**[Cisco ISE with Microsoft Active Directory, Entra ID, and Intune](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635)**

05-13-2025 06:29 PM

**Shortcut URL -**<https://cs.co/ise-entraid>

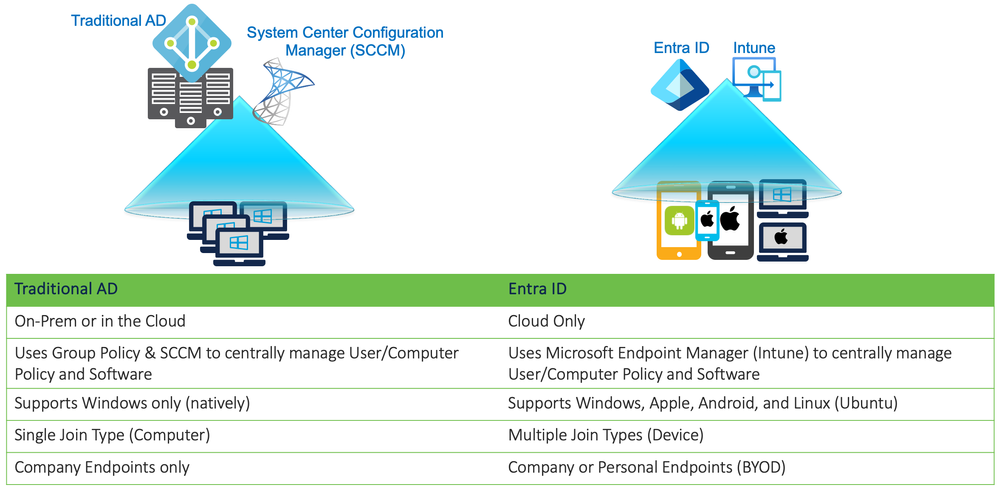
* [Introduction](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-1423455928)
* [Traditional AD Computer vs. Entra ID Device](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId--383998535)
* [Traditional AD User vs.Entra IDUser](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-2103514298)
* [Windows and 802.1x Authentication with Traditional AD](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-296059835)
* [TEAP authentication with Windows and Traditional AD](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId--1511394628)
* [Microsoft Intune Integration with ISE](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-976118205)
* [Licensing requirements for Intune MDM integration](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId--130271680)
* [Certificates and the GUID](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId--140774784)
* [Certificate Enrollment](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId--1948229247)
* [ISE Authentication Flow with Traditional AD & Intune MDM Compliance](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-539283586)
* [Authentication/Authorization with ISE and Entra ID](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId--2092417075)
* [User Authentication with Entra ID via REST ID](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-524178477)
* [User Authorization with Entra ID and EAP-TLS](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId--1283275986)
* [User Attributes from Entra ID](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-1333319566)
* [Authentication/Authorization of an Entra Joined Device using EAP-TLS](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId--603217616)
* [Entra Joined Device and Entra User with TEAP(EAP-TLS) and EAP Chaining](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-1884295217)
* [Entra Joined Device and AD User with TEAP(EAP-TLS) and EAP Chaining](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-76840754)
* [Entra Joined Device with TEAP(EAP-TLS) and AD User with TEAP(MSCHAPv2) and EAP Chaining](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId--1730613709)
* [Entra ID Multi-User Scenario](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-756899124)
* [Mixed Entra Joined Device & Traditional AD User Scenario with EAP-TLS](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-2135119435)
* [Additional Use Cases](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId-198582253)
* [Summary](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hId--1608872210)

**Introduction**

***\*\*\* NOTE: Microsoft has now renamed Azure AD to Entra ID. For all references to Azure AD in this document, the same concepts apply to Entra ID.***

With many customers moving to a cloud-first strategy, it is important to understand the differences between traditional Active Directory and Entra ID and the caveats and limitations with how Cisco ISE integrates and/or interacts with these solutions. Understanding the additional value that Intune (Microsoft Endpoint Manager) can provide is also useful in many environments.

Let’s start by comparing some of the basic concepts between traditional Active Directory (On-Prem or Public Cloud) versus Entra ID.

