/12	-8/-20	Global plan
2023-07-18/11:33:54	1	c444-7d60-6000	0	6/1	20M/20M	40/9	-1/-93	Global plan
2023-07-18/11:33:54	0	20ab-48f8-67d0	1	149/52	40M+/40M+	30/30	0/-95	Global plan
2023-07-18/11:33:54	0	20ab-48f8-67d0	0	6/11	20M/20M	29/9	0/-36	Global plan
2023-07-18/11:23:54	1	c444-7d60-6000	0	11/6	20M/20M	40/40	-22/-95	Global plan
2023-07-18/11:23:54	0	20ab-48f8-67d0	1	52/149	40M+/40M+	30/30	-95/-95	Global plan
2023-07-18/11:23:54	0	20ab-48f8-67d0	0	1/6	20M/20M	29/29	-25/-29	Global plan

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.



AP ID	AP Name	Radio L.	AP Group	Freq.	Working	Radio Sta.	Band Width / Channel
0	20ab-48f8-67..	0	SEUDC	2.4G	Normal	on	Auto 20M/1
0	20ab-48f8-67..	1	SEUDC	5G	Normal	on	Auto 40M+/52
1	c444-7d60-b..	0	SEUDC	2.4G	Normal	on	Auto 20M/11
1	c444-7d60-b..	1	SEUDC	5G	Normal	on	Auto 40M+/149
4	f4a4-d586-40..	0	default	2.4G	Normal	on	Auto --/--
4	f4a4-d586-40..	1	default	5G	Normal	off	Auto --/--
2	mpp	0	mpp	2.4G	Normal	on	Auto 20M/1

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.

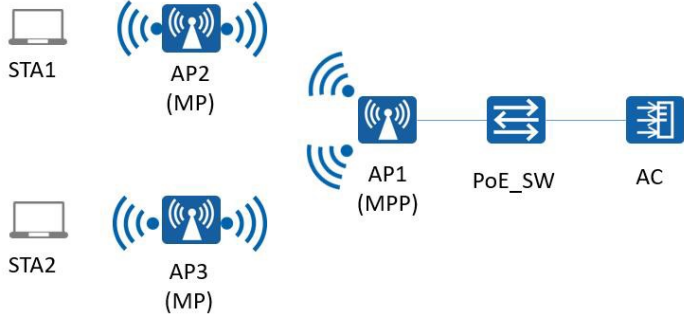


PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

**Mesh Network**

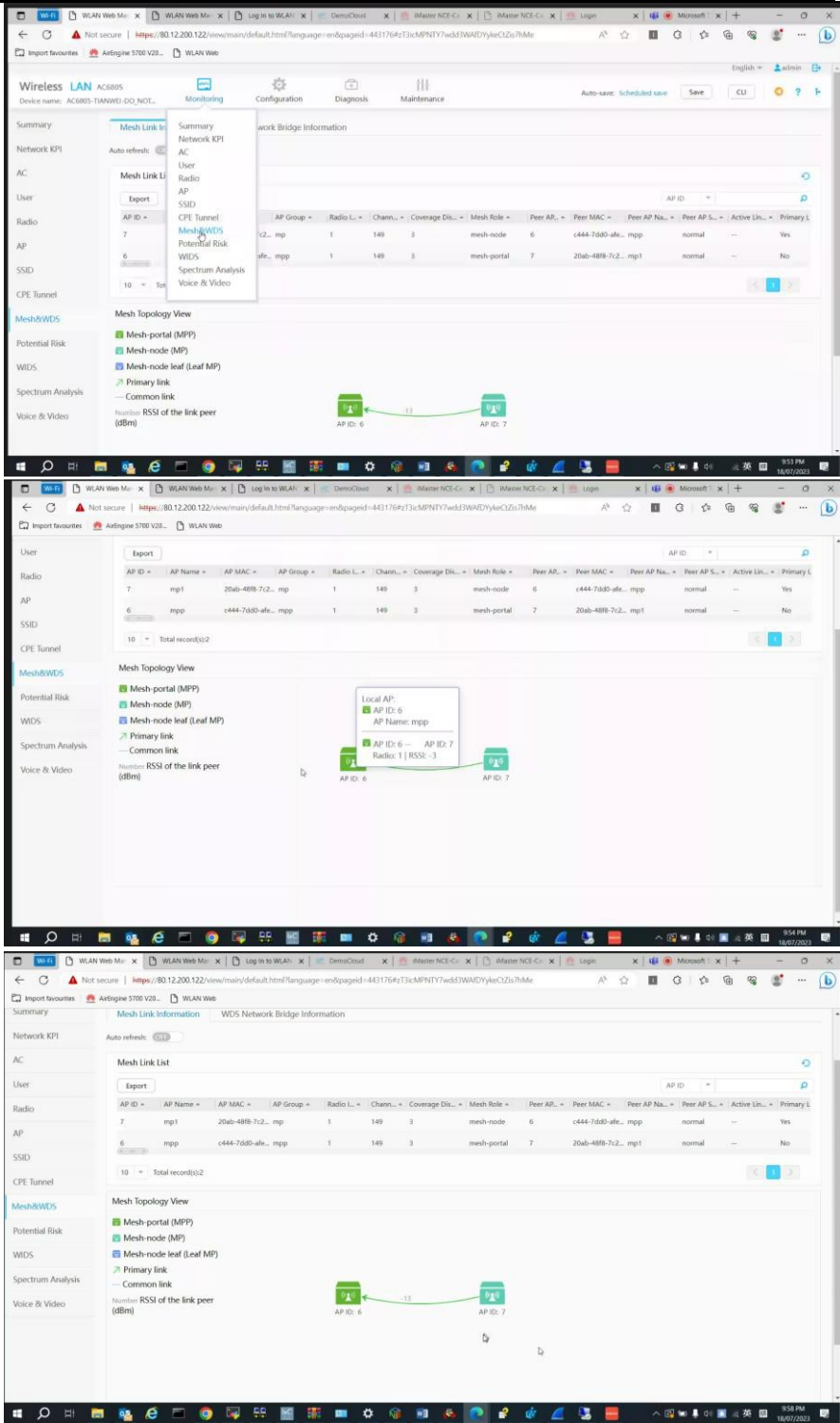
5.6.7.14 Deve permitir operação em modo Mesh, garantindo o estabelecimento da conexão por meio do rádio Wi-Fi com outros pontos de acesso;

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

<b>Item de teste</b>	Rede Mesh
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Rede Mesh
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	1) Configurar a função Mesh na AC e APs
<b>Resultado esperado</b>	1) Verificar informação de link mesh na AC e sua operação;

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

**Resultado**



The screenshots show the following data from the dashboard:

AP ID	AP Name	AP MAC	AP Group	Radio L.	Chann.	Coverage Dis.	Mesh Role	Peer AP	Peer MAC	Peer AP Na.	Peer AP S.	Active Lin.	Primary L
7	mp1	20ab-48b-7c2...	mp	1	149	3	mesh-node	6	c444-76d0-afe...	mpgp	normal	--	Yes
6	mpp	c444-76d0-afe...	mpp	1	149	3	mesh-portal	7	20ab-48b-7c2...	mp1	normal	--	No

The Mesh Topology View shows a connection between AP ID 6 (Local AP) and AP ID 7 (Peer AP) with an RSSI of -3 dBm.

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

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

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)”

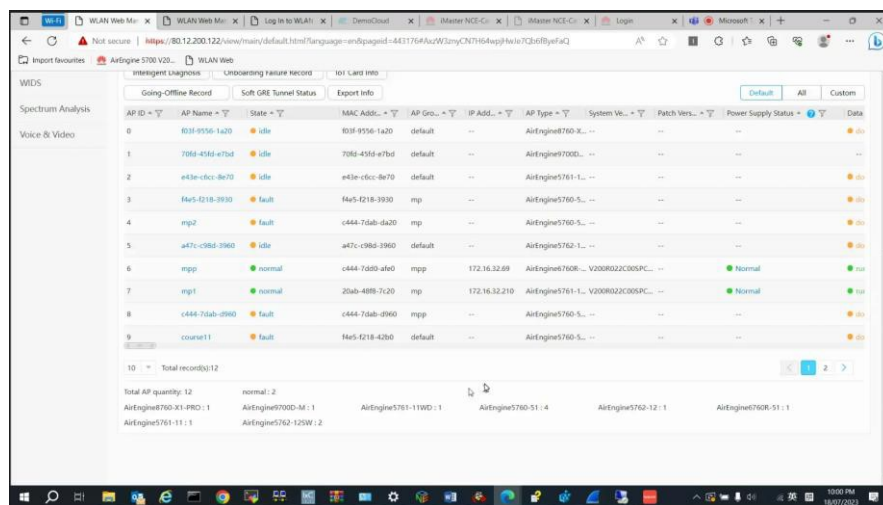


Figura 4 – Na listagem de todos os APs disponíveis e gerenciados, o funcionamento do AP ID 6 e 7, aparecem com o status de operação normal.


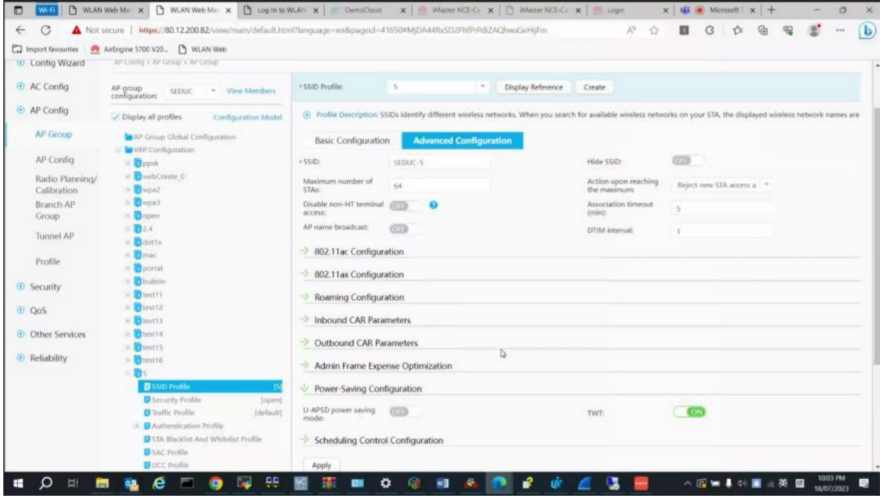
### Target Wake Time (TWT)

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

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

<b>Item de teste</b>	Target Wake Time (TWT)
<b>Objetivo do teste</b>	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**

<p align="center"><b>Configuração de teste</b></p>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p align="center"><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Configure a AC corretamente,</li> <li>2) Habilite TWT</li> </ol>
<p align="center"><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) O status TWT pode ser verificado nos detalhes de perfil SSID.</li> <li>2) Frames referentes a tecnologia TWT capturados</li> </ol>
<p align="center"><b>Resultado</b></p>	 <p>Figura 1 – Dentro do VAP Configuration, nas opções de “Power-Saving Configuration”, foi mostrado onde habilitar a opção de TWT.</p> <pre> 17668 AtherosC_12:79:79 Broadcast 802.11 459 Beacon frame, SN=645, FN=0, Flags=.....C, BI=100, SSID=5g-wifi6 17669 HuaweiIte_F8:67:F0 Broadcast 802.11 387 Beacon frame, SN=1628, FN=0, Flags=.....C, BI=100, SSID=SEDC-PPSK 17670 HuaweiIte_F8:67:F1 Broadcast 802.11 357 Beacon frame, SN=1627, FN=0, Flags=.....C, BI=100, SSID=test  ..0.. ..0.. ..0.. = Fine Timing Measurement Responder: False 0... ..0.. ..0.. = Fine Timing Measurement Initiator: False Extended Capabilities: 0x40 (octet 10) ... ..0.. = FILS Capable: False ... ..0.. = Extended Spectrum Management Capable: False ... ..0.. = Future Channel Capable: False ... ..0.. = Reserved: 0x0 ... ..0.. = Reserved: 0x0 ... ..0.. = TWT Requester Support: False ..1.. ..0.. = TWT Responder Support: True                     </pre>

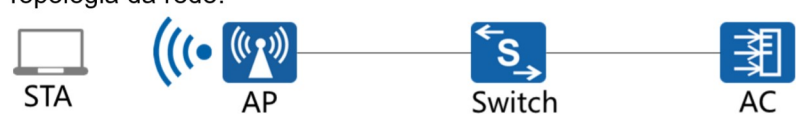
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	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;

<b>Item de teste</b>	<b>BSS Coloring</b>
<b>Objetivo do teste</b>	<b>Validar se o AP suporta coloração BSS</b>
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure a AC corretamente,</li> <li>2) Habilite BSS Coloring</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) O status TWT pode ser verificado nos detalhes de perfil SSID.</li> <li>2) Pacotes referentes a tecnologia TWT capturados</li> </ol>

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

**Resultado**

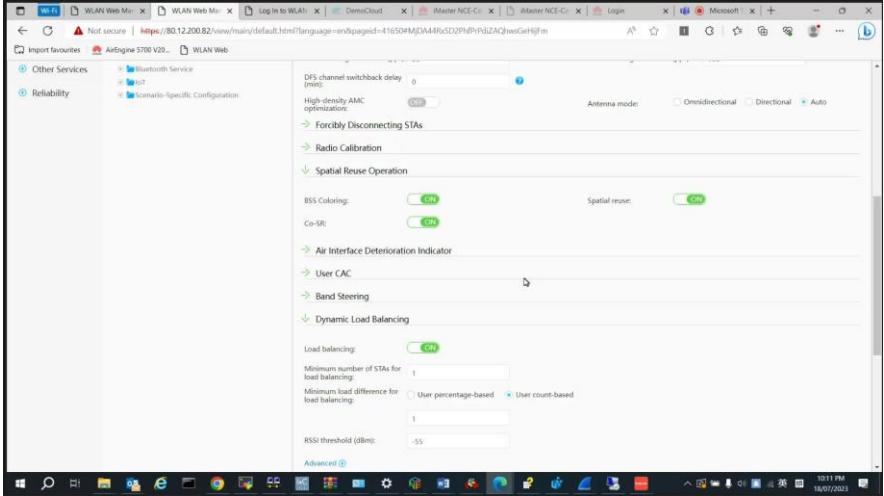


Figura 1 – Dentro do VAP Configuration, nas opções de “Spatial Reuse Operation”, foi mostrado onde habilitar a opção de BSS Coloring.

**Resultado**

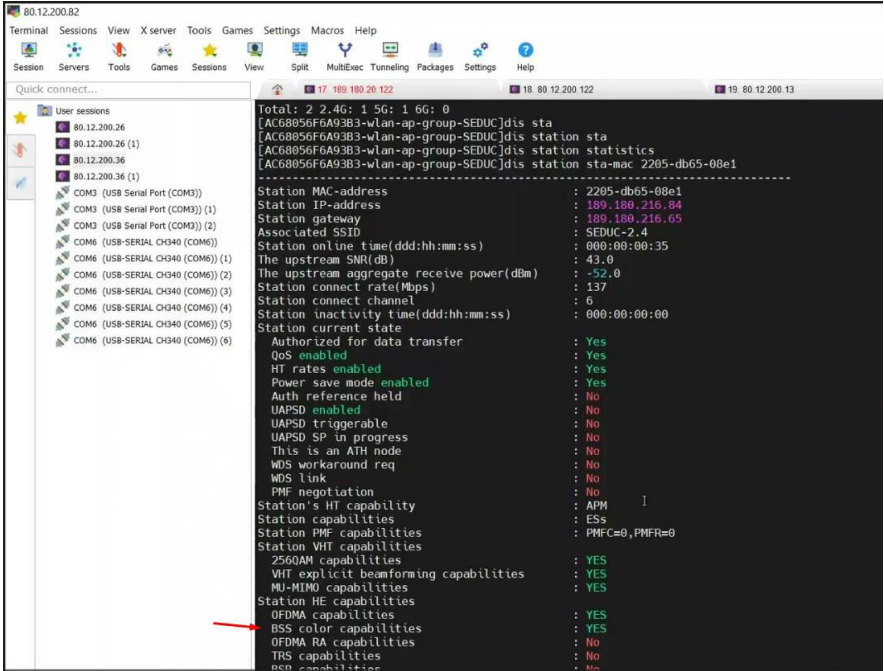


Figura 1 – Via CLI, foi listada através do comando “display station sta-mac 2205-db-65-08e1”, todas as informações de um dispositivo conectado ao SSID SEDUC-2.4, criado no procedimento anterior.

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

	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->

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

---

[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](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



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

---

## 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](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](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100302331&id=EN-US_CONCEPT_0000001386088048&lang=en)

Chassis height [U] 1 U

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

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

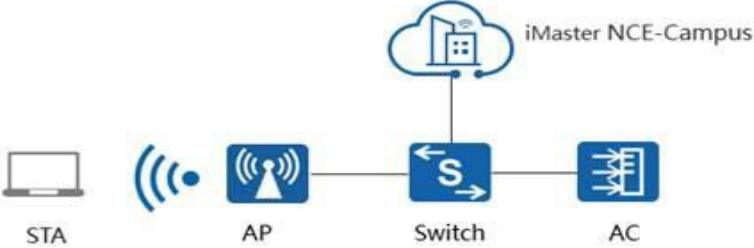
CloudEngine S5735-L-V2 Series Switches Datasheet.pdf

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

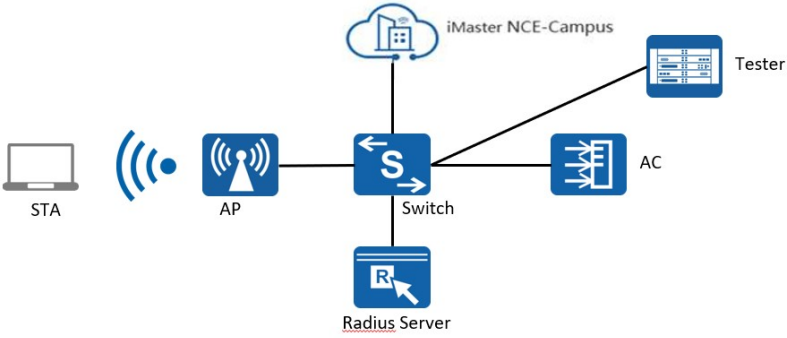
**Suporte a autenticação via servidores RADIUS**

5.8.18 Suportar autenticação em servidores RADIUS ou TACACS;

5.9.15 Suportar autenticação em servidores RADIUS ou TACACS;

<b>Item de teste</b>	<b>Suporte de autenticação para servidores RADIUS</b>
<b>Objetivo do teste</b>	Suporta autenticação para servidores RADIUS;
<b>Configuração de teste</b>	<p>Topologia da rede 1:</p>  <pre> graph LR     STA[STA] --- AP[AP]     AP --- Switch[Switch]     Switch --- AC[AC]     AC --- iMaster[iMaster NCE-Campus]             </pre> <p>Topologia de rede 2 (com RADIUS externo):</p>

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

	<div style="text-align: center;">  </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Selecione “Provision&gt; Device &gt; Site Configuration &gt; Site &gt; Device Login Configuration” no menu principal .Clique ”Create“; Depois, configure regras de autenticação, regras de autorização e os resultados da autorização.</li> <li>2) Selecione “Provision&gt; Device &gt; Site Configuration” depois configure as interfaces por onde os usuários serão autenticados</li> </ol>
<p><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) A configuração é entregue e autenticada com sucesso.</li> </ol>

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

**Resultado**

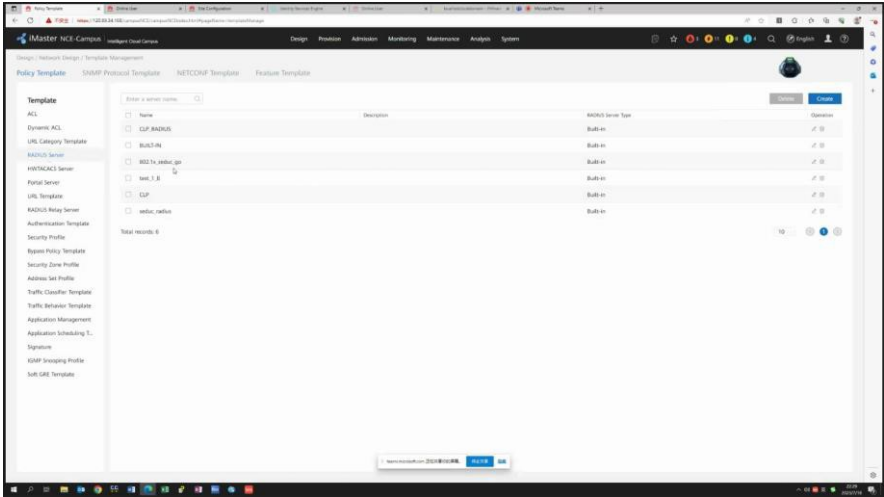


Figura 1 – Dentro da plataforma iMaster NCE Campus, foi criado alguns templates de servidores Radius

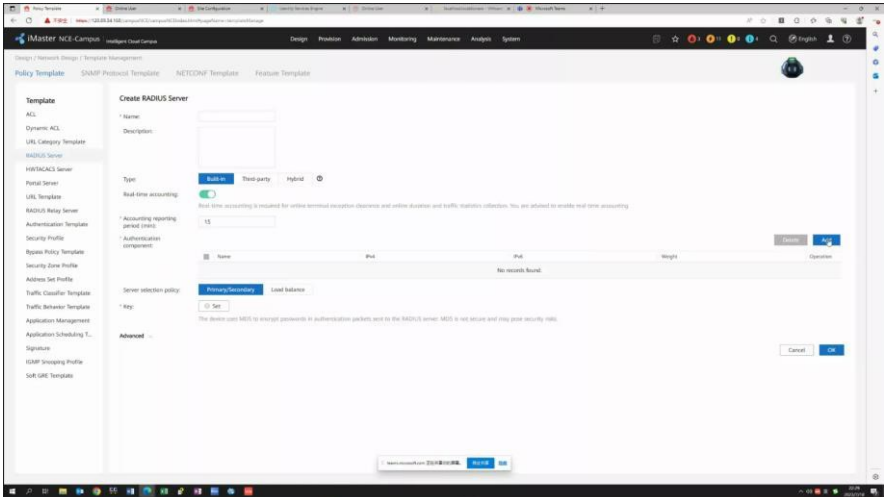
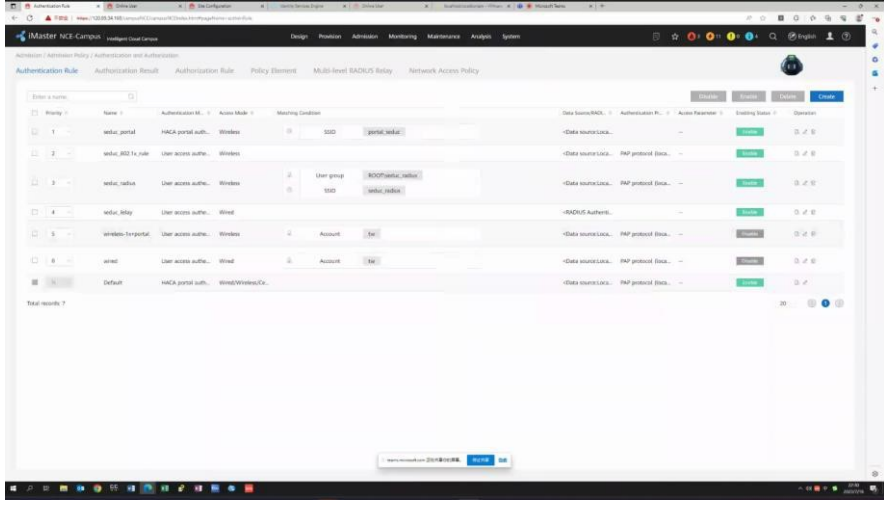
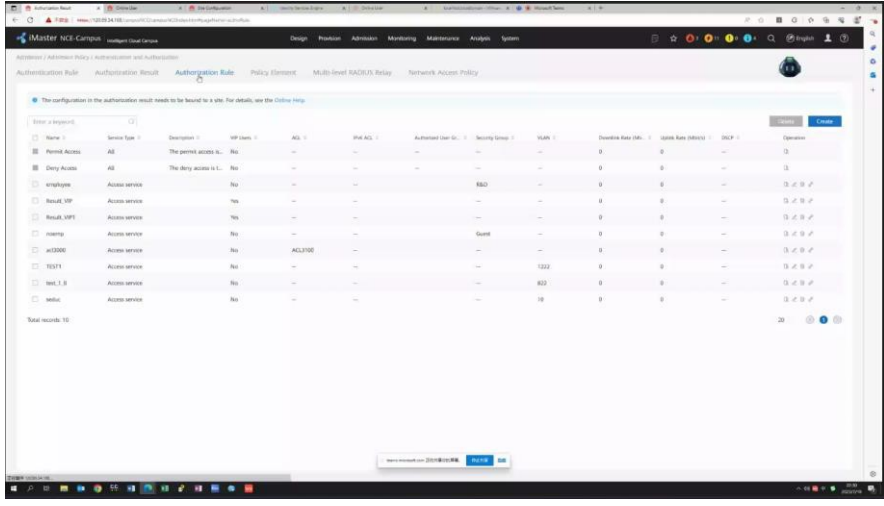
  


Figura 2 – O procedimento para isso é baseado em inserir as informações necessárias, como a “shared secret” que vai ser compartilhada entre os dispositivos.

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



ID	Name	Authentication Method	Access Mode	Matching Location	User Source	Authentication Protocol	Access Parameter	Enabling Status	Operation
1	redes_portal	HMAC portal auth.	Windows	SSID	portal@redes	-	-	Active	0 / 0 / 0
2	redes_802.1x_pole	User access auth.	Windows	SSID	redes@redes	-	-	Active	0 / 0 / 0
3	redes_redes	User access auth.	Windows	User group	8021x@redes	-	-	Active	0 / 0 / 0
4	redes_redes	User access auth.	Windows	SSID	redes@redes	-	-	Active	0 / 0 / 0
5	redes_802.1x_pole	User access auth.	Windows	Account	redes	-	-	Active	0 / 0 / 0
6	redes	User access auth.	Windows	Account	redes	-	-	Active	0 / 0 / 0
7	Default	HMAC portal auth.	Windows/WindowsC	-	-	-	-	Active	0 / 0 / 0

Name	Service Type	Operation	IP Users	ACL	Port ACL	Authorized User	Security Group	VLAN	Dynamic Rate	Weak Rate	DSCP	Operation
Remot Access	All	The permit access is.	No	-	-	-	-	0	0	-	0	0
Deny Access	All	The deny access is.	No	-	-	-	-	0	0	-	0	0
employee	Access service	No	-	-	-	802	-	0	0	-	0 / 0 / 0	0
Result_SPT	Access service	No	-	-	-	-	-	0	0	-	0 / 0 / 0	0
Result_SPT	Access service	No	-	-	-	-	-	0	0	-	0 / 0 / 0	0
empty	Access service	No	-	-	-	Guest	-	0	0	-	0 / 0 / 0	0
all5000	Access service	No	-	ACL100	-	-	-	0	0	-	0 / 0 / 0	0
10071	Access service	No	-	-	-	1002	-	0	0	-	0 / 0 / 0	0
net_1,8	Access service	No	-	-	-	802	-	0	0	-	0 / 0 / 0	0
redes	Access service	No	-	-	-	-	-	0	0	-	0 / 0 / 0	0

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.

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

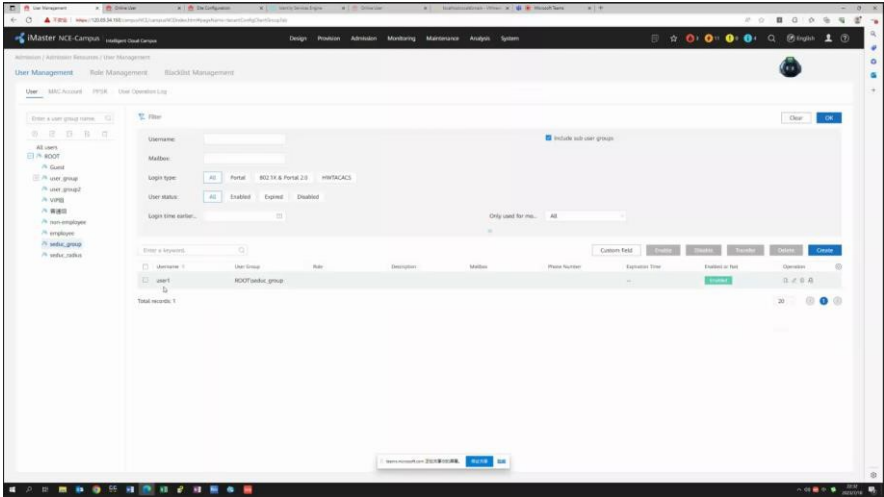


Figura 5 – Foi criado um grupo de usuários, chamado `seduc_group`, onde foi adicionado um usuário nomeado como `user1`, o qual utilizamos para autenticar o dispositivo.

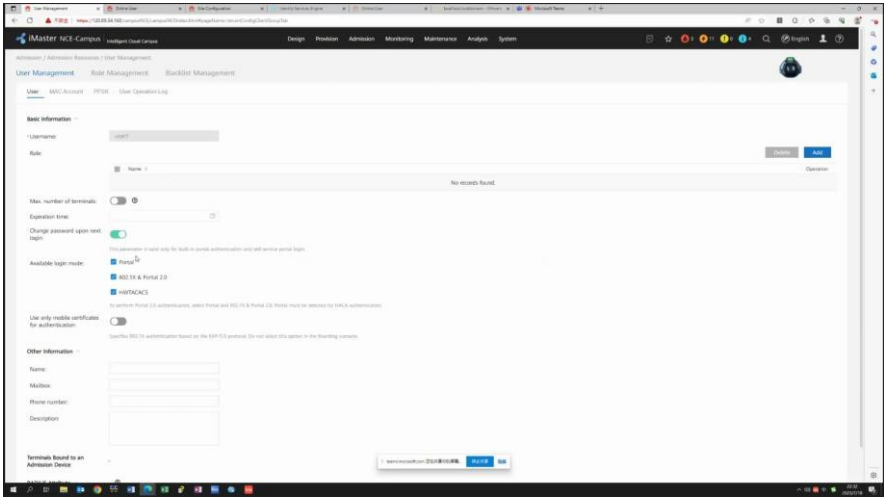


Figura 6 – Esse usuário, em suas permissões, foi configurado para que possa se autenticar via Portal, 802.1x e HWTACACS.

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

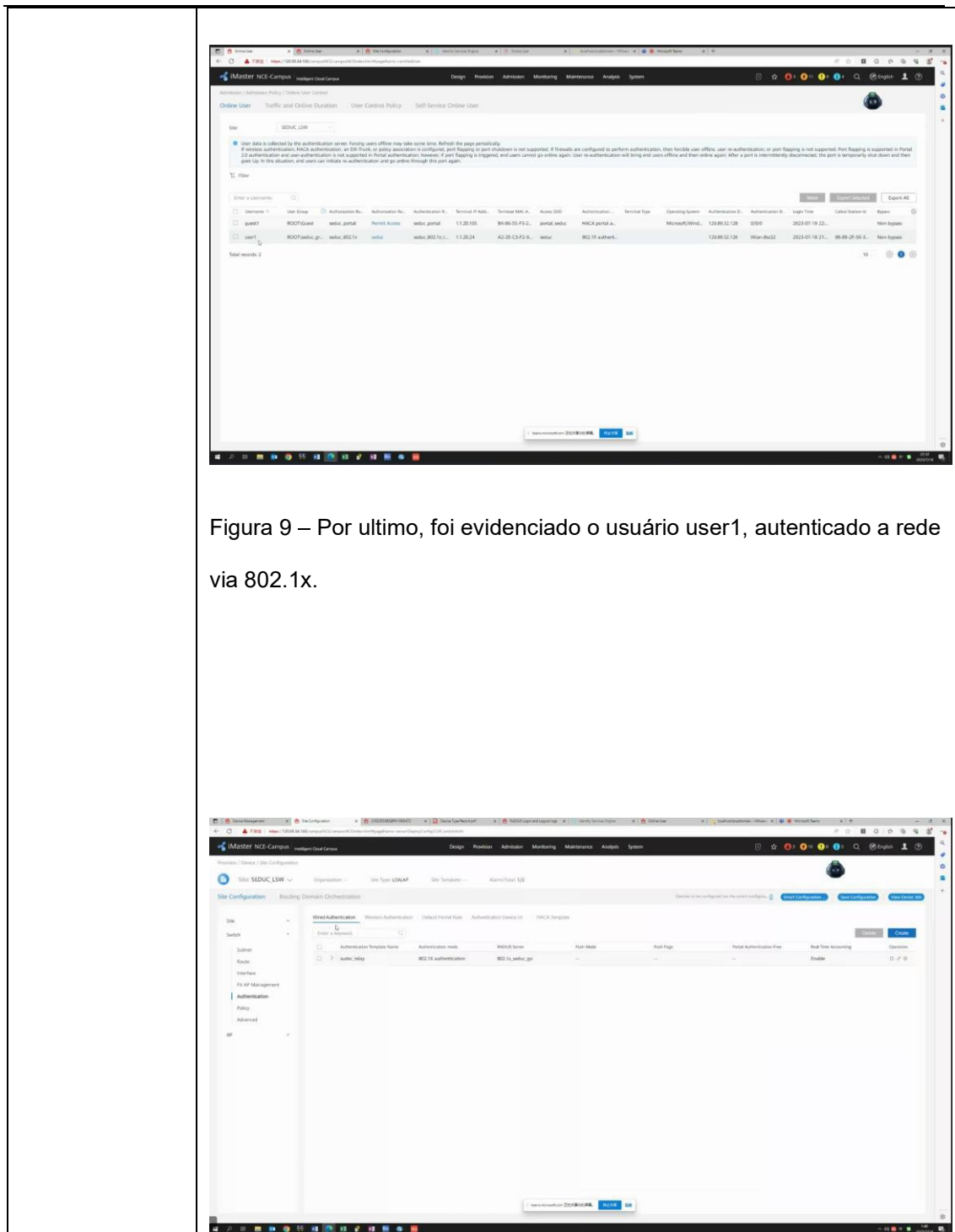


Figura 9 – Por ultimo, foi evidenciado o usuário user1, autenticado a rede via 802.1x.

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

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.

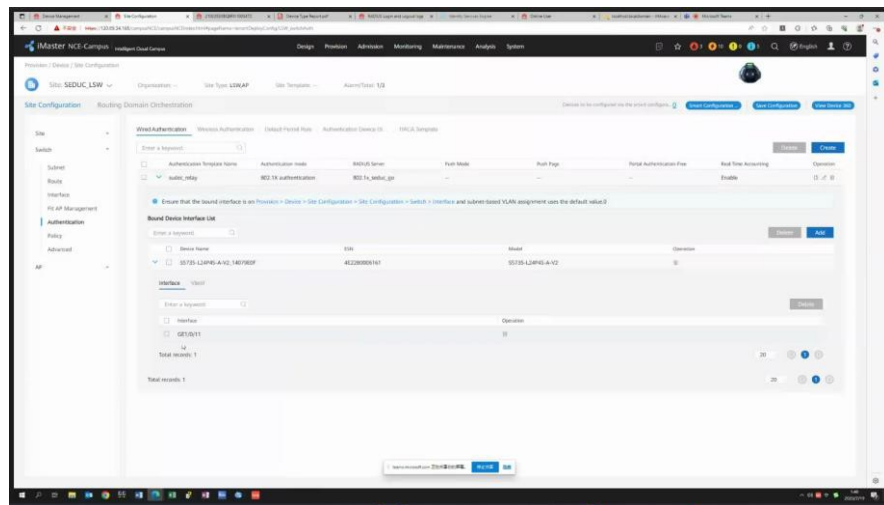


Figura 11 – Em seguida, foi feita associação da interface GE1/0/11, ao servidor.



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

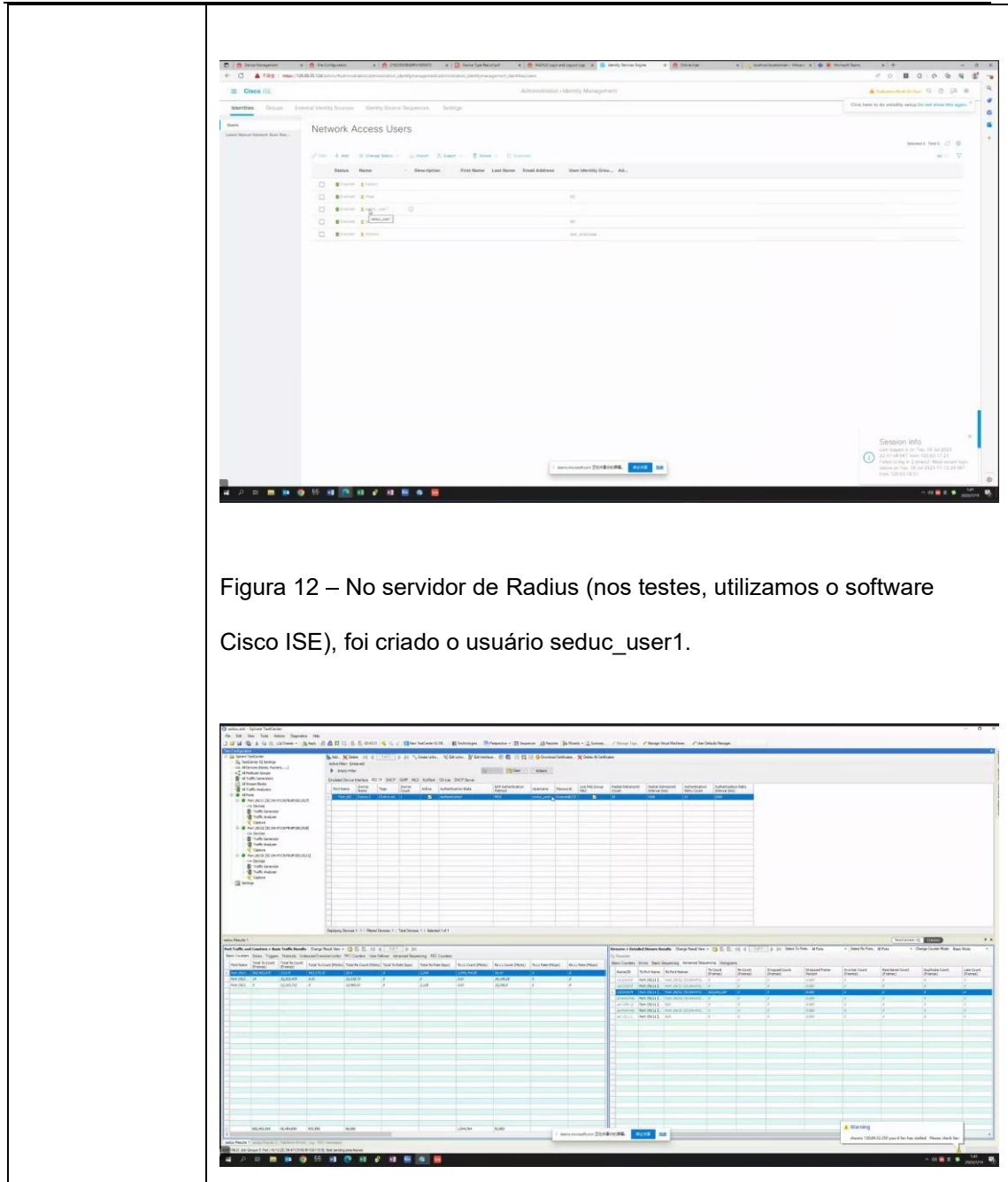


Figura 12 – No servidor de Radius (nos testes, utilizamos o software Cisco ISE), foi criado o usuário seduc\_user1.

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

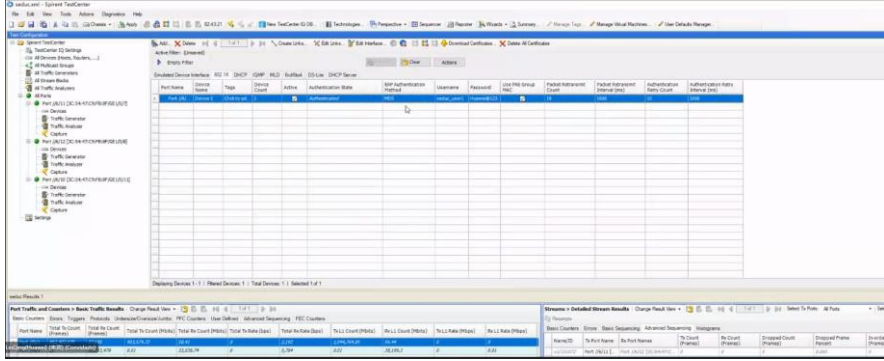


Figura 13 e 14 – Com o auxílio de um gerador de tráfego, foi simulada uma autenticação, utilizando o mesmo usuário criado no passo anterior.

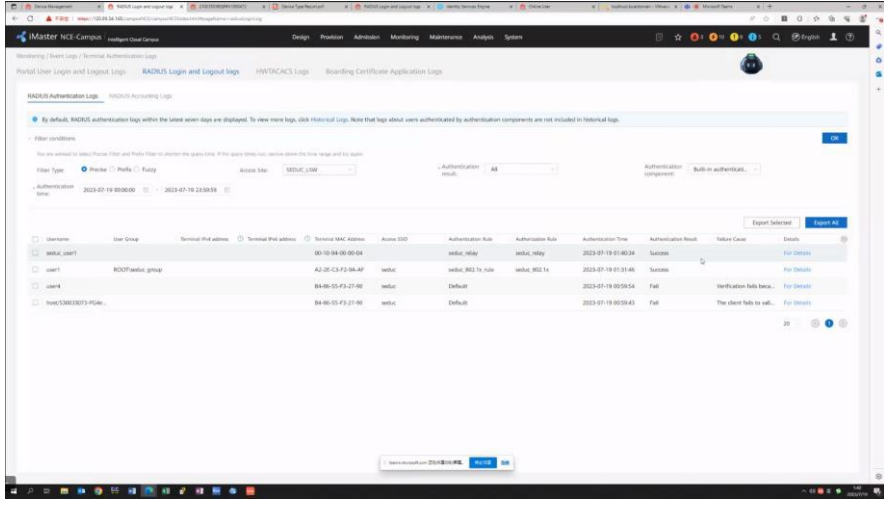


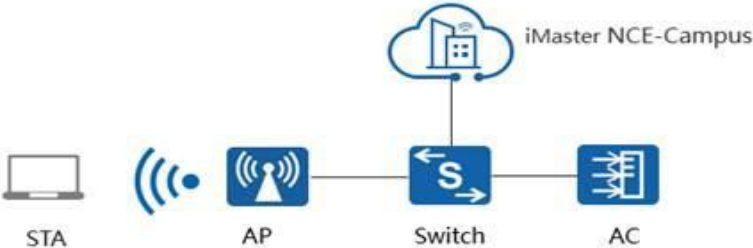
Figura 15 – Na plataforma iMaster NCE Campus, conseguimos listar os usuários conectados e autenticados via 802.1x. O usuário em destaque é o mesmo utilizado, com o nome seduc\_user1.

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;

<b>Item de teste</b>	<b>LLDP e LLDP-MED</b>
<b>Objetivo do teste</b>	<b>Implementar LLDP e LLDP-MED;</b>
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Exibir as o suporte a LLDP no equipamento</li> </ol>



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

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

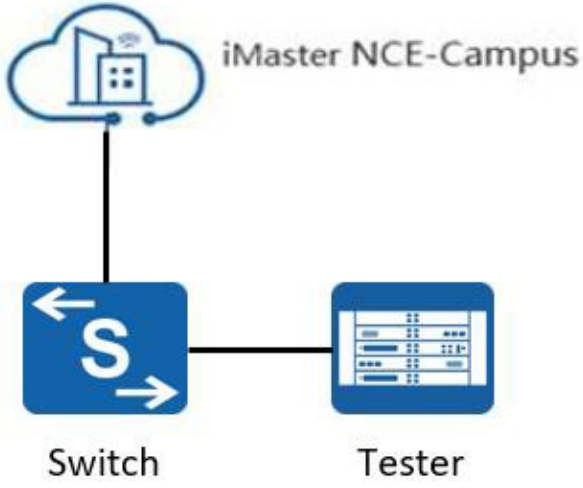
### ACL

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;

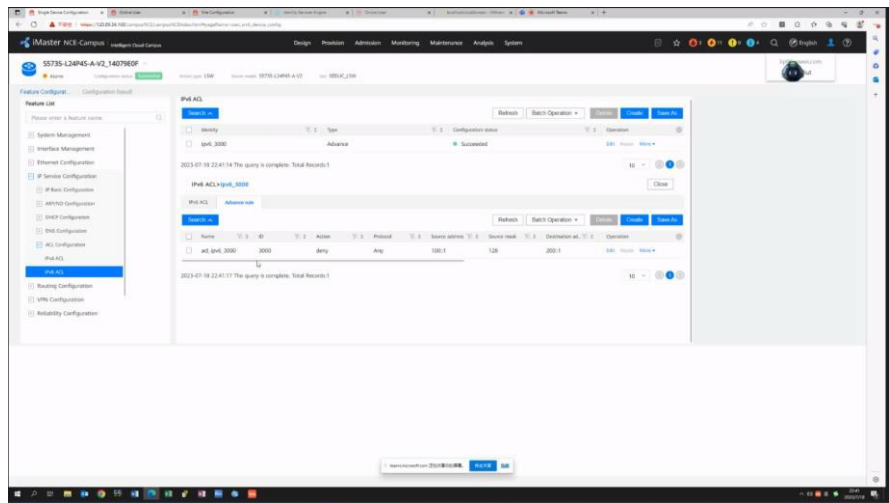
5.9.21. Deve Implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino ou VLAN;

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

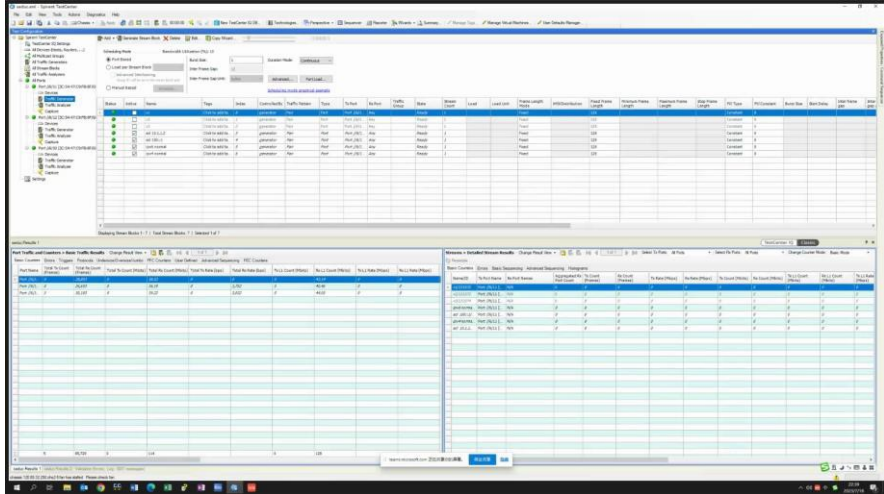
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	<div style="text-align: center;">  <p style="text-align: center;">iMaster NCE-Campus</p> <p style="text-align: center;">Switch                      Tester</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Enviar dois fluxos via gerador de tráfego, um dos quais está em conformidade com a política criada pela ACL e o outro não.</li> </ol>
<p><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) A configuração é entregue com sucesso.</li> <li>2) O tráfego que corresponde às regras ACL é processado com base nas políticas correspondentes.</li> </ol>

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

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

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



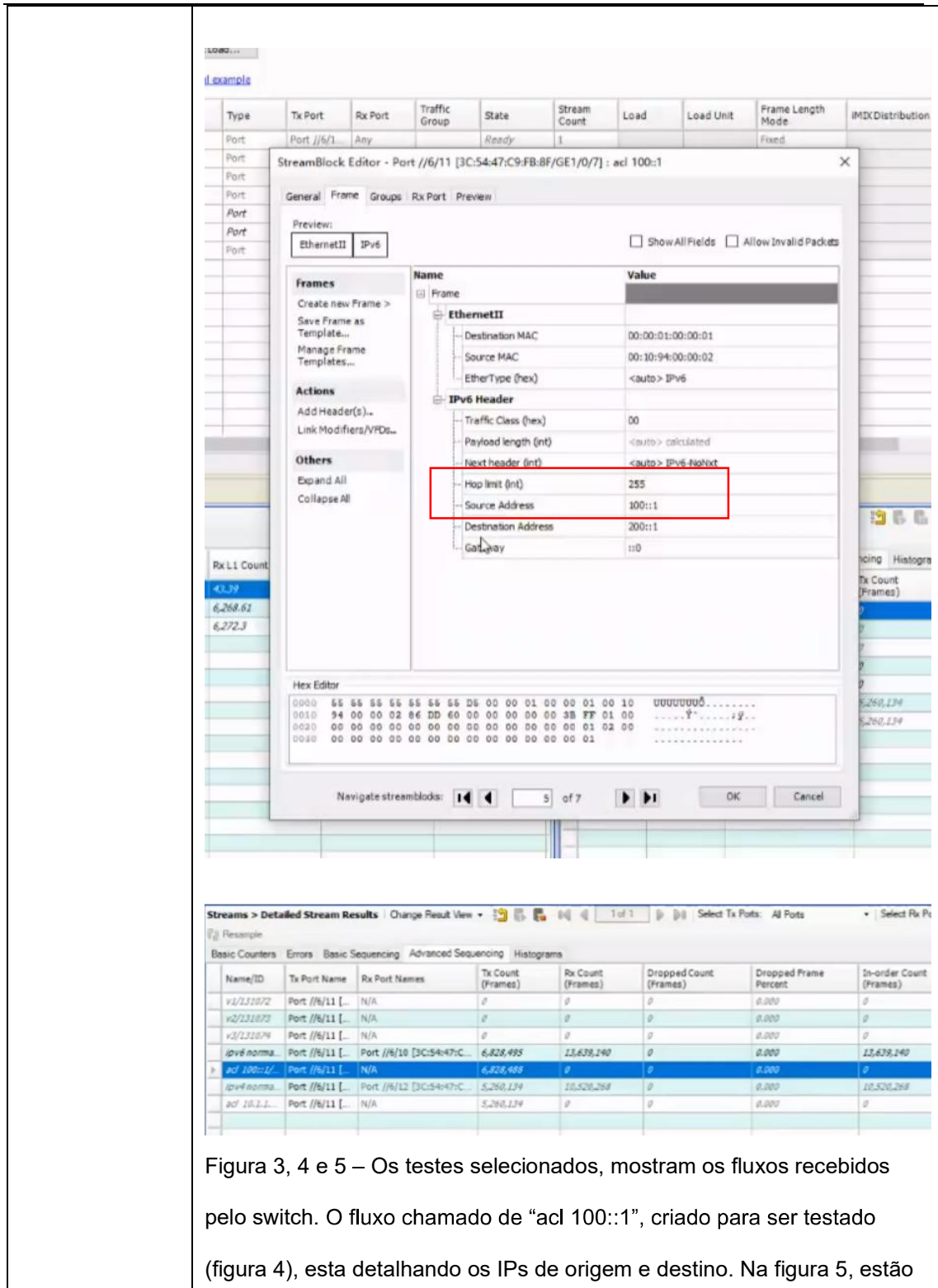
The screenshot shows the Mikrotik WinBox interface. The top window displays the configuration of an ACL (Access Control List) with several rules. The bottom window shows the results of traffic generation, with a table of generated traffic statistics.