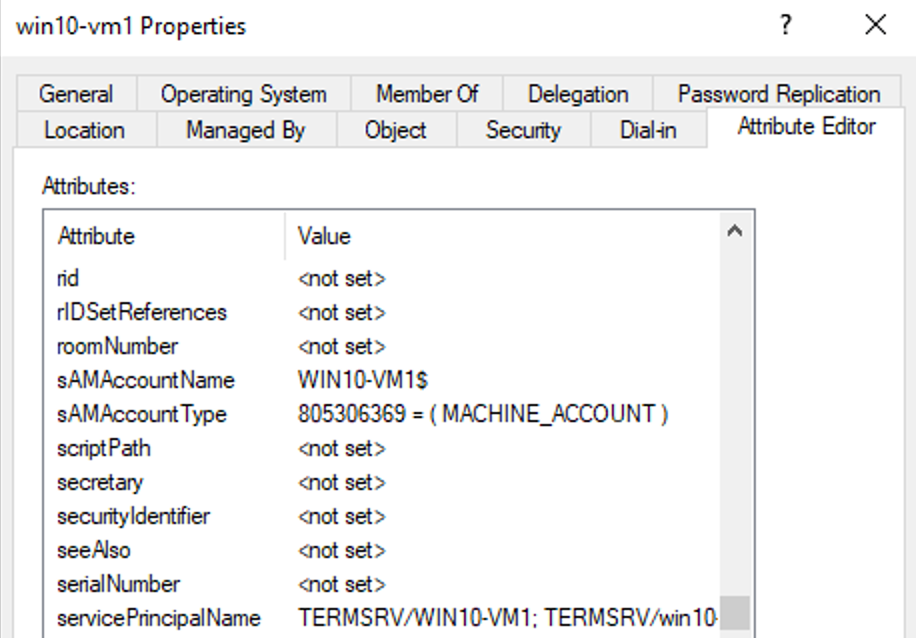


**Traditional AD Computer vs. Entra ID Device**

A Windows Computer account in Active Directory is significantly different than a Windows Device in Entra ID.

The Computer account is an object created in Active Directory and used to assign Group Policy as well as perform various other operations within the domain. When a Computer joins the domain, a password is generated for that account which is rotated and synchronized with the domain every 30 days by default. This Computer account has an associated sAMAccountName, distinguishedName, objectSID, as well as various other attributes used within the domain.

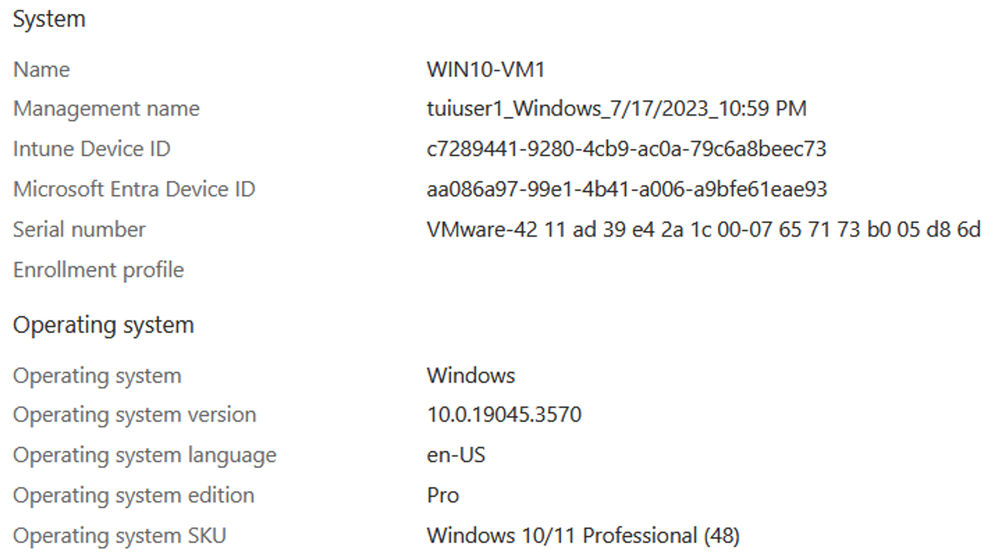
Example Computer account attributes:



In contrast, a Device is a basic construct in Entra ID that is created at the time of the Entra ID join operation and used for applying Configuration Profiles, Conditional Access Policies, and Compliance Policies via Intune (Microsoft Endpoint Manager). The Device account does not have an associated UPN. The main attributes used to identify the Device within Entra ID is a GUID (Globally Unique Identifier) labelled as the Entra Device ID. If the Device is managed by Intune, it will also have a GUID labelled as the Intune Device ID.