Serial	Adress	Name	Type	State	Connections	Traffic In/Out	Type	% Pack	Seq Pack	Traffic	State	Queue	Level	Level Size	Items Length	Items Distribution	Items Length	Items Distribution	Items Length	Items Distribution	Items Length	Items Distribution	Items Length	Items Distribution	Items Length	Items Distribution
1	192.168.1.1	ACL	generator	Ready	0/0	0/0	0/0	0%	0	0/0	Ready	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
2	192.168.1.2	ACL	generator	Ready	0/0	0/0	0/0	0%	0	0/0	Ready	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
3	192.168.1.3	ACL	generator	Ready	0/0	0/0	0/0	0%	0	0/0	Ready	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
4	192.168.1.4	ACL	generator	Ready	0/0	0/0	0/0	0%	0	0/0	Ready	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
5	192.168.1.5	ACL	generator	Ready	0/0	0/0	0/0	0%	0	0/0	Ready	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

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



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



The image displays two screenshots from a network monitoring application. The top screenshot shows the 'StreamBlock Editor' window for a port configuration. The 'IPv6 Header' section is highlighted with a red box, showing the following details:

Name	Value
Destination MAC	00:00:01:00:00:01
Source MAC	00:10:94:00:00:02
EtherType (hex)	<auto> IPv6
Traffic Class (hex)	00
Payload length (int)	<auto> calculated
Next header (int)	<auto> IPv6-NQtxt
Hop limit (int)	255
Source Address	100::1
Destination Address	200::1
Gateway	::0

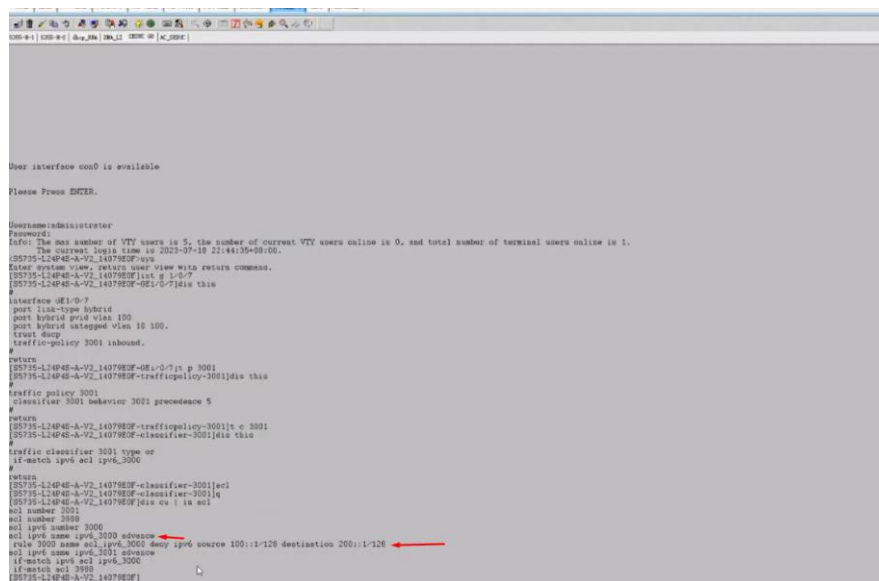
The bottom screenshot shows the 'Streams - Detailed Stream Results' table. The table lists various stream configurations and their corresponding traffic counts. The row for 'acl 100::1' is highlighted in blue, indicating it is the selected test.

Name/ID	Tx Port Name	Rx Port Names	Tx Count (Frames)	Rx Count (Frames)	Dropped Count (Frames)	Dropped Frame Percent	In-order Count (Frames)
v1/110/2	Port //6/11 [...]	N/A	0	0	0	0.000	0
v2/110/3	Port //6/11 [...]	N/A	0	0	0	0.000	0
v3/110/4	Port //6/11 [...]	N/A	0	0	0	0.000	0
ipv6 norma...	Port //6/11 [...]	Port //6/10 [3C:54:47:C...	6,828,495	22,638,240	0	0.000	22,638,240
acl 100::1	Port //6/11 [...]	N/A	6,828,498	0	0	0.000	0
ipv6 norma...	Port //6/11 [...]	Port //6/12 [3C:54:47:C...	5,260,134	10,520,268	0	0.000	10,520,268
acl 10.1.1...	Port //6/11 [...]	N/A	5,260,134	0	0	0.000	0

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

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

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



```

User interface con0 is available

Please Press ENTER.

Username:(admin):trator
Password:
Info: The total number of VTY users is 5, the number of current VTY users online is 0, and total number of terminal users online is 1.
The current login time is 2023-07-18 22:44:35:08:00.
[S5735-L24P48-A-V2_140798DF>]
factor system view, return user view with return command.
[S5735-L24P48-A-V2_140798DF]int g 1/0/7
[S5735-L24P48-A-V2_140798DF-GE1/0/7]dis this
#
interface GE1/0/7
port link-type hybrid
port hybrid pvid vlan 100
port hybrid untagged vlan 10 100.
trust dhcp
traffic-policy 3001 inbound.
#
return
[S5735-L24P48-A-V2_140798DF-GE1/0/7]p 3001
[S5735-L24P48-A-V2_140798DF-trafficpolicy-3001]dis this
#
traffic policy 3001
classifier 3001 behavior 3001 precedence 5
#
return
[S5735-L24P48-A-V2_140798DF-trafficpolicy-3001]t c 3001
[S5735-L24P48-A-V2_140798DF-classifier-3001]dis this
#
traffic classifier 3001 type or
if-match ip6 acl 3000
return
[S5735-L24P48-A-V2_140798DF-classifier-3001]a1
[S5735-L24P48-A-V2_140798DF-classifier-3001]4
[S5735-L24P48-A-V2_140798DF]dis cu | in ac1
ac1 number 3001
ac1 number 3000
ac1 ip6 num ip6_3000 advance ←
rule 3000 name ac1_ip6_3000 deny ip6 source 100::1:128 destination 200::1:128 ←
ac1 ip6 num ip6_3001 advance
if-match ip6 ac1 ip6_3000
if-match ac1 3000
[S5735-L24P48-A-V2_140798DF]
    
```

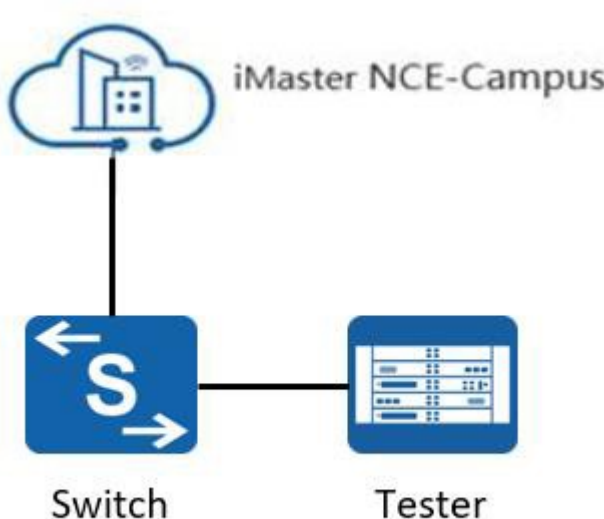
Figura 6 – Checando a CLI do switch, mostramos a sequência de ações para a implementação das regras. Primeiro foi definida a ACL, com as permissões e/ou bloqueios. Segundo, configuramos em Traffic Classifier, para que seja validada as regras da ACL. Terceiro, inserimos o Traffic Classifier dentro de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

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

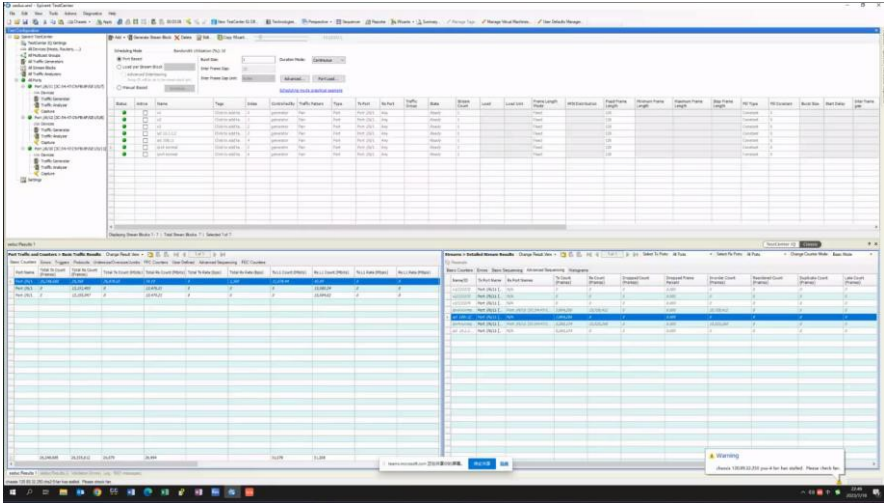
**IGMP snooping**

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

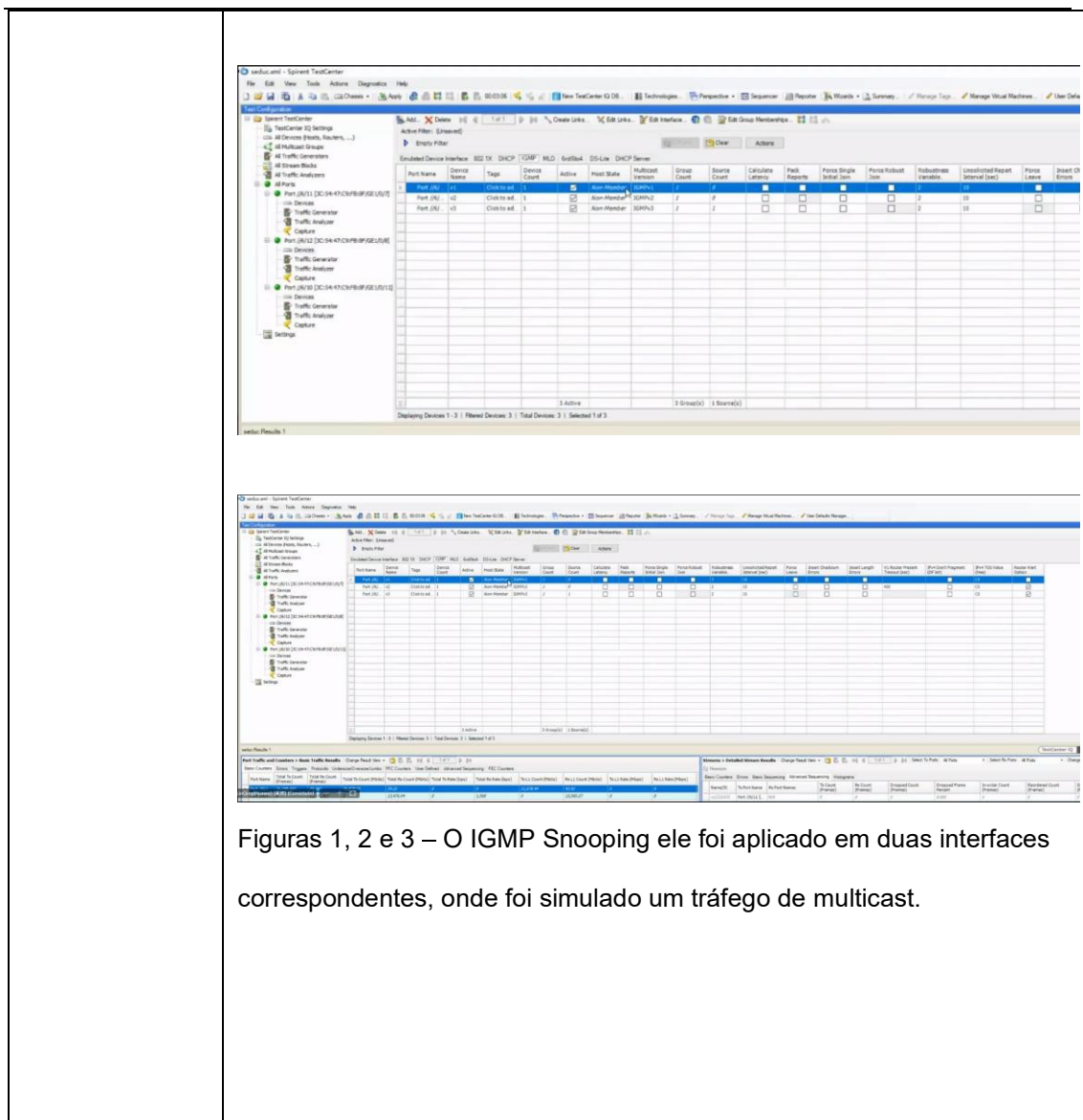
5.9.23. Implementar IGMP v1, IGMP v2 e IGMP v3 snooping;

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

**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
<b>Procedimento de teste</b>	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.
<b>Resultado esperado</b>	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.
<b>Resultado</b>	

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



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



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

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

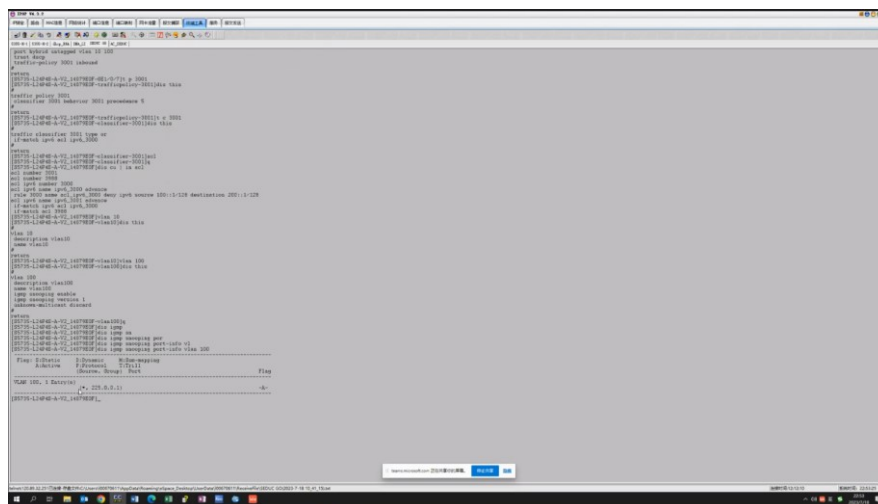
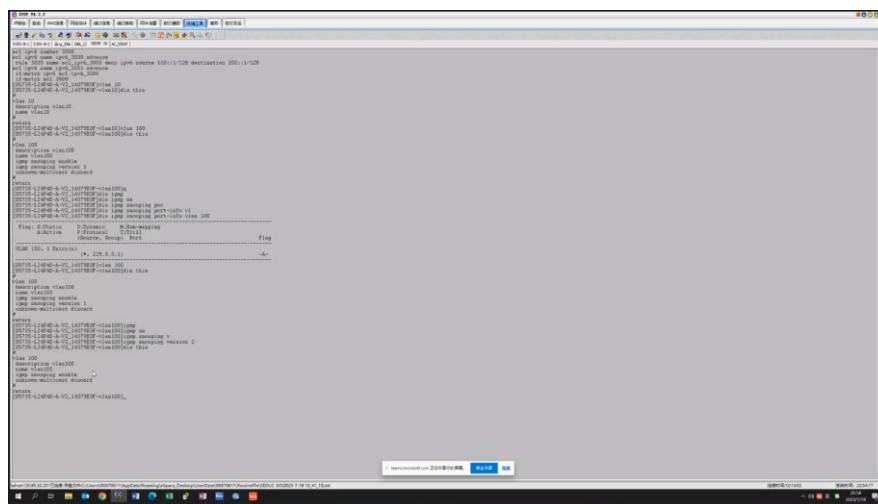


Figura 9 – Novamente no switch, através do comando “display igmp snooping port info”, é mostrado um grupo identificado para a VLAN 100.



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

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 explicitamente a versão. Isso só é mostrado para as versões 1 e 3, as quais não são o padrão.

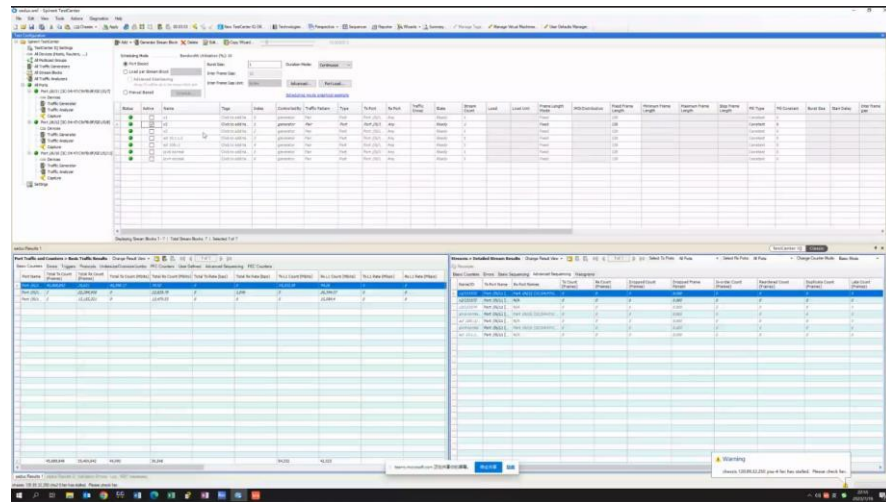


Figura 11 – No gerador, foi iniciado o trafego multicast, agora para IGMP Snooping versão 2.



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

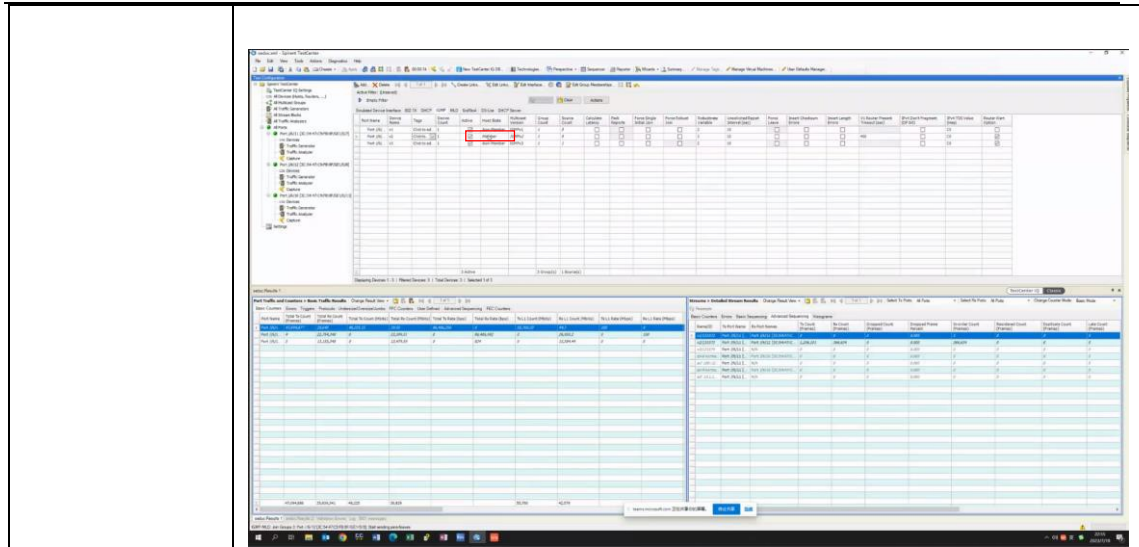


Figura 13 – No gerador, foi evidenciado que a interface é parte do grupo IGMP V2 criado

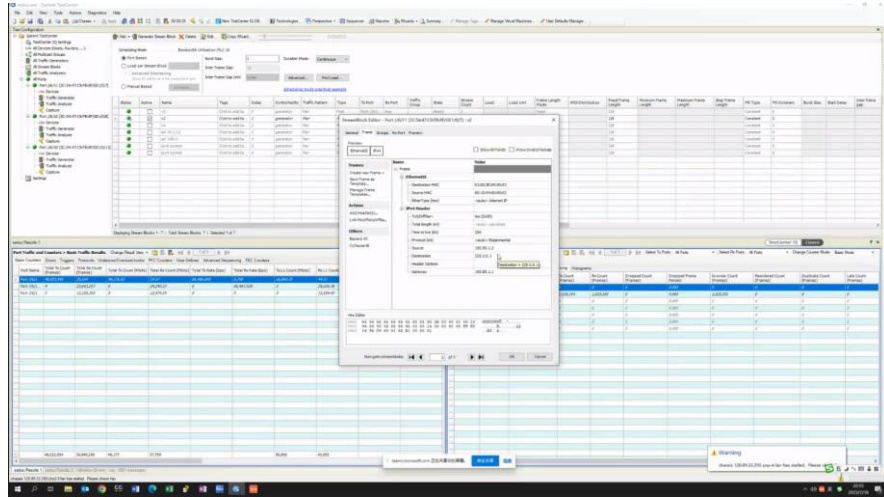
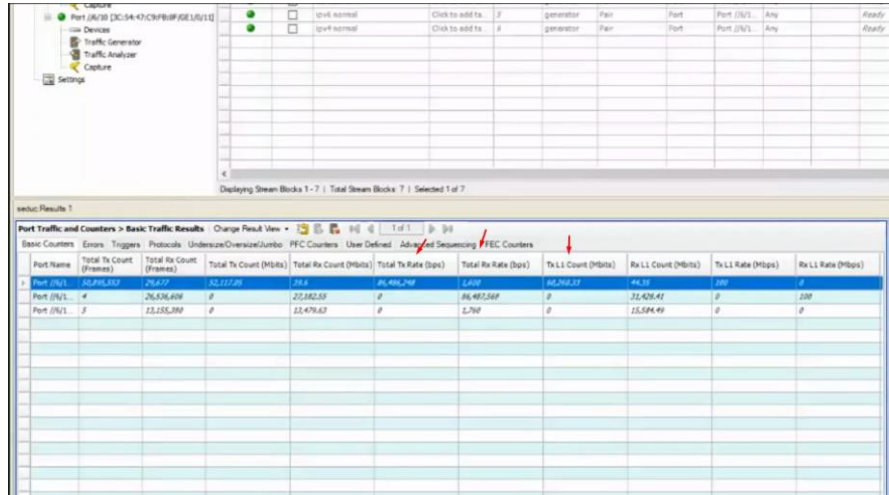


Figura 14 – O destino multicast é o 225.0.0.1

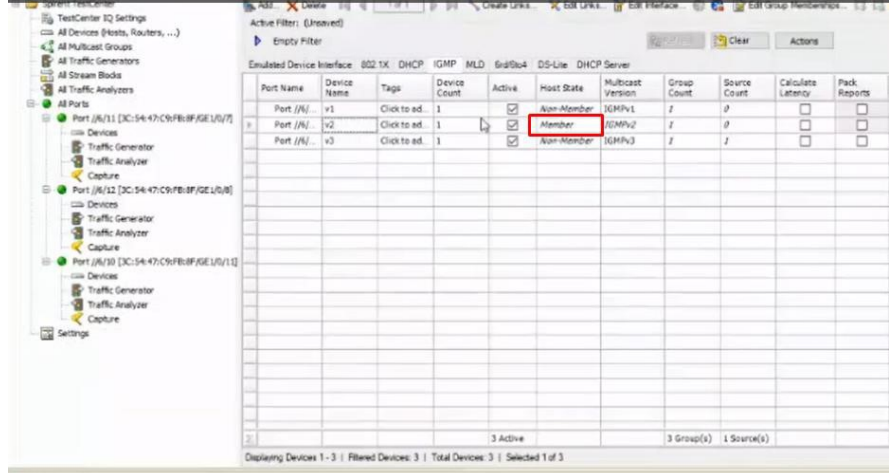
**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**



The screenshot displays a traffic analysis window with a table of results. The table has the following columns: Port Name, Total Tx Count (Frames), Total Rx Count (Frames), Total Tx Count (Mbps), Total Rx Count (Mbps), Total Tx Rate (bps), Total Rx Rate (bps), Tx LL Count (Mbps), Rx LL Count (Mbps), Tx LL Rate (Mbps), and Rx LL Rate (Mbps). The data shows traffic on ports J/1, J/2, and J/3.

Port Name	Total Tx Count (Frames)	Total Rx Count (Frames)	Total Tx Count (Mbps)	Total Rx Count (Mbps)	Total Tx Rate (bps)	Total Rx Rate (bps)	Tx LL Count (Mbps)	Rx LL Count (Mbps)	Tx LL Rate (Mbps)	Rx LL Rate (Mbps)
Port J/1	26,636,609	23,355,389	25,882,53	22,476,63	86,497,568	2,797	0	22,426,41	0	208
Port J/2	26,636,609	23,355,389	25,882,53	22,476,63	86,497,568	2,797	0	22,426,41	0	208
Port J/3	26,636,609	23,355,389	25,882,53	22,476,63	86,497,568	2,797	0	22,426,41	0	208

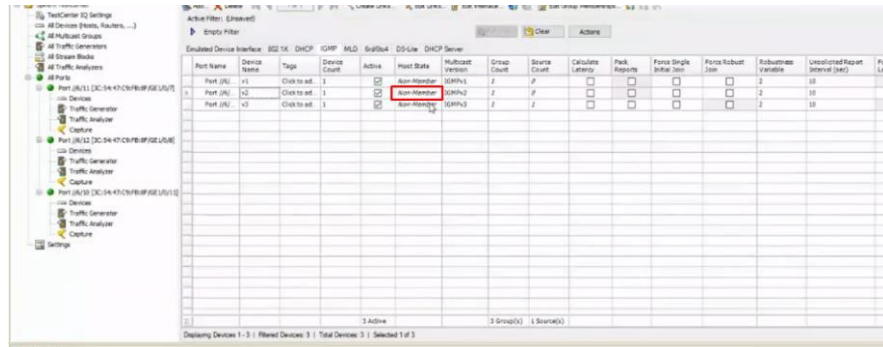
Figura 15 – No gerador, é possível identificar que esse tráfego está sendo encaminhado normalmente.



The screenshot shows a table of emulated device interfaces. The table has columns: Port Name, Device Name, Type, Device Count, Active, Host State, Multicast Version, Group Count, Source Count, Calculate Latency, and Pack Reports. The 'Active' column for all three ports (v1, v2, v3) is checked, and the 'Host State' is 'Member'.

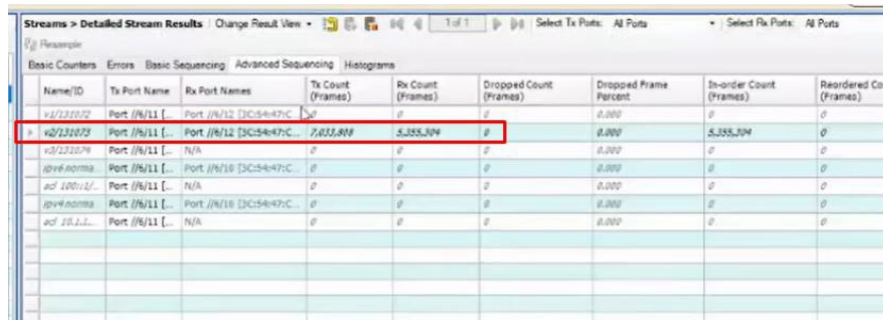
Port Name	Device Name	Type	Device Count	Active	Host State	Multicast Version	Group Count	Source Count	Calculate Latency	Pack Reports
Port J/1	v1	Click to ad.	1	<input checked="" type="checkbox"/>	Non-Member	IGMPv1	7	0	<input type="checkbox"/>	<input type="checkbox"/>
Port J/2	v2	Click to ad.	1	<input checked="" type="checkbox"/>	Member	IGMPv2	7	0	<input type="checkbox"/>	<input type="checkbox"/>
Port J/3	v3	Click to ad.	1	<input checked="" type="checkbox"/>	Non-Member	IGMPv3	7	7	<input type="checkbox"/>	<input type="checkbox"/>

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

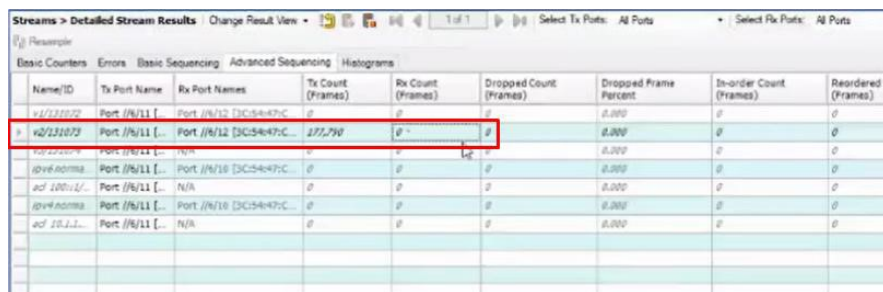


Port Name	Device Name	Tags	Device Count	Active	Host State	Protocol Version	Group Count	Source Count	Calculate Latency	Peak Requests	Force Single Initial Join	Force Robust Join	Robustness Variable	Unadmitted Request Interval (sec)	Port Lease
Port /N1	v1	Click to edit...	1	<input checked="" type="checkbox"/>	MEMBER	IGMPv2	1	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	10	
Port /N2	v2	Click to edit...	1	<input checked="" type="checkbox"/>	MEMBER	IGMPv2	1	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	10	

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”



Name/ID	Tx Port Name	Rx Port Names	Tx Count (Frames)	Rx Count (Frames)	Dropped Count (Frames)	Dropped Frame Percent	In-order Count (Frames)	Reordered Count (Frames)
v1/231072	Port /N11 [..	Port /N12 [3C5447C...	0	0	0	0.000	0	0
v2/231072	Port /N11 [..	Port /N12 [3C5447C...	2,655,809	5,355,304	0	0.000	5,355,304	0



Name/ID	Tx Port Name	Rx Port Names	Tx Count (Frames)	Rx Count (Frames)	Dropped Count (Frames)	Dropped Frame Percent	In-order Count (Frames)	Reordered Count (Frames)
v1/231072	Port /N11 [..	Port /N12 [3C5447C...	0	0	0	0.000	0	0
v2/231072	Port /N11 [..	Port /N12 [3C5447C...	0	0	0	0.000	0	0

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

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

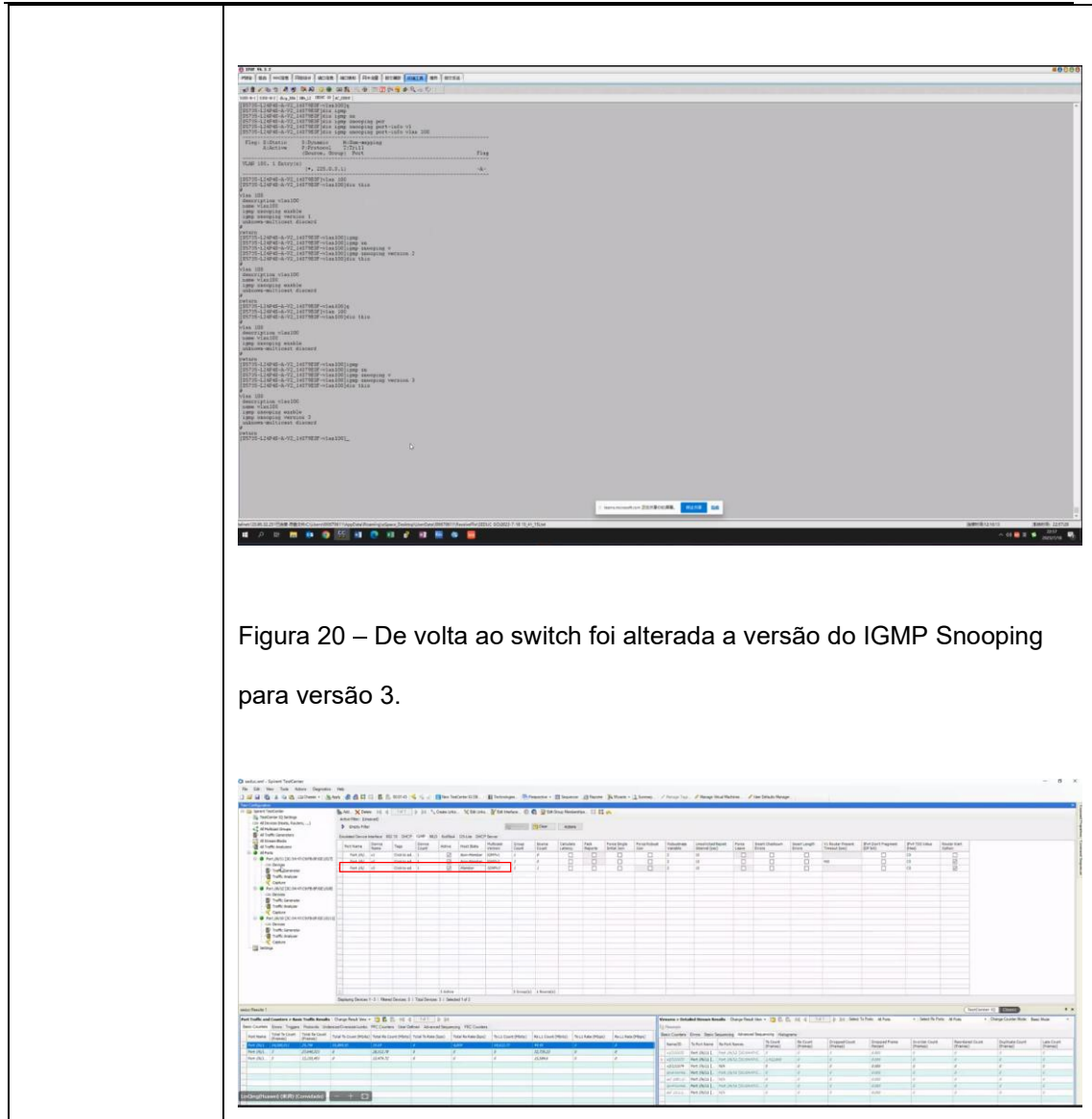
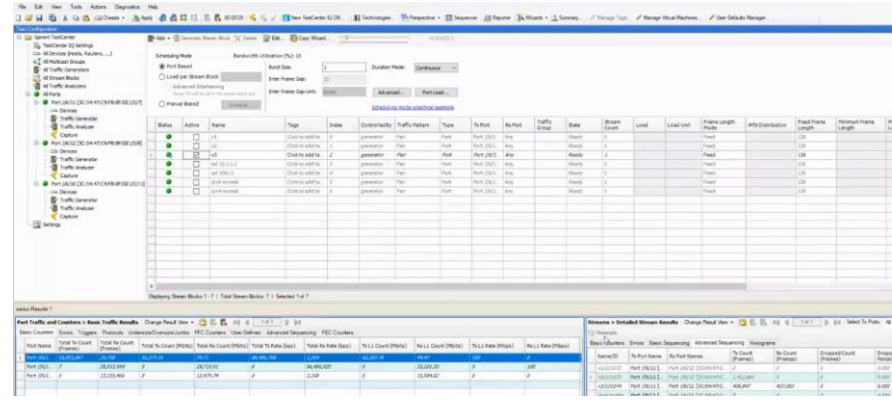


Figura 20 – De volta ao switch foi alterada a versão do IGMP Snooping para versão 3.

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



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 estatísticas do gerador.

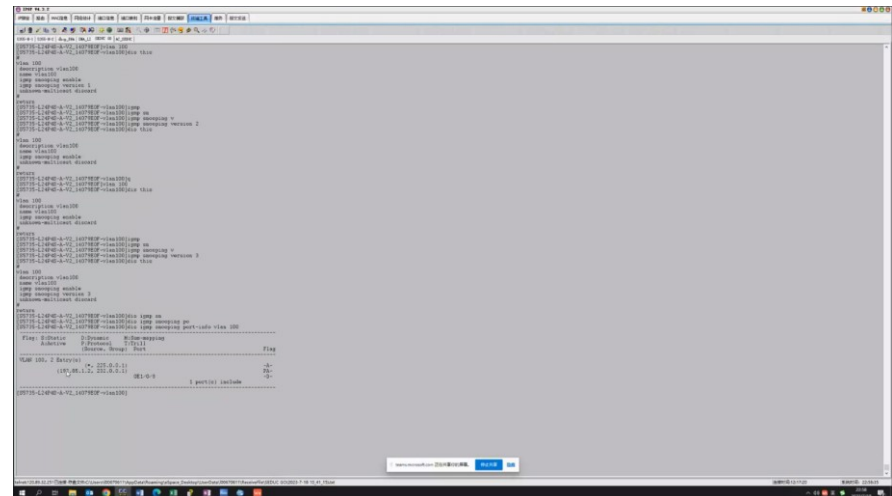


Figura 23 – Executando o comando “igmp snooping port-info vlan 100”, é mostrado que agora os membros na interface que está recebendo o tráfego multicast.

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

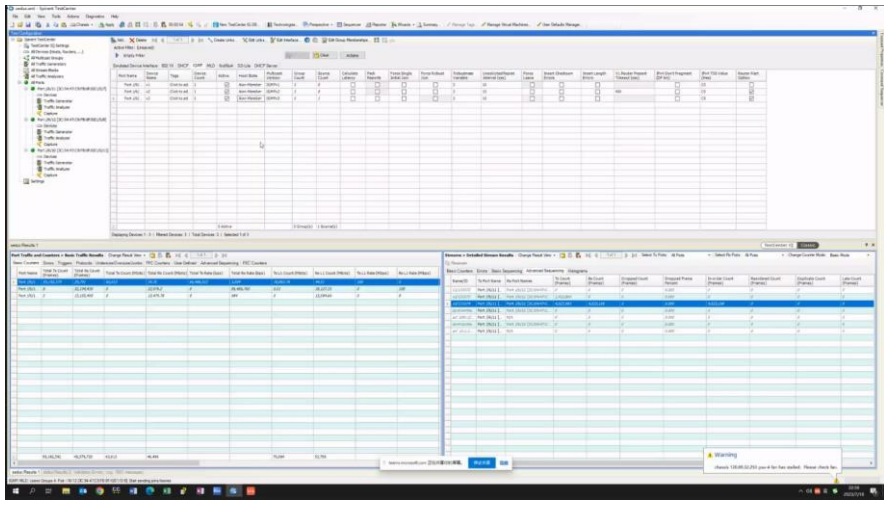


Figura 24 – Novamente, foi simulado uma mensagem de “LEAVE”, para este grupo IGMP V3, e logo as interfaces alteraram o status de “MEMBER” para “NON MEMBER”, e seus contadores, ficaram como zero.

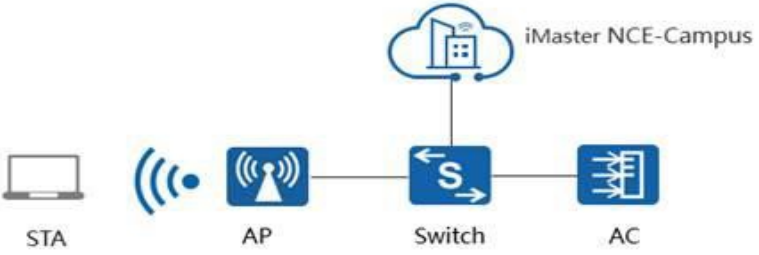
### Autenticação 802.1x

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;

<b>Item de teste</b>	<b>Autenticação 802.1x (5.8.28)</b>
----------------------	-------------------------------------

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

<b>Objetivo do teste</b>	Implementar IEEE 802.1x para autenticação de usuários, permitindo a associação dinâmica de utilizadores a uma determinada VLAN;
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Conectar usuários via 802.1x</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) A autenticação 802.1X é bem sucedida e o usuário pode acessar a rede;</li> </ol>

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

**Resultado**

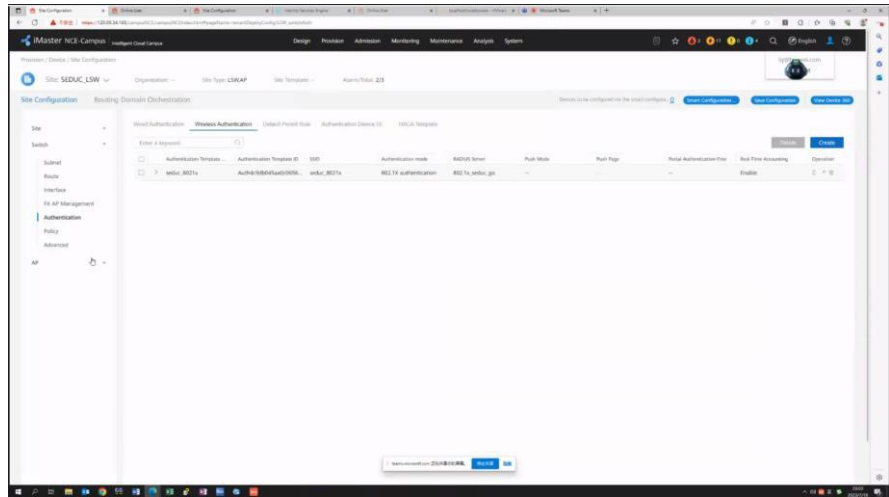


Figura 1 – Foi associado ao switch o template de servidor RADIUS

**Resultado**



Figura 2 – No ponto de acesso, foi criado um SSID chamado seduc, com a política de segurança “Secure networks (802.1x Authentication).”



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

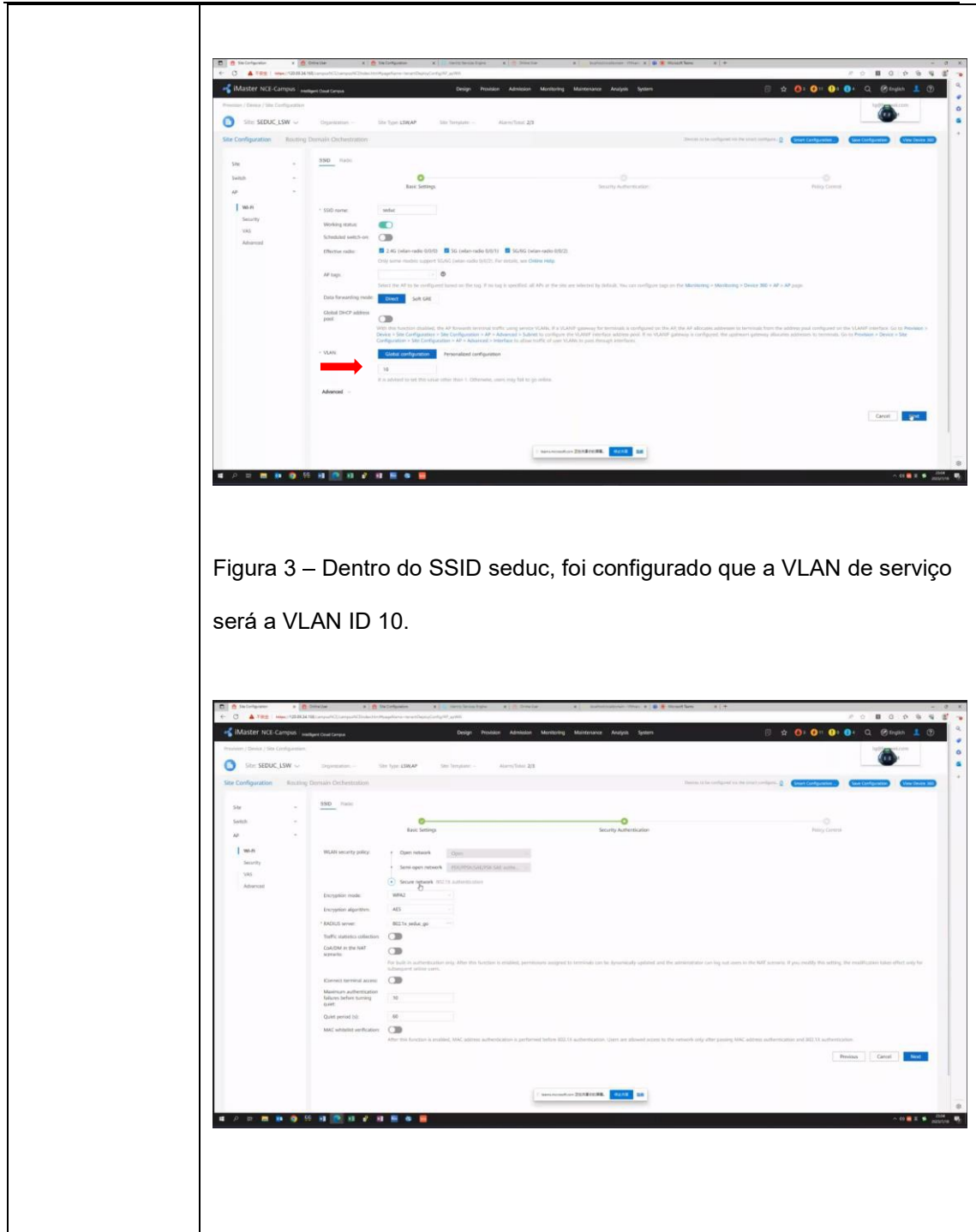
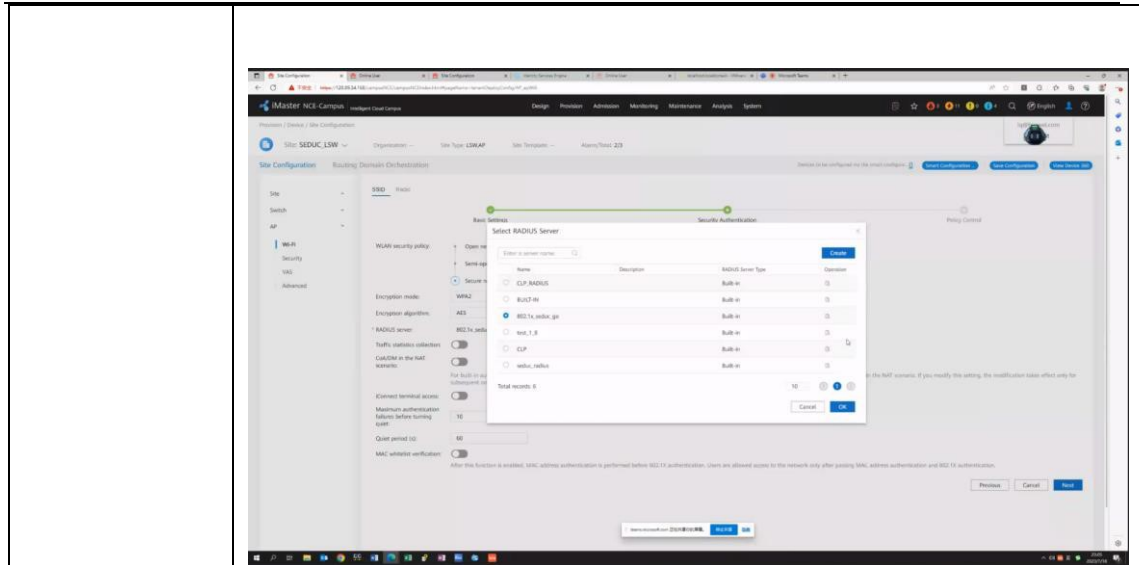


Figura 3 – Dentro do SSID seduc, foi configurado que a VLAN de serviço será a VLAN ID 10.

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



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

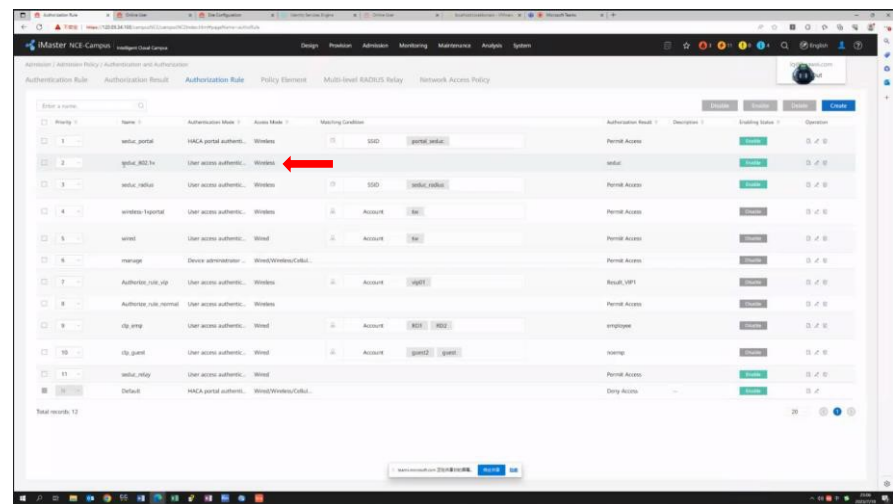


Figura 6 – Nas configurações de AAA, utilizamos a regra “seduc\_802.1x”

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



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

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

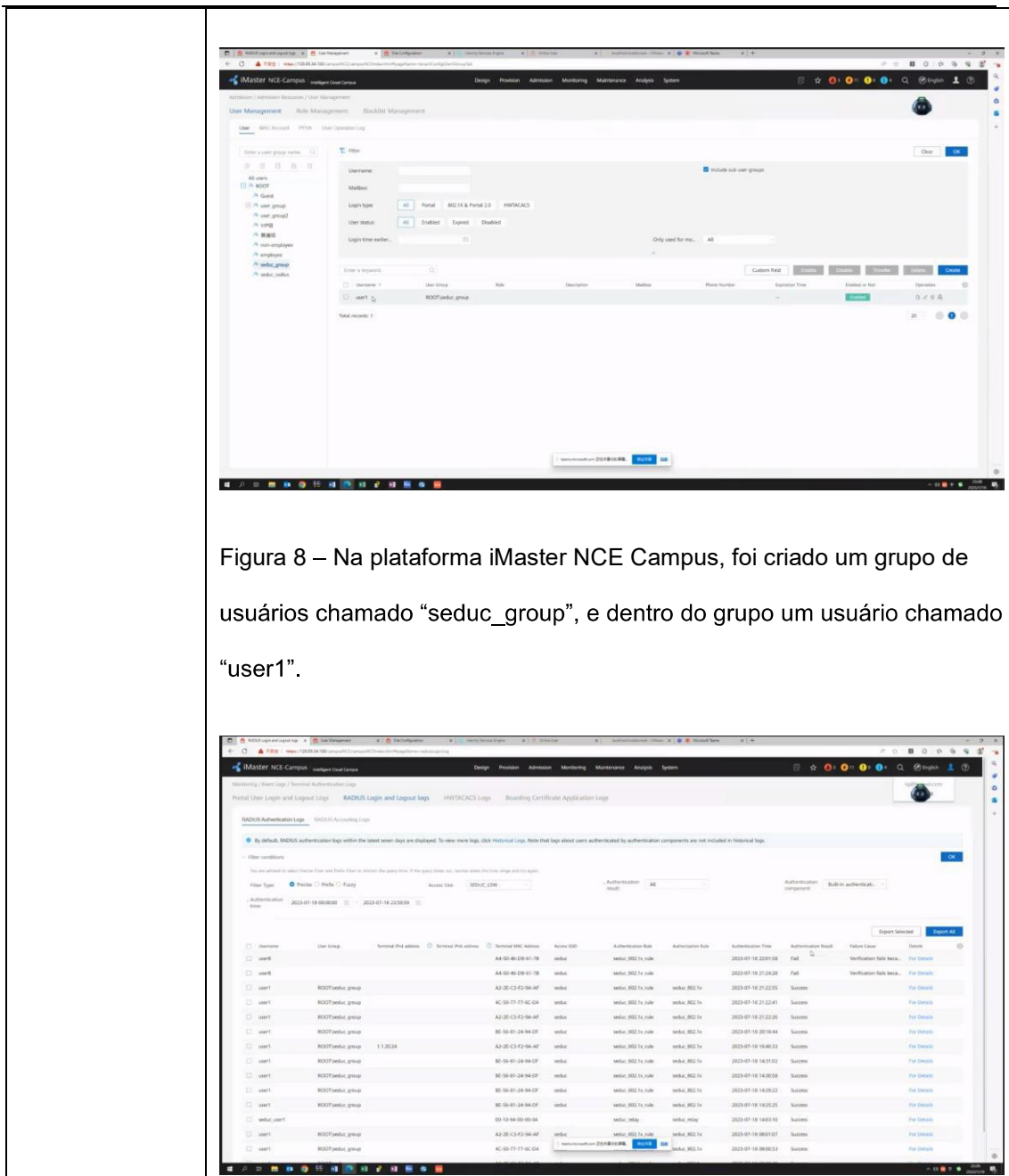
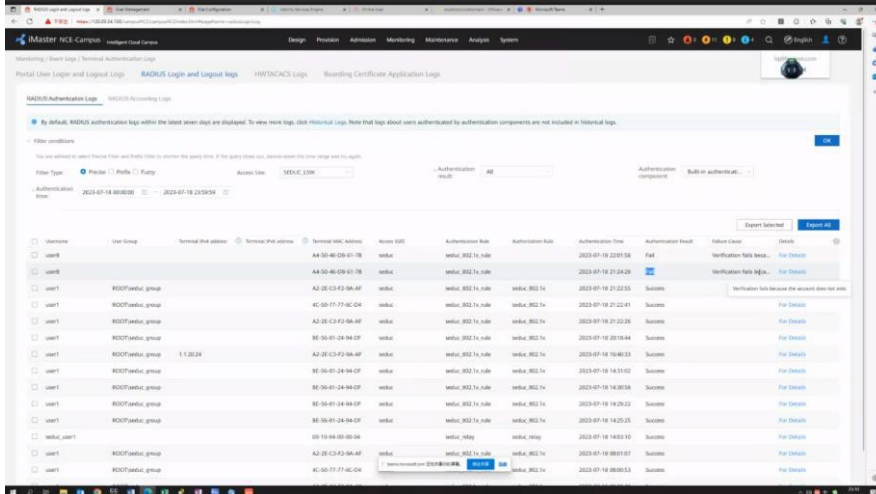
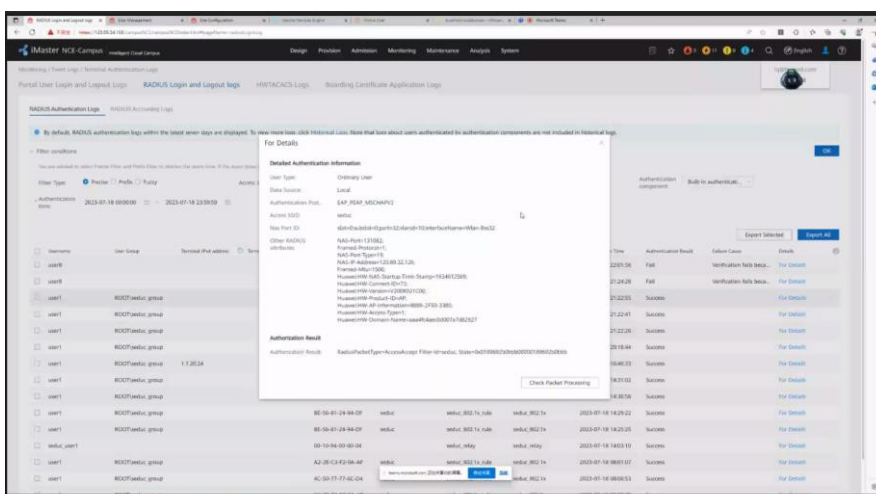


Figura 8 – Na plataforma iMaster NCE Campus, foi criado um grupo de usuários chamado “seduc\_group”, e dentro do grupo um usuário chamado “user1”.

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



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.



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

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.

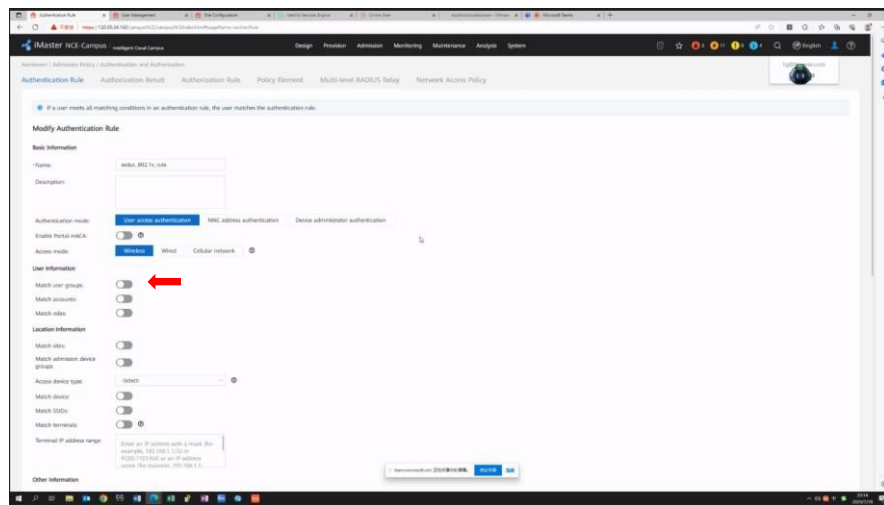
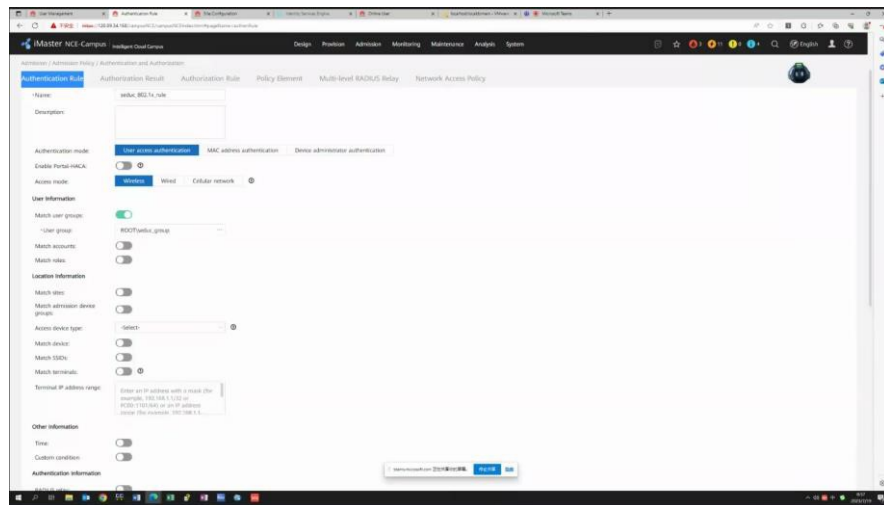
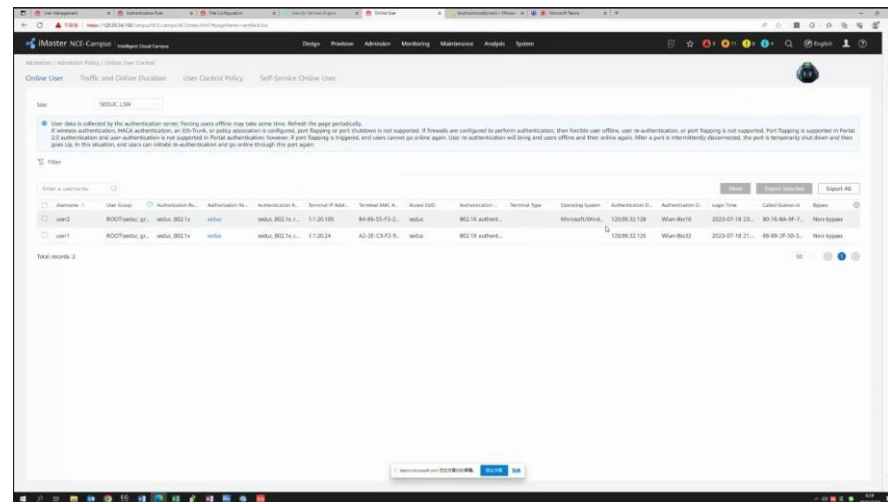
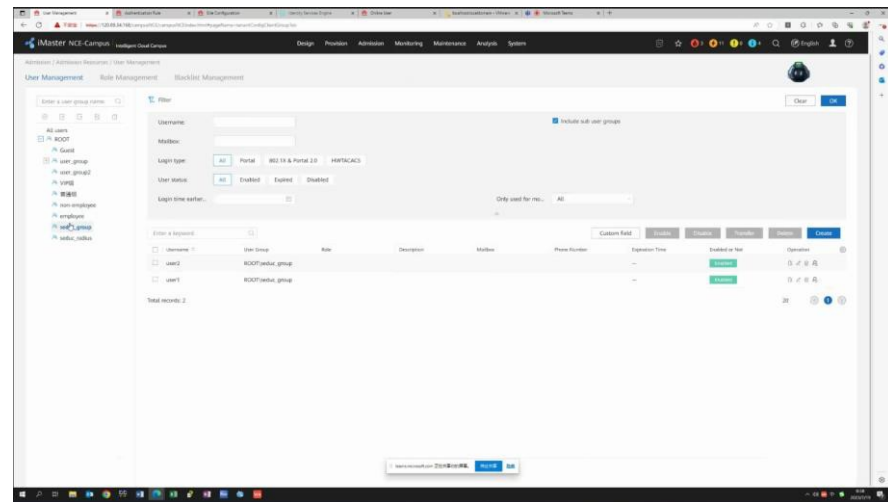


Figura 11 – Retornando a regra, foi evidenciado que não haviam condições especificando o grupo de usuários.



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

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.

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

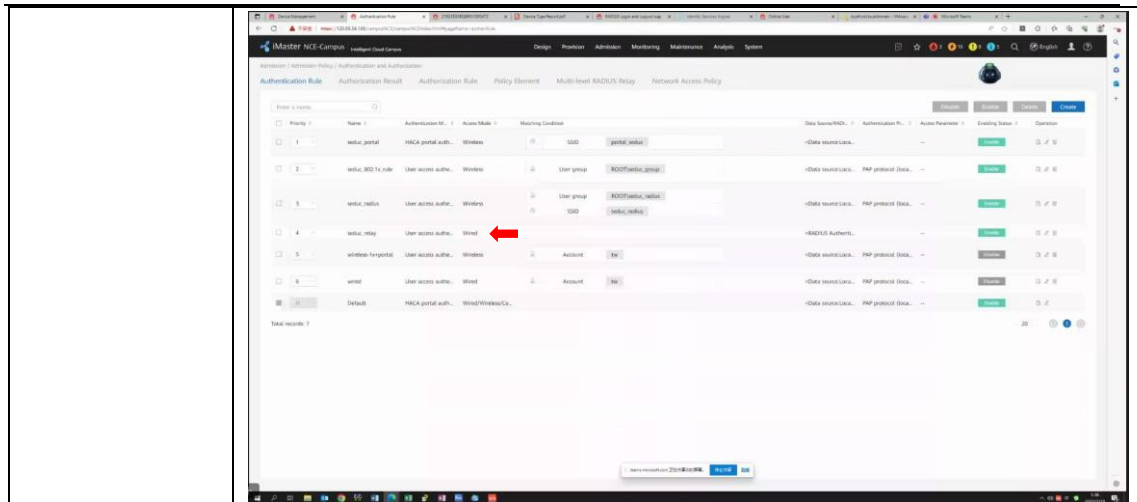


Figura 15 – Novamente, nas configurações de AAA, foi inserida uma nova regra, agora para autenticação 802.1x, em rede cabeada.

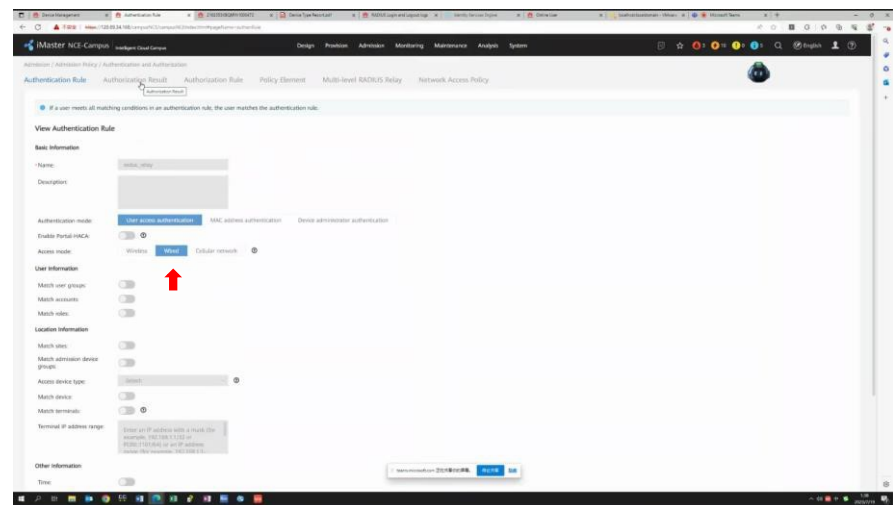
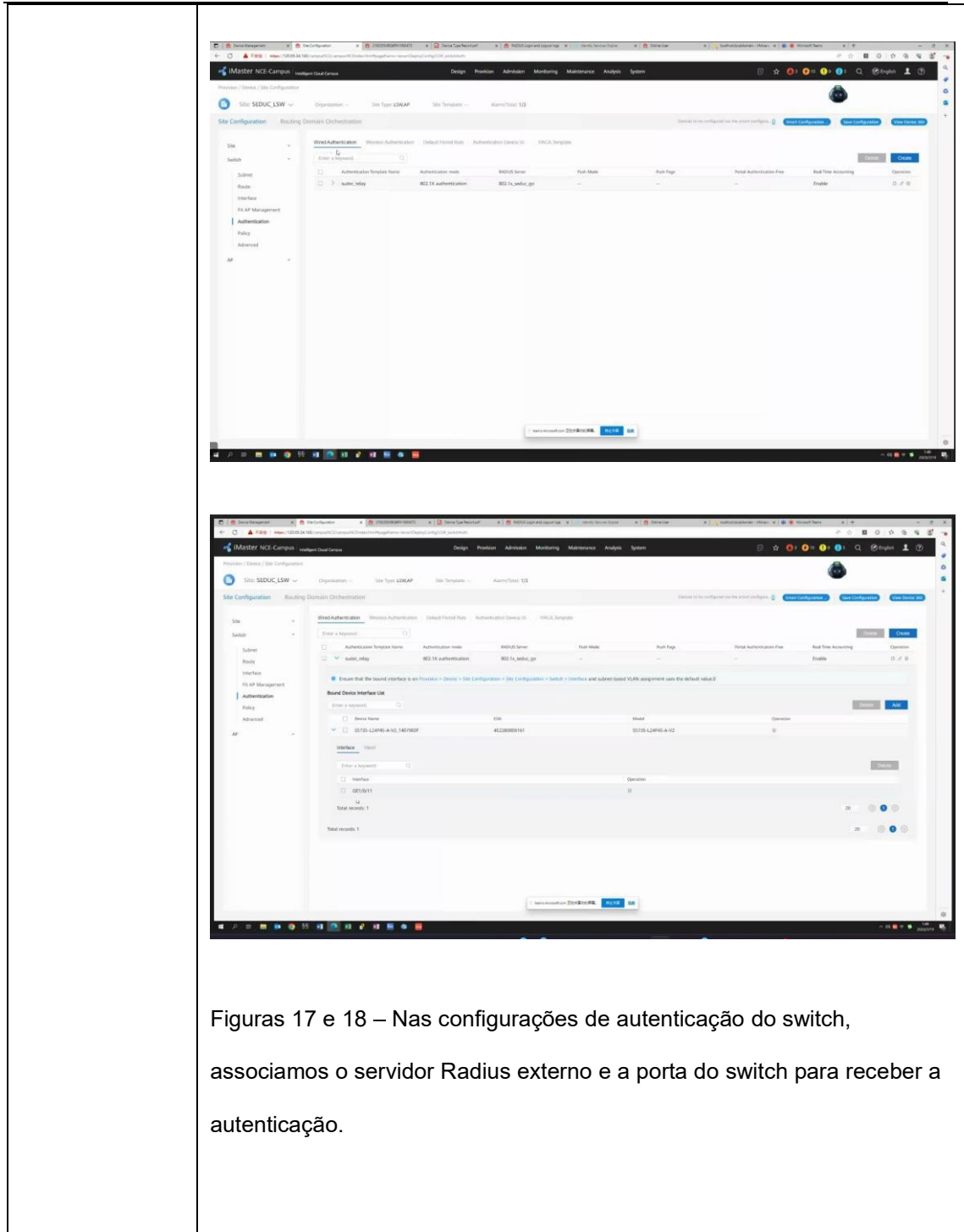


Figura 16 – Na edição da regra, podemos evidenciar o modo de acesso, como “Wired”



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



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

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

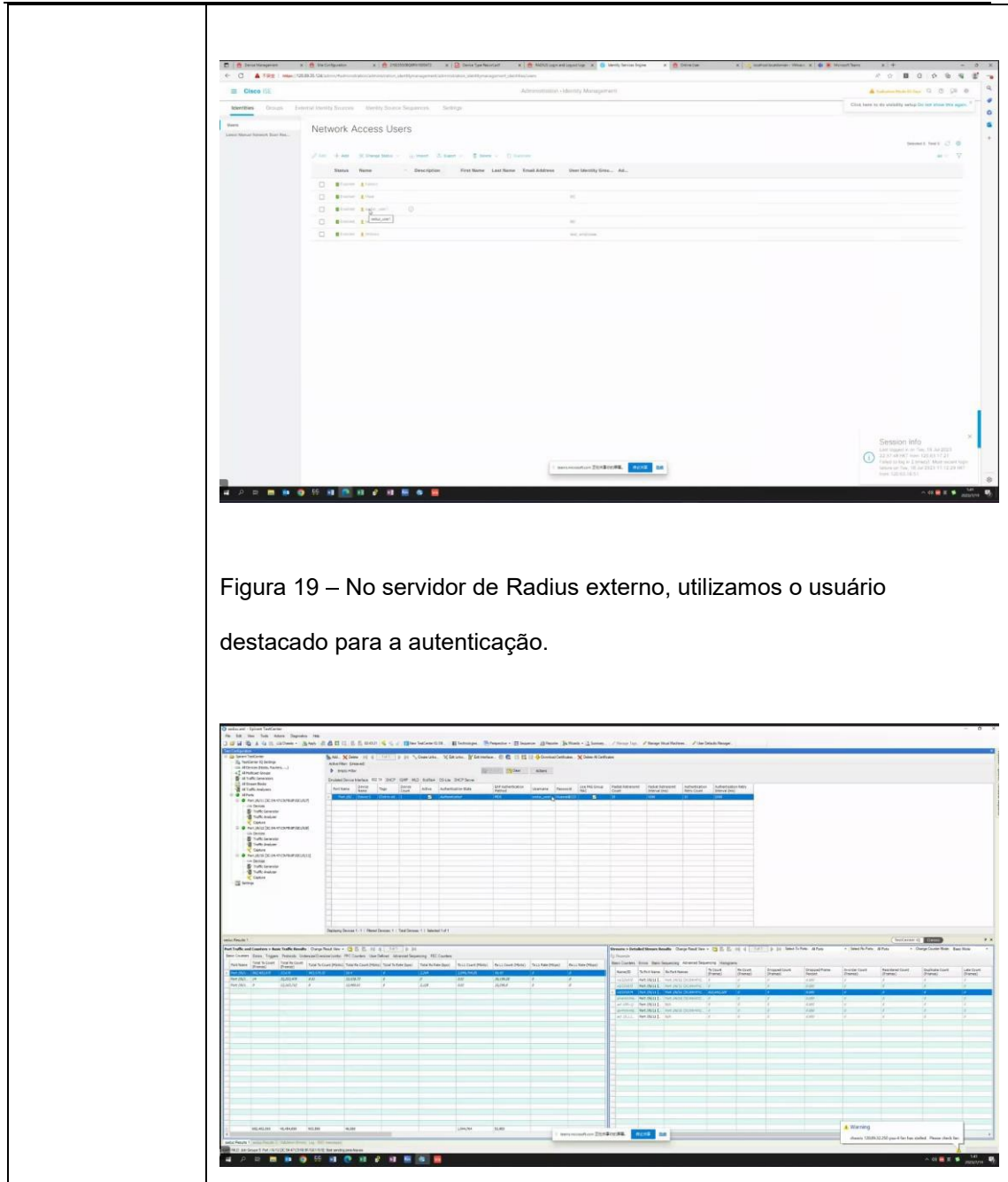
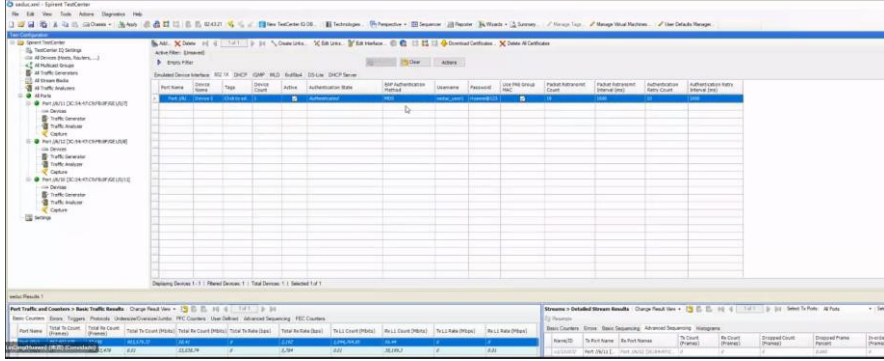


Figura 19 – No servidor de Radius externo, utilizamos o usuário destacado para a autenticação.

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



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.

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

--	--

### 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



#### iMaster NCE-Campus Product Documentation

Product Version: V300R021C00 | Library Version: 03 | Date: 2023-02-13

## iMaster NCE-Campus

iMaster NCE-Campus is a centralized management and web-based control system designed for the CloudCampus solution. It supports a wide range of functions, including network service management, network security management, network access management, network monitoring, network quality analysis, network application analysis, alarm management, report management. As well as these, it supports big data analytics and open application programming interfaces (APIs) to facilitate integration with other platforms. Enterprise users can use iMaster NCE-Campus to implement service provisioning, configuration, and routine maintenance for multiple tenant networks separately, enabling management of large-scale devices on the cloud.

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\\_000001089252652](https://support.huawei.com/hedex/hdx.do?docid=EDOC1100211132&id=EN-US_TOPIC_000001089252652)

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

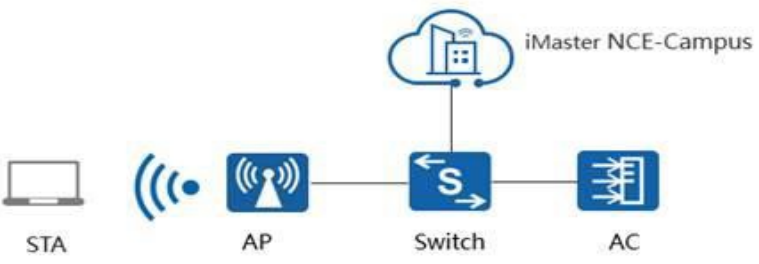
<b>Virtualization Solution</b>	VMWare vSphere 6.5/6.7
<b>Operating System</b>	SUSE Linux Enterprise 12 SP4 (English) SUSE Linux Enterprise 12 SP5 (English)

Comprovações com configurações:

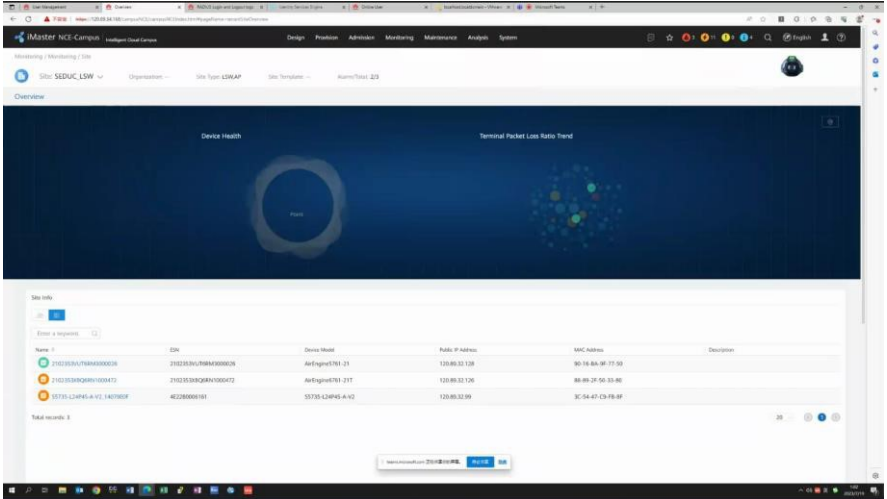
### Monitoramento e geração de relatórios

5.10.4 A solução deve ser capaz de centralizar o monitoramento e relatórios de todo o parque de dispositivos, através de console única;

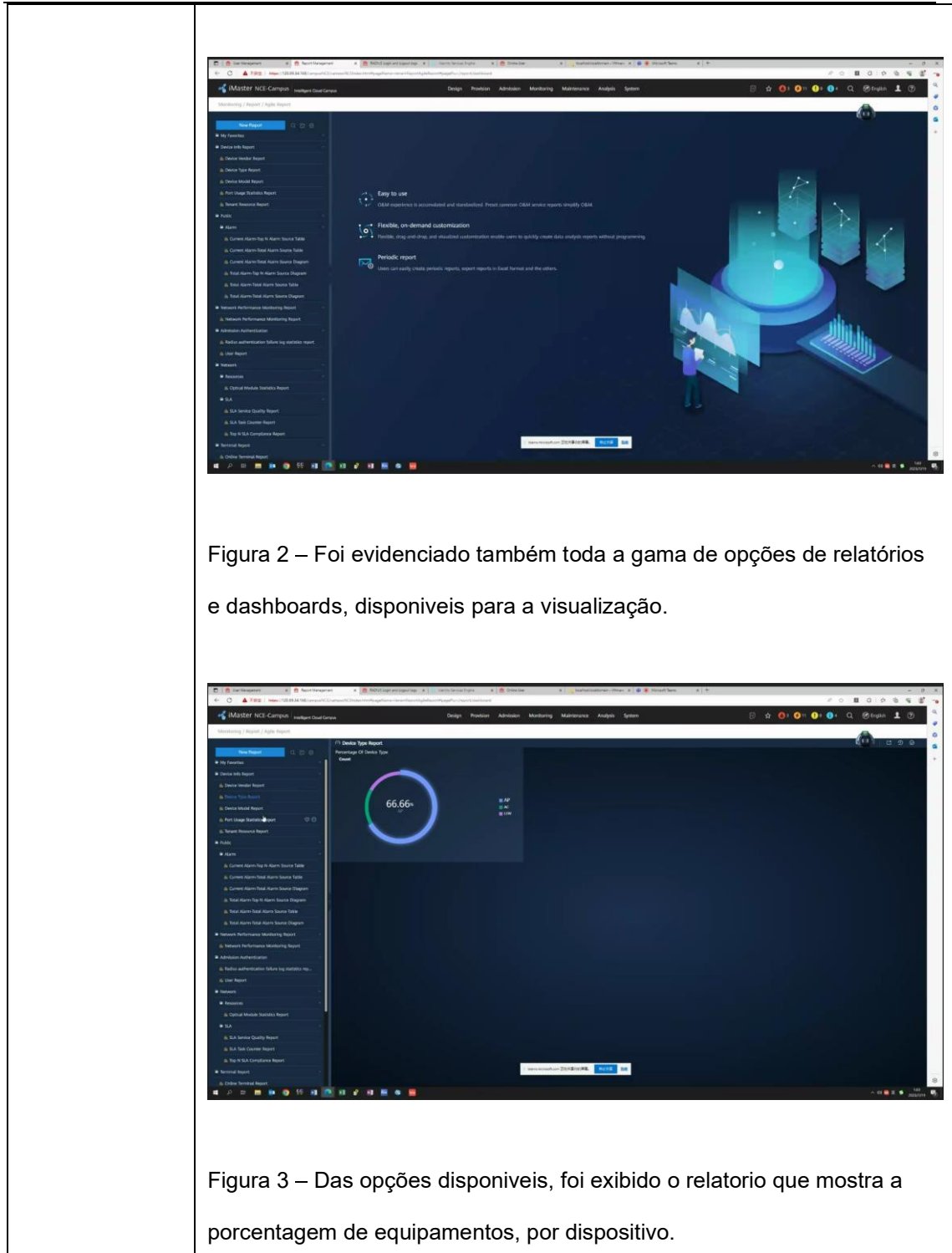
5.10.17 Monitorar o desempenho da rede wireless;

<b>Item de teste</b>	<b>Monitoramento e geração de relatórios e desempenho da rede</b>
<b>Objetivo do teste</b>	<b>A solução deve ser capaz de centralizar o monitoramento e relatórios de todo o parque de dispositivos, através de console única.</b>
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>The diagram illustrates a network topology for testing. It includes a STA (Station) connected to an AP (Access Point), which is connected to a Switch. The Switch is connected to an AC (Access Controller), which is connected to iMaster NCE-Campus (Network Cloud Element).</p>

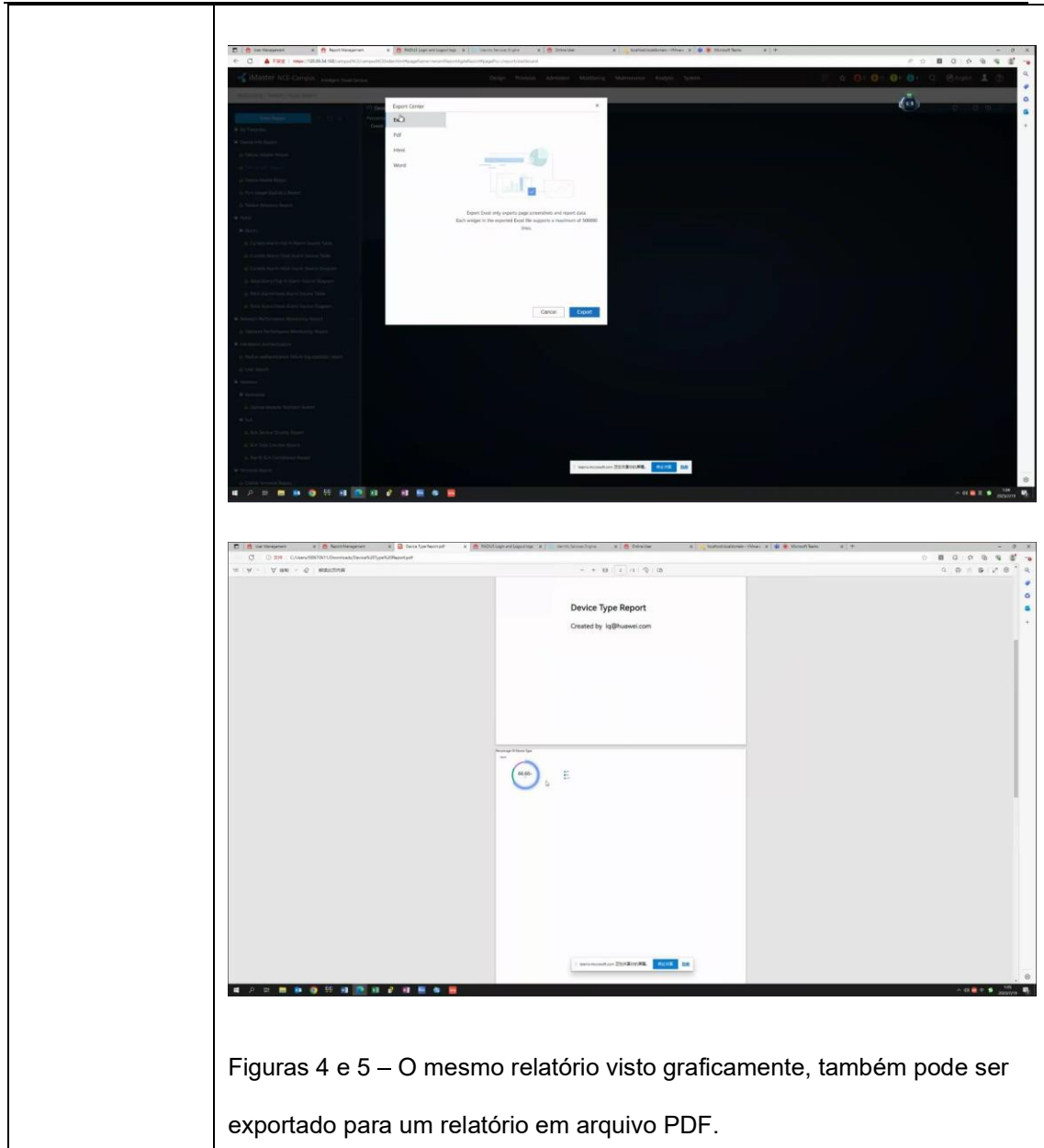
**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

	<p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Exibir as dashboards disponíveis na ferramenta</li> </ol>
<p><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) Monitorar todo o parque de dispositivos, através de console única;</li> <li>2) Gerar relatórios de todo o parque de dispositivos, através de console única;</li> </ol>
<p><b>Resultado</b></p>	 <p>Figura 1 – Na ferramenta iMaster NCE Campus, foram exibidas de forma geral as informações dos dispositivos.</p>

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



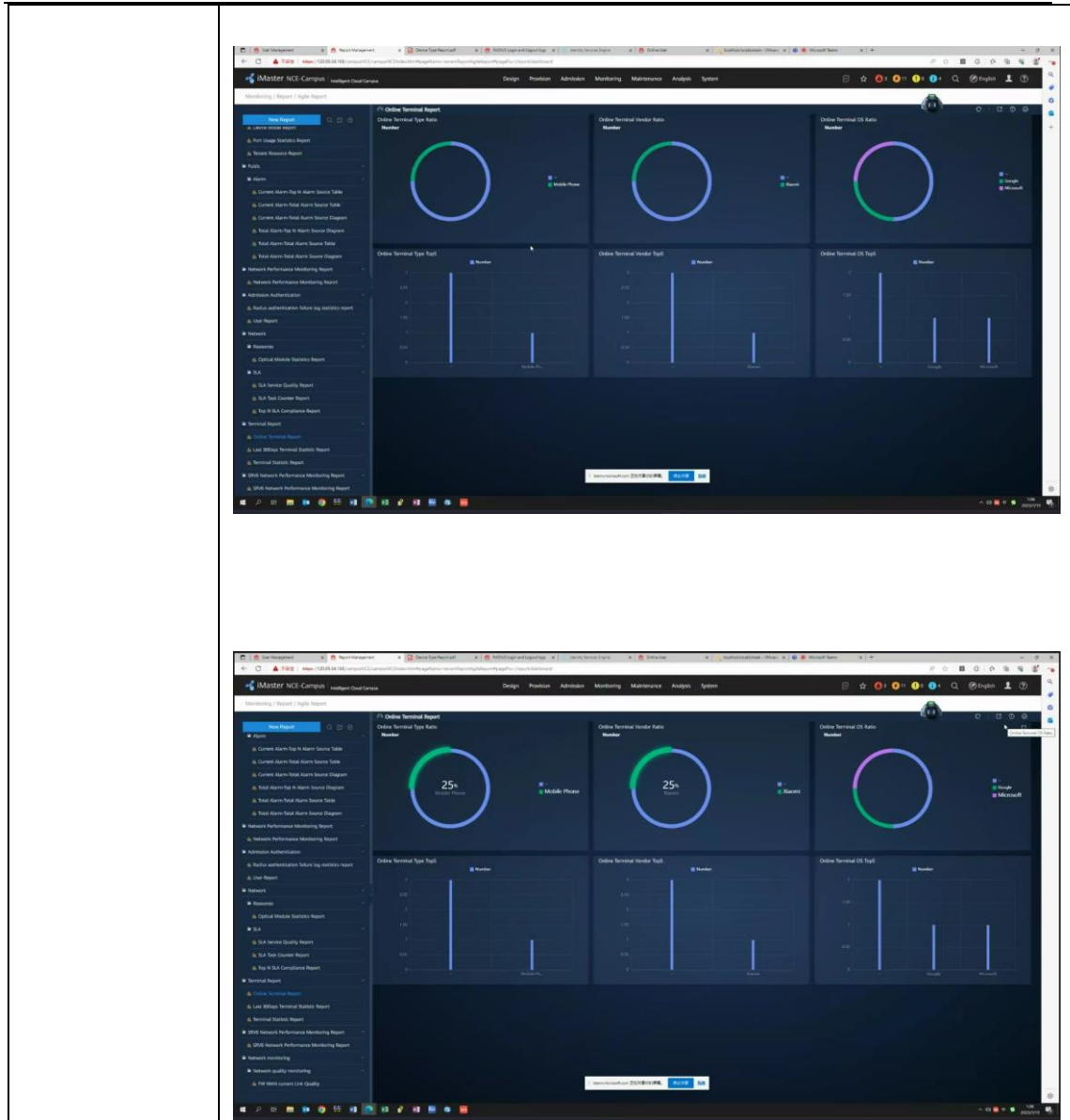
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES



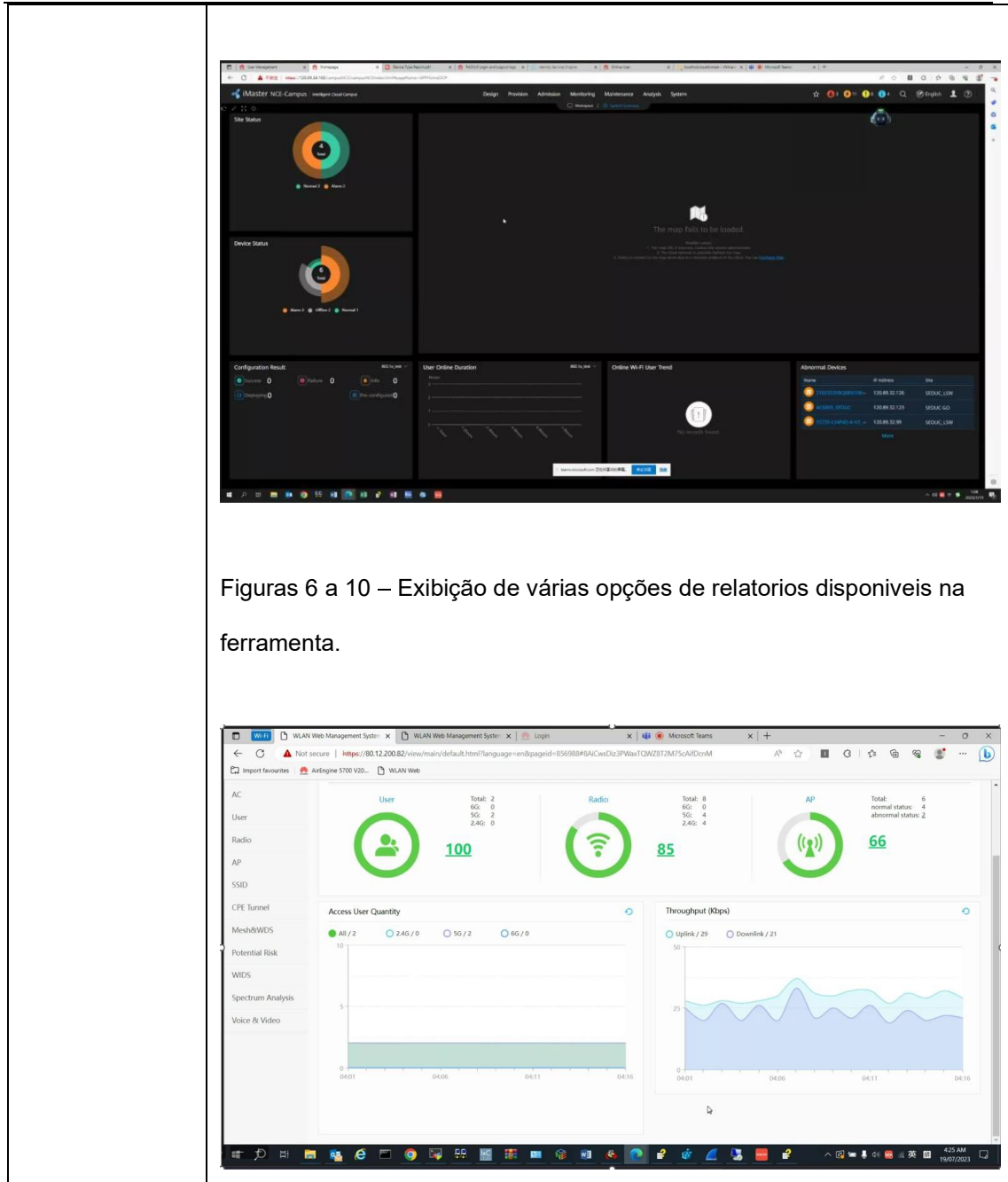




**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

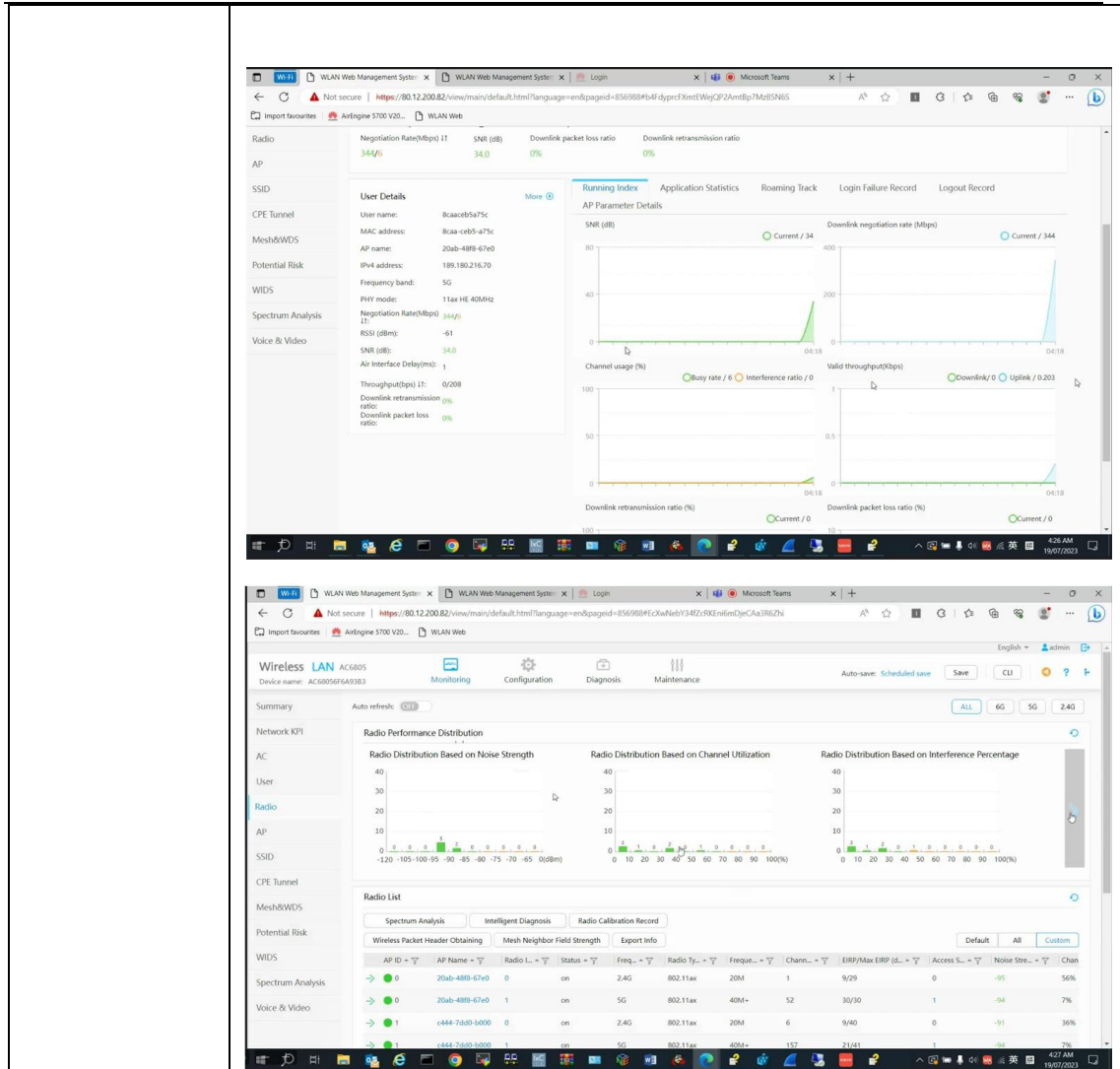


**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**



Figuras 6 a 10 – Exibição de várias opções de relatórios disponíveis na ferramenta.