Computer accounts in traditional AD can be synchronized with Entra ID using the Entra Connect application.

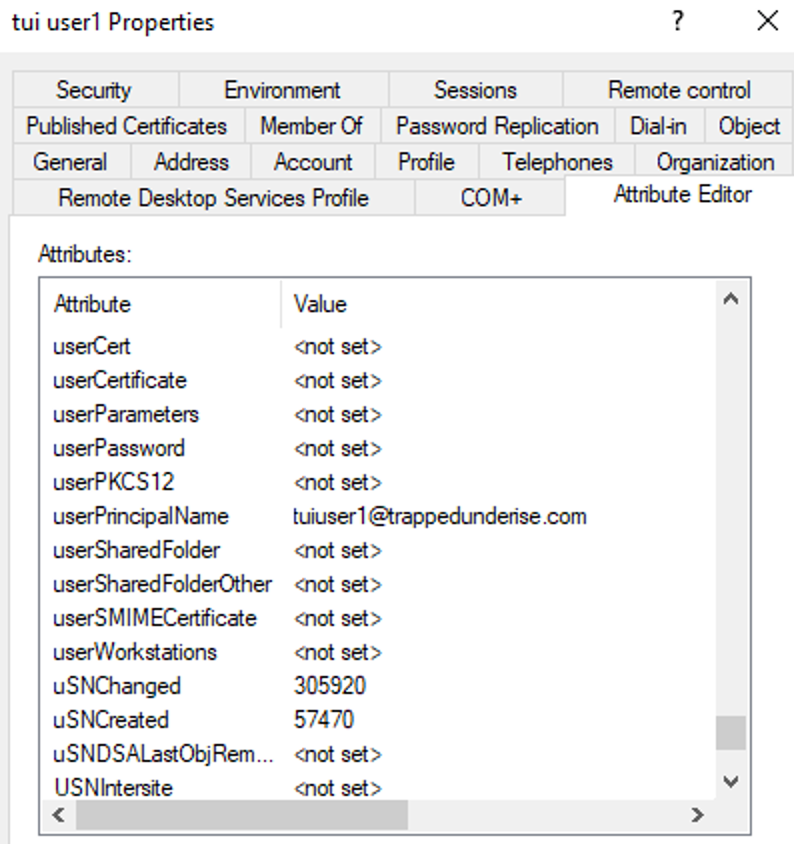
The following screenshot is Entra ID’s view of the same domain computer above that was learned via the Entra Connect application.



**Traditional AD User vs. Entra ID User**

With traditional AD, User accounts are manually created (or orchestrated) by domain administrators. Like Computer accounts, the User accounts are used to assign Group Policy as well as perform various other operations within the domain. The password is managed by the user and rotated manually based upon the requirements of the domain policy. The User account has an associated sAMAccountName, objectSID, userPrincipalName, as well as various other attributes used by the domain.