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



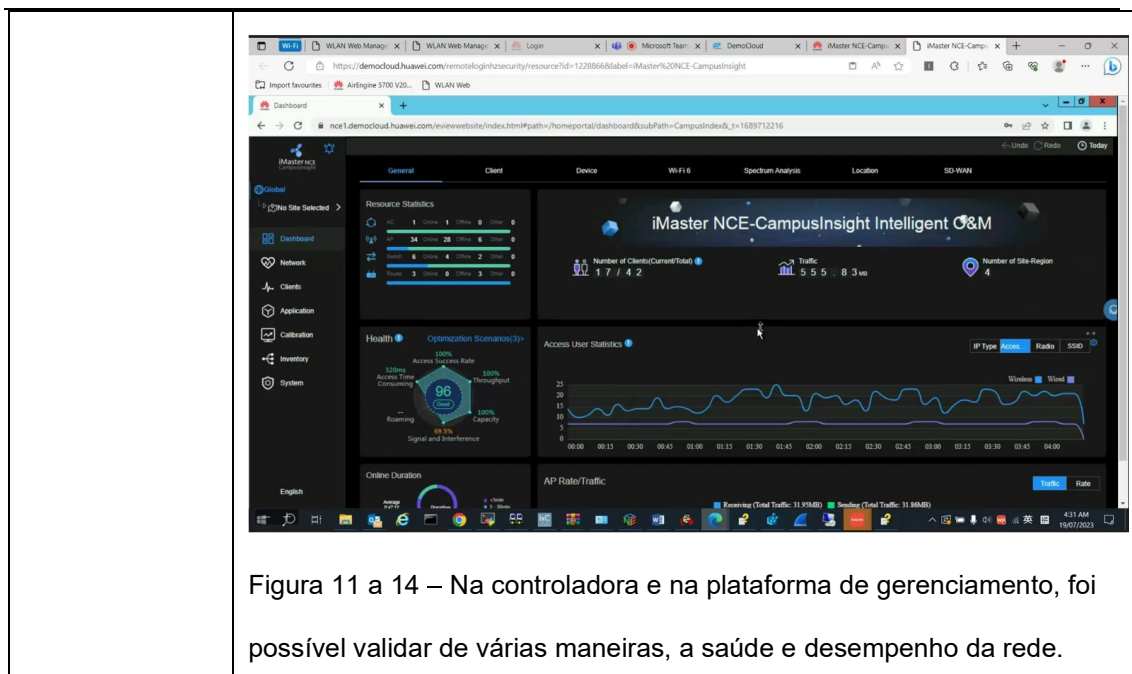
The top screenshot displays the 'User Details' for a radio with the following information:

- User name: 8caace5a75c
- MAC address: 8caa-ceb5-a75c
- AP name: 20ab-488b-67e0
- IPv4 address: 189.180.216.70
- Frequency band: 5G
- PHY mode: 11ax HE 40MHz
- Negotiation Rate(Mbps): 344
- SNR (dBm): 34.0
- RSSI (dBm): -41
- Air Interface Delay(ms): 1
- Throughput(Mbps): 0/208
- Downlink retransmission ratio: 0%
- Downlink packet loss ratio: 0%

The bottom screenshot shows the 'Radio Performance Distribution' dashboard for device AC6805 (AC6805FA93B3). It includes three charts: Radio Distribution Based on Noise Strength, Radio Distribution Based on Channel Utilization, and Radio Distribution Based on Interference Percentage. Below the charts is a 'Radio List' table:

AP ID	AP Name	Radio L	Status	Freq.	Radio Ty.	Frequ.	Chan.	ERP/Max ERP	Access S.	Noise Stre.	Chan
0	20ab-488b-67e0	0	on	2.4G	802.11ax	20M	1	9/29	0	-95	56%
0	20ab-488b-67e0	1	on	5G	802.11ax	40M+	52	30/30	1	-94	7%
1	c444-76d9-6000	0	on	2.4G	802.11ax	20M	6	9/40	0	-91	36%
1	c444-76d9-6000	1	on	5G	802.11ax	40M+	157	21/41	1	-94	7%

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



### Gerenciamento de permissões e domínio

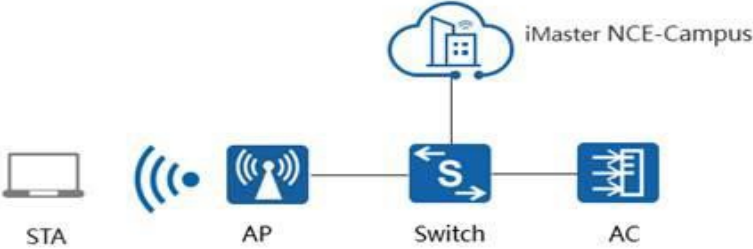
5.10.15 Permitir a customização do a acesso administrativo através de atribuição de grupo de função do usuário administrador.

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;

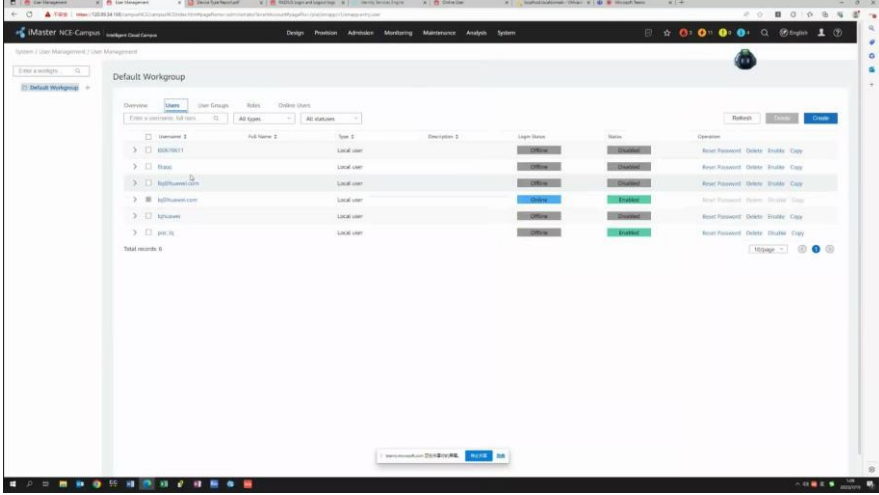
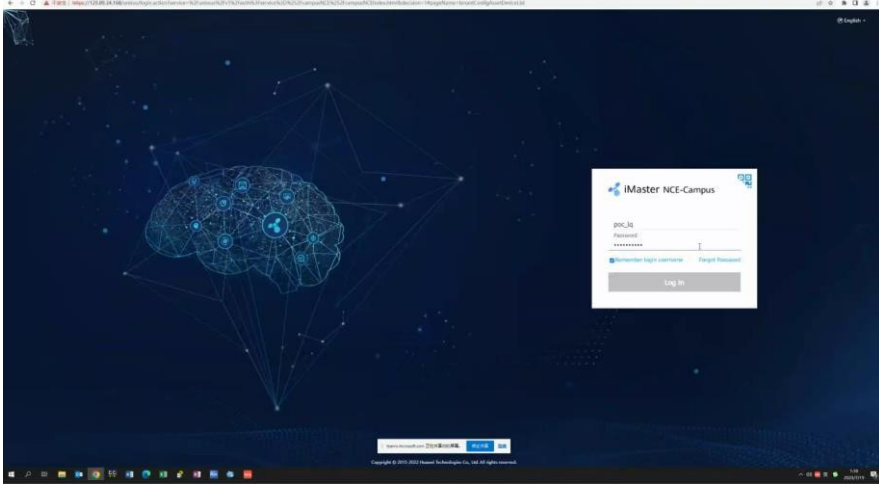
5.10.28 Gerenciar de forma centralizada a autenticação de usuários;

<b>Item de teste</b>	<b>Gerenciamento de permissões e domínio</b>
<b>Objetivo do teste</b>	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**

<p align="center"><b>Configuração de teste</b></p>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p align="center"><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Adicionar usuários administrativos a ferramenta, e atribuir suas permissões.</li> </ol>
<p align="center"><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) Usuários adicionados, com opções de customização de permissões e objetos/sites utilizados.</li> </ol>

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

<p>Resultado</p>	 <p>The screenshot shows the 'Default Workgroup' user management interface. It features a table with columns for 'Overview', 'User Group', 'User Name', 'Type', 'Observation', 'Login Status', and 'Name'. The table lists several users, including 'poc_lq', with their respective details and operation buttons like 'About', 'Password', 'Delete', 'Enable', and 'Copy'.</p>
	<p>Figura 1 – Na base de dados da ferramenta iMaster NCE Campus, foi evidenciado os usuários criados.</p>
	 <p>The screenshot shows the login page for iMaster NCE-Campus. It features a dark blue background with a network diagram and a login form on the right. The login form includes fields for 'poc_lq' (username) and a password, along with a 'Log In' button.</p>
	<p>Figura 2 – Utilizamos o usuário “poc_lq”, para efetuar o login administrativo ao sistema.</p>

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




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



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

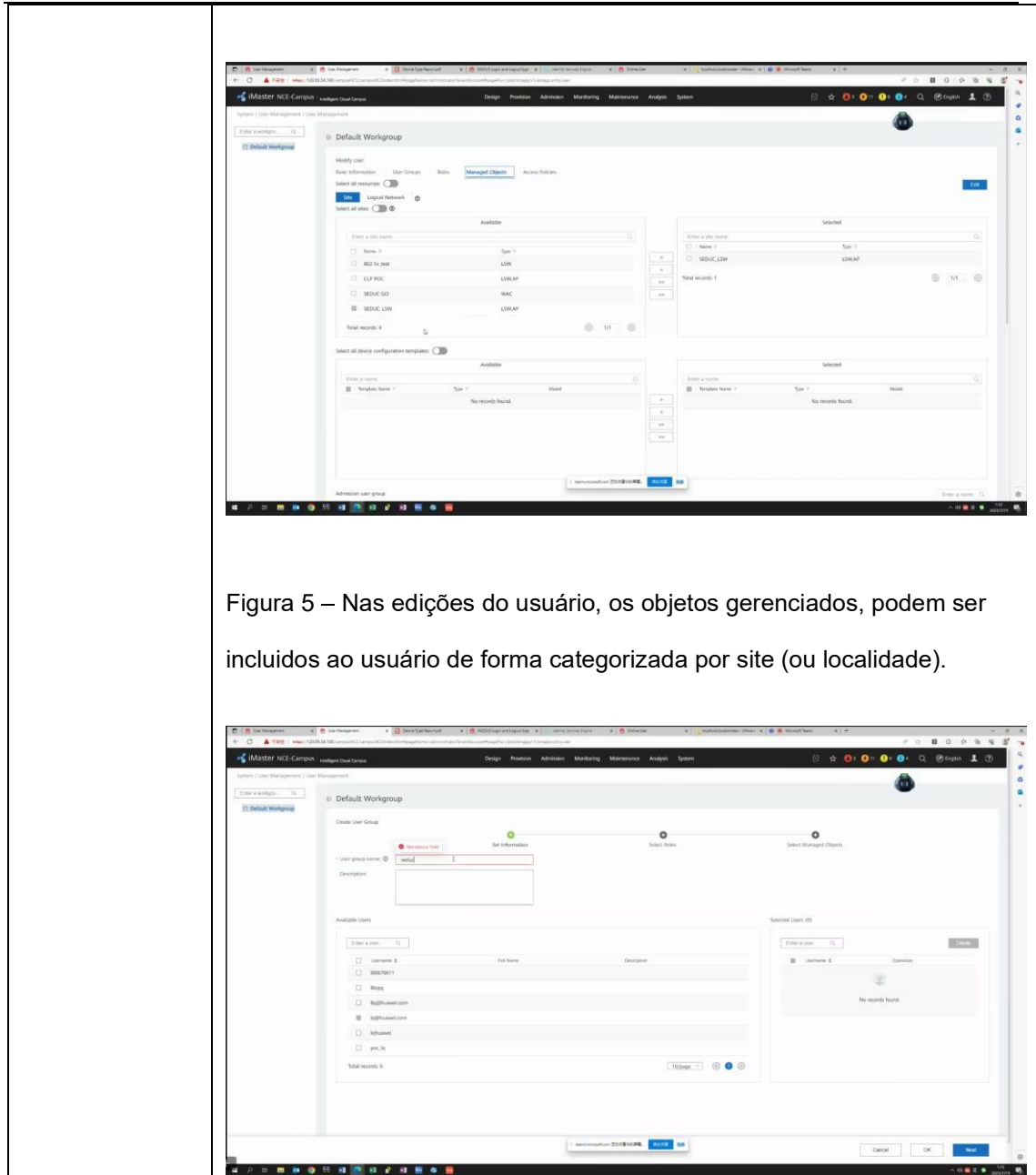
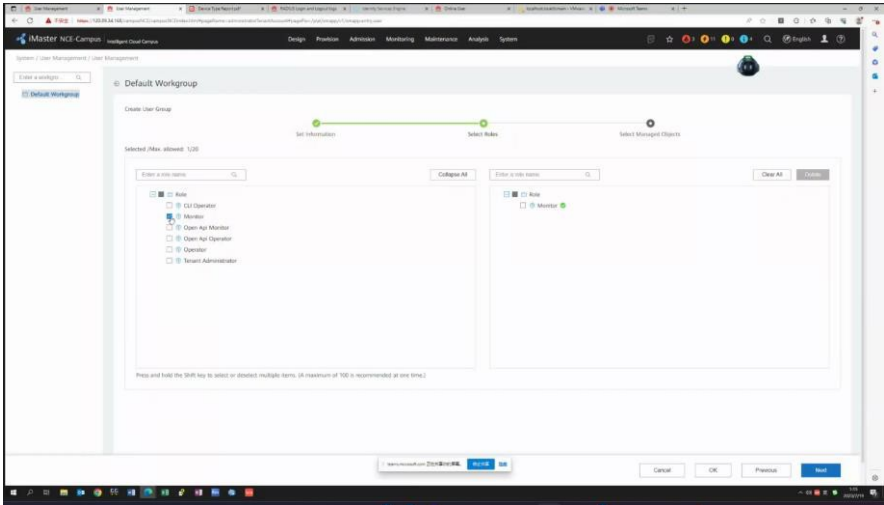
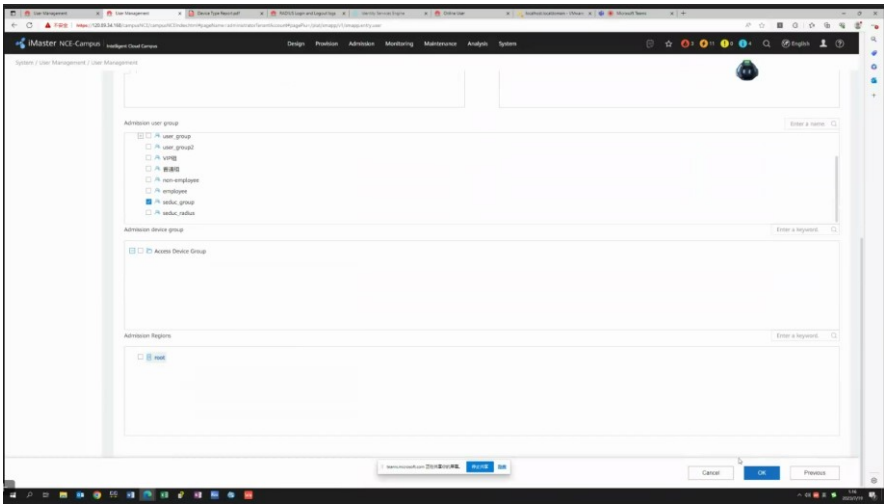


Figura 5 – Nas edições do usuário, os objetos gerenciados, podem ser incluídos ao usuário de forma categorizada por site (ou localidade).

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

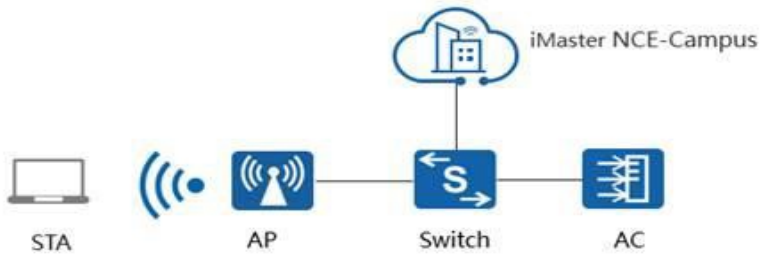
Figuras 6 a 8 – Os usuários administrativos, também podem ser organizados através de grupos de trabalho (workgroups), onde as permissões podem ser editadas a nível do grupo como um todo.

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

	Essas permissões, podem ser de nível 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;

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

**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
<b>Procedimento de teste</b>	1) Provisionar novos equipamentos e restaurar as configurações de fábrica dos dispositivos já gerenciados
<b>Resultado esperado</b>	1) Novos dispositivos em estado padrão de fábrica são remotamente provisionados para um estado totalmente provisionado
<b>Resultado</b>	 <p>The screenshots show the 'Device Management' interface in iMaster NCE-LAMPDR. The top screenshot displays a list of devices with columns for Name, EDN, Status, Rule, Site, and Device Model. A red arrow points to the first record. The bottom screenshot shows the same interface after filtering for 'SEDUC_LSW', resulting in two records.</p>

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

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.

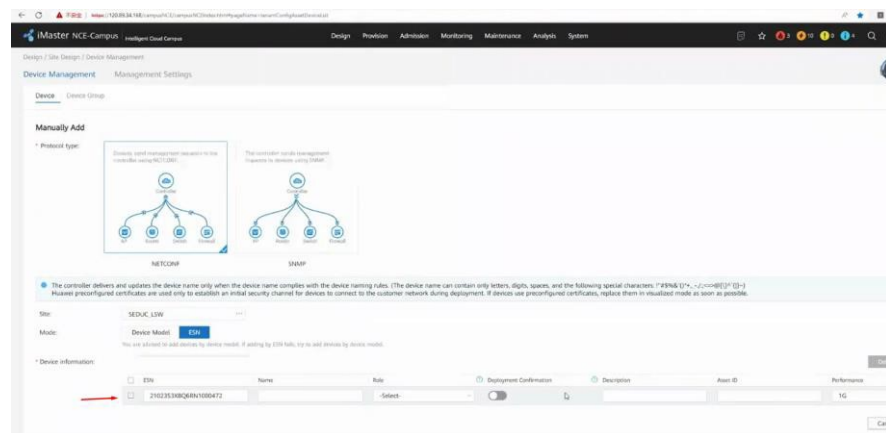


Figura 3 – Em seguida, novamente esse equipamento foi adicionado a ferramenta, inserindo apenas seu ESN (numero de série), para ser gerenciado.

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

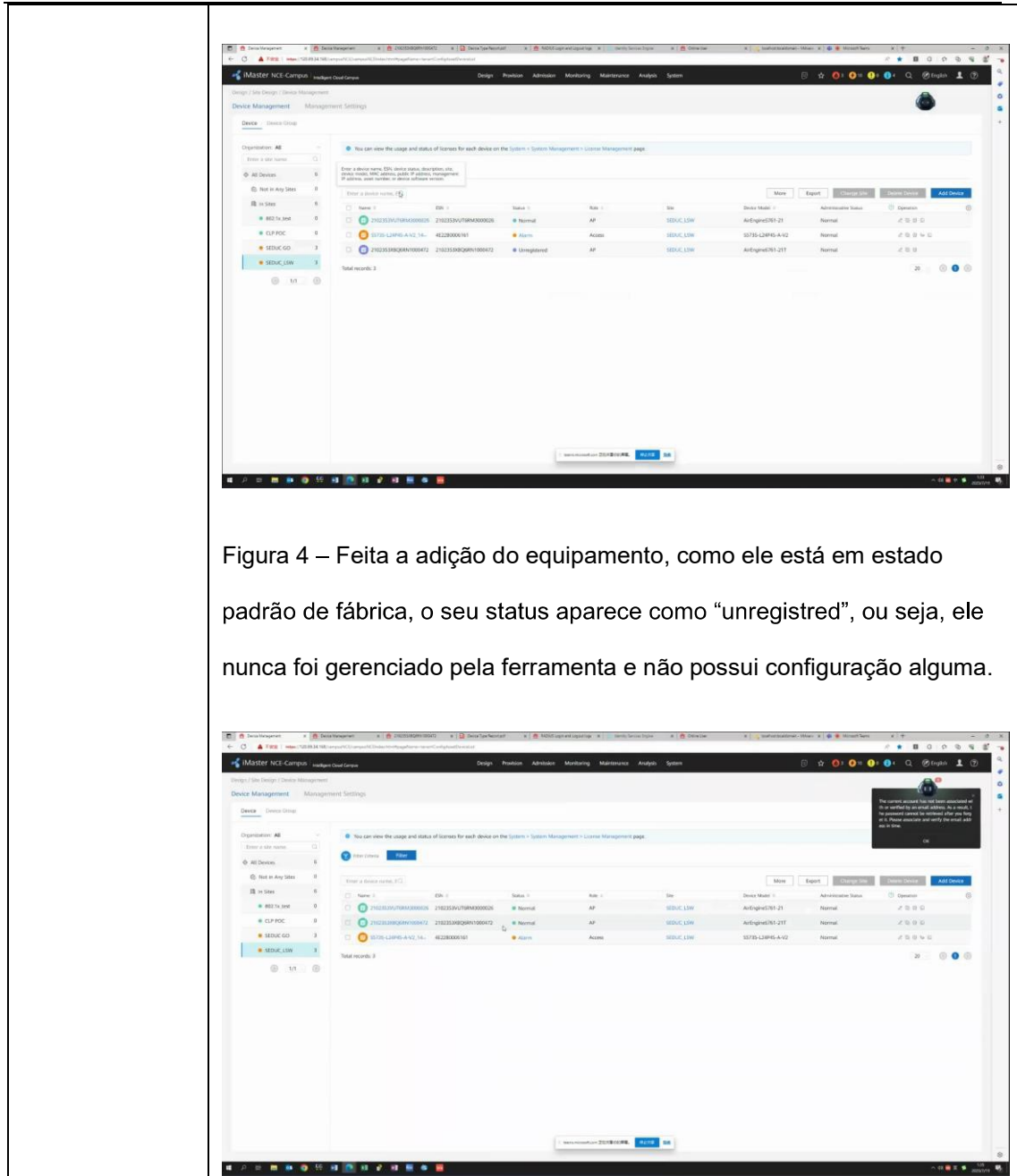
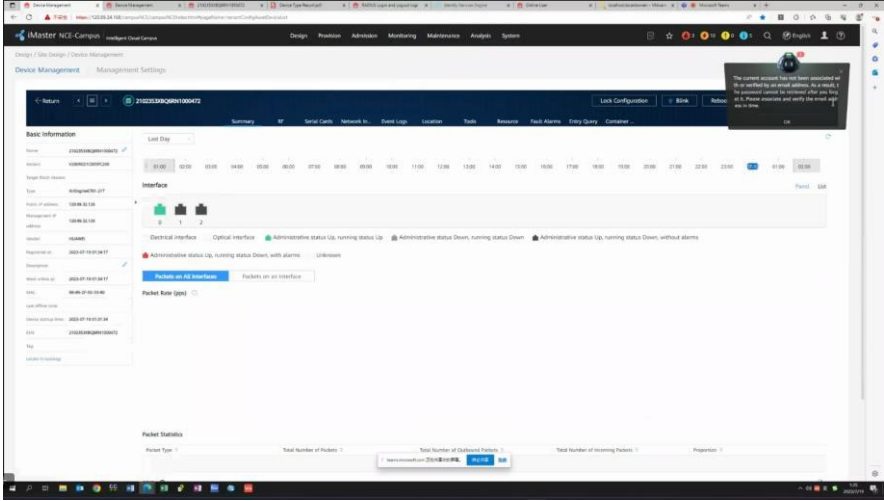


Figura 4 – Feita a adição do equipamento, como ele está em estado padrão de fábrica, o seu status aparece como “unregistred”, ou seja, ele nunca foi gerenciado pela ferramenta e não possui configuração alguma.

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



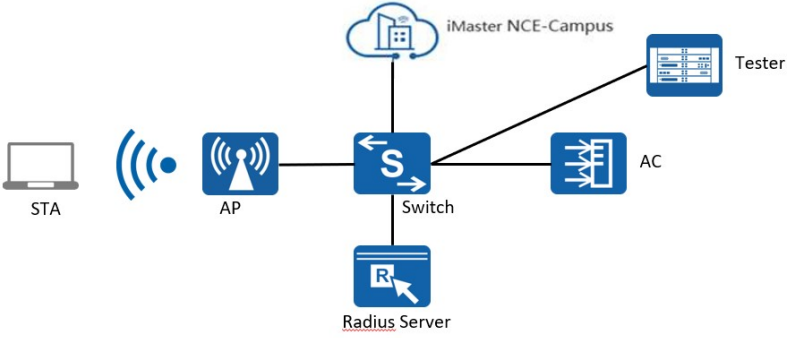
Figuras 5 e 6 – Alguns poucos minutos depois, o equipamento está com o status “normal” e gerenciado pela ferramenta.

### Radius relay

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

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

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

	 <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Selecione “Designn &gt; Network Design &gt; Template Management” a partir do menu principal. Clique em criar.Resultado esperado 1 é obtido.</li> </ol>
<p><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) Servidor RADIUS relay created com sucesso</li> </ol>



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

**Resultado**

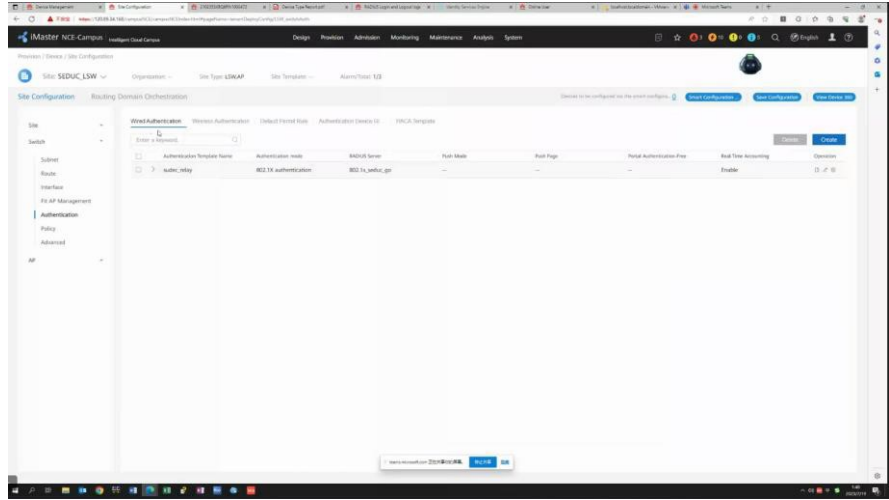


Figura 1 – Nas configurações do switch, através da plataforma iMaster NCE Campus, foi atrelado um servidor de Radius (externo), para a autenticação de usuários na rede cabeada.

**Resultado**

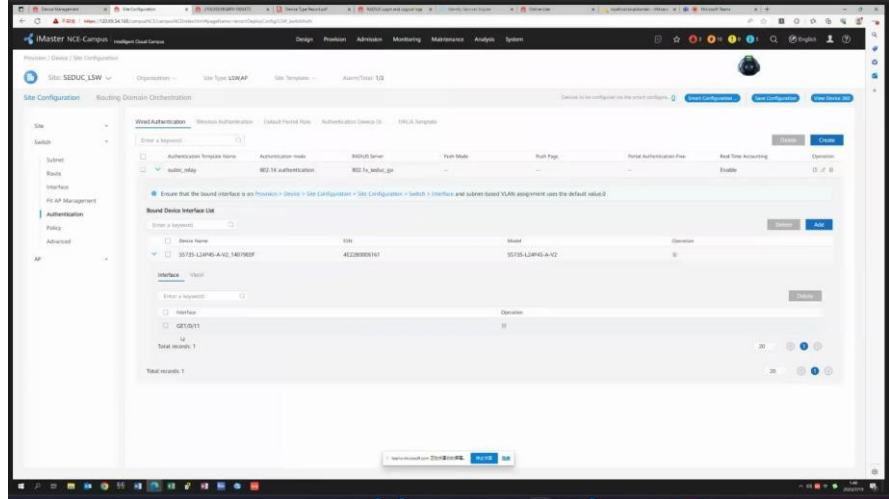
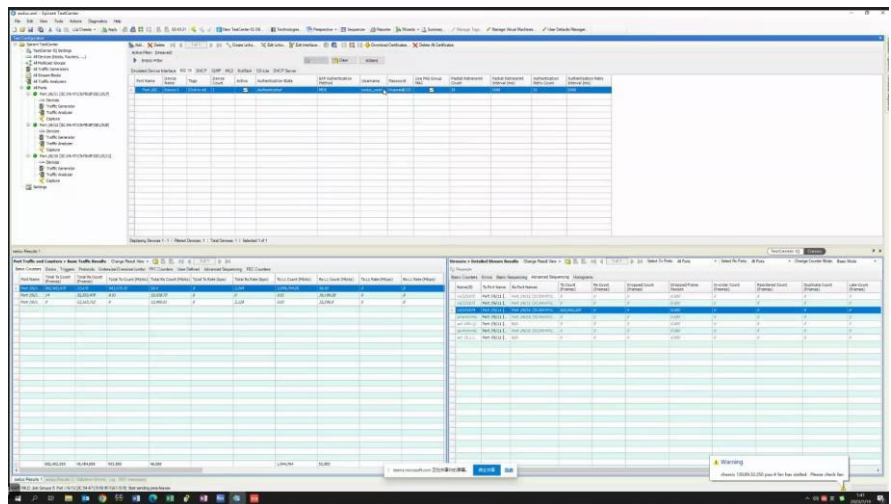


Figura 2 – Em seguida, foi feita associação da interface GE1/0/11, ao servidor.

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



Figura 3 – No servidor de Radius (nos testes, utilizamos o software Cisco ISE), foi criado o usuário seduc\_user1.



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

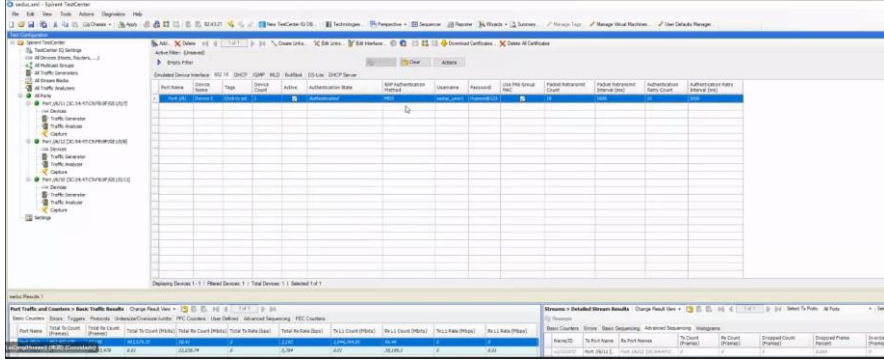


Figura 4 e 5 – Com o auxílio de um gerador de tráfego, foi simulada uma autenticação, utilizando o mesmo usuário criado no passo anterior.

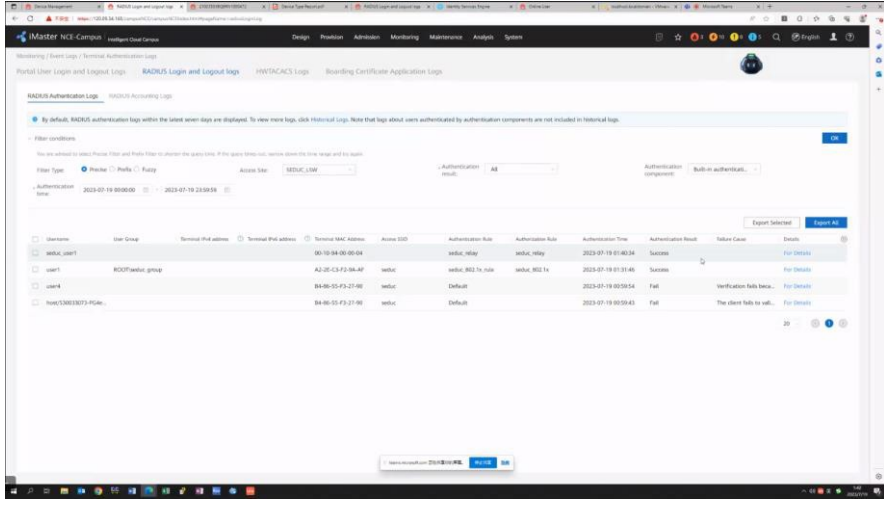
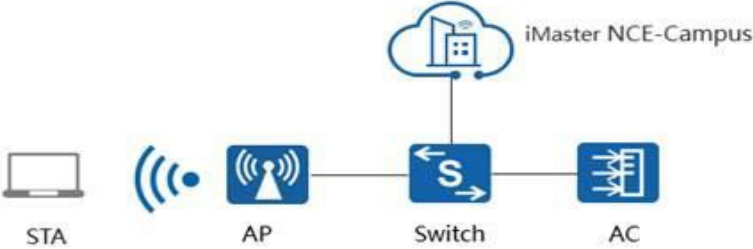


Figura 6 – Na plataforma iMaster NCE Campus, conseguimos listar os usuários conectados e autenticados via 802.1x. O usuário em destaque é o mesmo utilizado, com o nome seduc\_user1.

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;

<b>Item de teste</b>	Permitir autenticação de usuário via portal customizado (5.10.33)
<b>Objetivo do teste</b>	Permitir a customização da página de autenticação do usuário, com inclusão de texto e logo;
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Customizar as páginas utilizadas para autenticação</li> </ol>

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

<p><b>Resultado esperado</b></p>	<p><b>1) Permitir a customização da página de autenticação do usuário, com inclusão de texto e logo;</b></p>
<p><b>Resultado</b></p>	<div data-bbox="480 600 1366 1093" data-label="Image"> </div> <p>Figura 1 – Foi evidenciada a possibilidade de criação e edição das páginas web utilizadas nas autenticações.</p> <div data-bbox="480 1301 1366 1794" data-label="Image"> </div> <p>Figura 2 – Criação de templates de página</p>

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

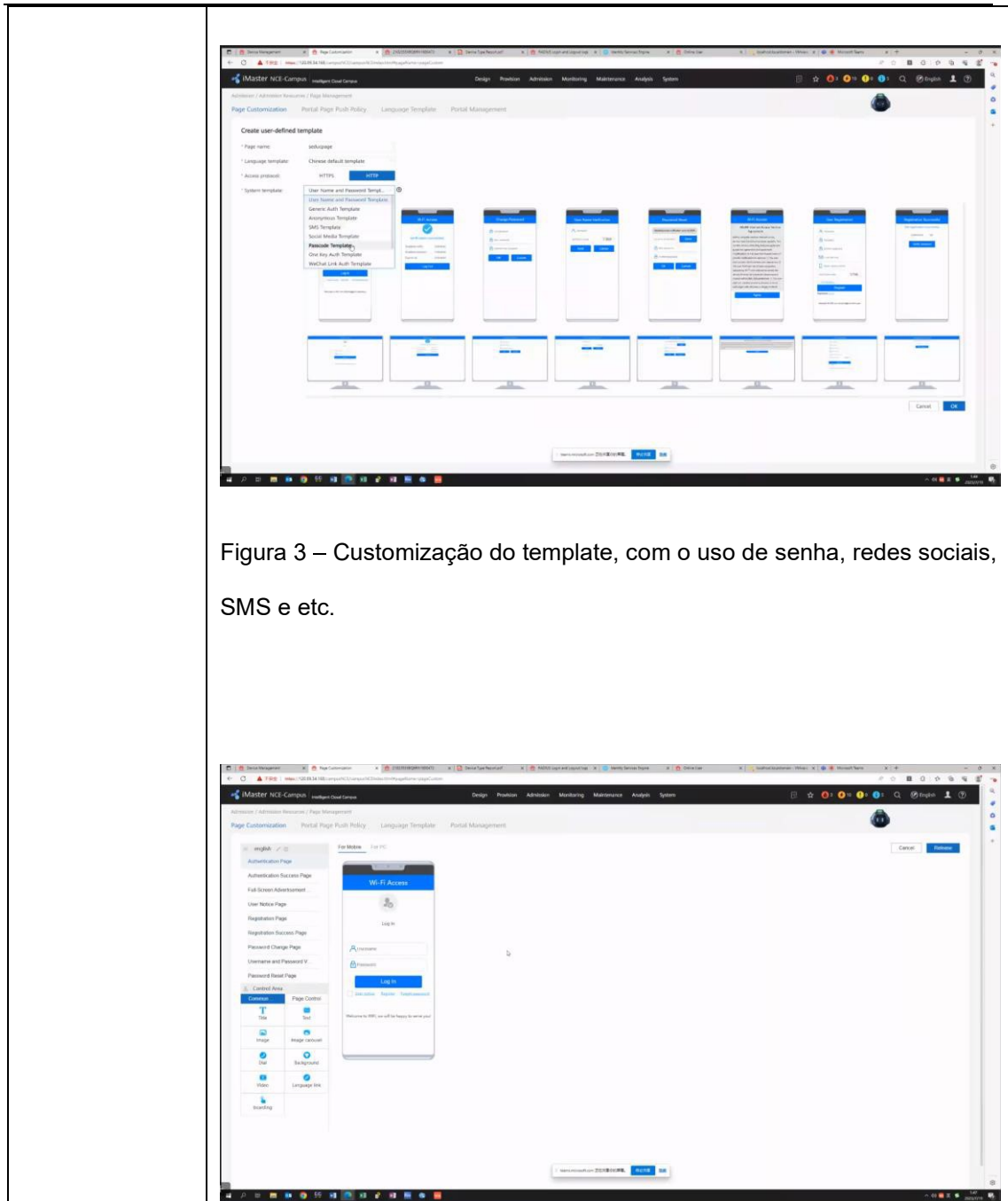
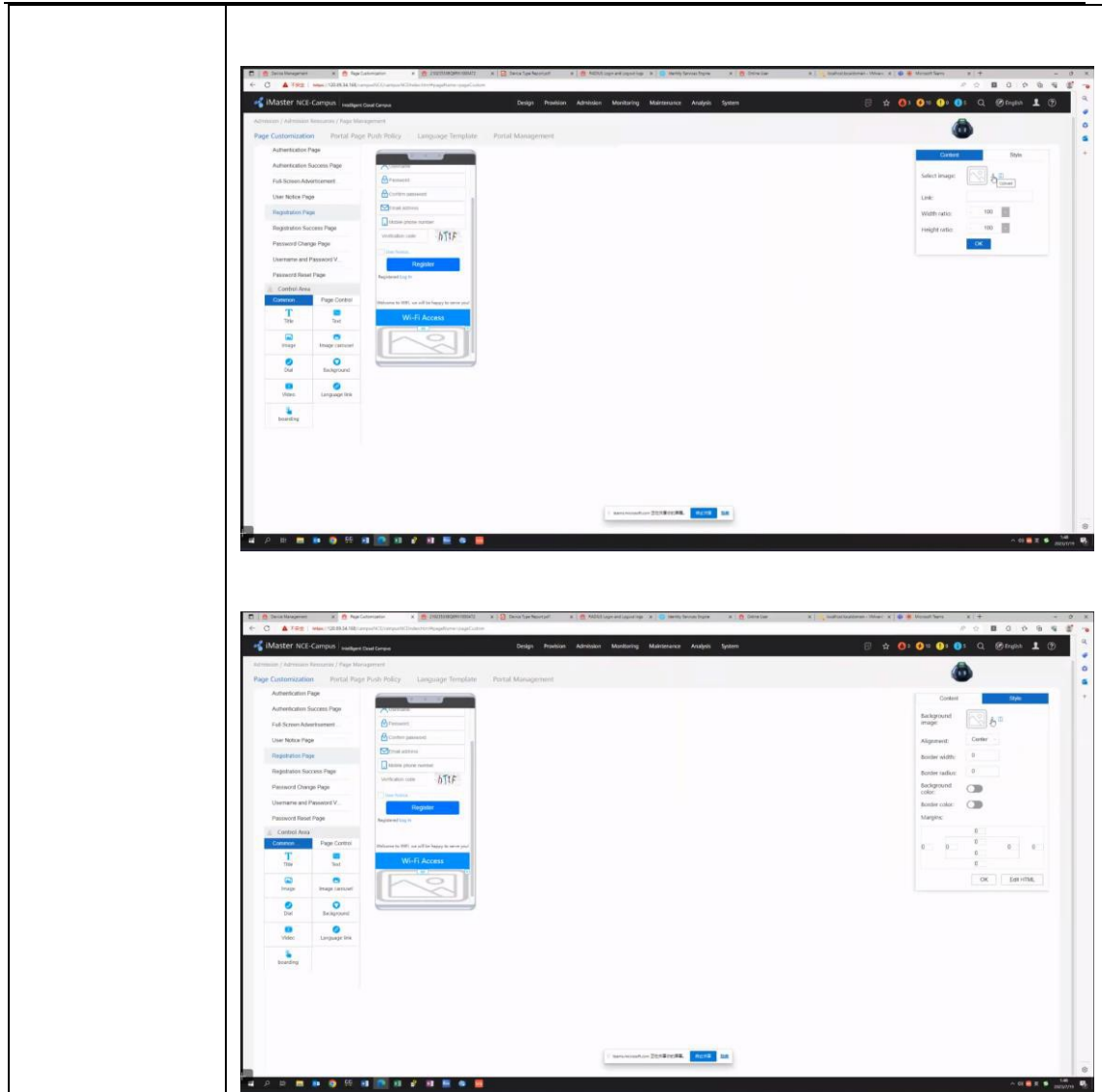


Figura 3 – Customização do template, com o uso de senha, redes sociais, SMS e etc.