*Example User account attributes:*

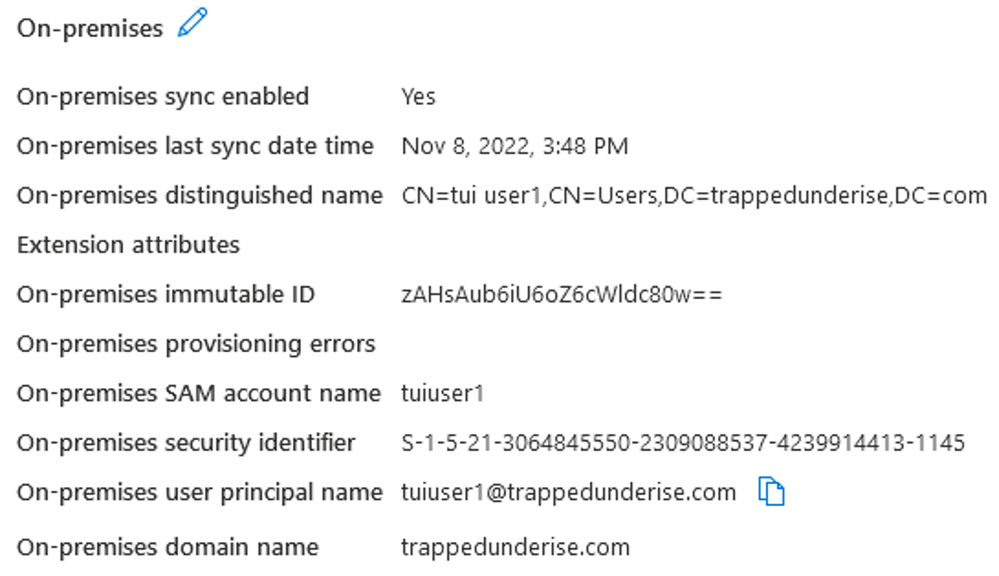
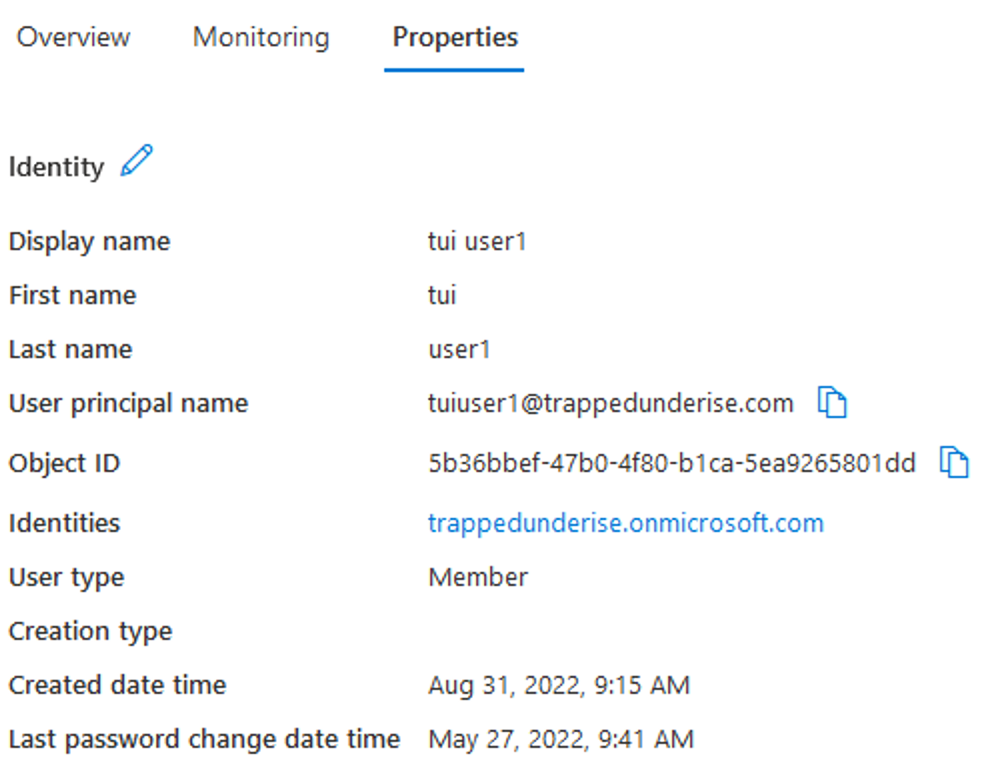


With Entra ID, there are different ways that User accounts are created. Existing or new User accounts in traditional AD can be synchronized to Entra ID using the Entra Connect application. Groups created within traditional AD are also synchronized, so the group memberships associated with a User account are preserved. User accounts can also be created natively in Entra ID using multiple methods including manually via the portal or using the Entra APIs.

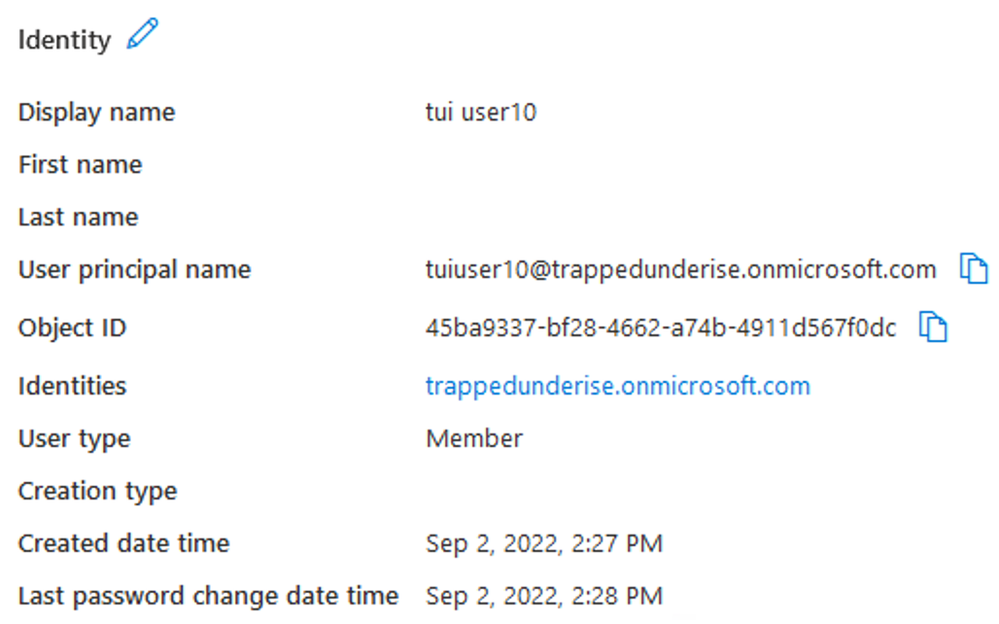
User accounts in Entra ID have an Object ID (unique within Entra ID) and a User Principal Name. For User accounts synchronized from Entra Connect, the User Principal Name will be the same in both Entra ID and traditional AD. Various other attributes are learned from Entra Connect, including the SAM account name and SID.