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**

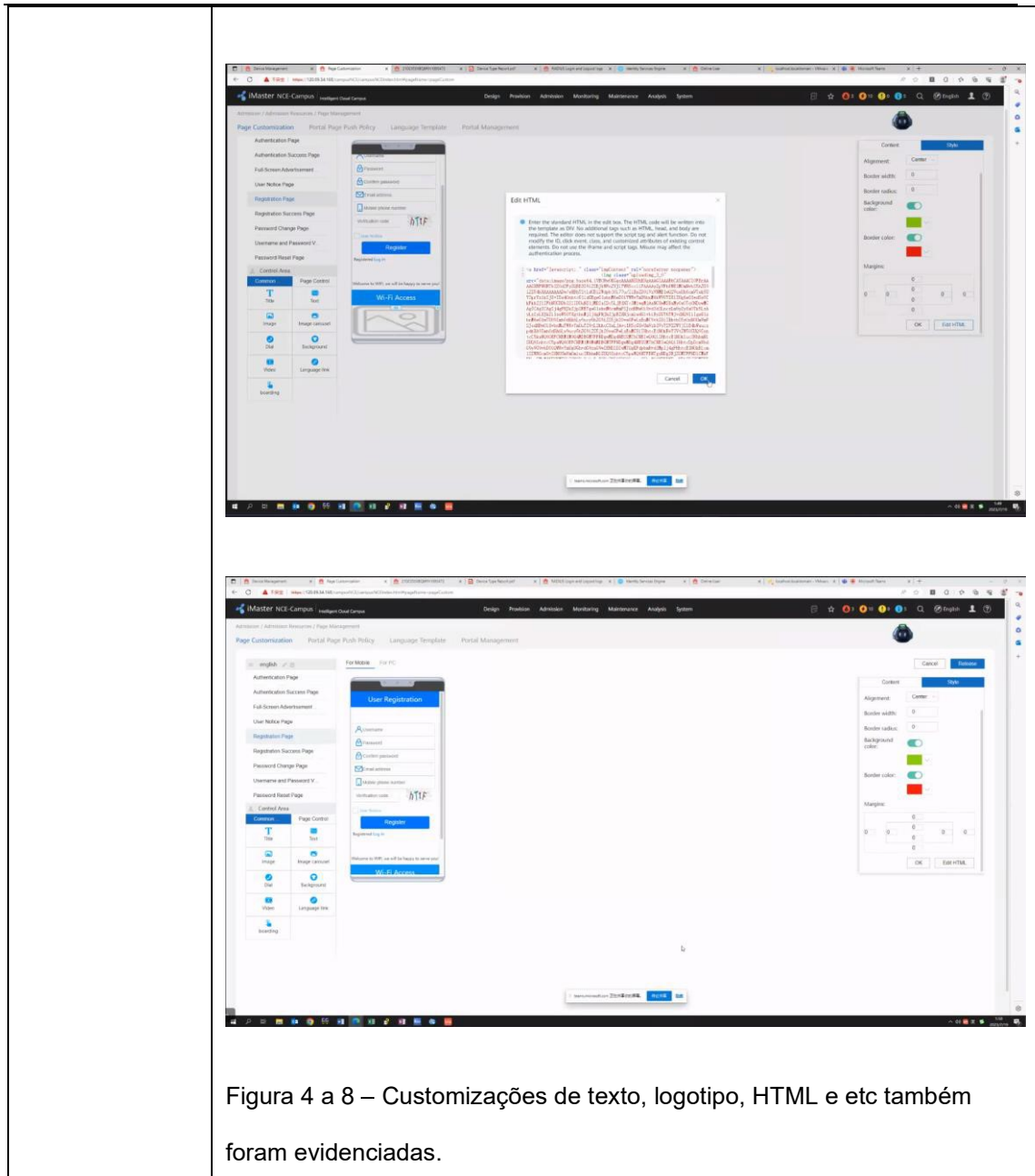


Figura 4 a 8 – Customizações de texto, logotipo, HTML e etc também foram evidenciadas.

### Identificar usuários conectados e informação de dispositivos

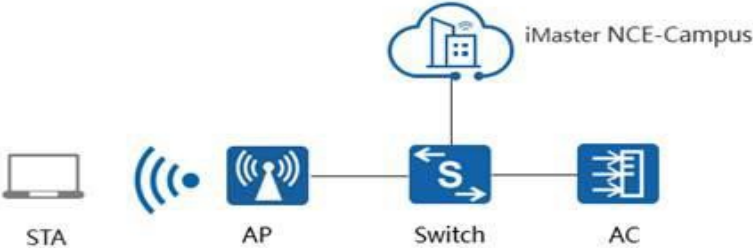
5.10.36 Identificar usuários e dispositivo conectados e permitir a visualização de, no mínimo:

- 5.10.36.1 Nome usuário conectado;
- 5.10.36.2 Endereço MAC;

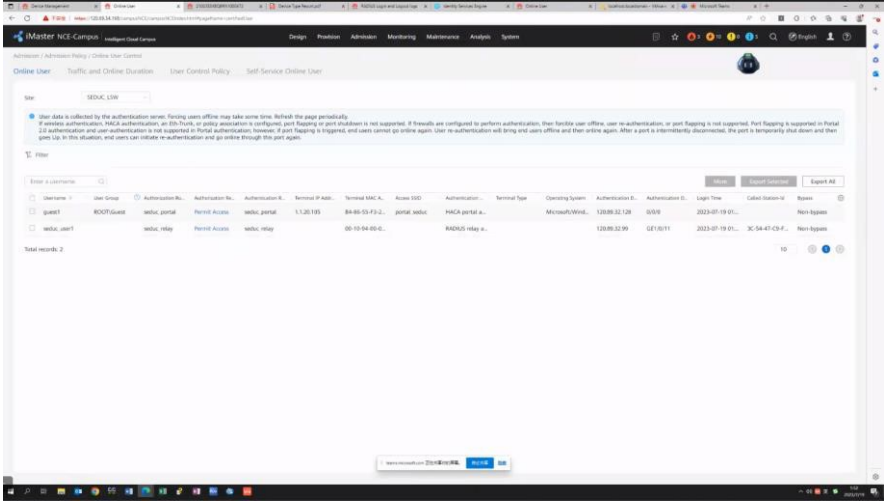


PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

- 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;

<b>Item de teste</b>	<b>Identificação de informações de dispositivos de usuário.</b>
<b>Objetivo do teste</b>	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;
<b>Configuração de teste</b>	Topologia da rede:   <p>The diagram illustrates a network topology for testing. It consists of four main components: a STA (Station) represented by a laptop icon, an AP (Access Point) represented by a wireless antenna icon, a Switch represented by a square with an 'S' and arrows, and an AC (Access Controller) represented by a server rack icon. The STA is connected to the AP, the AP is connected to the Switch, and the Switch is connected to the AC. Additionally, a cloud icon labeled 'iMaster NCE-Campus' is connected to the Switch.</p> Condições iniciais:  1) Todos os dispositivos funcionando normalmente  2) Montar o ambiente de teste de acordo com a topologia acima
<b>Procedimento de teste</b>	1) Selecione “Admission > Admission Policy > Online User Control > Online User > Site

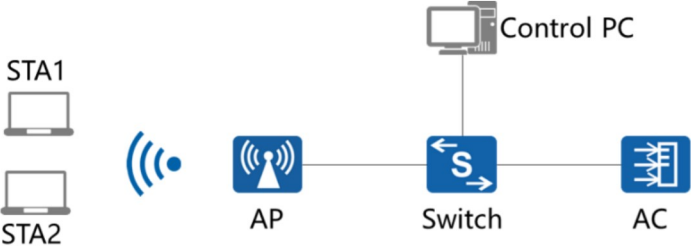
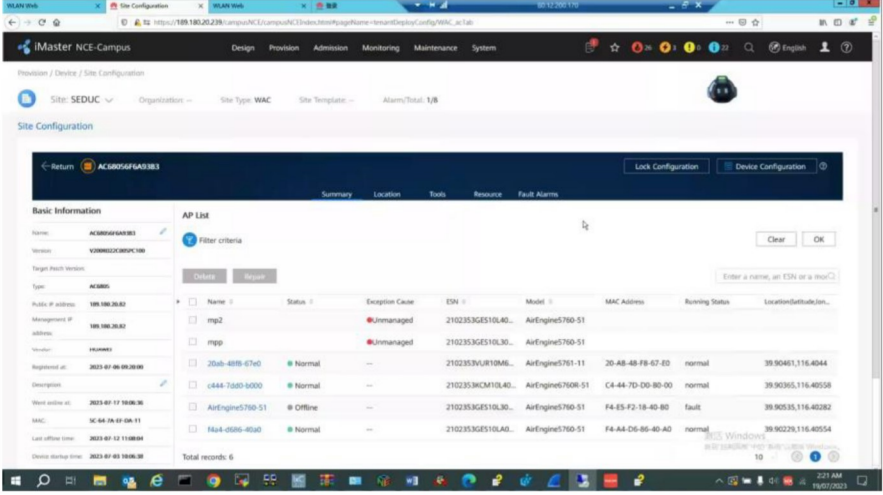
**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

<p align="center"><b>Resultado esperado</b></p>	<p>1) Identificar usuários conectados e dispositivos, e visualizar login de usuário, endereço MAC, status autenticação, horário de início de sessão, ou tempo de conexão e sistema operacional.</p>
<p align="center"><b>Resultado</b></p>	 <p>Figura 1 – Listagem de usuários conectados com suas devidas informações.</p>

**WLAN AC GUI**

<p align="center"><b>Item de teste</b></p>	WLAN AC Web Management
<p align="center"><b>Objetivo do teste</b></p>	Validar que a WLAN AC suporta Web Management
<p align="center"><b>Configuração de teste</b></p>	Topologia da rede:

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

	 <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p align="center"><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Configure Switch, AC e Control PC, Control PC pode acessar a AC;</li> <li>2) Login à AC GUI por meio da controladora do iMaster NCE Campus.</li> </ol> <p>Resultado esperado 1.</p>
<p align="center"><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>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.</li> </ol>
<p align="center"><b>Resultado</b></p>	 <p>Figura 1 – Gerenciamento via interface gráfica através da plataforma gerenciamento iMaster NCE Campus.</p>

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

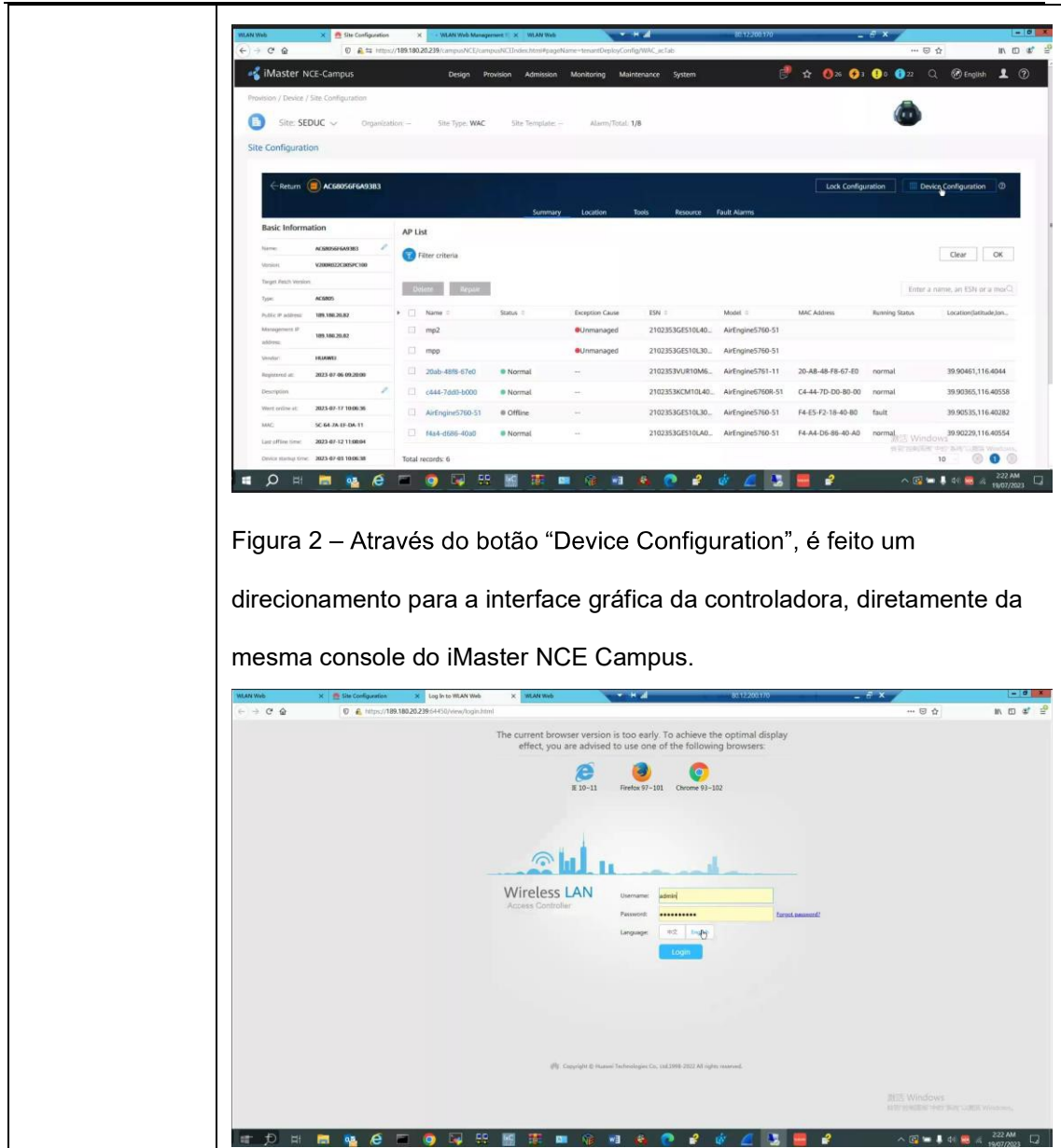
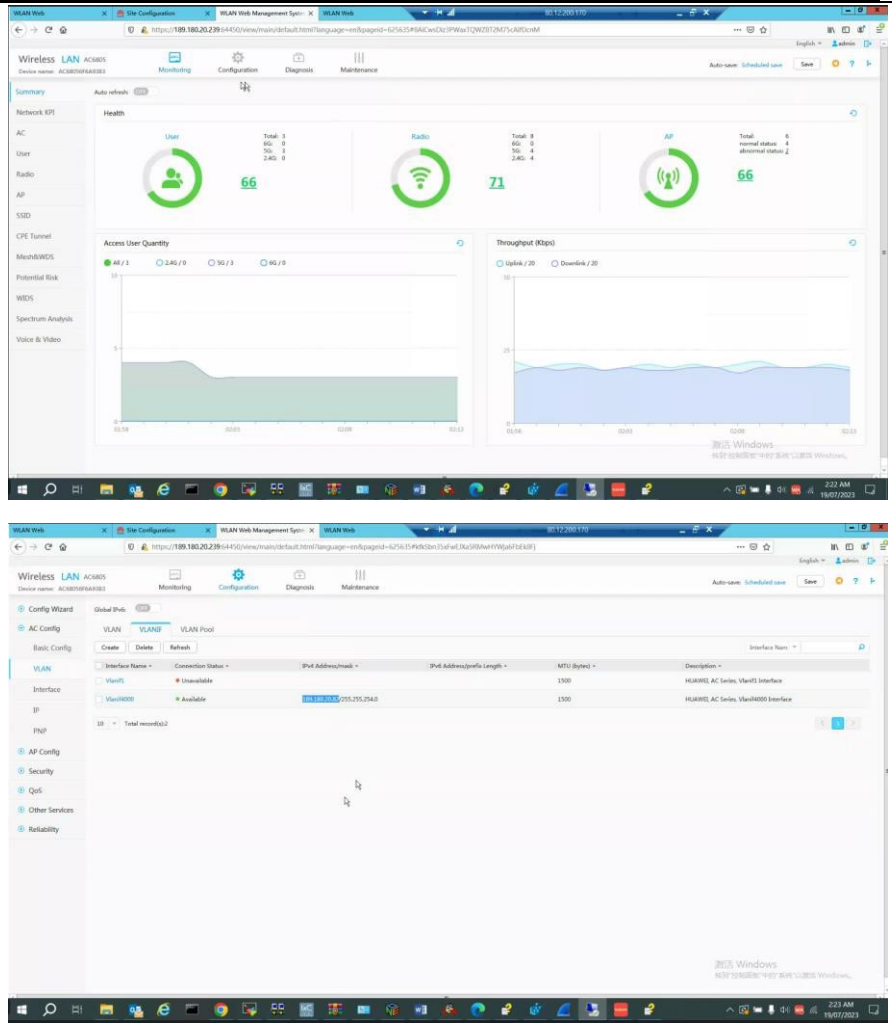


Figura 2 – Através do botão “Device Configuration”, é feito um direcionamento para a interface gráfica da controladora, diretamente da mesma console do iMaster NCE Campus.

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



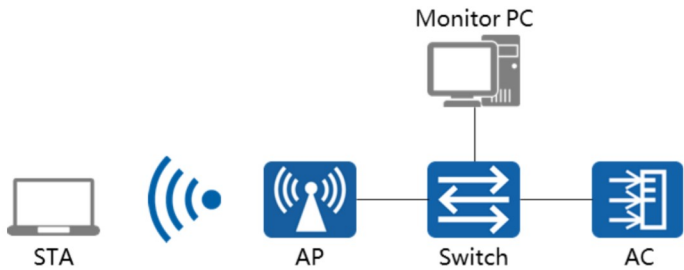
Figuras 3 a 5 – Diretamente do iMaster NCE Campus, uma vez direcionado a controladora.

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**

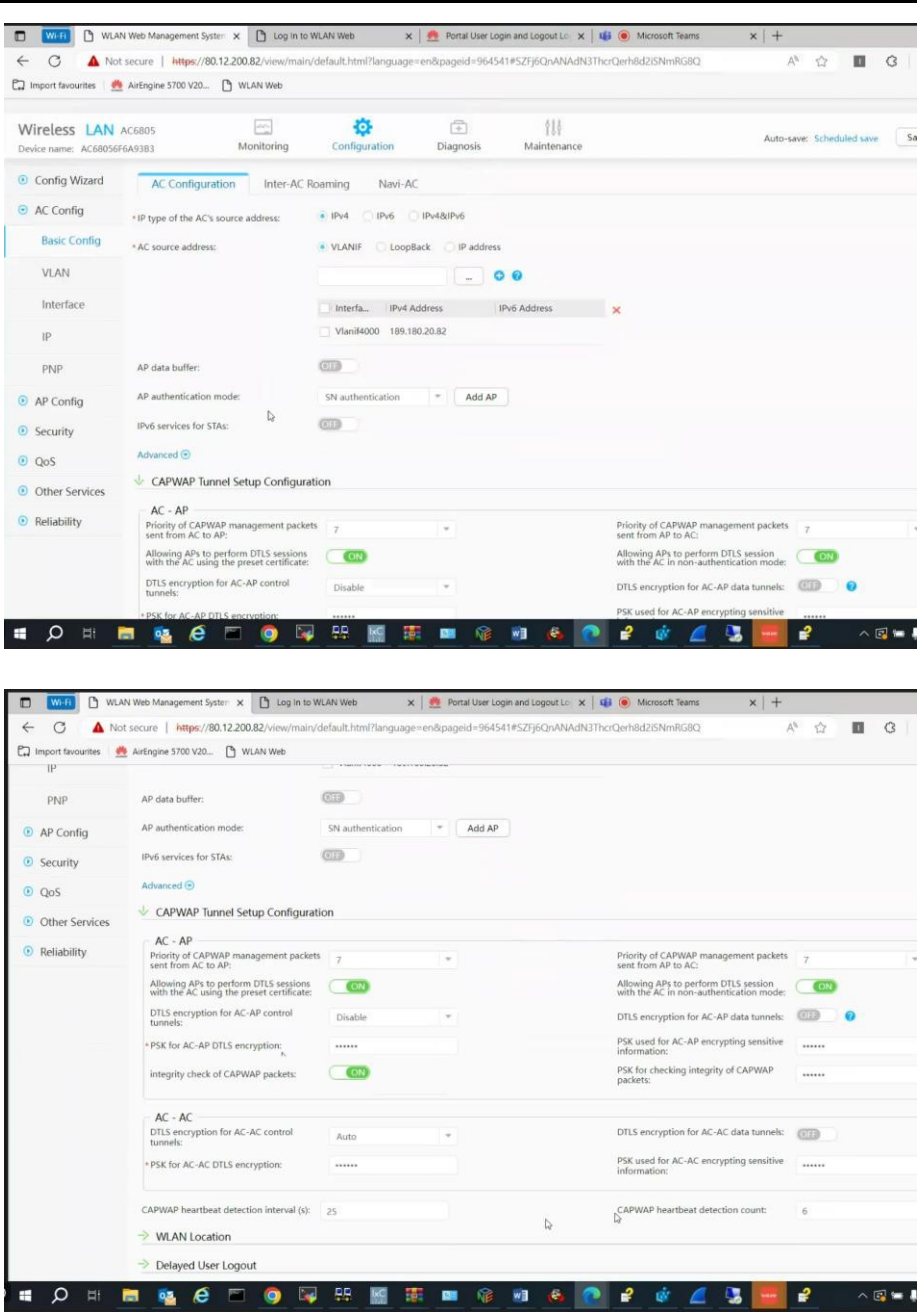
5.10.6 A comunicação entre a solução de Gerenciamento e os access Points/Switches deve ser criptografada;

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

<b>Item de teste</b>	CAPWAP Control-link DTLS Encrypt by PSK
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta CAPWAP control-link DTLS encrypt via PSK
<b>Configuração do teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos are funcionando normalmente.</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima.</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure os dispositivos de rede para que o AP possa comunicar com o AC.</li> <li>2) Habilite autenticação CAPWAP DTLS</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Pacotes trocados entre o AP e a AC mostram que o método de encriptação DTLS é PSK.</li> </ol>

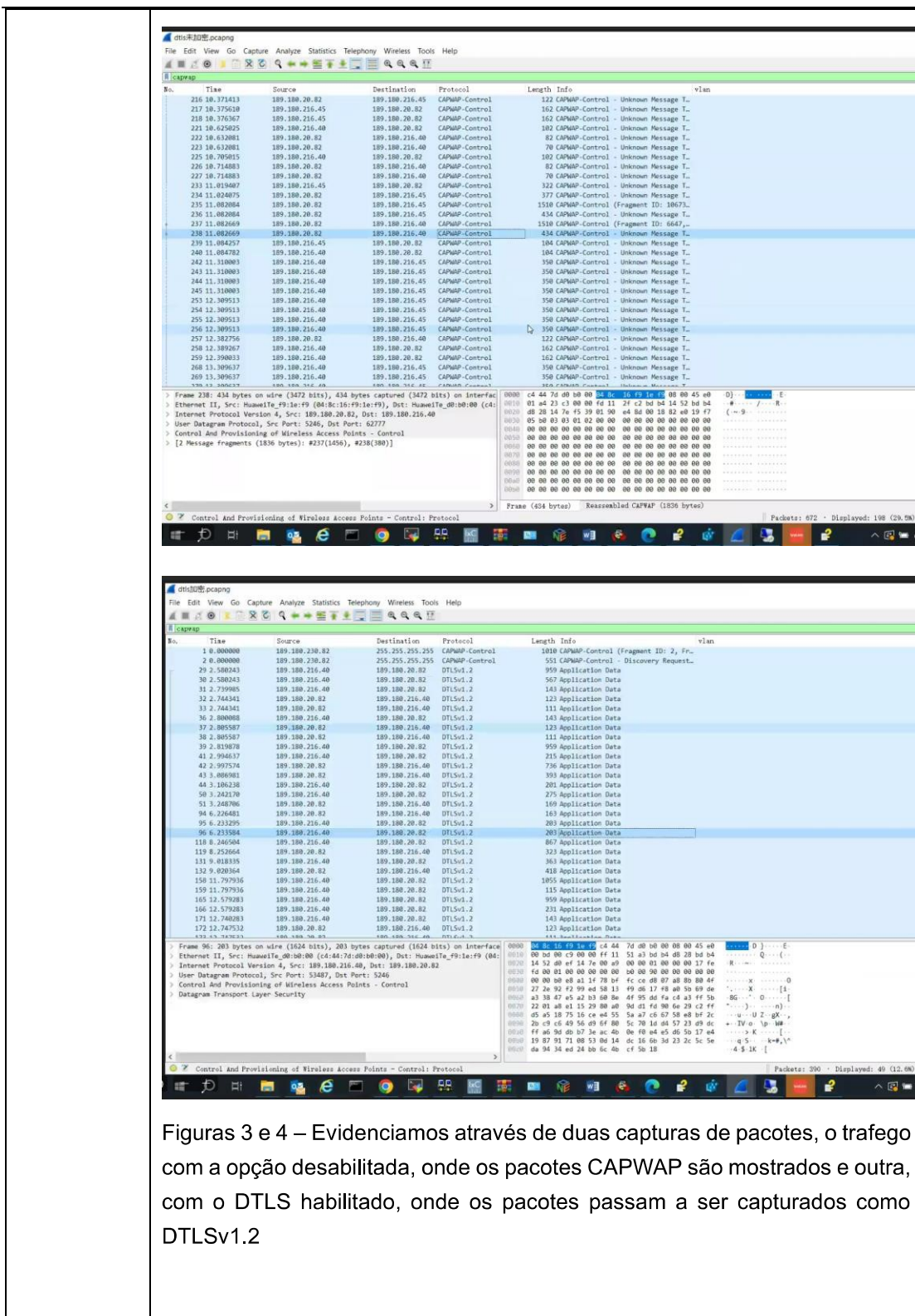
**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

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**



The figure consists of two screenshots of the Wireshark network traffic analysis tool. Both screenshots show traffic between source IP 189.180.20.82 and destination IP 189.180.216.45.

**Top Screenshot:** Shows a list of CAPWAP control messages. The protocol column is 'CAPWAP-Control'. The 'Info' column for several packets indicates 'Unknown Message T.'. The packet list pane shows details for a CAPWAP control message, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (Src Port: 5246, Dst Port: 6277). The packet bytes pane shows the raw data of the CAPWAP control message.

**Bottom Screenshot:** Shows a list of CAPWAP application data messages. The protocol column is 'DTLSv1.2'. The 'Info' column for several packets indicates 'Application Data'. The packet list pane shows details for a DTLSv1.2 application data message, including Ethernet II, Internet Protocol Version 4, and Datagram Transport Layer Security. The packet bytes pane shows the raw data of the DTLSv1.2 application data message.

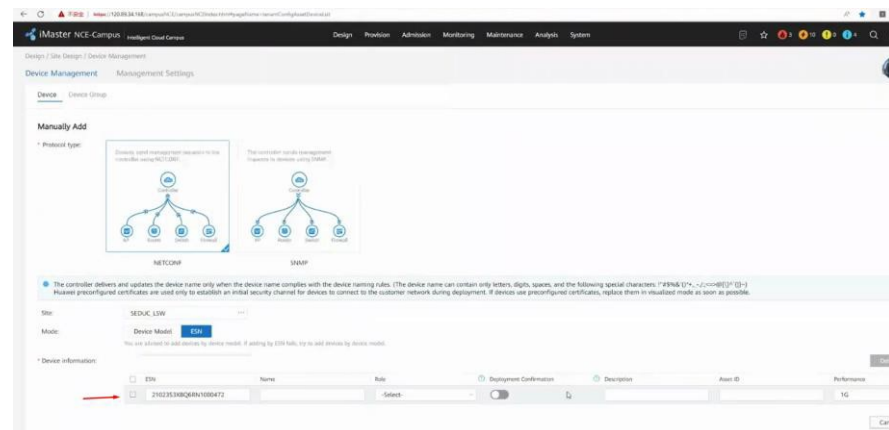
Figuras 3 e 4 – Evidenciamos através de duas capturas de pacotes, o trafego com a opção desabilitada, onde os pacotes CAPWAP são mostrados e outra, com o DTLS habilitado, onde os pacotes passam a ser capturados como DTLSv1.2



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

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:

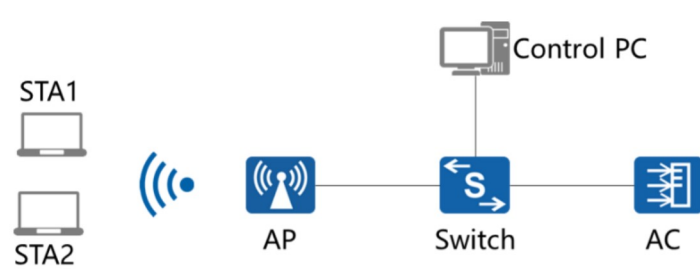
iMaster NCE-Campus Product Documentation

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

	<a href="https://support.huawei.com/hedex/hdx.do?docid=EDOC1100211132&amp;id=EN-US_CONCEPT_0000001172280645&amp;lang=en">https://support.huawei.com/hedex/hdx.do?docid=EDOC1100211132&amp;id=EN-US_CONCEPT_0000001172280645&amp;lang=en</a>
--	---

### 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.

<b>Item de teste</b>	WLAN AC Web Management
<b>Objetivo do teste</b>	Validar que a WLAN AC suporta gerenciamento via Web e é possível realizar configurações em grupos de AP
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	1) Configurar grupos de AP na controladora
<b>Resultado esperado</b>	1) AP gerenciados como grupos

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

**Resultado**

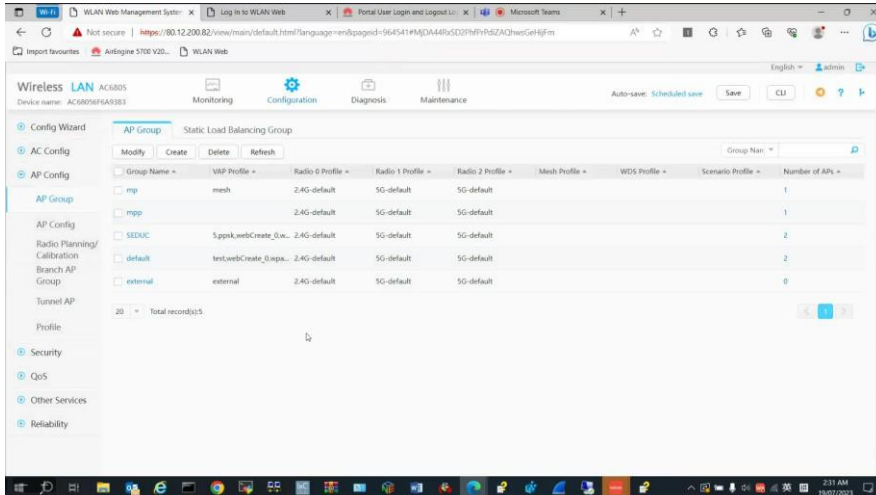


Figura 1 – Na controladora, foi evidenciado a função de criar grupos para gerenciamento de APs. Nesta opção, a quantidade de APs em cada grupo é mostrada na coluna a direita.

**Resultado**

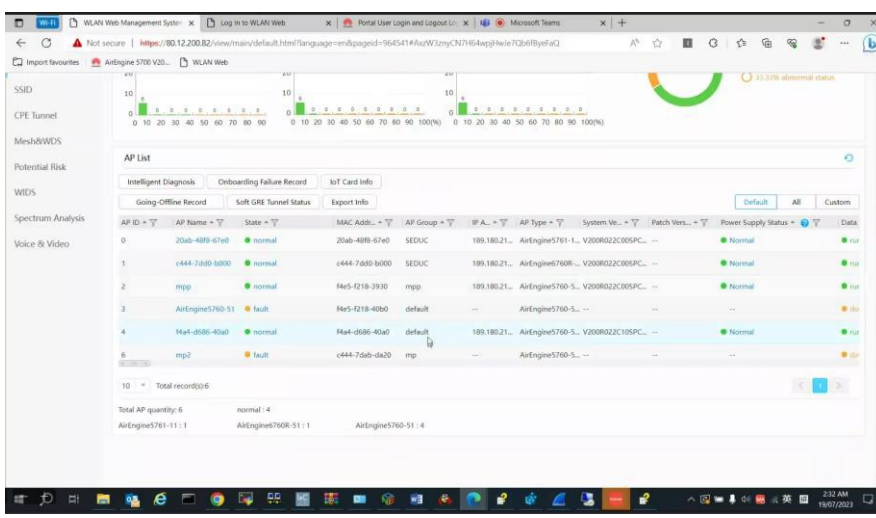


Figura 2 – Na listagem de APs gerenciados, existe uma coluna específica, identificando a qual grupo este AP pertence.

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

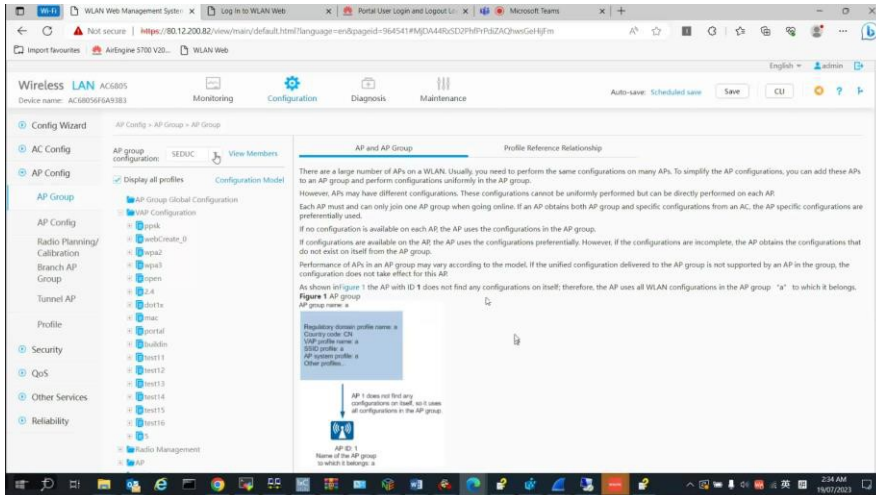


Figura 3 – Cada grupo de APs, tem o seu proprio VAP Configuration, onde cada parametro e configuração inserido, será aplicado apenas ao grupo. No exemplo, foi mostrado o grupo “SEDUC”.

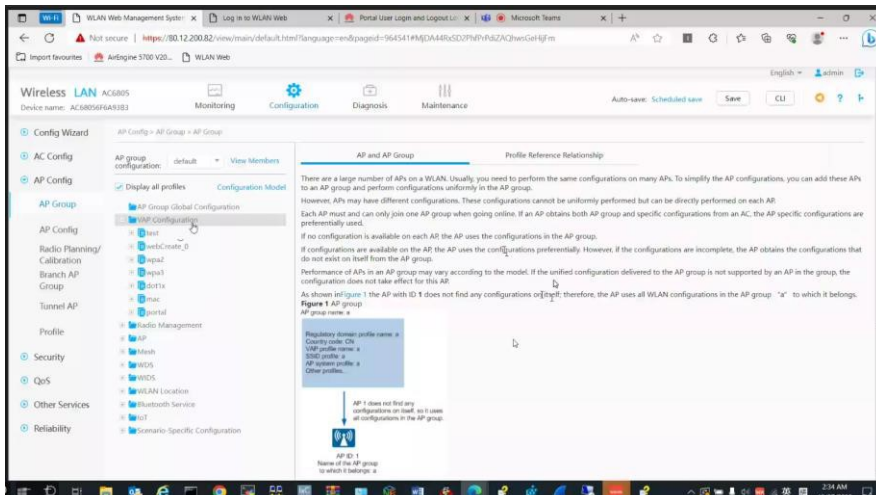
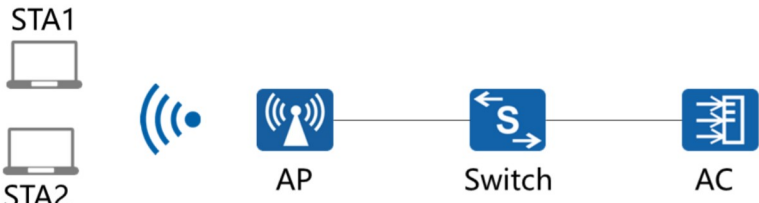
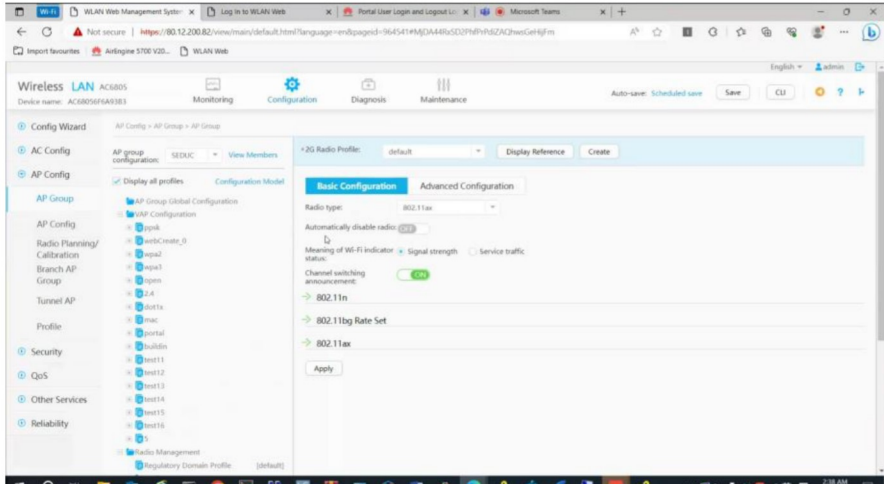


Figura 4 – Complementando a figura 3, agora foi mostrado o grupo “default”

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

**Auto-off radio**

<b>Item de teste</b>	Auto-off radio
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta shutdown em radios individuais de forma imediata ou agendada
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Desabilitar de forma automatica a operação dos radios de acordo com o agendamento.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Os radios param de funcionar no momento agendado</li> </ol>
<b>Resultado</b>	

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

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

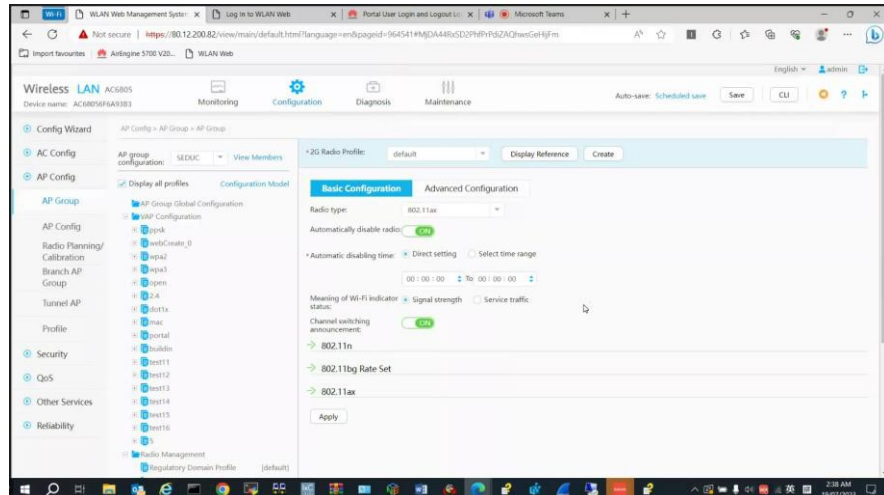


Figura 2 – Uma vez habilitada, podemos agendar o momento exato que este rádio deverá parar sua operação.

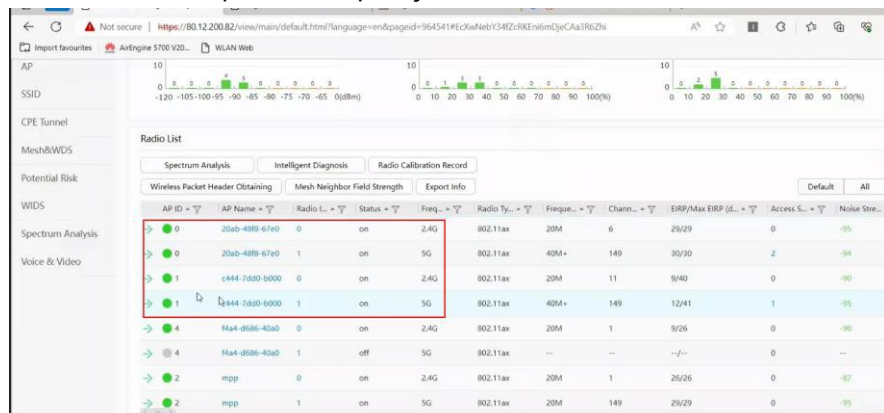


Figura 3 – Foi listado os rádios disponíveis de cada AP, e evidenciado que os APs sob teste, estão com os radios com status “on”.

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

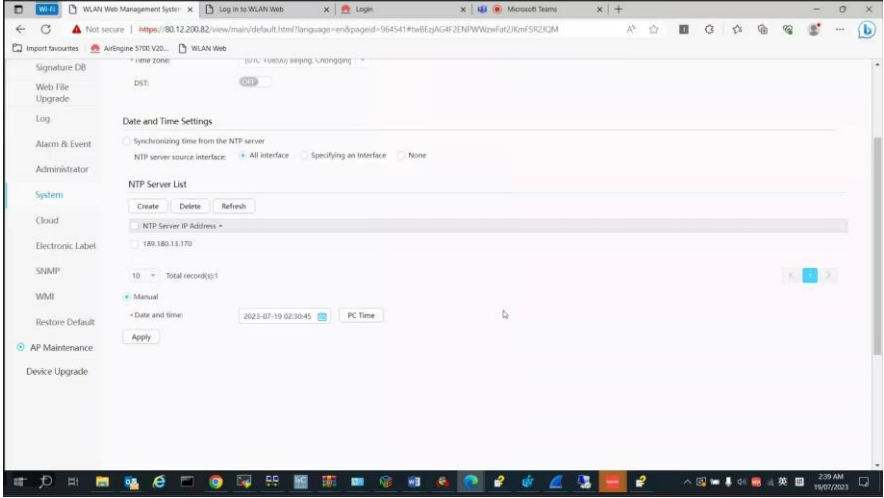


Figura 4 – Em seguida, foi mostrado o horário de operação da controladora, que no caso, é diferente do laptop, por estar sincronizado com o um servidor AD.

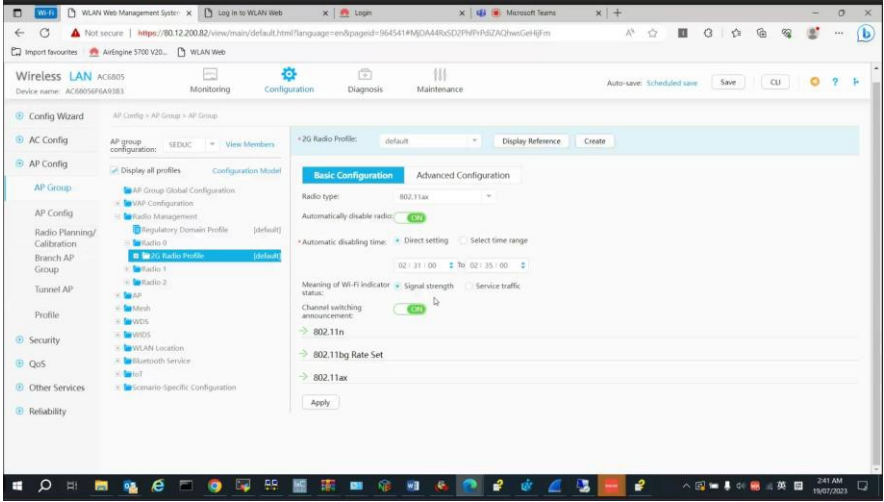


Figura 5 – Foi configurado o momento exato que este rádio (2.4Ghz) deverá parar com sua operação.

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

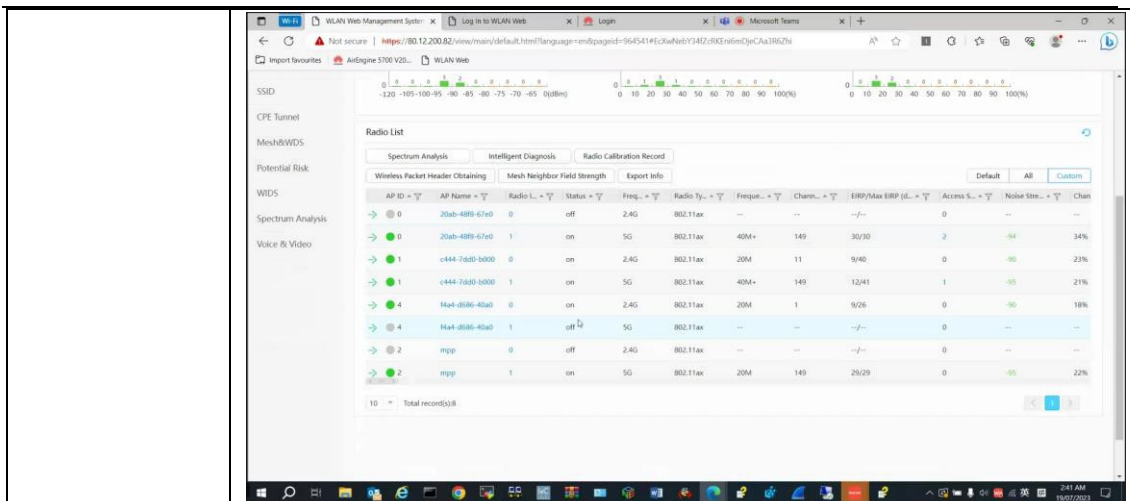
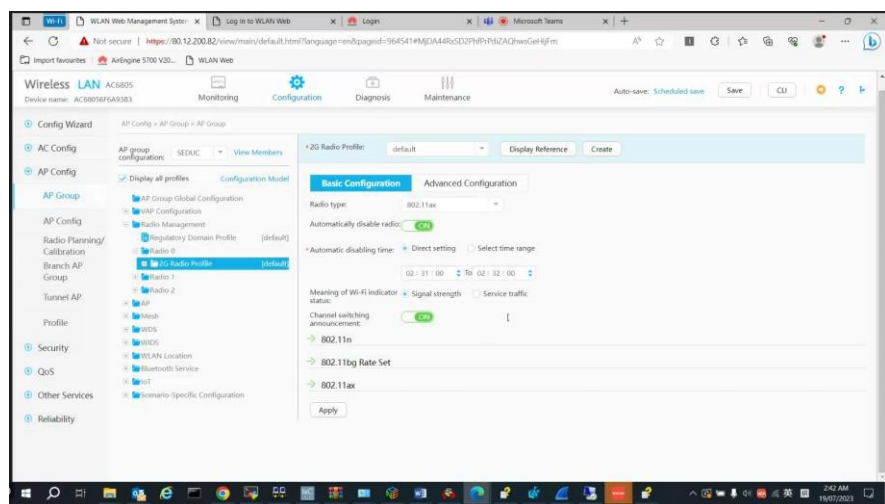


Figura 6 – Atingindo o tempo configurado, o radio 0, do AP ID 0, passou o status para “off”.