For User accounts created directly in Entra ID, the User Principal Name will end in ‘.onmicrosoft.com’ (unless another custom domain name is defined).

*Example Entra ID User account synced from Entra Connect:*



*Example Entra ID User account created directly in Entra ID (not synced with traditional AD):*



**Windows and 802.1x Authentication with Traditional AD**

When discussing 802.1x, it is important to understand that Windows computers have two distinct operating states; Computer and User.

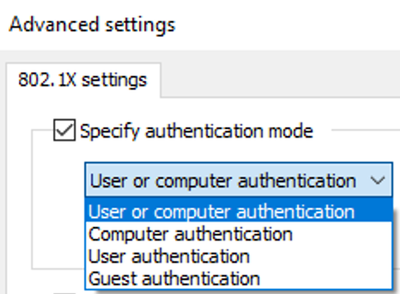
When a Windows computer is first powered on and prior to a User logging in, Windows is in a Computer state. If network connectivity is available, a domain-joined Windows computer will attempt to communicate with the AD domain and check for any available Computer Group Policy changes.

When a User logs in, Windows will transition to the User state. If network connectivity is available, a domain-joined Windows computer will attempt to communicate with the AD domain and check for any available User Group Policy changes.  
When a User logs out, Windows will again transition to the Computer state.

The state changes above are especially relevant when the Windows supplicant is enabled for 802.1x. There are three authentication modes commonly used in corporate environments using 802.1x authentication:

* User or computer authentication
* Computer authentication
* User authentication

*Example Windows supplicant options:*



With the authentication mode configured for ‘Computer authentication’ Windows will present only the Computer credential (either a Computer certificate for EAP-TLS, or a Computer hostname/password for PEAP-MSCHAPv2), regardless of whether Windows is in the Computer or User operational state.

With the authentication mode configured for ‘User authentication’ Windows will present only the User credential (either a User certificate for EAP-TLS, or a Username/Password for PEAP-MSCHAPv2), but only when Windows is in the User operational state. No credential is presented when Windows is in the Computer state, which typically means that the Computer has no authorization on the network prior to the User logging in.

With the authentication mode configured for ‘User or computer authentication’ Windows will present the Computer credential when in the Computer state. When the User logs in, a new session will be generated and Windows will present the User credential. Traditional 802.1x protocols like EAP-TLS and PEAP-MSCHAPv2 are only capable of presenting a single credential during the EAP communication, so the Computer and User sessions are not inherently related to each other.

The following diagram illustrates an example authentication flow using EAP-TLS with the supplicant configured for ‘User or computer authentication’.

A diagram of a network device

AI-generated content may be incorrect.

For the above example, the following screenshot shows the resulting RADIUS Live Logs in ISE.