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

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

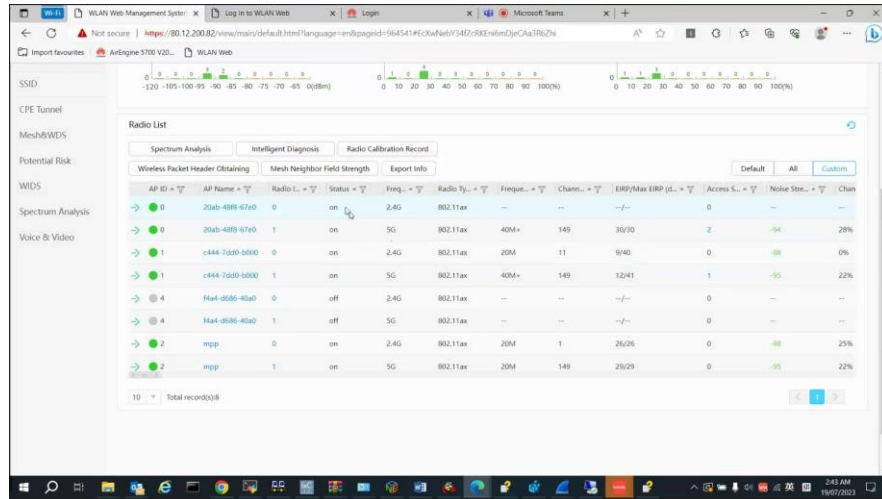


Figura 8 – Atingindo novamente o tempo estipulado, o radio passou seu status para “on”.

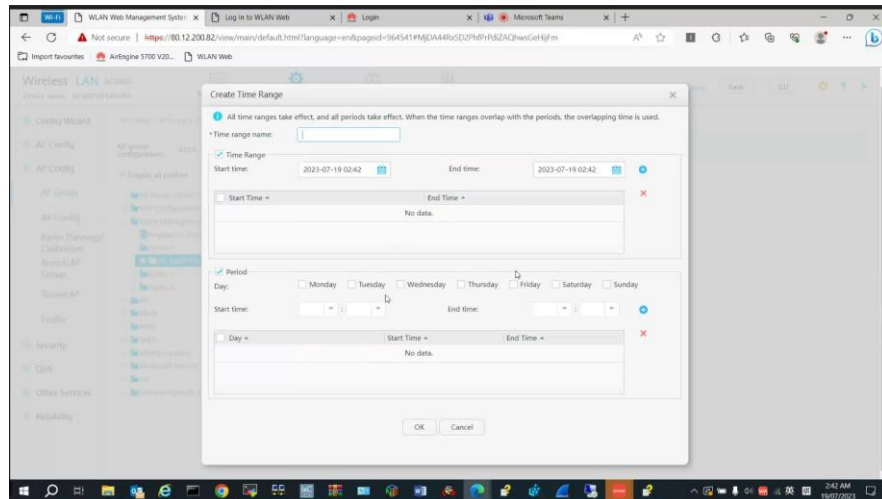



Figura 9 – Foi evidenciado também, a opção de agendamento, considerando períodos.

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)

<b>Item de teste</b>	Detecção de Rogue AP
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Rogue AP Detection
<b>Configuração de teste</b>	<p>Topologia da rede:</p> <div style="text-align: center;">  <p>Rogue AP      AP      Switch      AC</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure Rogue AP to deliver SSID: "SSID-Temp";</li> <li>2) Configure a ac corretamente, AP deliver SSID: "SSID-Temp";</li> <li>1) Habilite Rogue AP detection function na AC. Resultado esperado 1.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Rogue AP será detectado pelo sistema WLAN.</li> </ol>

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

**Resultado**

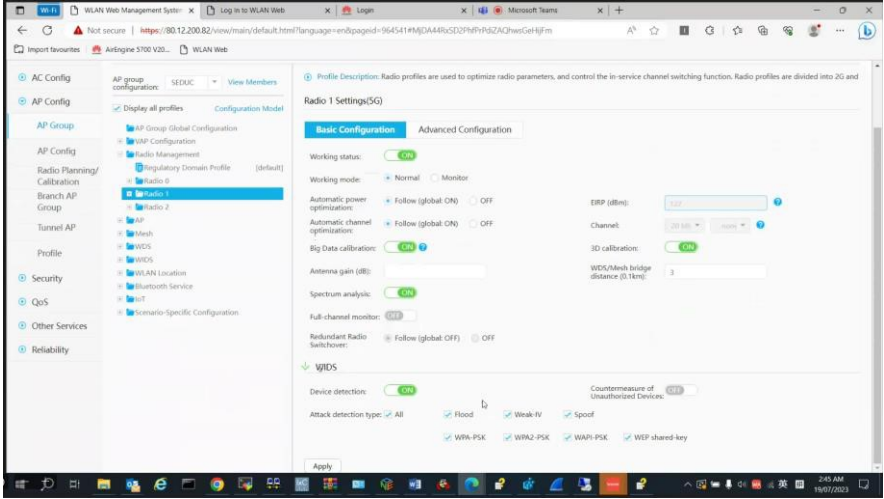


Figura 1 – Nas configurações dentro de VAP Configuration, foi evidenciada a opção de WIDS, onde foi habilitada a opção “Device detections”, e as opções de ataques disponíveis para identificação.

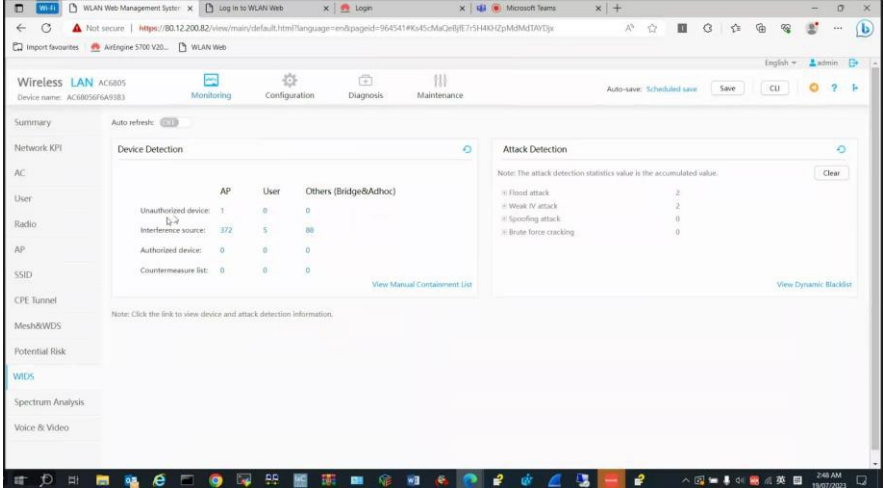


Figura 2 – Na controladora, foi mostrada todas as informações do WIDS, com a quantidade de origens com interferencia, APs não autorizados e etc.

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

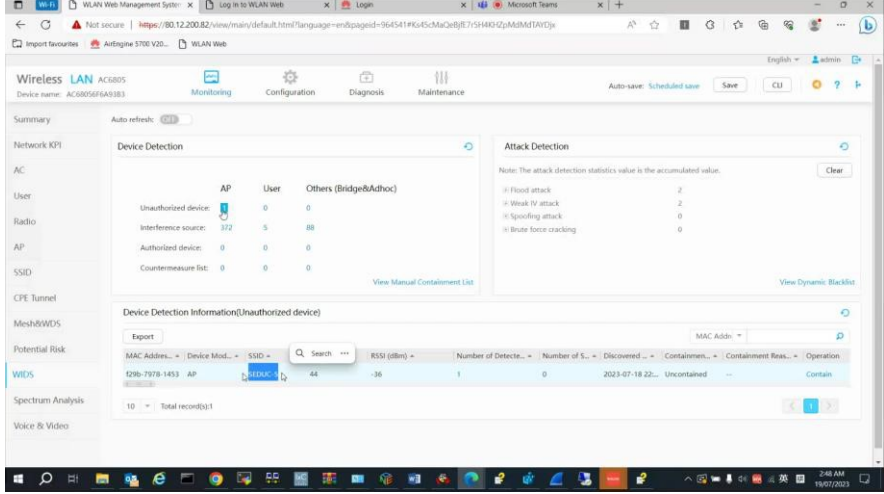
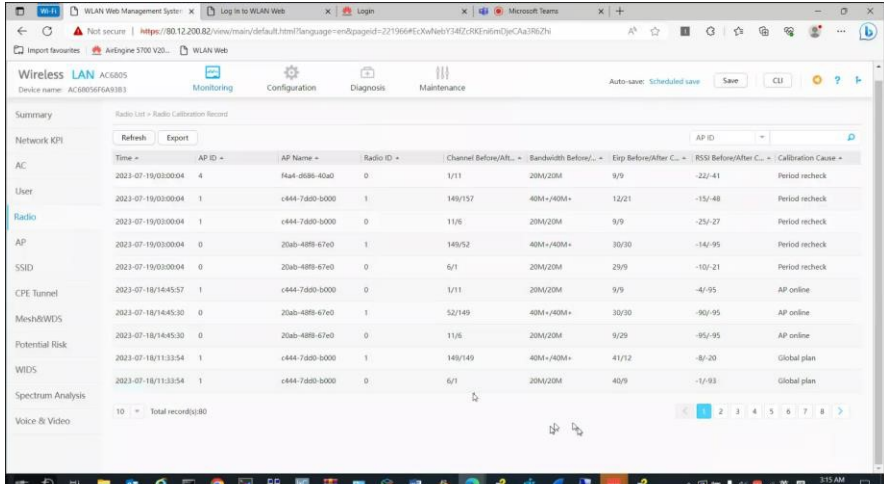


Figura 3 – Ao clicar em um AP não autorizado, identificamos o AP que havíamos simulado propagando o mesmo SSID configurado na controladora.

Obs.  
 O ajuste de radio frequência, 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.



Time	AP ID	AP Name	Radio ID	Channel Before/After	Bandwidth Before/After	ETP Before/After	RSSI Before/After	Calibration Cause
2023-07-19/03:00:04	4	Real-0086-40a0	0	1/11	20M/20M	9/9	-22/-41	Period check
2023-07-19/03:00:04	1	c444-76d0-b000	1	149/157	40M+/40M+	12/21	-15/-48	Period check
2023-07-19/03:00:04	1	c444-76d0-b000	0	11/5	20M/20M	9/9	-25/-27	Period check
2023-07-19/03:00:04	0	20a0-4895-67e0	1	149/52	40M+/40M+	30/30	-14/-95	Period check
2023-07-19/03:00:04	0	20a0-4895-67e0	0	6/1	20M/20M	29/9	-10/-21	Period check
2023-07-18/14:45:57	1	c444-76d0-b000	0	1/11	20M/20M	9/9	-4/-95	AP online
2023-07-18/14:45:30	0	20a0-4895-67e0	1	52/149	40M+/40M+	30/30	-90/-95	AP online
2023-07-18/14:45:30	0	20a0-4895-67e0	0	11/5	20M/20M	9/29	-95/-95	AP online
2023-07-18/11:33:54	1	c444-76d0-b000	1	149/149	40M+/40M+	41/12	-8/-20	Global plan
2023-07-18/11:33:54	1	c444-76d0-b000	0	6/1	20M/20M	40/9	-1/-93	Global plan

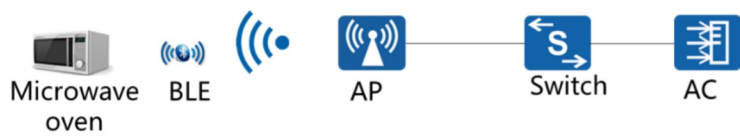
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
 PROCESSO Nº 2020.0000.604.5301  
 INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

	Calibração de rádio – item 5.10.20
--	------------------------------------

### Detecção de dispositivos não Wi-Fi e Análise de espectro

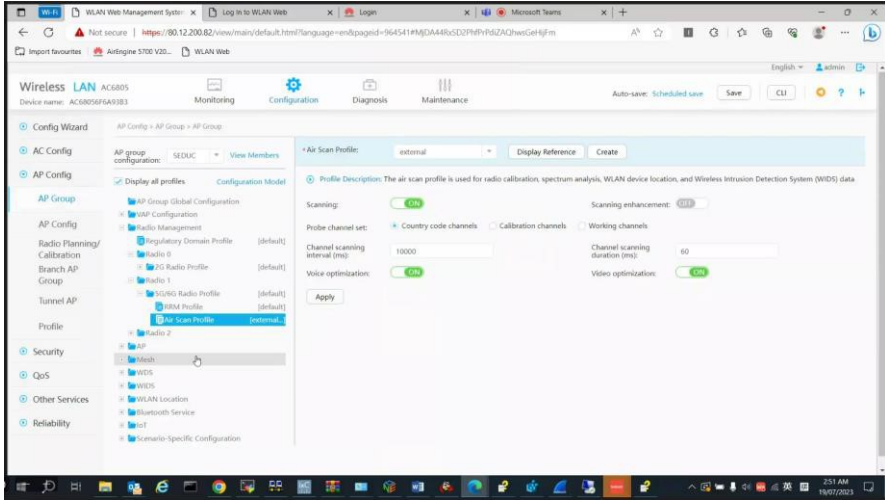
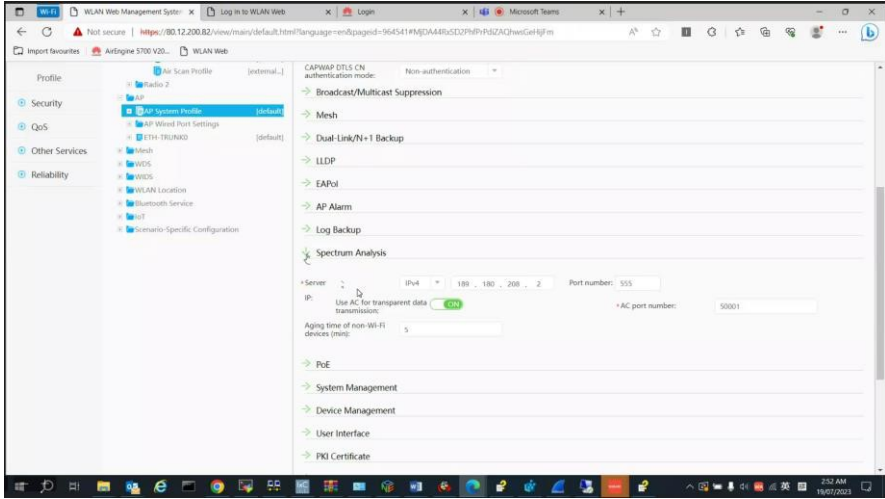
5.10.13 Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede sem fio (WLAN) e Rádio Frequência (RF).

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)

<b>Item de teste</b>	Detecção de dispositivos não Wi-Fi e Análise de espectro
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta detecção de fontes de RF Non-Wi-Fi função de análise de espectro.
<b>Configuração de teste</b>	<p>Topologia da rede:</p> <div style="text-align: center;">  <p>Microwave oven   BLE   AP   Switch   AC</p> </div> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	1) Detectar dispositivos de radio frecuencia não Wi-Fi no espectro da rede sem fio.
<b>Resultado esperado</b>	1) Dispositivos podem ser detectados na AC, e a informação sobre os dispositivos é listada pela AC.

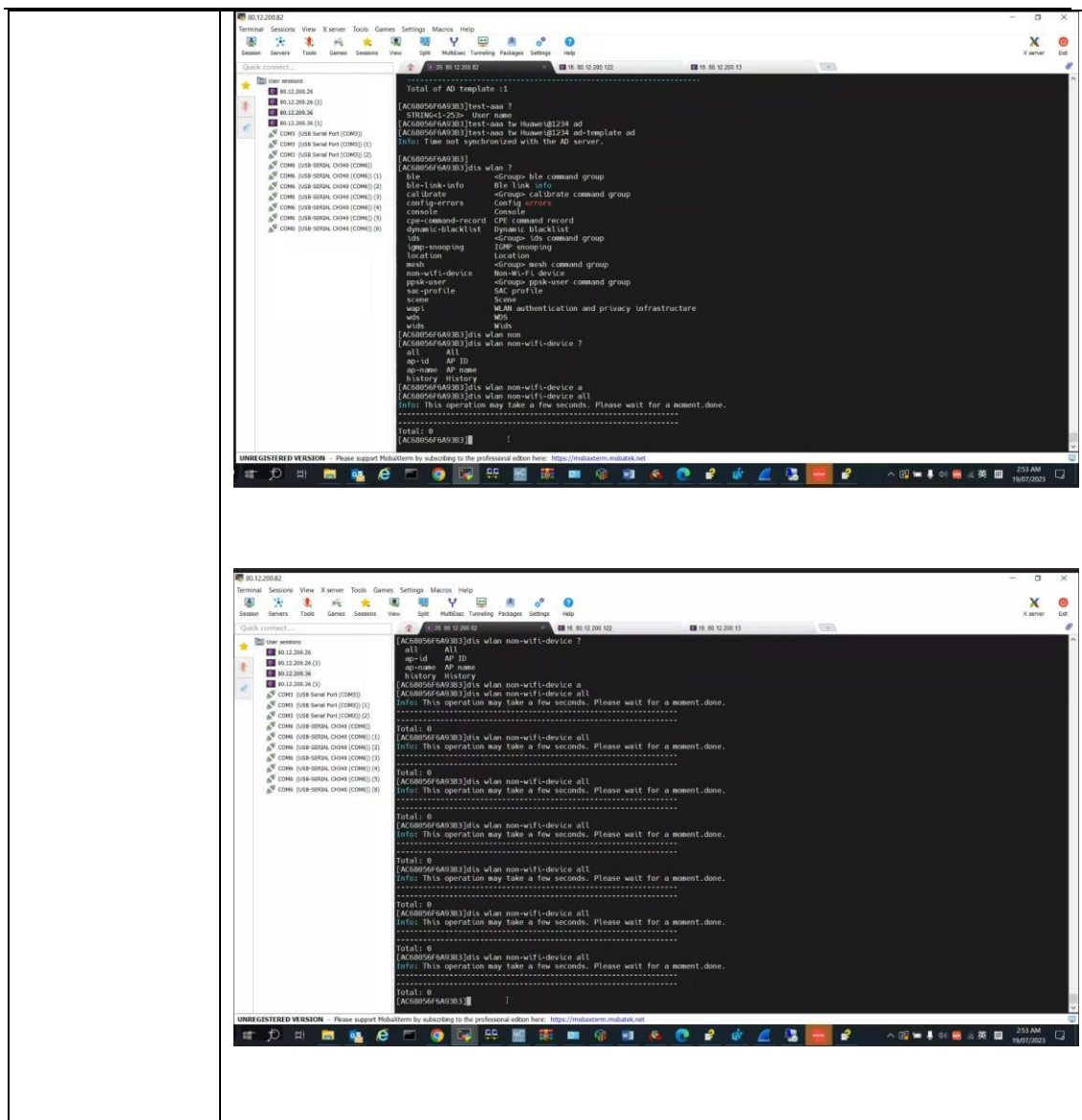
**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

Resultado

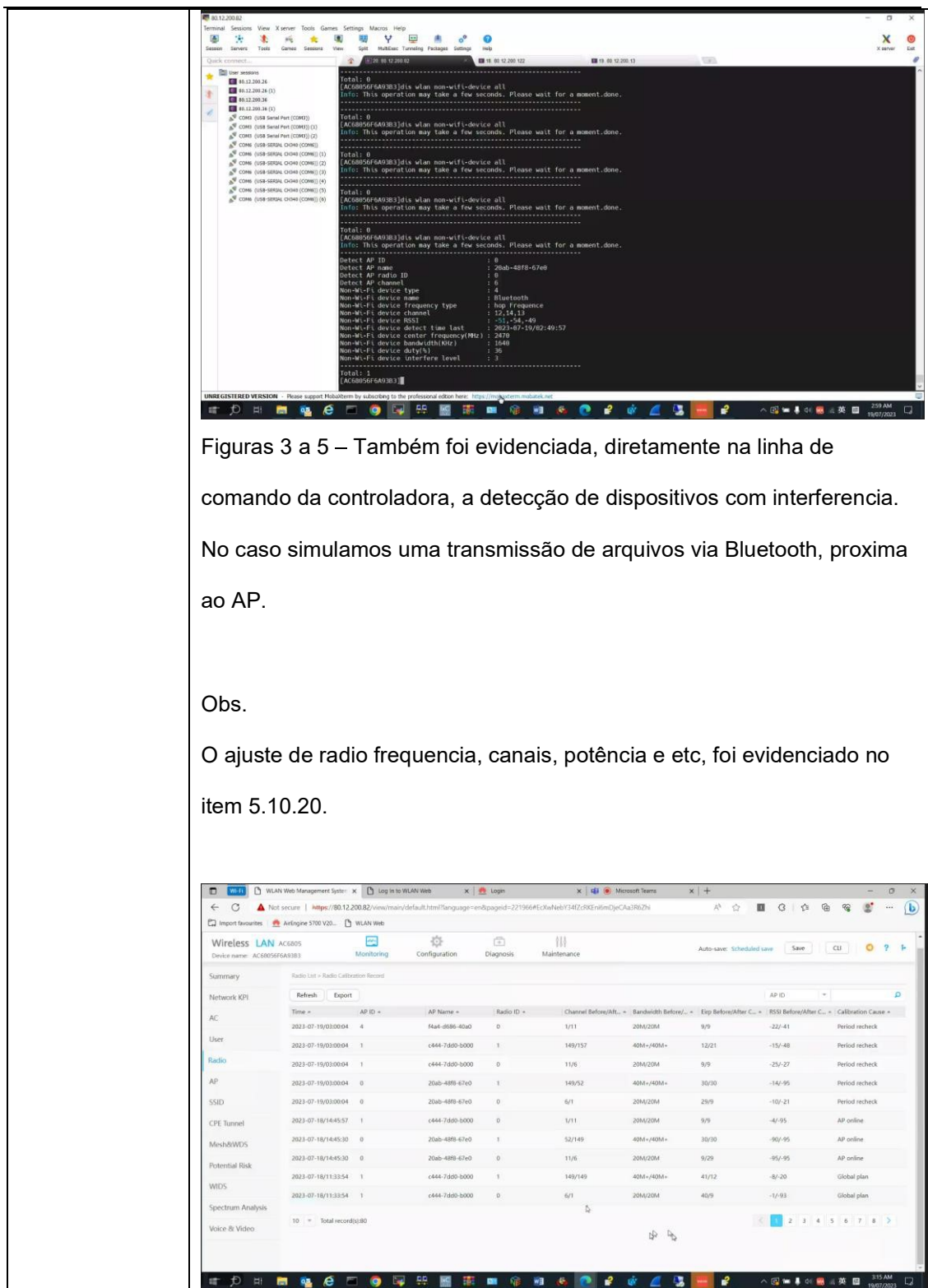



Figuras 1 e 2 – Nas configurações da controladora, habilitamos a opção “Scanning”, para que o AP seja utilizado com um sensor da rede sem fio. E também habilitamos a função de “Spectrum Analysis”.

**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 interferência. No caso simulamos uma transmissão de arquivos via Bluetooth, próxima ao AP.

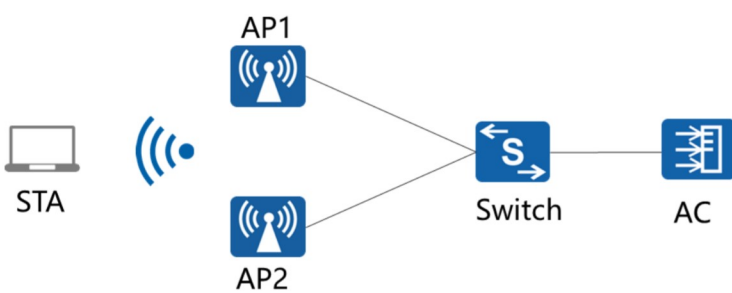
Obs.  
O ajuste de radio frequência, canais, potência e etc, foi evidenciado no item 5.10.20.



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

	Calibração de rádio – item 5.10.20
--	------------------------------------

**Balanceamento de carga dinâmico por sessão.**

<b>Item de teste</b>	<b>Balanceamento de carga dinâmico por sessão.</b>
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta session based dynamic load balancing – Balanceamento de carga dinâmico por sessão.
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure a ac corretamente,</li> <li>2) Habilite Dynamic load balancing function na AC,</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Balanceamento de dispositivos entre pontos de acesso</li> </ol>

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

Resultado

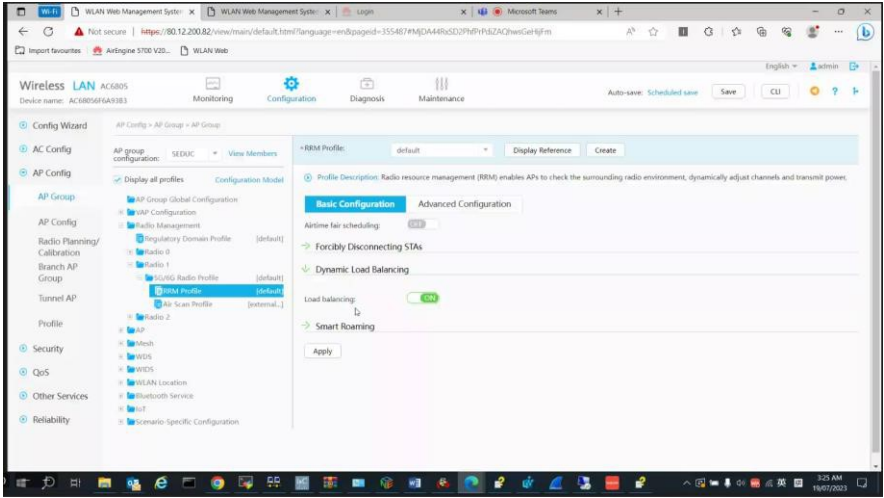


Figura 1 – Nas configurações da AC, outra opção habilitada foi a “Dynamic Load Balancing (balanceamento de carga dinâmico).”

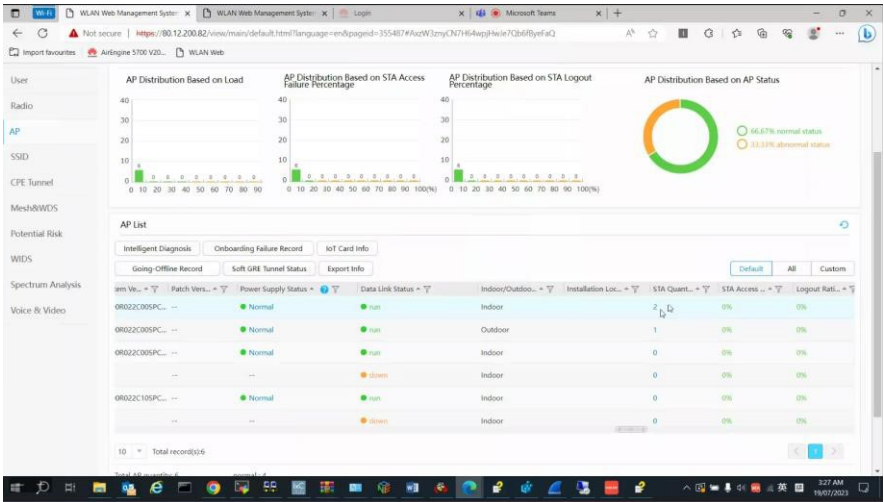


Figura 2 – Na listagem dos APs utilizados no ambiente de teste, podemos ver que existem 3 dispositivos sem fio conectados, sendo que 2 estão em um AP e 1 em outro AP.

```

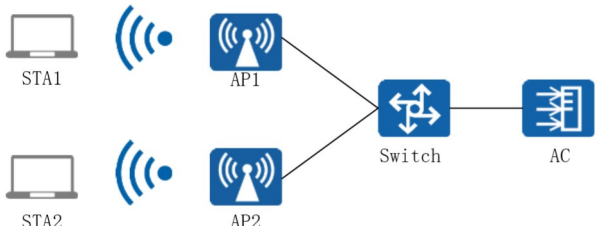
Total: 2
[AC6805-B2-02-200,82-SEDOC-tianwei-wlan-radio-0/1]dis ap all
Total AP information:
nor : normal [2]
ExtraInfo : Extra information
-----
ID      MAC          Name          Group  IP          Type          State  STA  Uptime      ExtraInfo
-----
0       20ab-48f8-67e0 20ab-48f8-67e0 default 189.180.216.45 AirEngine5761-11 nor 3    18h:47m:41s -
1       c444-7dd0-b000 c444-7dd0-b000 default 189.180.216.40 AirEngine6760R-51 nor 3    18h:47m:38s -
-----
Total: 2
[AC6805-B2-02-200,82-SEDOC-tianwei-wlan-radio-0/1]dis stat
[AC6805-B2-02-200,82-SEDOC-tianwei-wlan-radio-0/1]dis station a
[AC6805-B2-02-200,82-SEDOC-tianwei-wlan-radio-0/1]dis station all
    
```

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

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

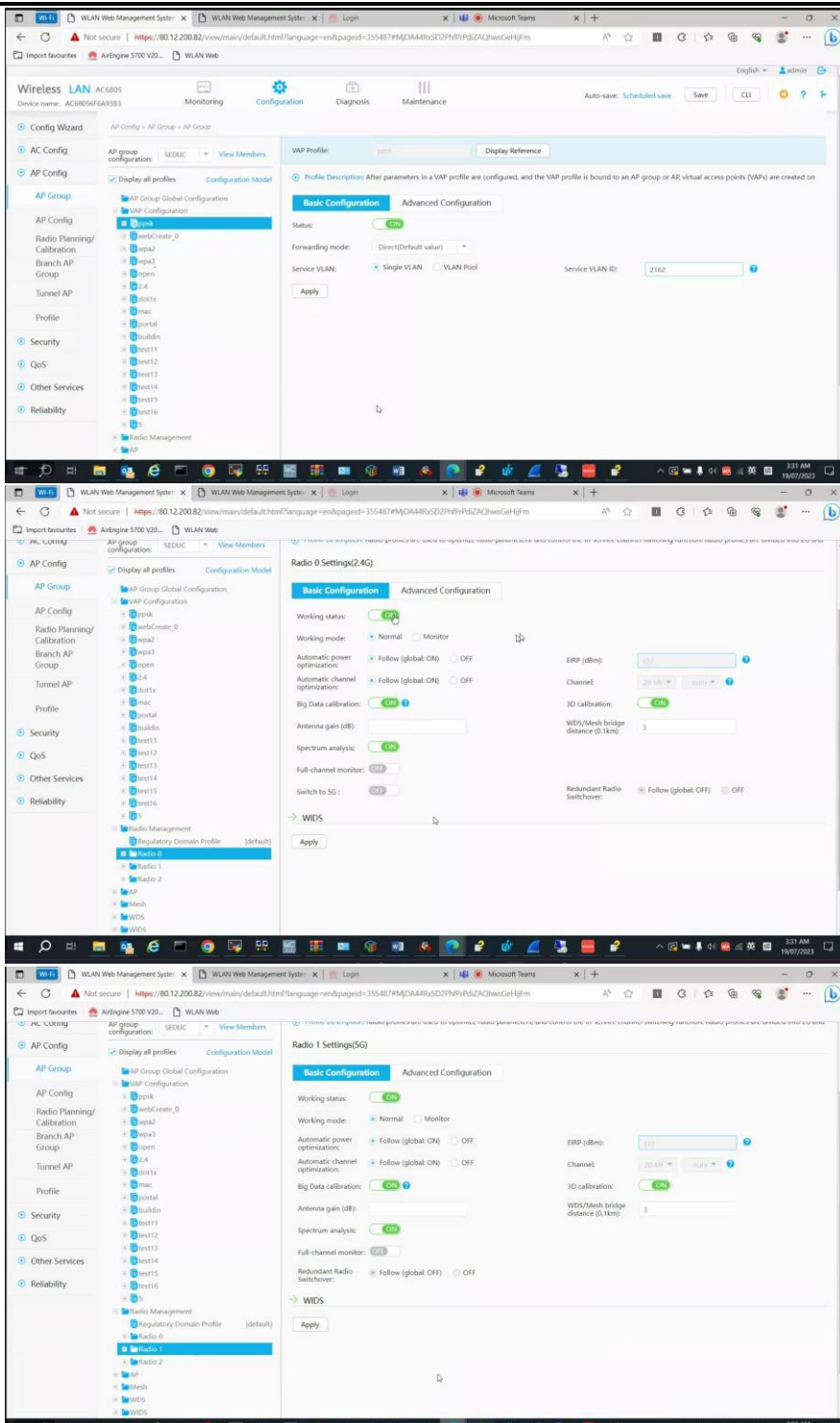
**Desabilitando o serviço sem fio.**

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

<b>Item de teste</b>	<b>Desabilitando o serviço sem fio.</b>
<b>Objetivo do teste</b>	Validar que o sistema suporta shutdown do serviço Wireless em um ou mais AP's
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configure a AC corretamente,</li> <li>2) Desabilitar todos os radios dos AP na AC.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) O serviço WLAN do AP é desabilitado</li> </ol>

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

Resultado



The figure consists of three vertically stacked screenshots of the WLAN Web Management System interface. Each screenshot shows a configuration page for a specific radio or VAP profile. The left sidebar contains a navigation tree with categories like 'Config Wizard', 'AC Config', 'AP Config', 'Radio Planning/Calibration', 'Profile', 'Security', 'QoS', 'Other Services', and 'Reliability'. The main content area is divided into 'Basic Configuration' and 'Advanced Configuration' tabs. In the top screenshot, the 'VAP Profile' configuration is shown with 'Status' set to 'ON'. The middle screenshot shows 'Radio 0 Settings(2.4G)' with 'Working status' set to 'OFF'. The bottom screenshot shows 'Radio 1 Settings(5G)' with 'Working status' set to 'OFF'. In all cases, the 'Apply' button is visible at the bottom of the configuration panel.

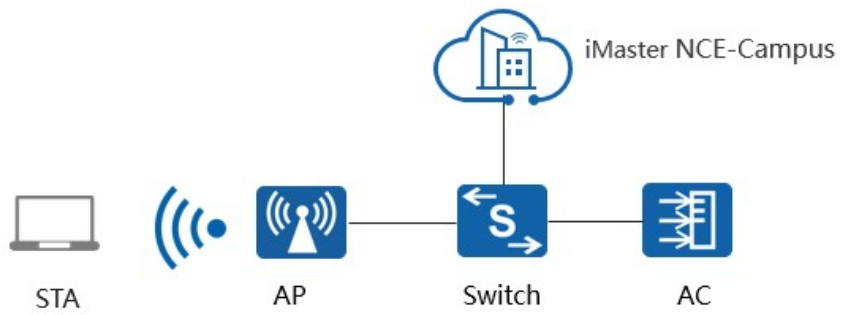
Figuras 1 a 3 – Na controladora, no VAP Configuration, podemos manter o AP operacional e desabilitar apenas o serviço do radio escolhido.

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

	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;

<b>Item de teste</b>	Autenticação via MAC
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Autenticação via MAC
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>The diagram illustrates a network topology for WLAN authentication. It includes a STA (Station) represented by a laptop icon, an AP (Access Point) represented by a wireless antenna icon, a Switch represented by a square with an 'S' and arrows, and an AC (Access Controller) represented by a server rack icon. The AP is connected to the Switch, and the Switch is connected to the AC. The AC is connected to a cloud icon labeled 'iMaster NCE-Campus'.</p> <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	1) Configure a autenticação via MAC para a rede WLAN
<b>Resultado esperado</b>	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**

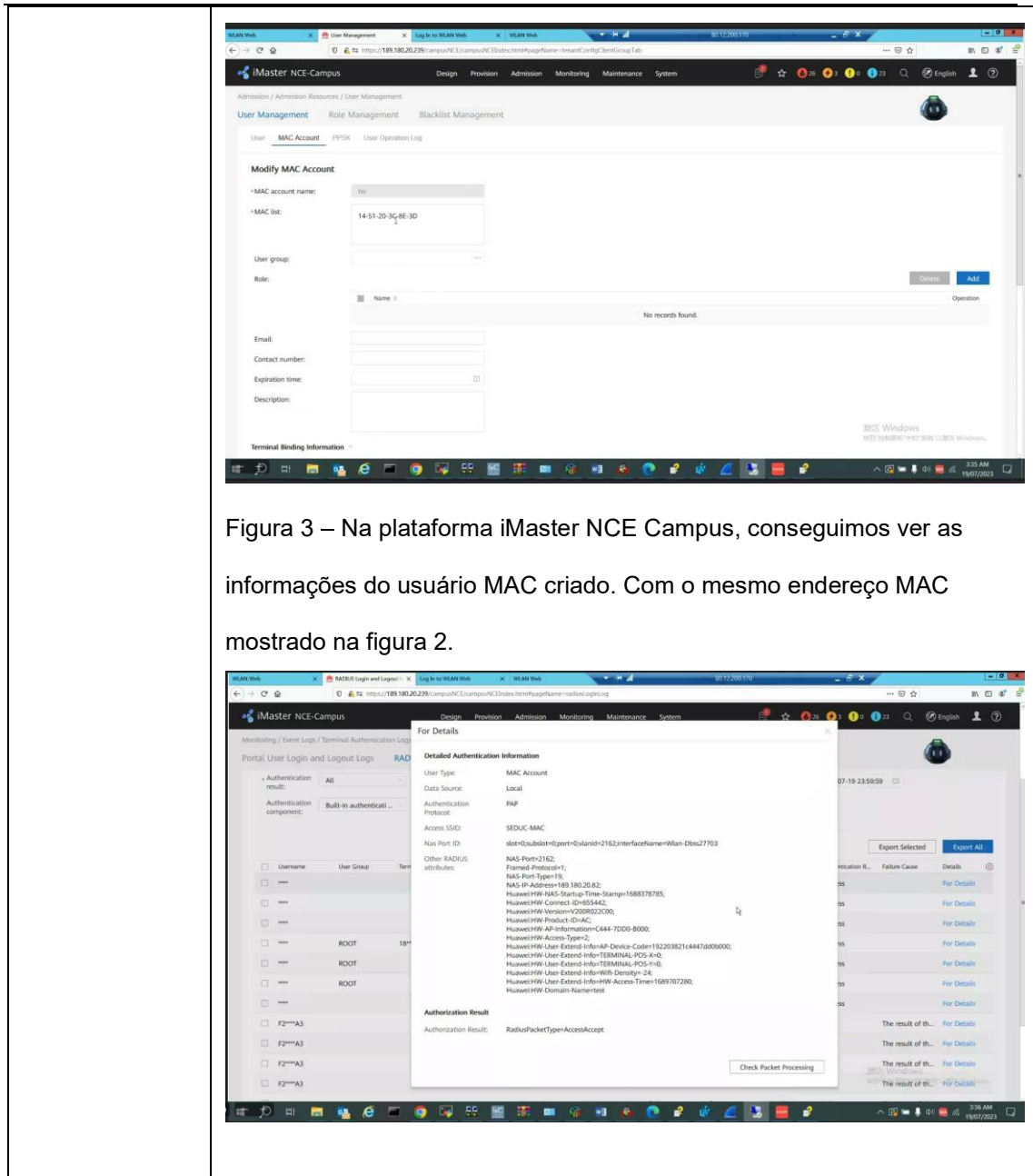


Figura 3 – Na plataforma iMaster NCE Campus, conseguimos ver as informações do usuário MAC criado. Com o mesmo endereço MAC mostrado na figura 2.

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

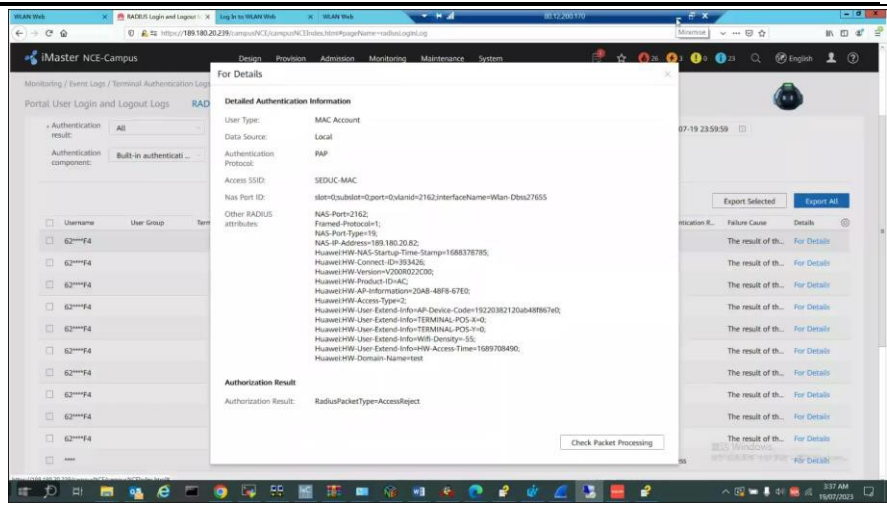


Figura 4 e 5 – Nos logs de autenticação Radius, também conseguimos validar todo o pacote com as informações da autenticação via MAC.

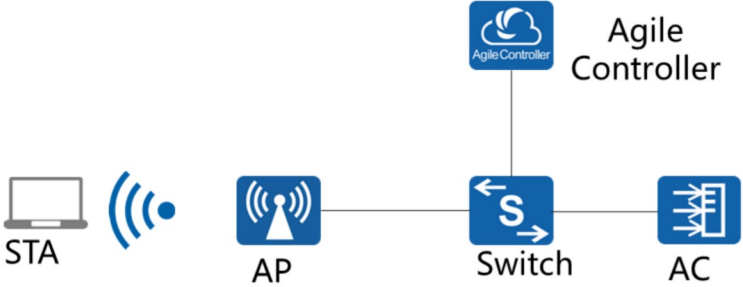
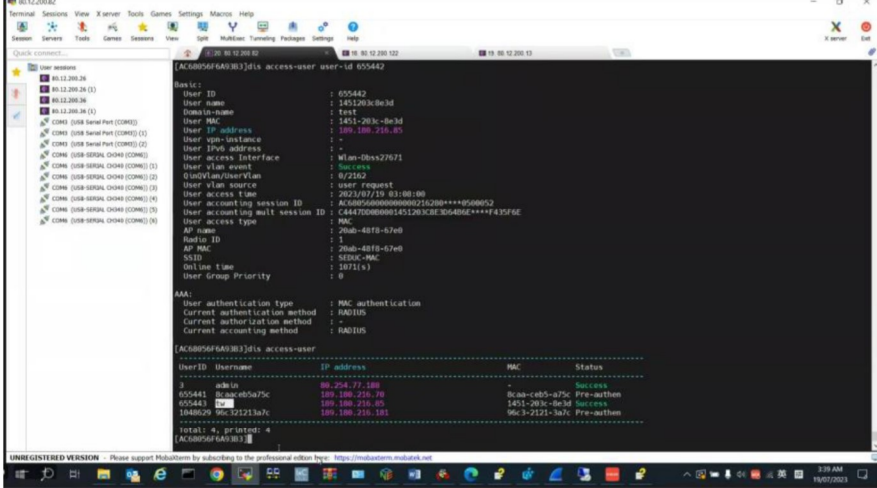
### Autenticação via Portal (iMaster NCE-Campus como servidor de Portal)

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

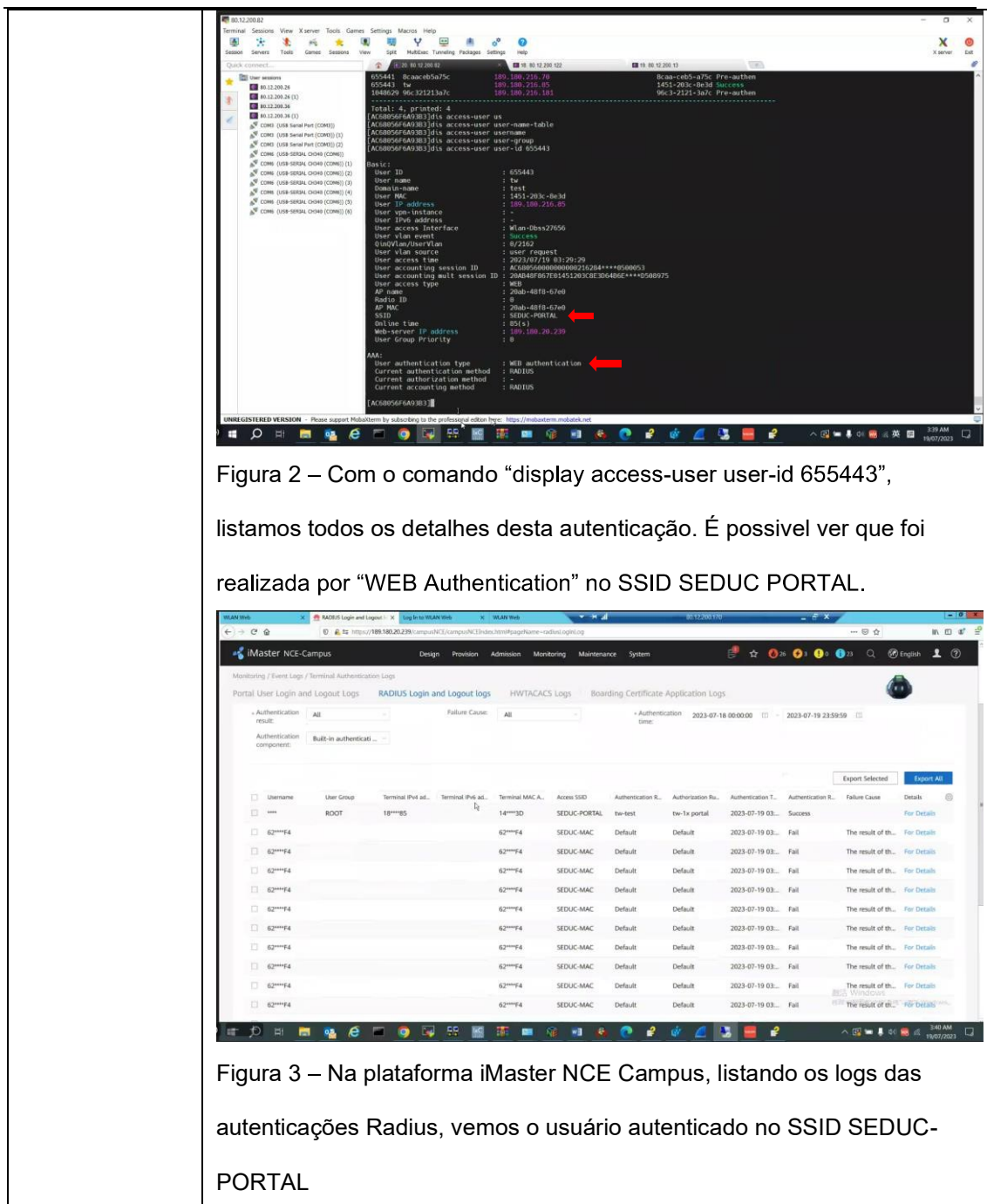
<b>Item de teste</b>	<b>Portal Autenticação</b>
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Portal Autenticação
<b>Configuração de teste</b>	Topologia da rede:



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

	 <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<p align="center"><b>Procedimento de teste</b></p>	<ol style="list-style-type: none"> <li>1) Configure a autenticação via Portal para a rede WLAN</li> </ol>
<p align="center"><b>Resultado esperado</b></p>	<ol style="list-style-type: none"> <li>1) O dispositivo cliente (STA1) se conecta e se autentica via Portal Authentication.</li> </ol>
<p align="center"><b>Resultado</b></p>	 <p>Figura 1 – Listando novamente os usuários autenticados na controladora, temos o usuário “tw”, que foi utilizado para o teste.</p>

**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**

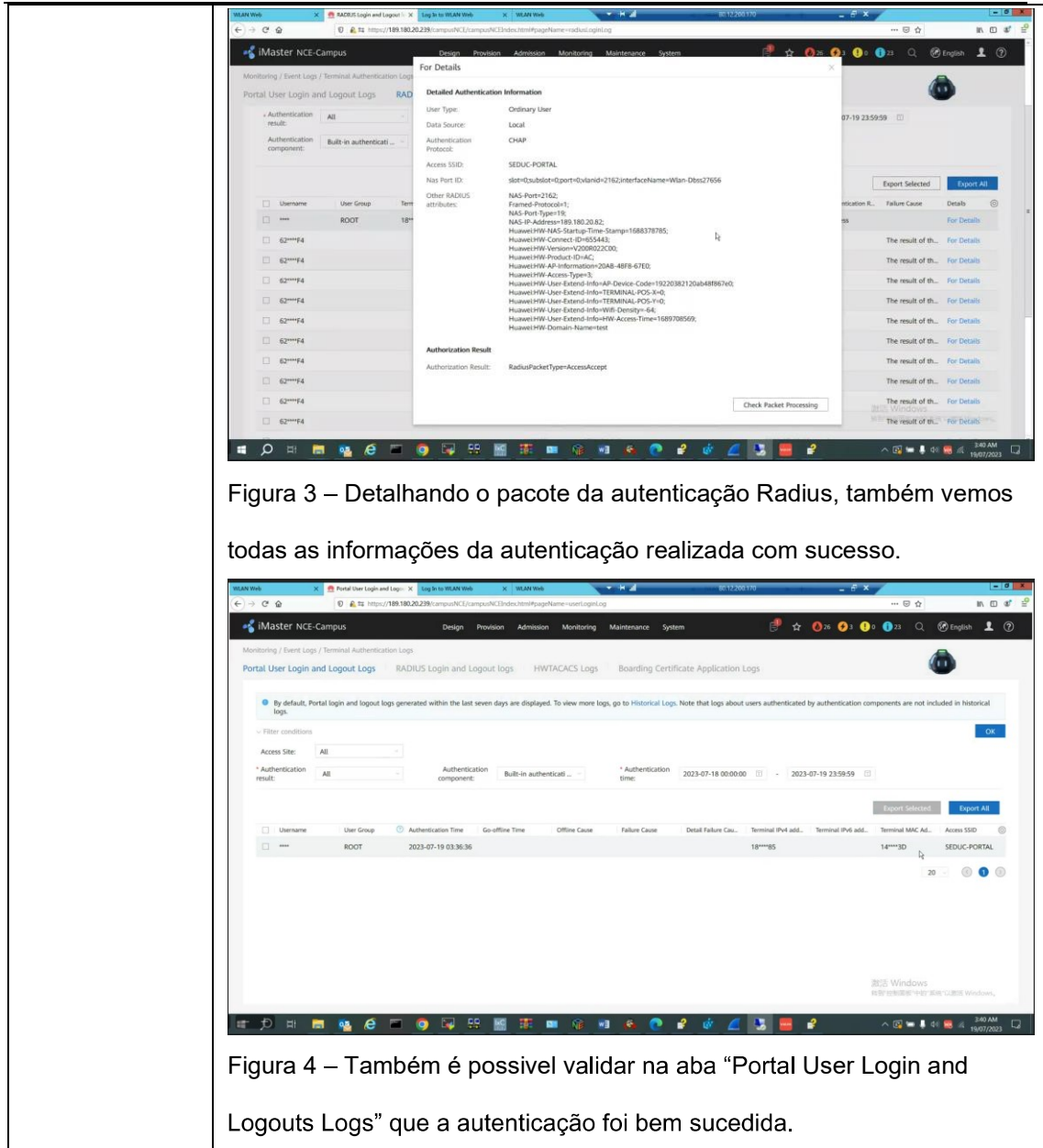


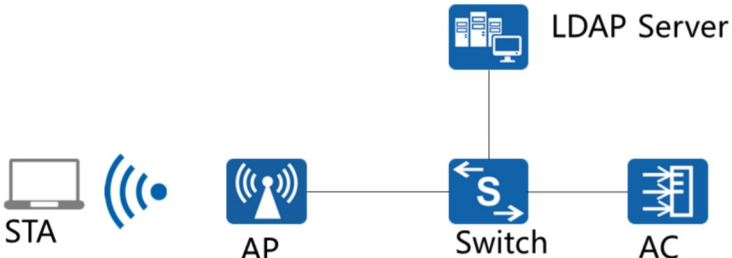
Figura 3 – Detalhando o pacote da autenticação Radius, também vemos todas as informações da autenticação realizada com sucesso.