**TEAP authentication with Windows and Traditional AD**

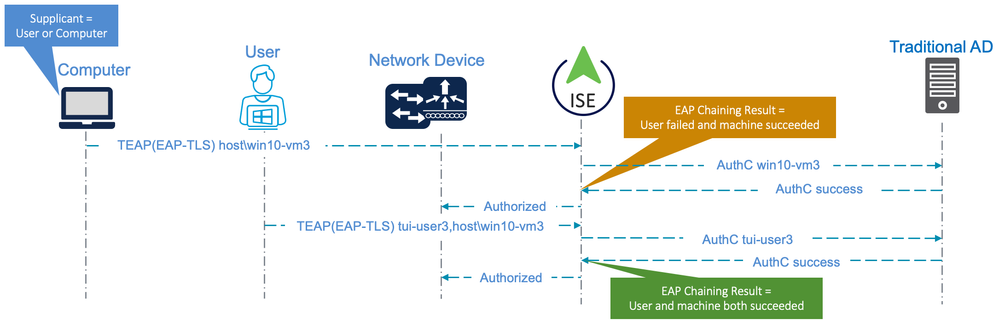
Windows 10 release 2004 and above supports a newer 802.1x EAP protocol called TEAP (Tunnel Extensible Authentication Protocol). TEAP is ratified by the IETF and is defined in the following RFC.  
<https://datatracker.ietf.org/doc/html/rfc7170>

TEAP provides the ability to pass more than one credential via EAP. When used with the ‘User or computer authentication’ method, it allows the supplicant to provide both the Computer and User credentials in a single session using a feature called EAP Chaining. Cisco ISE can use this EAP Chaining result as a matching condition in the Authorization Policy rules. Like PEAP, TEAP is an outer protocol method that uses inner protocol methods such as EAP-TLS and MSCHAPv2 to provide User and/or Computer credentials that ISE can then authenticate individually against traditional AD.

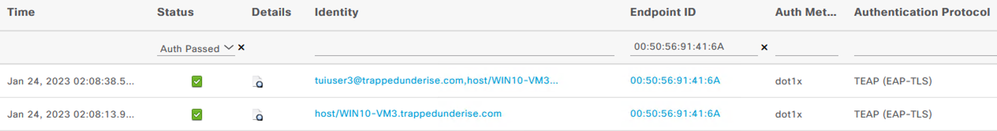
When used with traditional AD, TEAP with EAP Chaining is a useful option to ensure authorization is granted for a corporate User logging into a corporate Computer.

See the following document for an example of how to configure TEAP with Windows and Cisco ISE.  
<https://www.ise-support.com/2020/05/29/using-teap-for-eap-chaining/>

The following diagram illustrates an example authentication flow using TEAP (with an inner method of EAP-TLS) with the supplicant configured for ‘User or computer authentication’.



For the above example, the following screenshot shows the resulting RADIUS Live Logs in ISE.



The detailed ISE logs for the EAP Chained session reflect the EAPChainingResult of ‘User and machine both succeeded’.



**Microsoft Intune Integration with ISE**

Current versions of ISE also have the ability to integrate with Microsoft Intune (also known as Microsoft Endpoint Manager) to perform compliance checks for an endpoint. Cisco ISE version 3.1 and above support the MDM (Mobile Device Manager) APIv3. This version of the MDM API allows ISE to use a GUID (Globally Unique Identifier) value in the certificate presented by an endpoint using EAP-TLS to query the MDM vendor for compliance status. This compliance status (true/false) can then be used as a condition in the ISE Authorization Policy.

The MDM vendor must also support the Cisco ISE MDM APIv3 in leverage this feature. The following document provides information on integrating MDM and UEM (Unified Endpoint Management) systems with ISE.  
[Integrate MDM and UEM Servers with Cisco ISE](https://www.cisco.com/c/en/us/td/docs/security/ise/UEM-MDM-Server-Integration/b_MDM_UEM_Servers_CiscoISE/chapter.html)

In addition to GUID-based lookups, the updated [Microsoft Compliance Retrieval (NAC 2.0) API also supports MAC Address based lookups](https://learn.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate#data-shared-with-nac-partners).

Additional information on the benefits of using the MDM APIv3 and GUID-based lookups with Intune (as opposed to MAC Address based lookups) are discussed in the following webinar on ISE Integration with Intune MDM.  
[YouTube - Cisco ISE Integration with Intune MDM](https://www.youtube.com/watch?v=iAKyIHFqbgE)

Please note that the Microsoft TLS Issuing CA certificates formerly used by the ISE Intune MDM integration function will expire on 27 June 2024. However, Microsoft has already completed the rotation of the certificates used for the Compliance Retrieval (NAC 2.0) API endpoints.

With those changes, ISE is now only required to have the DigiCert Global Root G2 CA certificate in Trusted Certificates store for the MDM lookups to work properly. Although this Root Certificate is installed in the Trusted Certificates store by default, you should ensure that the option for 'Trust for authentication within ISE' is enabled under the Usage options.

<https://techcommunity.microsoft.com/t5/intune-customer-success/intune-certificate-updates-action-may-be-required-for-continued/ba-p/1839655>

Licensing requirements for Intune MDM integration

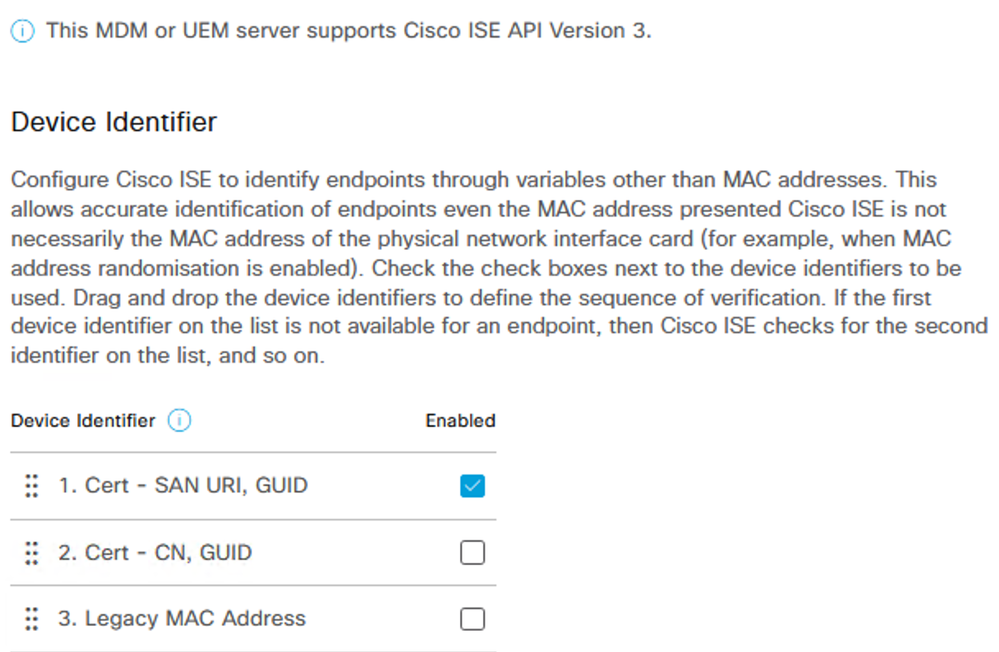
The Intune MDM lookups described in this blog are optional, but add an additional level of authorization for the User and Device sessions. As the Intune Registration and/or Compliance lookups are functions of the MDM Compliance feature in ISE, any sessions using these conditions will require a Premier license as per the [Cisco ISE Licensing Guide](https://cs.co/ise-licensing).

**Certificates and the GUID**

For ISE to leverage the GUID for MDM lookups, it must be present in the certificate presented by an endpoint for EAP-TLS. ISE 3.1+ supports the GUID value present in either of the following certificate attribute fields.

* Subject – Common Name
* Subject Alternative Name – URI

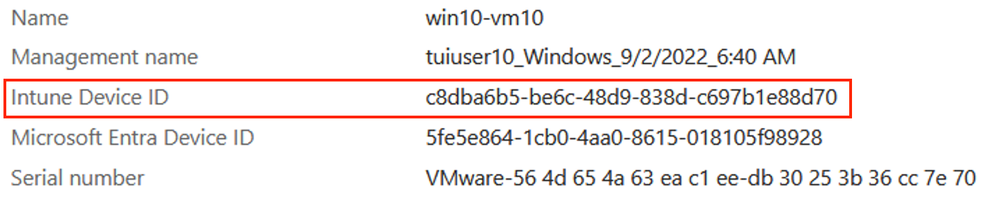
The screenshot below shows the configuration options from the ***Administration > Network Resources > External MDM > MDM Servers < [server]*** menu in the ISE GUI. In this example, Intune is configured as an External MDM and ISE is configured to use the GUID value found in the ‘SAN URI’ field of the certificate as the Device Identifier to perform compliance checks against Intune.



This GUID is the same value as the Intune Device ID for an endpoint that is managed by Intune. The screenshot below shows an example User certificate that includes the GUID in the SAN URI field.



The screenshot below shows the Intune Device ID for the same endpoint in which the above User certificate is enrolled. This value is the same as the GUID shown in the certificate above.