Figura 4 – Também é possível 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;

<b>Item de teste</b>	Built-in Portal Authentication
<b>Objetivo do teste</b>	Validar que o Sistema WLAN suporta Autenticação e autorização via LDAP
<b>Configuração de teste</b>	<p>Topologia da rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	1) Configura a autenticação WEB com usuários de uma base LDAP
<b>Resultado esperado</b>	1) O dispositivo cliente (STA1) se conecta e se autentica via Portal Authentication.
<b>Resultado</b>	

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

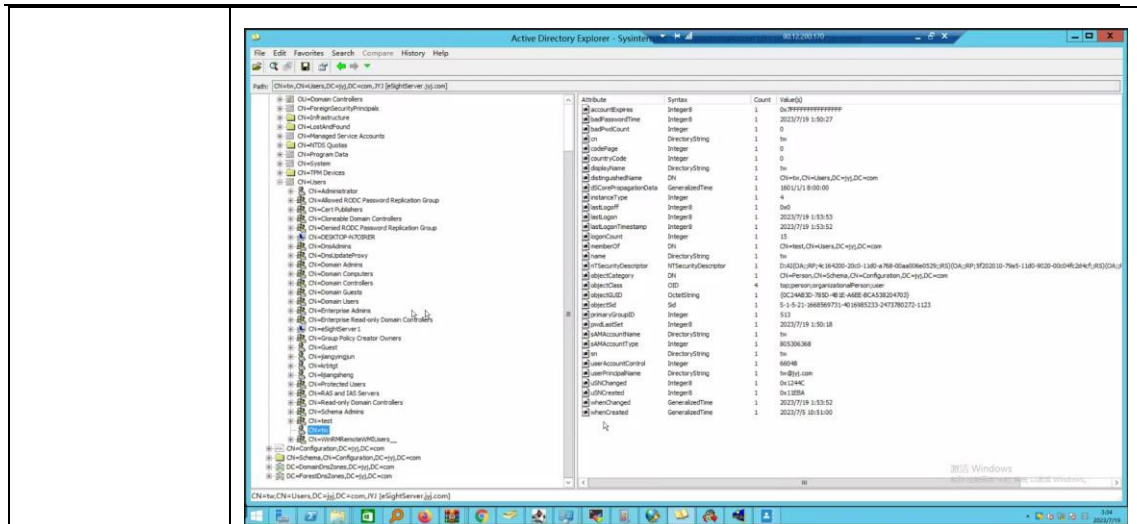


Figura 1 – Em um Active Directory do Windows Server, foi criado o usuário

“tw”

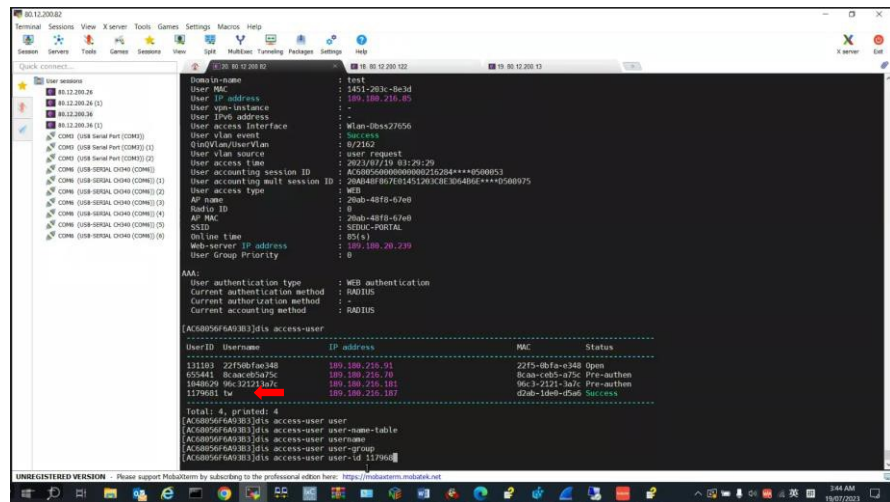
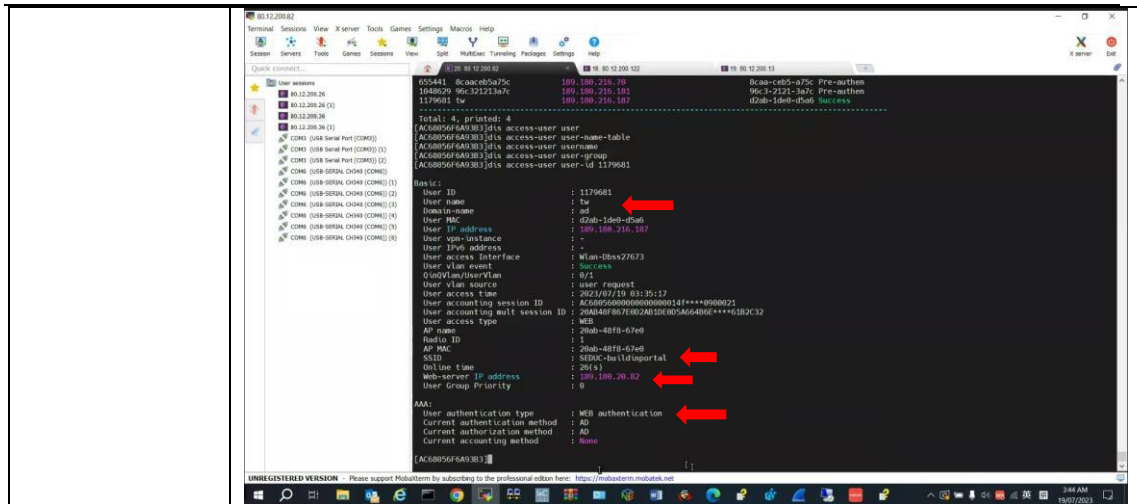


Figura 2 – Listando os usuários autenticados na controladora.

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



```

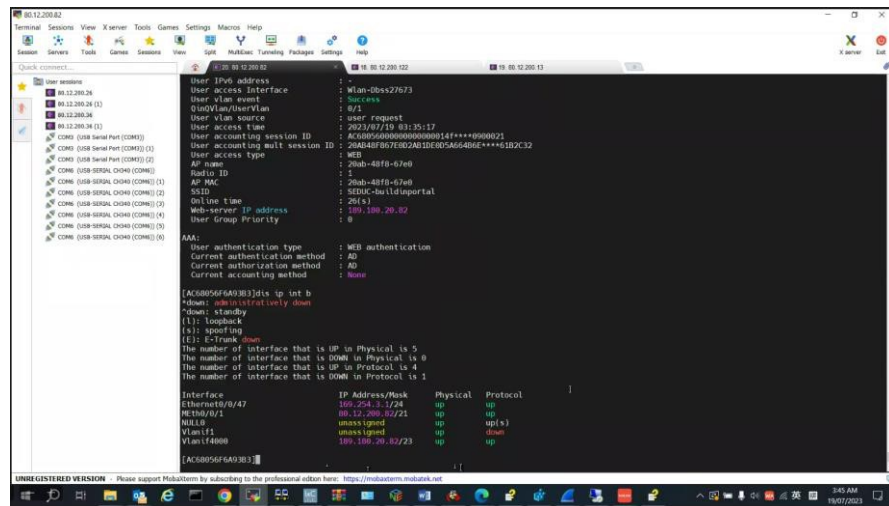
[AC@8056F6A0383]dis access-user user
[AC@8056F6A0383]dis access-user user-name-table
[AC@8056F6A0383]dis access-user username
[AC@8056F6A0383]dis access-user user-group
[AC@8056F6A0383]dis access-user user-id 1179681

Total: 4, preferred: 4
-----
User ID      : 1179681
User name    : tw
Domain name  : ad
User MAC     : 42ab-19e8-d5e8
User IP      : 189.189.216.187
User vpn-instance : -
User IPv6 address : -
User access interface : wlan-0bss27673
User vlan event : Success
User vlan source : 8/2
User access time : 2023/07/19 03:35:17
User accounting session ID : AC0895600000000000014****9908021
User accounting mult session ID : 20A048F807E0D2A01E005A56486E****61B2C32
User access type : WEB
AP name      : 29ab-48f8-67e8
Radio ID     : 1
AP MAC       : 29ab-48f8-67e8
SSID         : SEDUC-builddportal
OnLine time  : 29(s)
Web-server IP address : 189.189.20.82
User Group Priority : 0

AAA:
User authentication type : WEB authentication
Current authentication method : AD
Current authorization method : AD
Current accounting method : None

[AC@8056F6A0383]
    
```

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.



```

[AC@8056F6A0383]dis ip int br
#down: administratively down
#down: standby
(1): loopback
(1): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 9
The number of interface that is DOWN in Physical is 0
The number of interface that is UP in Protocol is 4
The number of interface that is DOWN in Protocol is 1

Interface      IP Address/Mask      Physical      Protocol
Ethernet0/0/47 189.204.1.1/24        up            up
Neth0/0/1      189.12.206.0/21       up            up
NULL0          unassigned            up            up(s)
Vlan11         unassigned            up            down
Vlan114600     189.189.20.82/23      up            up

[AC@8056F6A0383]
    
```

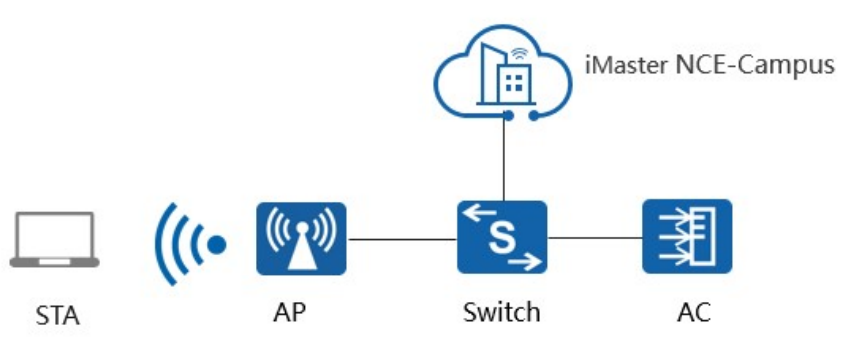
Figura 4 – O endereço do portal utilizado, é o mesmo da controladora.

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

### 802.1x Authentication Escape

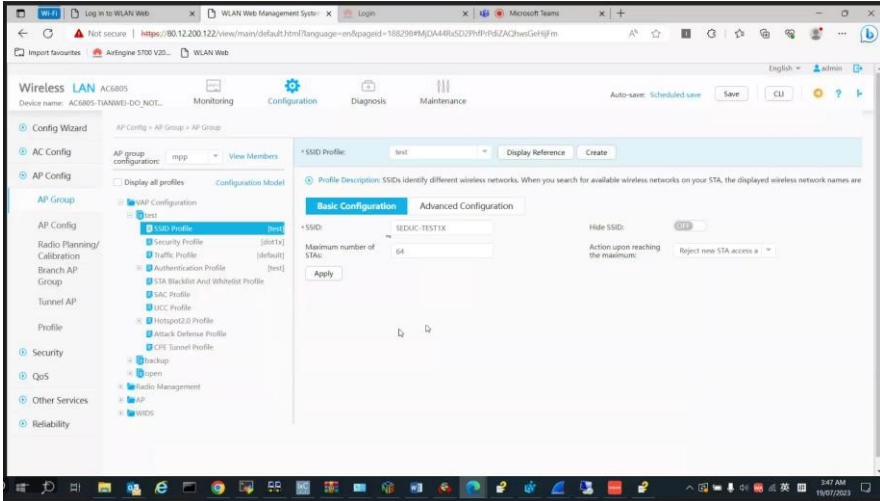
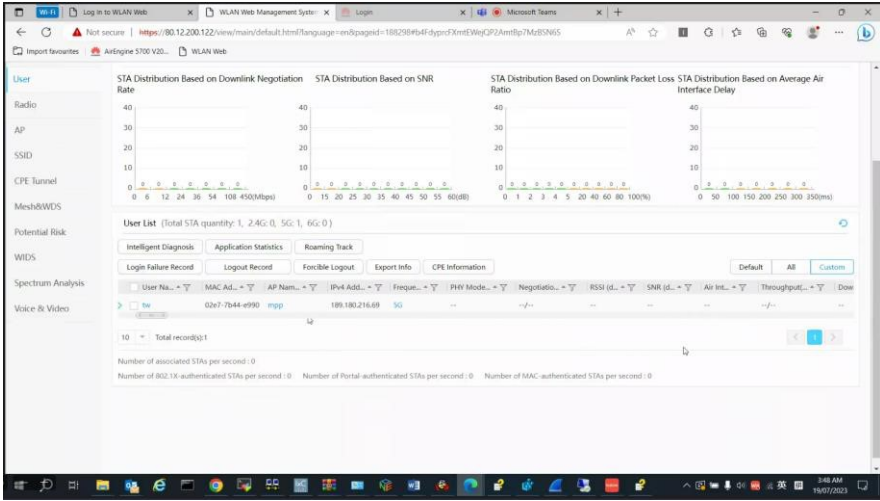

5.10.18 A falha de comunicação entre o sistema de Gerenciamento e os Pontos de Acesso não devem interferir na operação dos Pontos de Acesso;

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;

<b>Item de teste</b>	802.1x Authentication Escape
<b>Objetivo do teste</b>	Valida que o sistema WLAN suporta a função de Radius server backup
<b>Configuração de teste</b>	<p>Topologia da Rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Configurar as políticas de “escape” na controladora</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Propagação de SSIDs de backup quando os eventos ocorrerem</li> </ol>

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

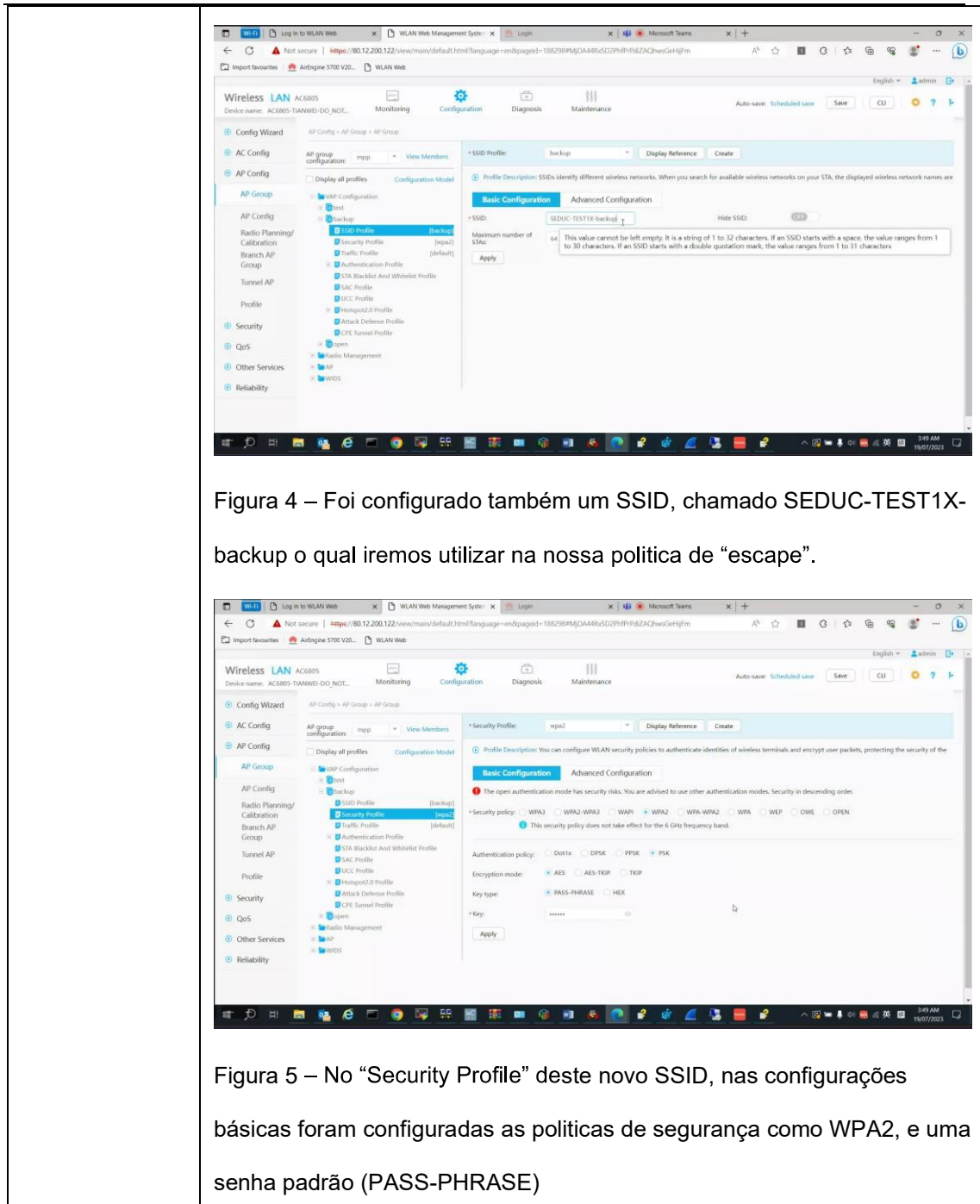
**Resultado**

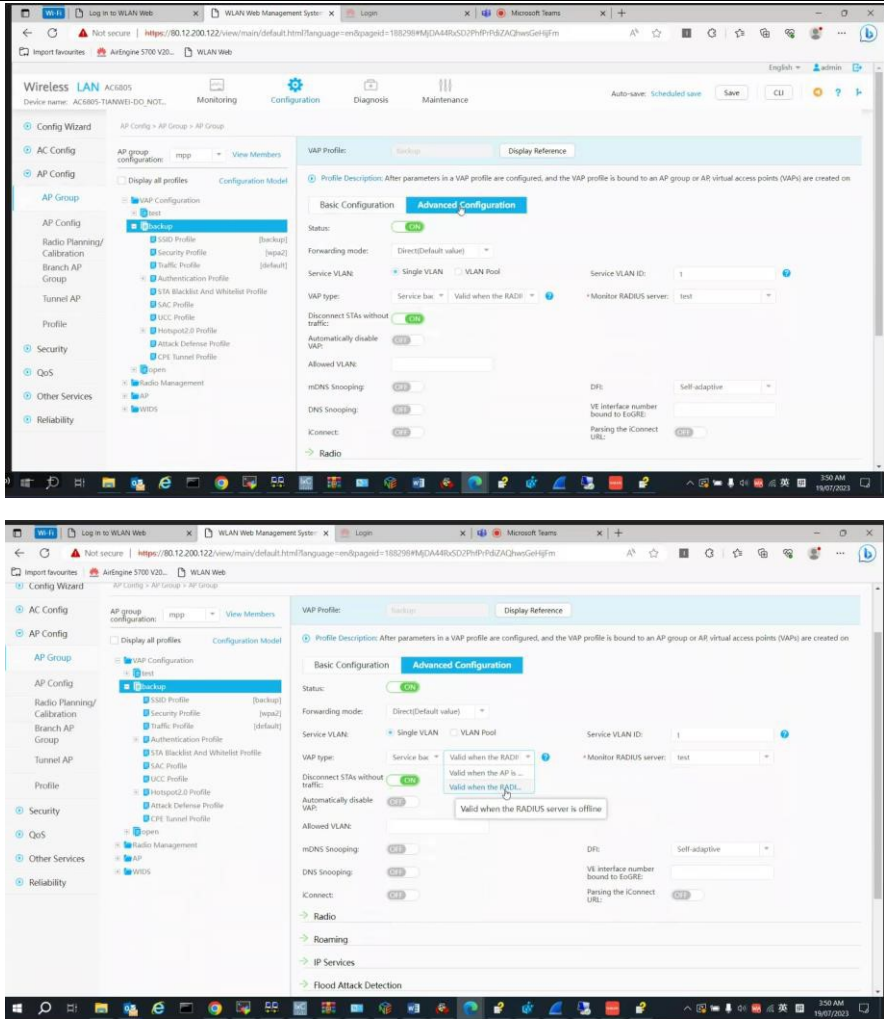
Figuras 1 a 3 – Na controladora, temos um SSID SEDUC-TEST1X, configurado e operando normalmente.



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

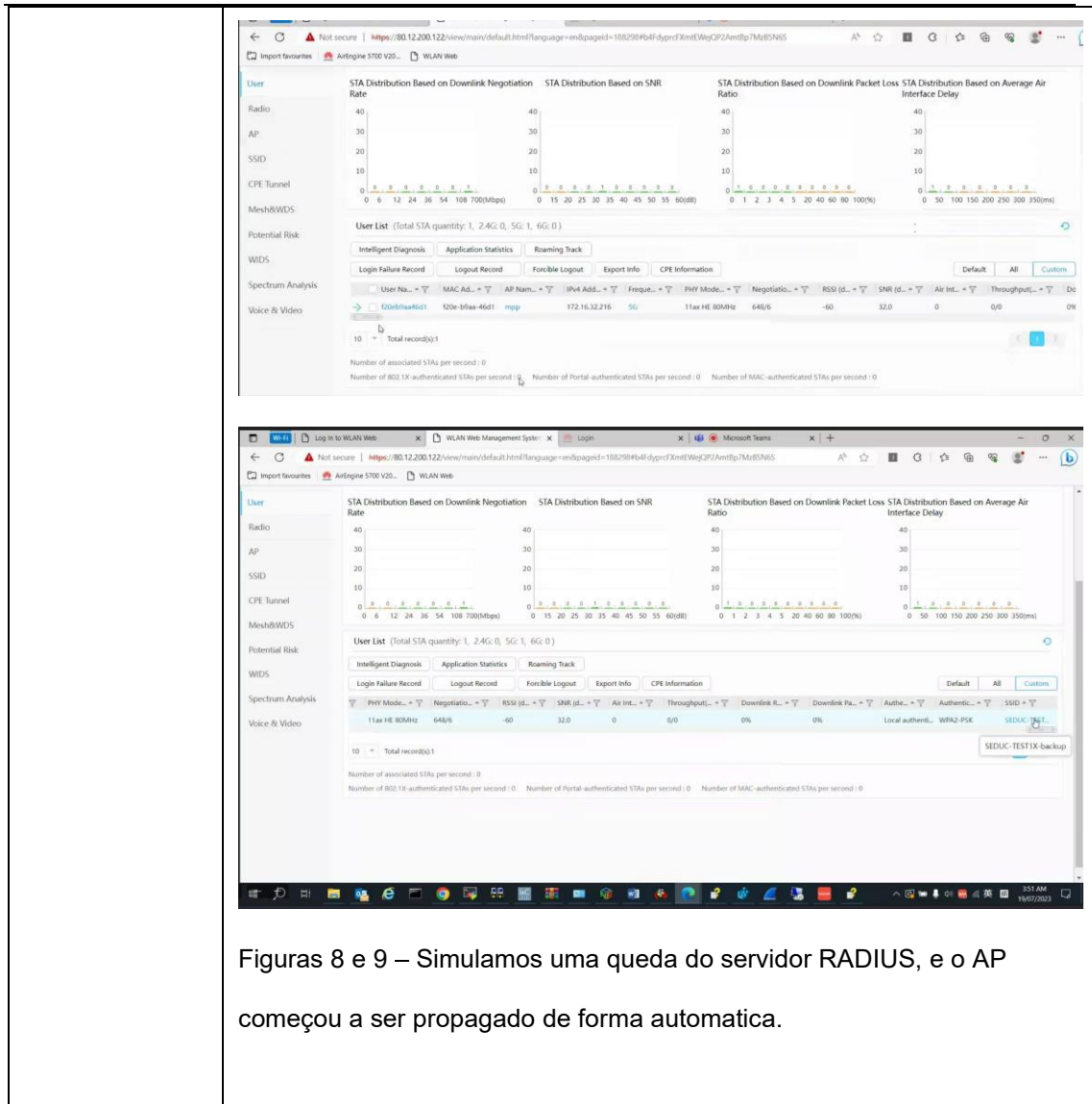


**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**



Figuras 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.

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



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

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

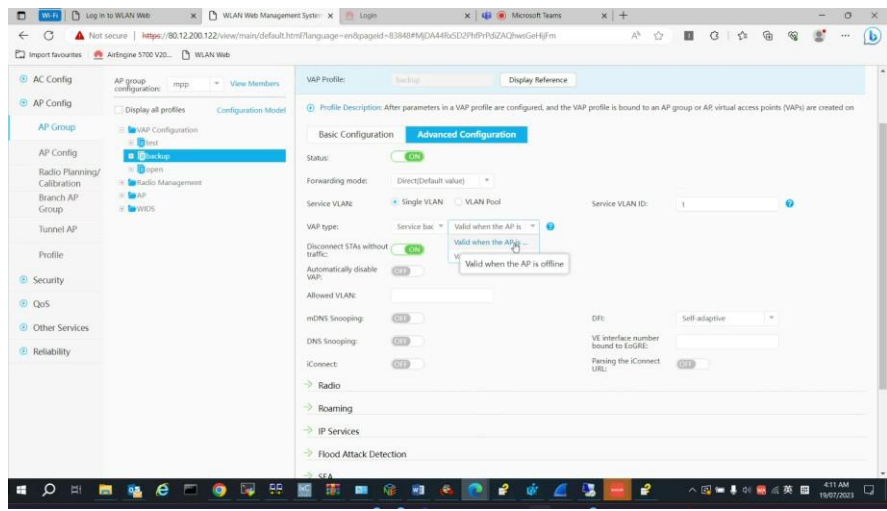
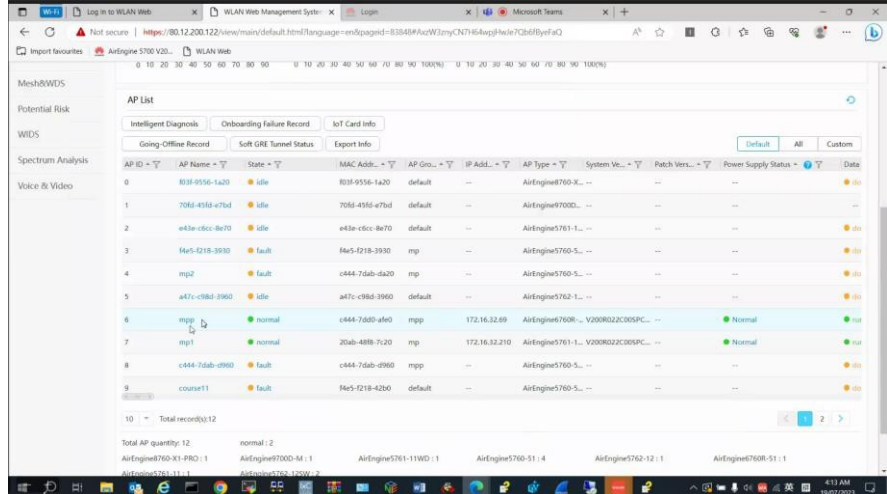


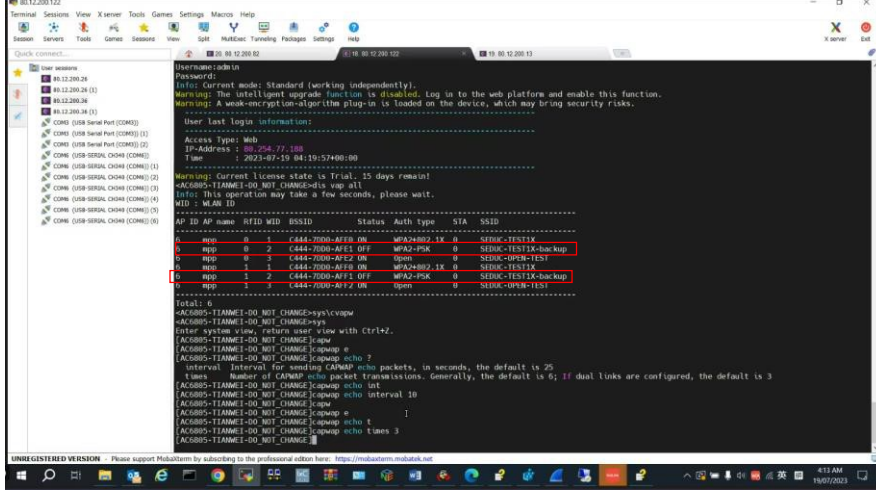
Figura 10 – Na segunda etapa, trocamos a condição de quando este SSID ficará operacional. Agora escolhemos a opção “Valid when the AP is offline”, ou seja, quando não houver conectividade entre controladora e AP.



AP ID	AP Name	State	MAC Addr.	AP Group	IP Addr.	AP Type	System Ver.	Patch Ver.	Power Supply Status
0	8038-9556-1a20	idle	8038-9556-1a20	default	---	AirEngine7600-S...	---	---	---
1	7064-4354-a75d	idle	7064-4354-a75d	default	---	AirEngine7600...	---	---	---
2	e43e-c8cc-8e70	idle	e43e-c8cc-8e70	default	---	AirEngine5761-1...	---	---	---
3	fa5-1218-9930	fault	fa5-1218-9930	mpp	---	AirEngine5760-S...	---	---	---
4	mp2	fault	c444-7dab-da20	mpp	---	AirEngine5760-S...	---	---	---
5	a47c-c98d-3960	idle	a47c-c98d-3960	default	---	AirEngine5762-1...	---	---	---
6	mpp2	normal	c444-7dab-a4e0	mpp	172.16.32.69	AirEngine760R... V200R022C05P...	---	---	Normal
7	mp1	normal	20ab-4889-7120	mpp	172.16.32.210	AirEngine5761-1... V200R022C05P...	---	---	Normal
8	c444-7dab-d960	fault	c444-7dab-d960	mpp	---	AirEngine5760-S...	---	---	---
9	course11	fault	fa5-1218-4260	default	---	AirEngine5760-S...	---	---	---

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

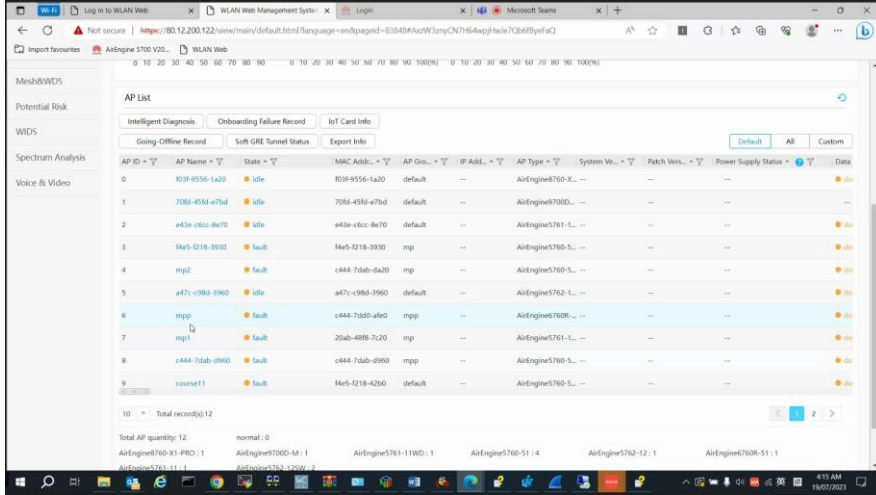
**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**



```

AC8885-TIAMEI-DO_M01_CHMGE>syslogwpa
AC8885-TIAMEI-DO_M01_CHMGE>sys
Enter system view, return user view with Ctrl+Z.
AC8885-TIAMEI-DO_M01_CHMGE>system-view
AC8885-TIAMEI-DO_M01_CHMGE>capwap e
AC8885-TIAMEI-DO_M01_CHMGE>capwap echo ?
Interval Interval for sending CAPWAP echo packets, in seconds, the default is 25
Times Number of CAPWAP echo packets. Transmissions. Generally, the default is 6; if dual links are configured, the default is 3
AC8885-TIAMEI-DO_M01_CHMGE>capwap echo int
AC8885-TIAMEI-DO_M01_CHMGE>capwap echo interval 10
AC8885-TIAMEI-DO_M01_CHMGE>capwap e
AC8885-TIAMEI-DO_M01_CHMGE>capwap echo t
AC8885-TIAMEI-DO_M01_CHMGE>capwap echo times 3
AC8885-TIAMEI-DO_M01_CHMGE>
    
```

Figura 12 – Listando os SSIDs, disponíveis 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.



AP ID	AP Name	State	MAC Addr.	AP Group	IP Addr.	AP Type	System Ver.	Patch Ver.	Power Supply Status	Data
0	803f-4556-1a2b	idle	803f-4556-1a2b	default	--	AirEngine760-XL	--	--	--	--
1	7084-4564-e7bd	idle	7084-4564-e7bd	default	--	AirEngine9700D	--	--	--	--
2	e43e-cfbc-8e7d	idle	e43e-cfbc-8e7d	default	--	AirEngine5761-L	--	--	--	--
3	84e5-d218-393d	fault	84e5-d218-393d	mpp	--	AirEngine5760-SL	--	--	--	--
4	mpp2	fault	c444-7dad-dab0	mpp	--	AirEngine5760-SL	--	--	--	--
5	e47c-c984-396d	idle	e47c-c984-396d	default	--	AirEngine5762-L	--	--	--	--
6	mpp	fault	c444-7dad-a6d0	mpp	--	AirEngine7608L	--	--	--	--
7	mpp1	fault	20ab-488b-7c2d	mpp	--	AirEngine5761-L	--	--	--	--
8	c444-7dad-d96d	fault	c444-7dad-d96d	mpp	--	AirEngine5760-SL	--	--	--	--
9	conner11	fault	84e5-d218-426d	default	--	AirEngine5760-SL	--	--	--	--
10	Total record(s):12									

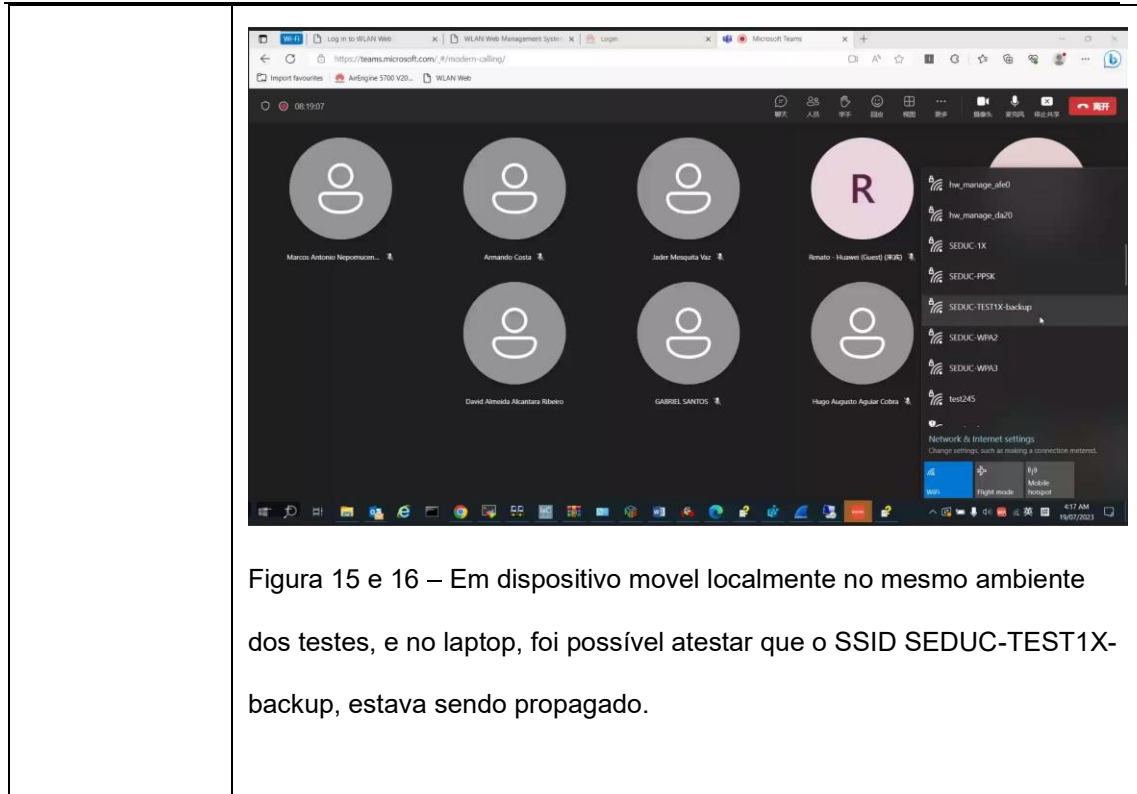
Figura 13 – Retornando a lista de APs disponíveis, verificamos que o AP ID 6, está com o status “fault”, ou seja, está offline.

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



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

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



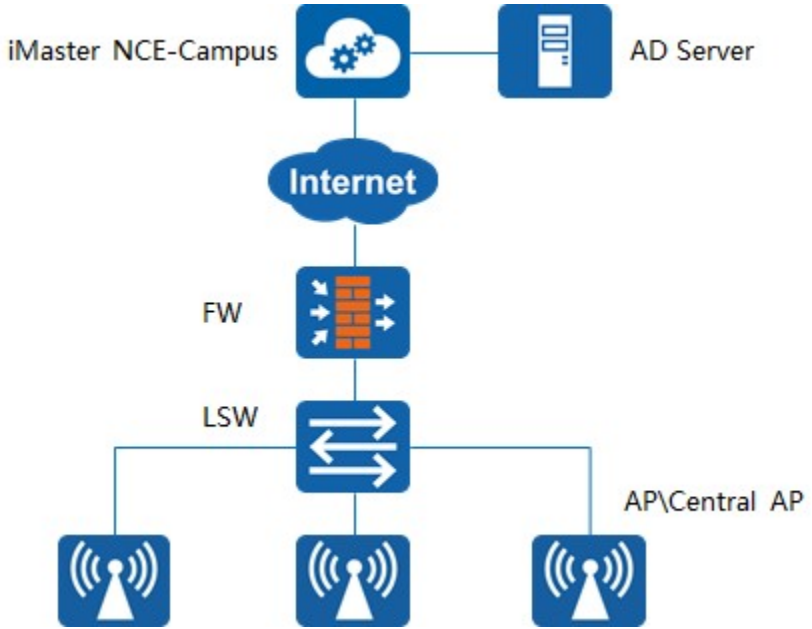
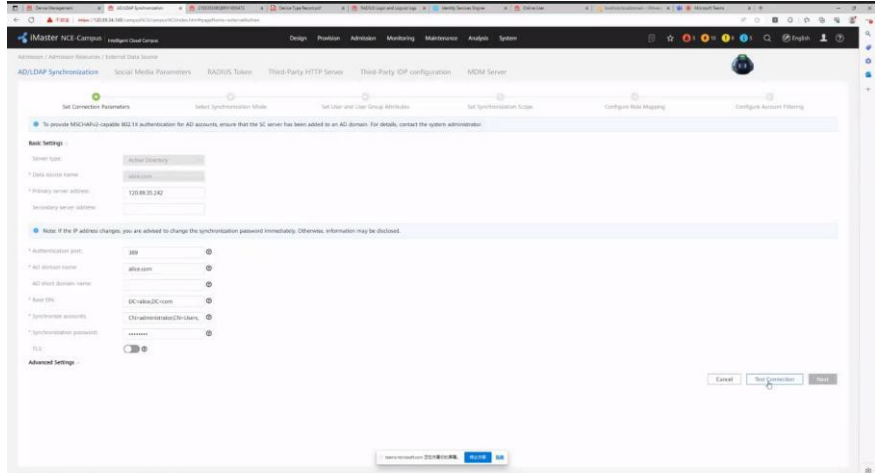
### Integração com domínio AD/LDAP para Autenticação

5.10.30 Implantar autenticação de usuários nas redes wireless por:

5.10.30.2 LDAP;

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

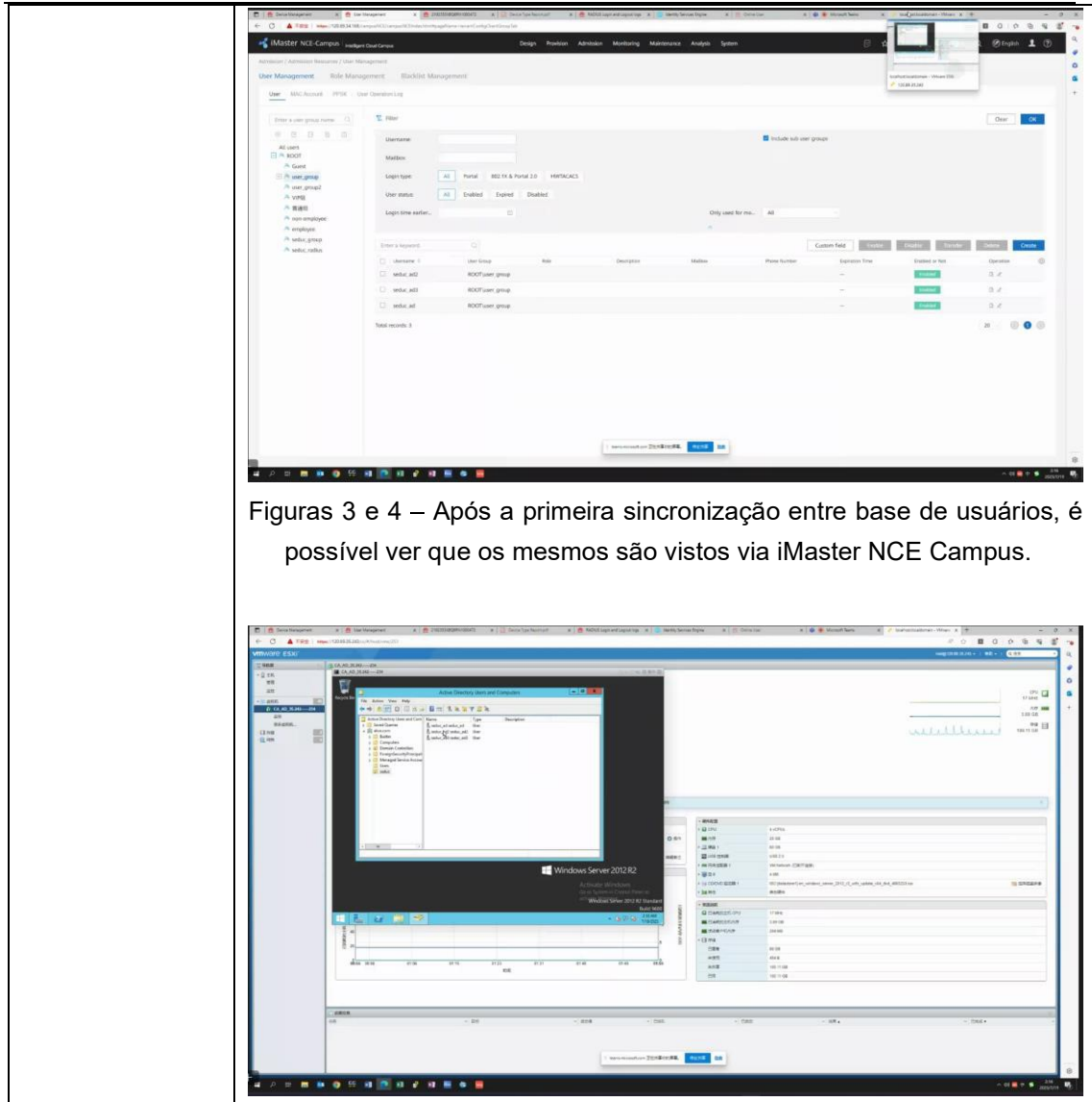
**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**

	 <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1) Integrar o AD/LDAP a plataforma iMaster NCE Campus</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>1) Sincronizar a base de usuários do AD/LDAP com o iMaster NCE Campus</li> </ol>
<b>Resultado</b>	

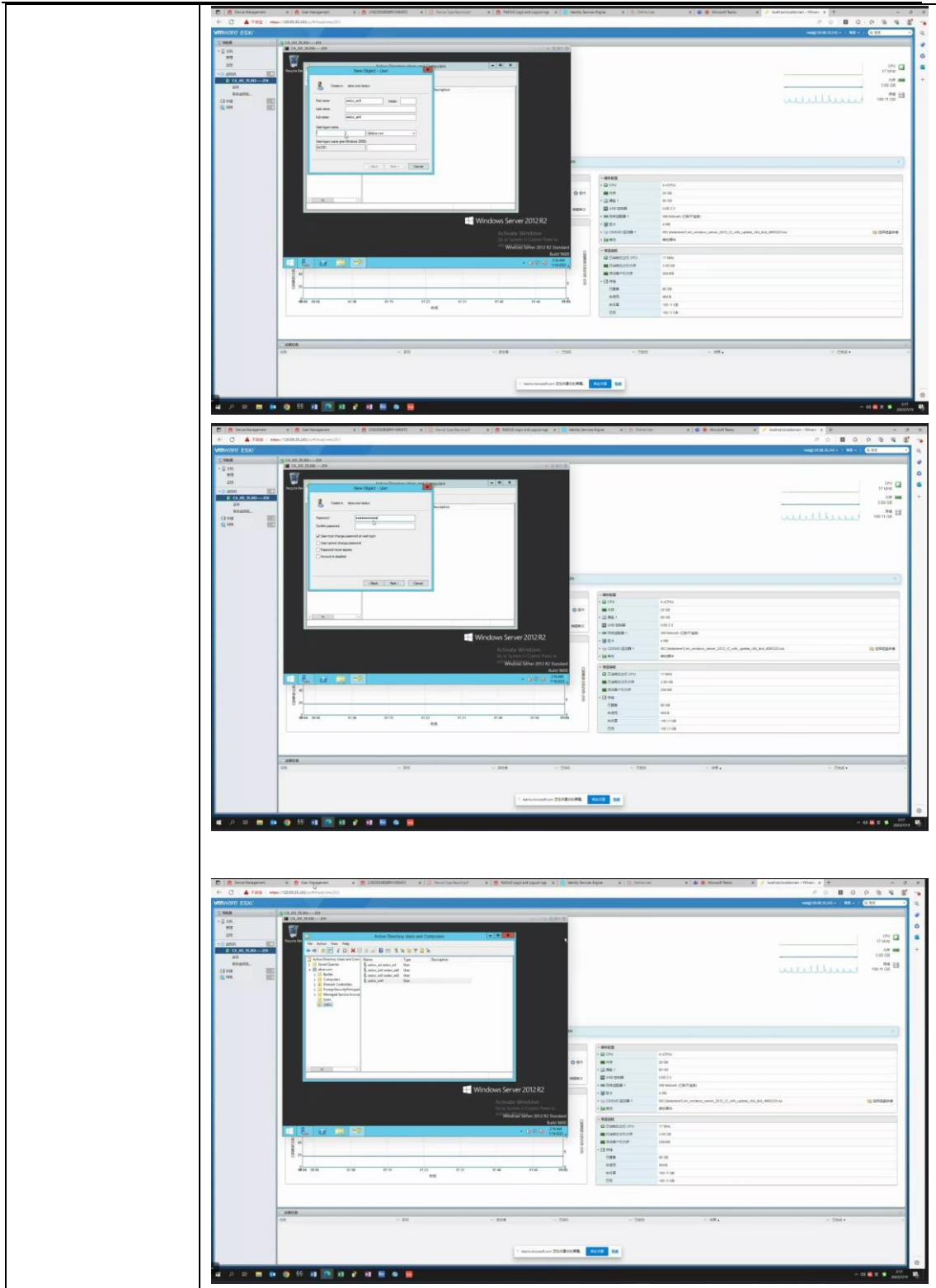




**PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO**  
**PROCESSO Nº 2020.0000.604.5301**  
**INTERESSADO: GERÊNCIA DE SUPORTE DE REDES**



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



**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”

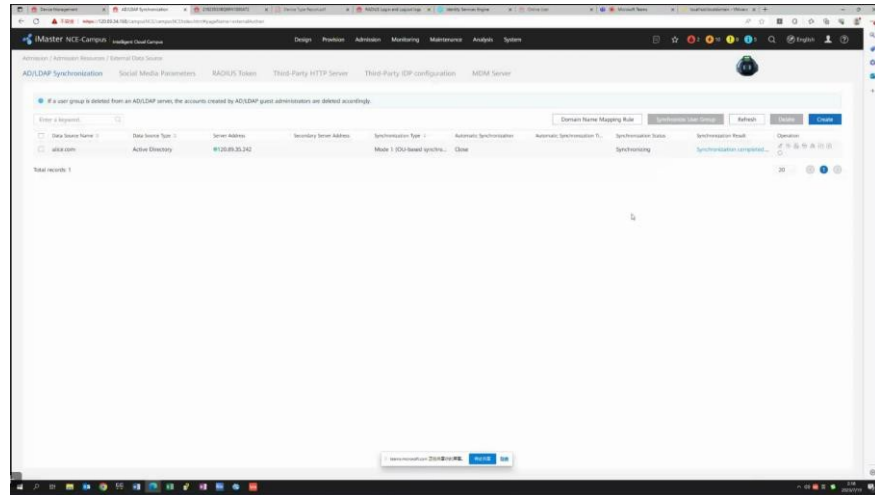


Figura 9 – Foi feita uma nova sincronização entre as bases de usuários.

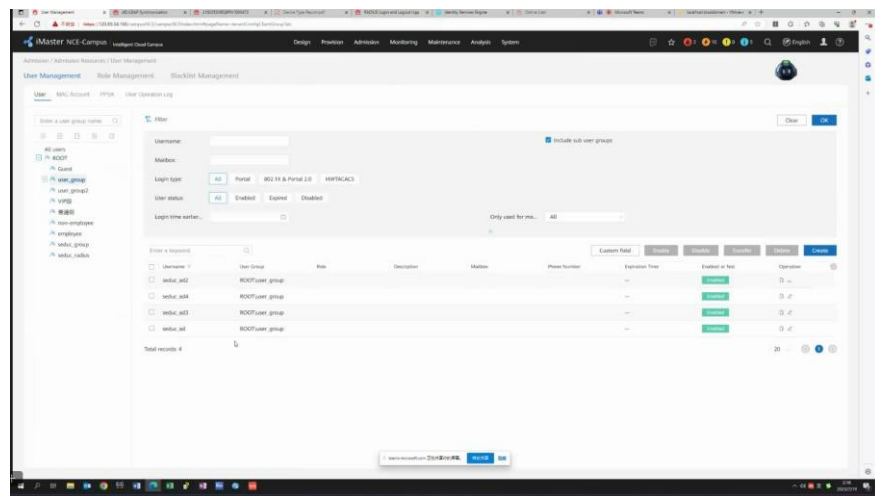


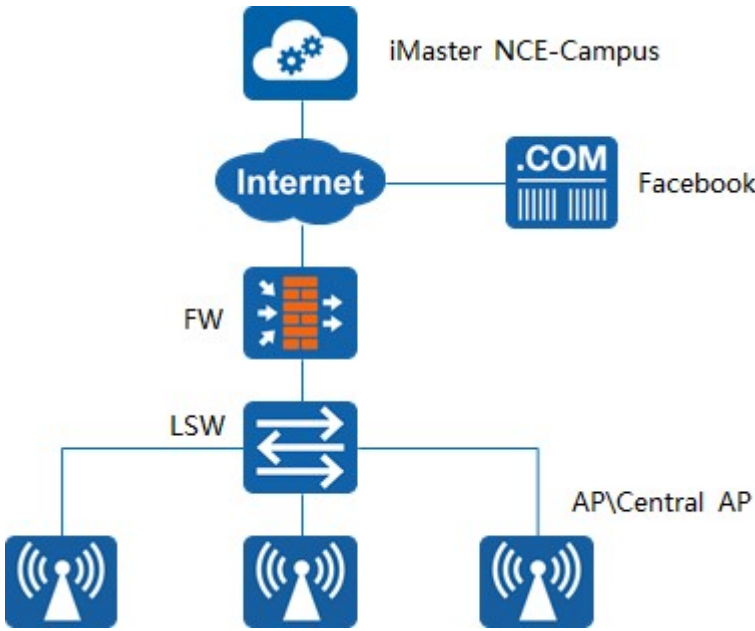
Figura 10 – O usuário “seduc\_ad4” passa a ser listado no iMaster NCE Campus.

## Facebook Authentication

5.10.30 Implantar autenticação de usuários nas redes wireless por:

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

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;

<b>Item de teste</b>	Autenticação via Facebook e Google
<b>Objetivo do teste</b>	Verificar se o CloudCampus da Huawei suporta funcionar como servidor de portal para fornecer autenticação do Facebook e Google para usuários Guest
<b>Configuração de teste</b>	<p>Topologia da Rede:</p>  <p>Condições iniciais:</p> <ol style="list-style-type: none"> <li>1) Todos os dispositivos funcionando normalmente</li> <li>2) Montar o ambiente de teste de acordo com a topologia acima</li> <li>3) Os parâmetros da conta facebook estão configurados corretamente.</li> </ol>
<b>Procedimento de teste</b>	1) Configurar os parâmetros de autenticação via mídia social
<b>Resultado esperado</b>	1) O terminal móvel pode acessar a rede através de autenticação via Facebook e Google;
<b>Resultado</b>	

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

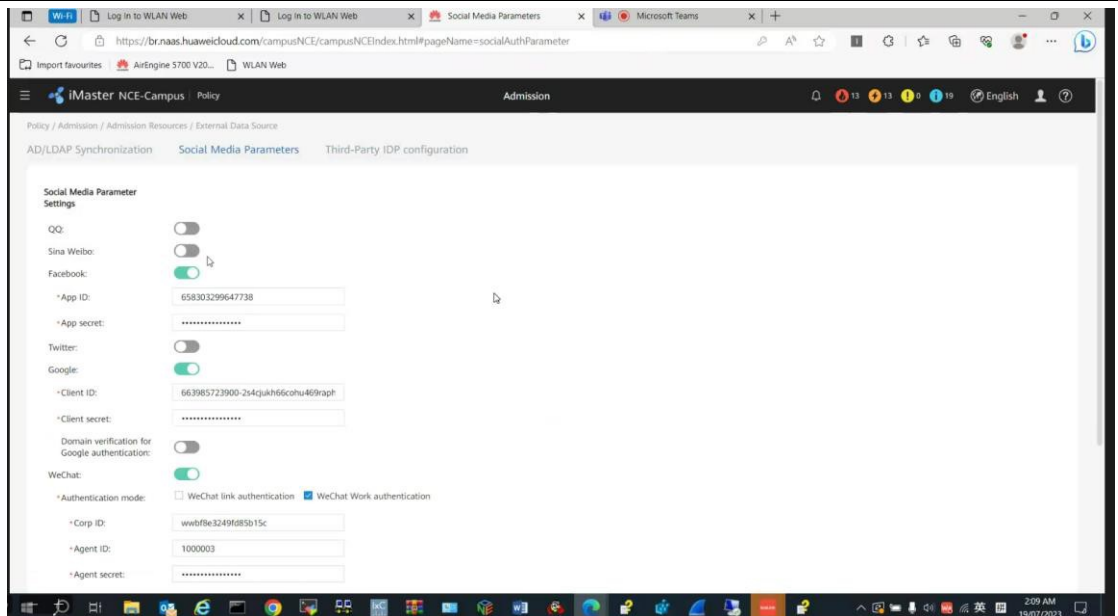


Figura 1 – Configurações para autenticação via redes sociais, onde estão configurados os dados para Facebook e Google.

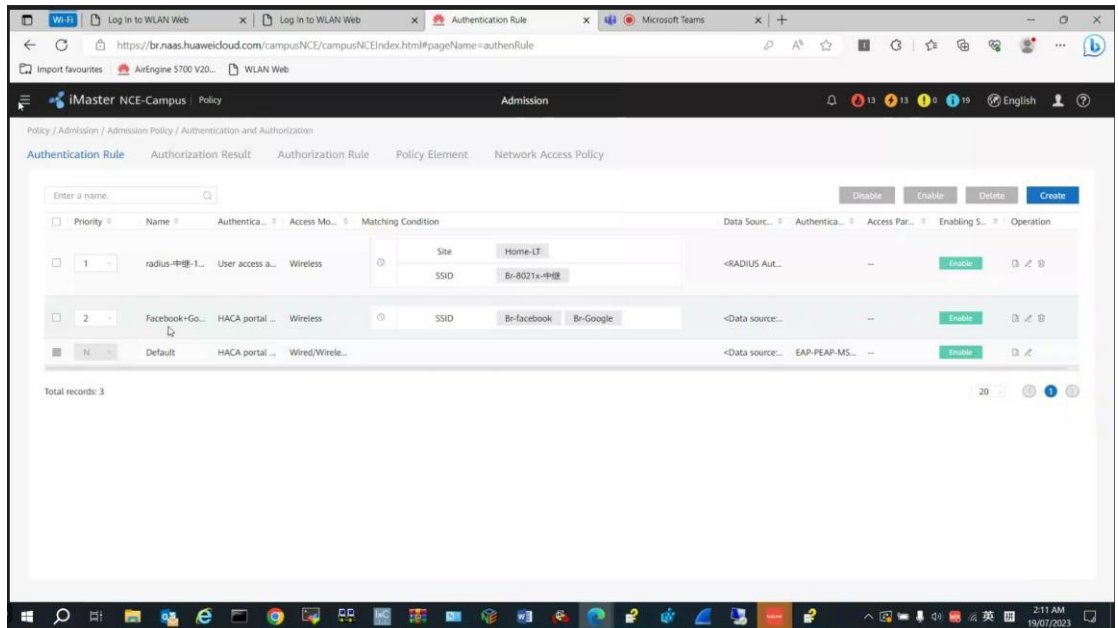
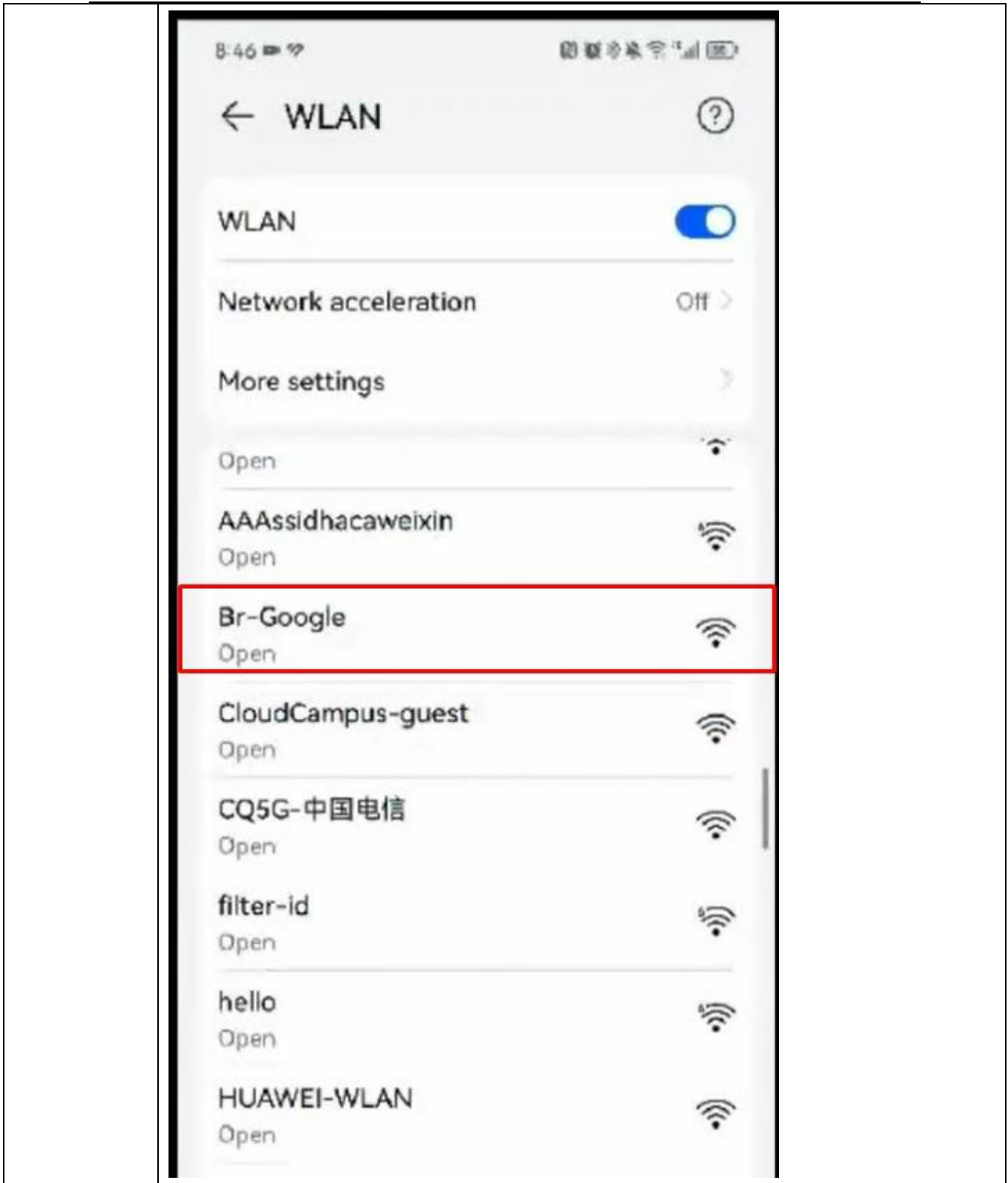


Figura 2 – Dentro das configurações de AAA, vemos as regras de autenticação tanto para Facebook quanto para Google, com os SSIDS Br-facebook e Br-Google

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

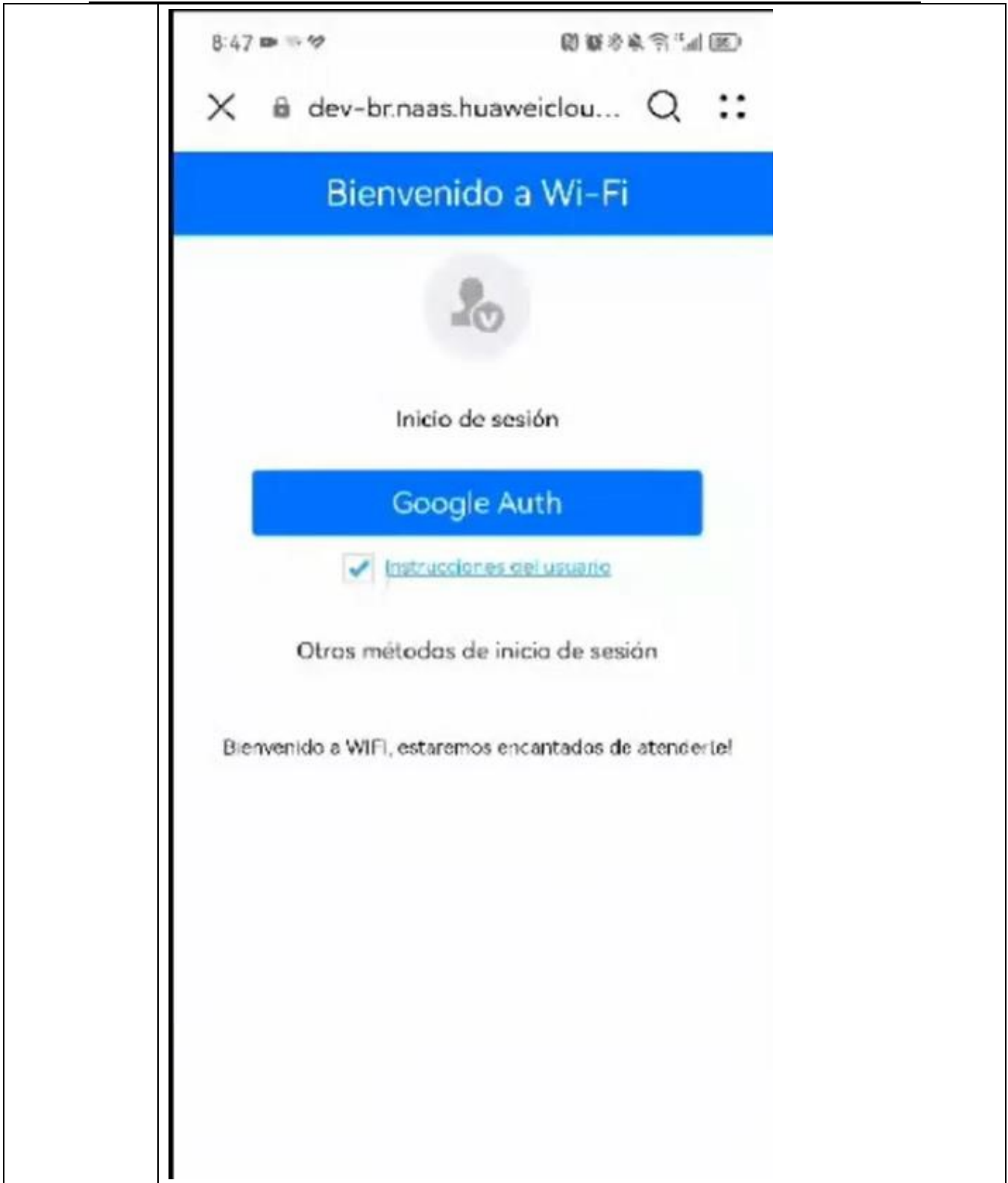


PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

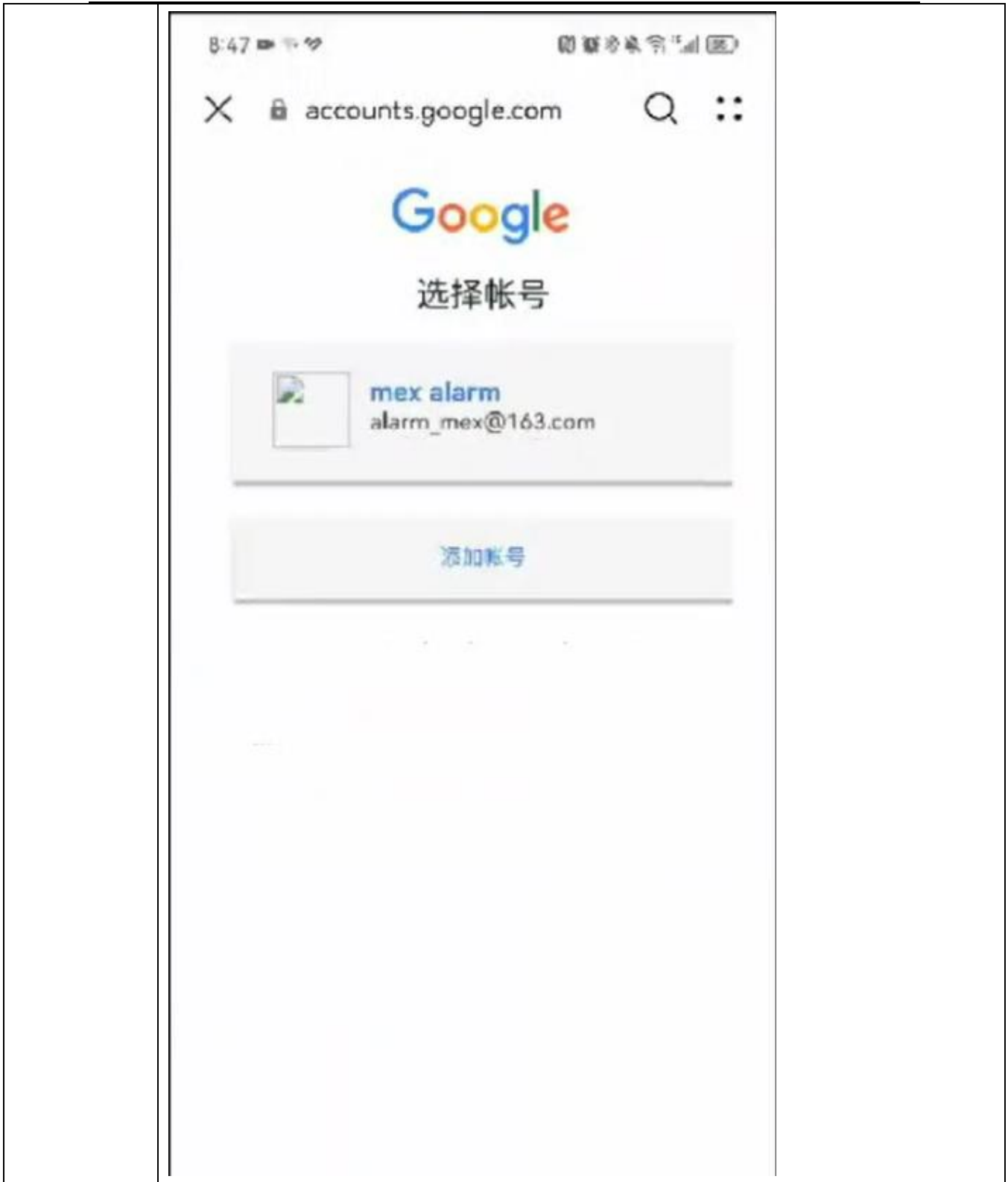




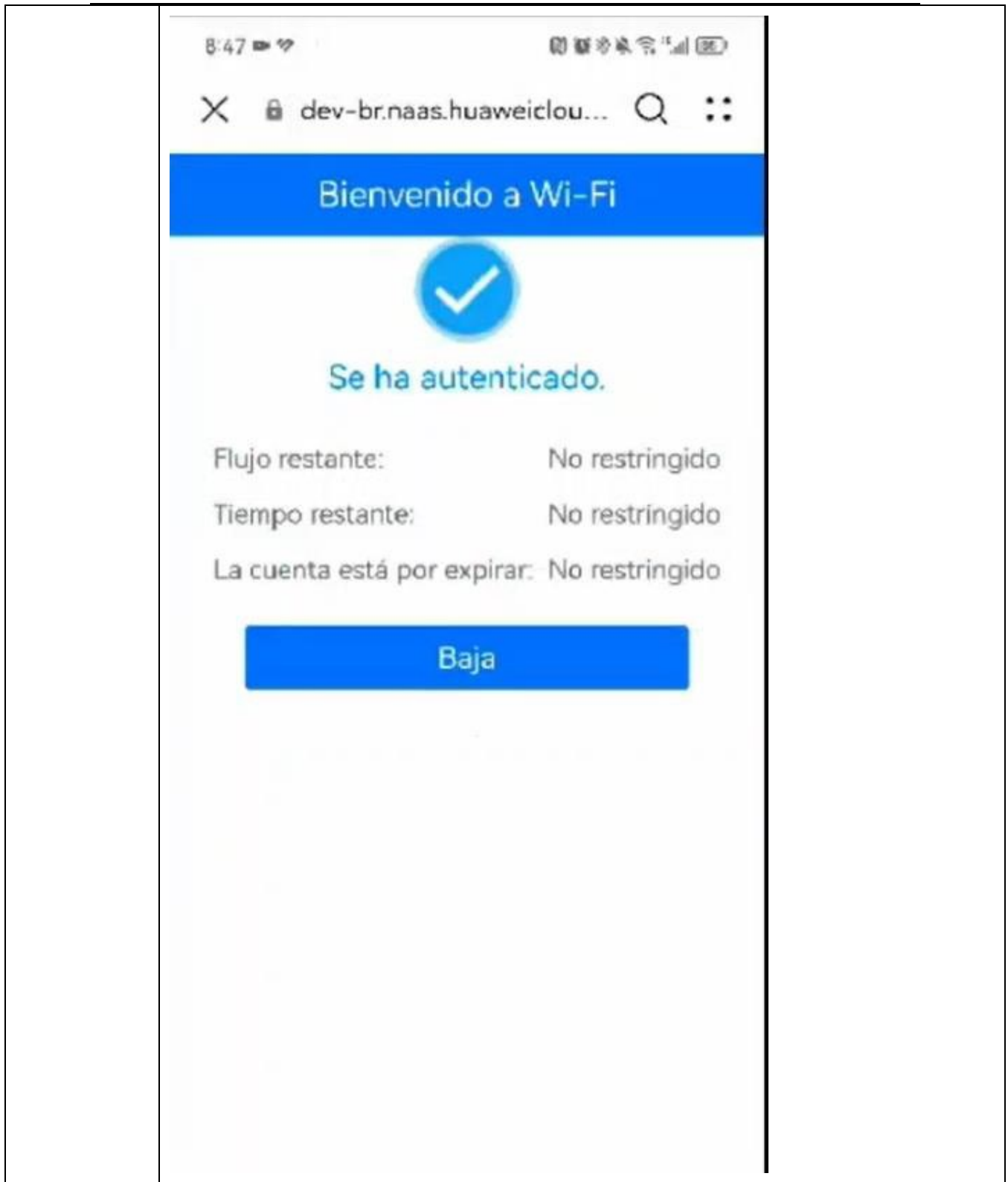
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES



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



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

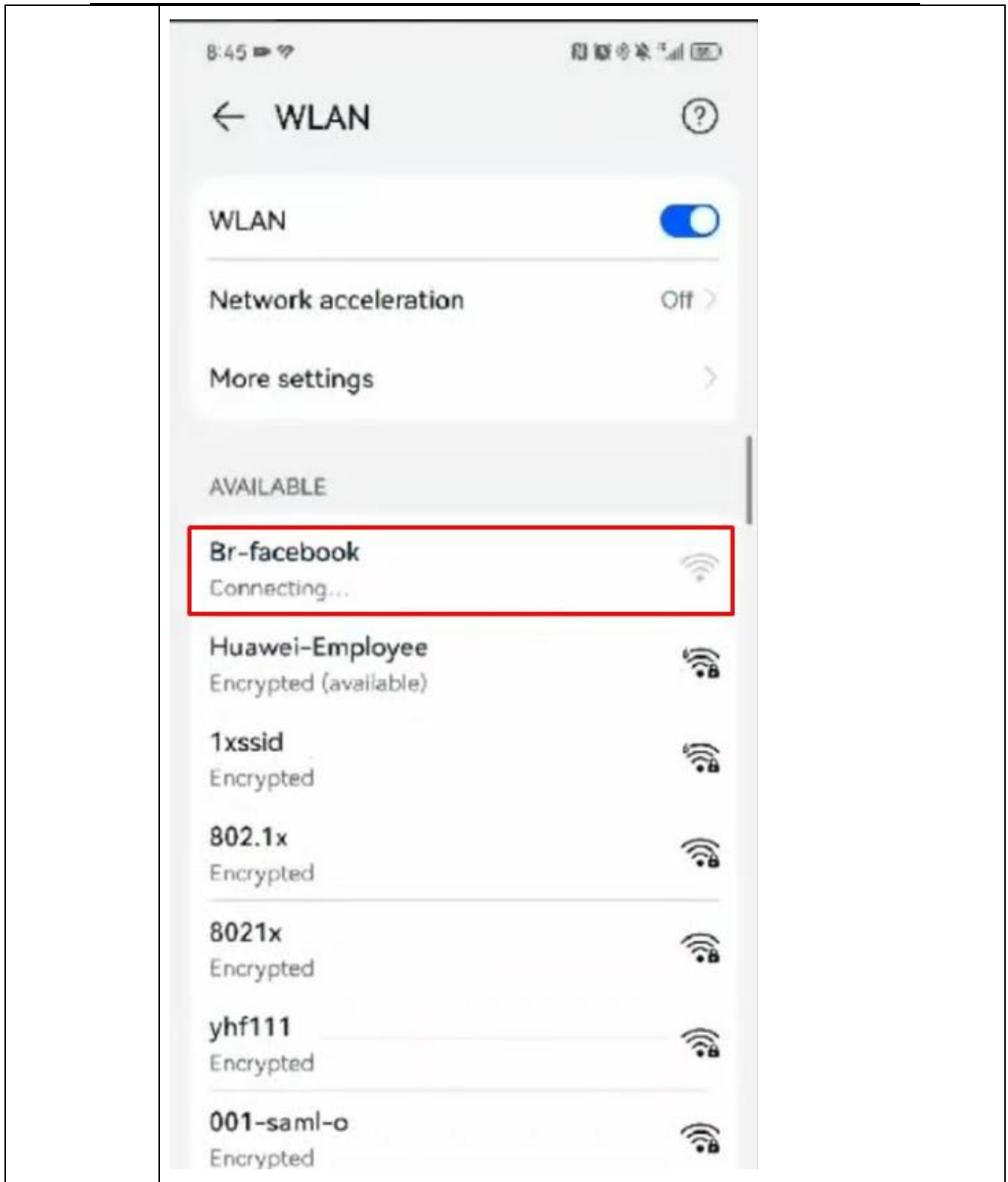




PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES

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

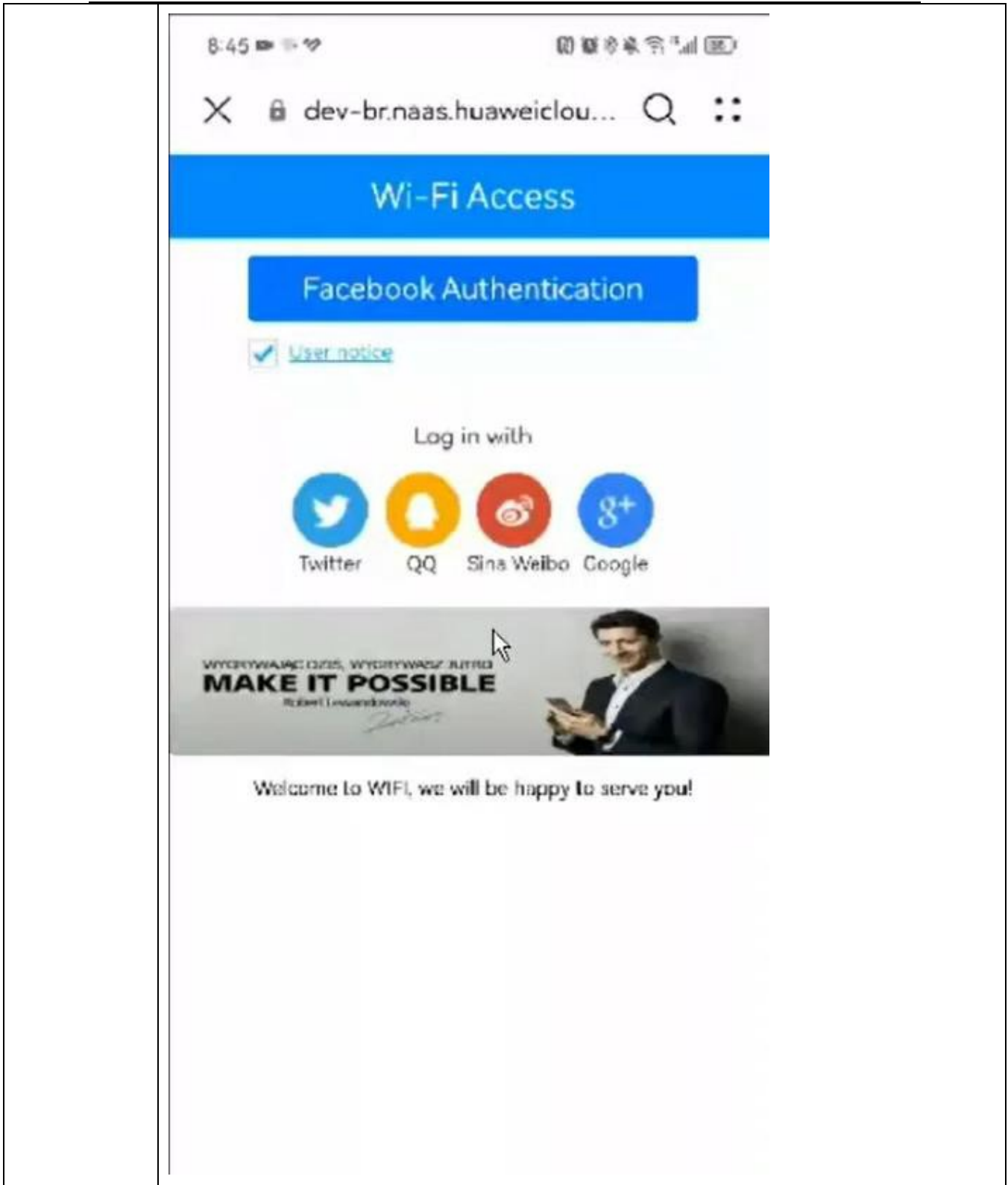
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES



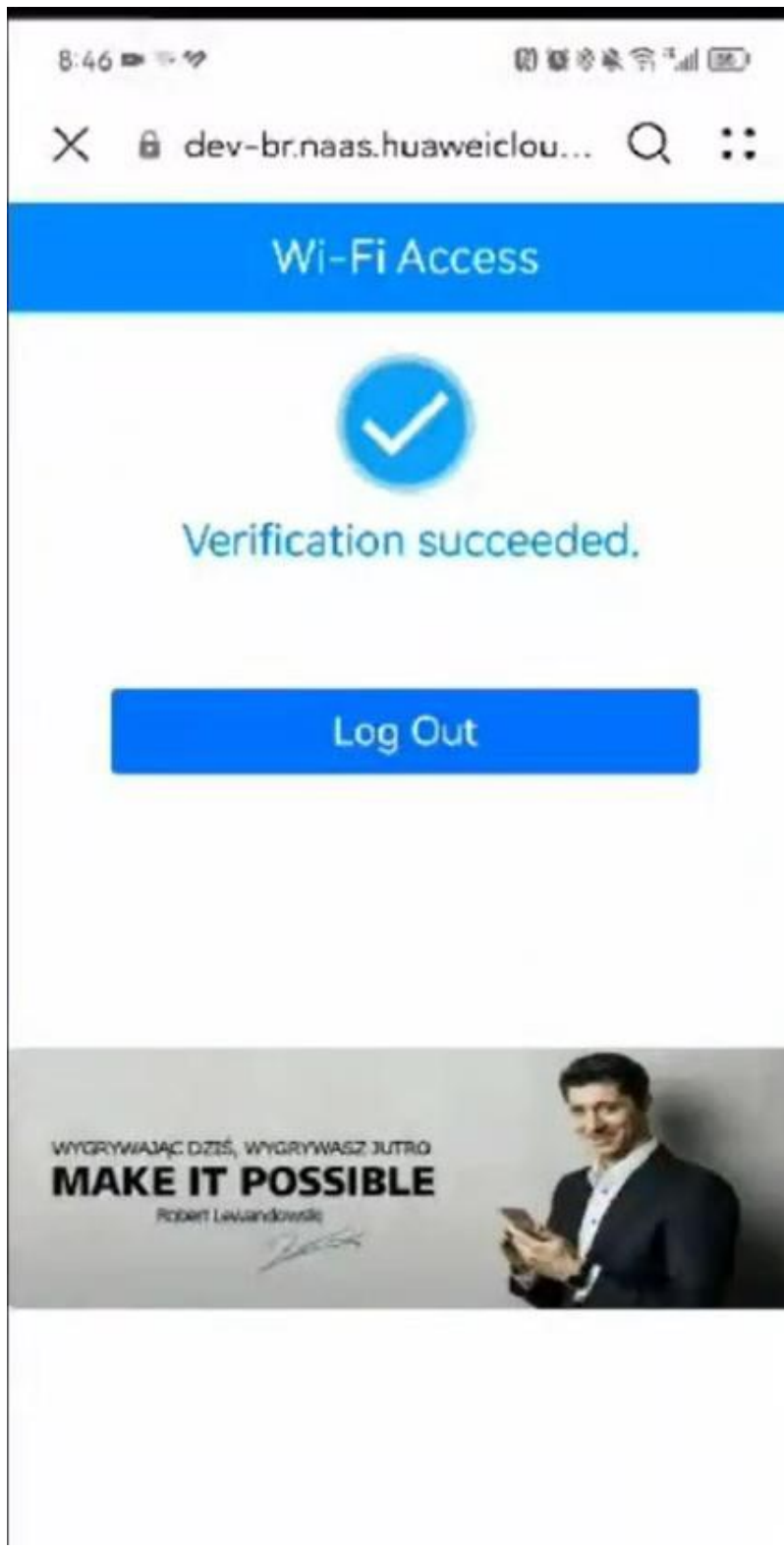
PREGÃO ELETRÔNICO Nº 001/2023 – SEDUC/GO  
PROCESSO Nº 2020.0000.604.5301  
INTERESSADO: GERÊNCIA DE SUPORTE DE REDES



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





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

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

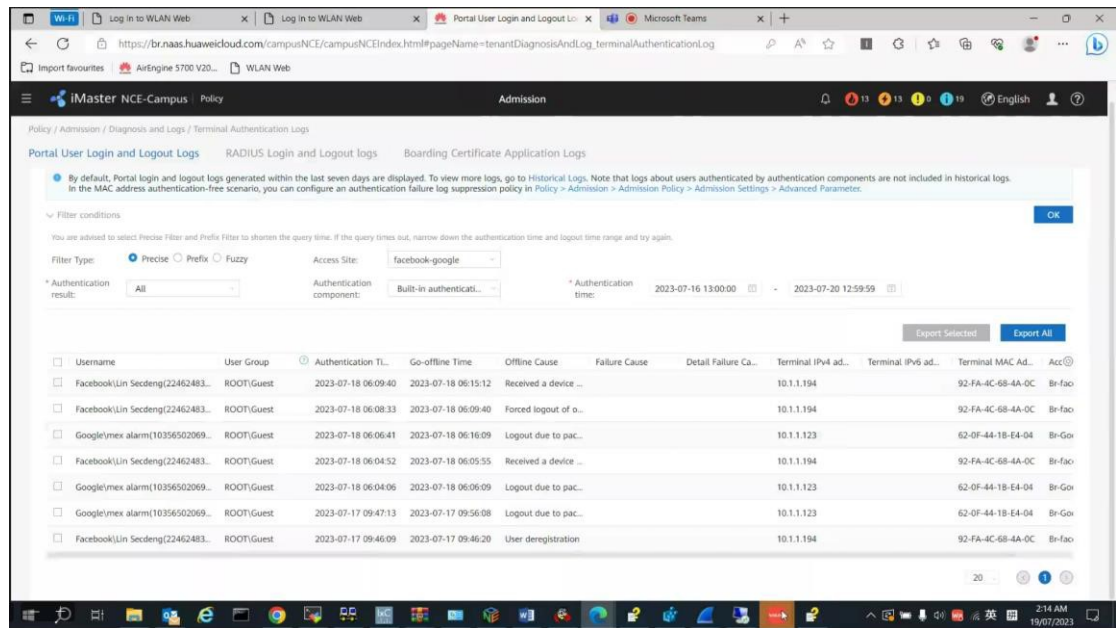


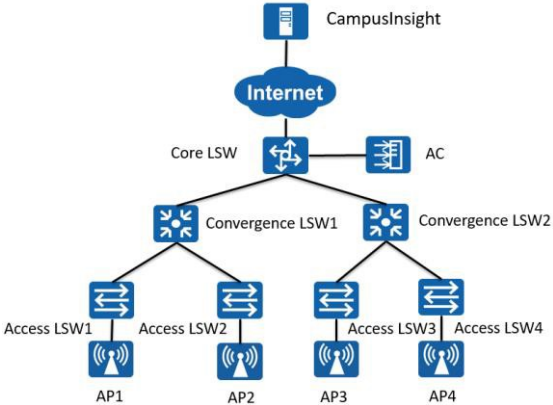
Figura 12 – Na plataforma iMaster NCE Campus, estão os registros das autenticações com mídias sociais.

## Wireless Location and Heatmap

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

<b>Item de</b>	Wireless Location and Heatmap
----------------	-------------------------------

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

<b>teste</b>	
<b>Objetivo do teste</b>	Para verificar a função de localizar terminais sem fio na topologia WLAN..
<b>Topologia da Rede:</b>	<div style="text-align: center;">  </div> <p>Prerequisites:</p> <ol style="list-style-type: none"> <li>1. O CampusInsight e o pacote de patch de localização sem fio foram instalados e o sistema está funcionando corretamente.</li> <li>2. A AC e os APs foram configurados para relatar toda a telemetria necessária.</li> </ol>
<b>Procedimento de teste</b>	<ol style="list-style-type: none"> <li>1. Realizar login no CampusInsight e selecionar <b>Inventory &gt; Service Topology</b> do menu principal. Clique no ícone <b>Enter WLAN Topology</b> na esquerda. Na página de topologia de WLAN exibida, selecione um piso planejado no painel de navegação e clique <b>Wireless Location</b> no canto superior direito. Resultado esperado 1.</li> <li>2. Selecione o <b>Heat Map of Pedestrian Flow</b> e clique <b>OK</b>. Resultado esperado 3.</li> <li>3. Selecionar <b>Wi-Fi Interference</b> e clique <b>OK</b>. Resultado esperado 4.</li> </ol>
<b>Resultado esperado</b>	<ol style="list-style-type: none"> <li>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.</li> </ol>

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

**Resultado**

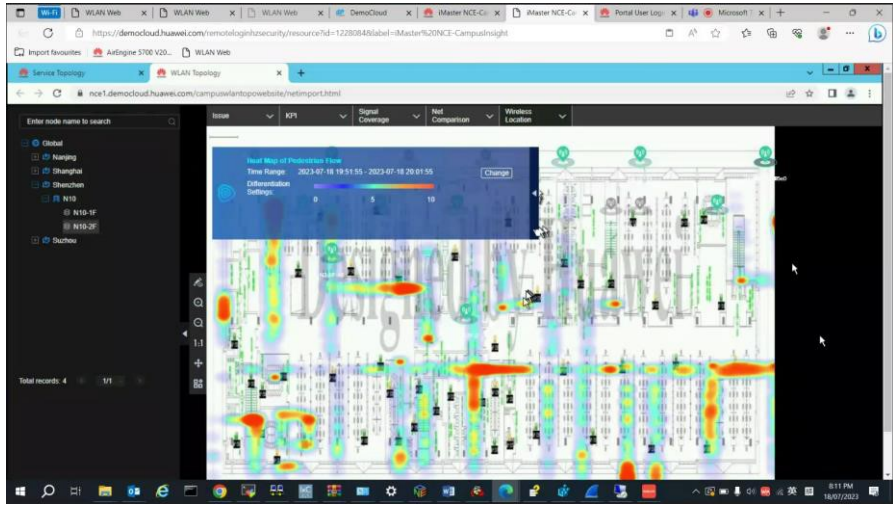


Figura 1 – O mapa de calor é mostrado na plataforma iMaster NCE CampusInsight.