It is also important to note that this GUID can be present in the User certificate, Computer certificate, or both depending on how the Certificate Templates and enrollment policies (Group Policy, Intune Device Configuration Policies, etc.) are defined.

To perform device compliance checks in ISE for both Computer and User sessions, for example, the GUID would need to be present in both certificates. As the GUID relates to the Intune Device ID, the GUID value would be the same in both certificates.

**Certificate Enrollment**

As stated above, for ISE to leverage the GUID for MDM compliance checks, it must be present in the certificate. When using Intune, the GUID is inserted into the certificate at the time of enrollment by the User or Computer (or Device, in Azure terminology).

This end-to-end functionality requires the use of multiple solutions including traditional Active Directory [AD] and AD Certificate Services [ADCS] (On-Prem or in the cloud), Entra Connect, and the Intune Certificate Connector.

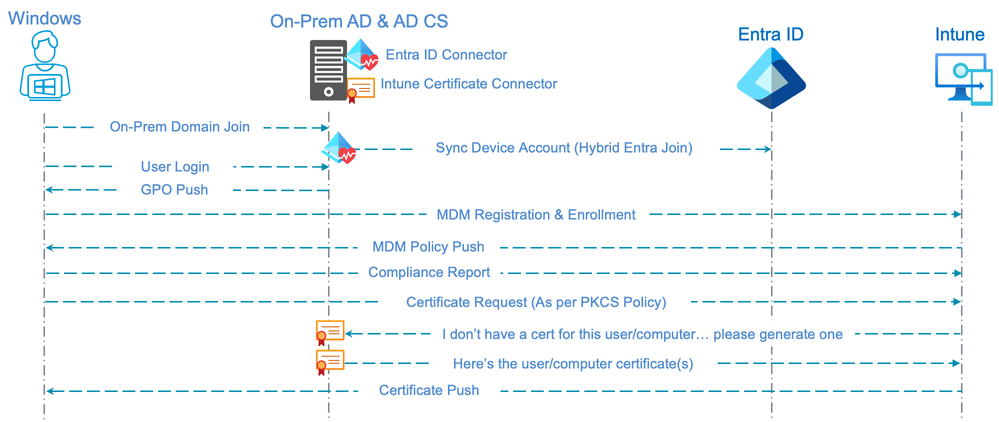
While this example uses ADCS, some of the same functionality can be provided now by the Microsoft Cloud PKI solution. See this article for more information about the use of MS Cloud PKI.  
[Cisco ISE with Microsoft Cloud PKI](https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-cloud-pki/ta-p/5198483)

More information about AD Certificate Services [ADCS] can be found here:  
[Microsoft - Active Directory Certificate Services Overview](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831740(v=ws.11))

More information about Entra ID Connect can be found here:  
[Microsoft - What is Microsoft Entra Connect?](https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/whatis-azure-ad-connect)

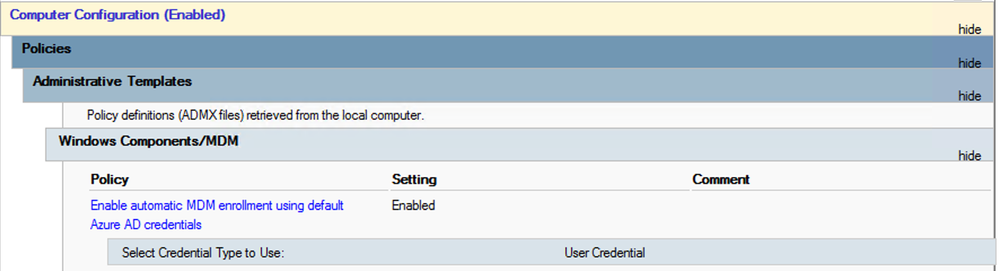
More information about the Intune Certificate Connector can be found here:  
[Microsoft - Certificate Connector for Microsoft Intune](https://learn.microsoft.com/en-us/mem/intune/protect/certificate-connector-overview)

The following diagram illustrates the basic flow for a Hybrid Entra Joined computer from the traditional AD join through the Intune MDM and certificate enrollment.



The following steps occur as part of the flow illustrated above:

1. The Computer is joined to the traditional (On-Prem or in the cloud) AD domain
2. The Entra Connector synchronizes the Computer account with Entra ID
3. The Computer account is assigned Group Policy to perform an automatic enrollment with the Intune MDM using the User credentials provided when the User logs in  
     
   *Example Group Policy Object:*

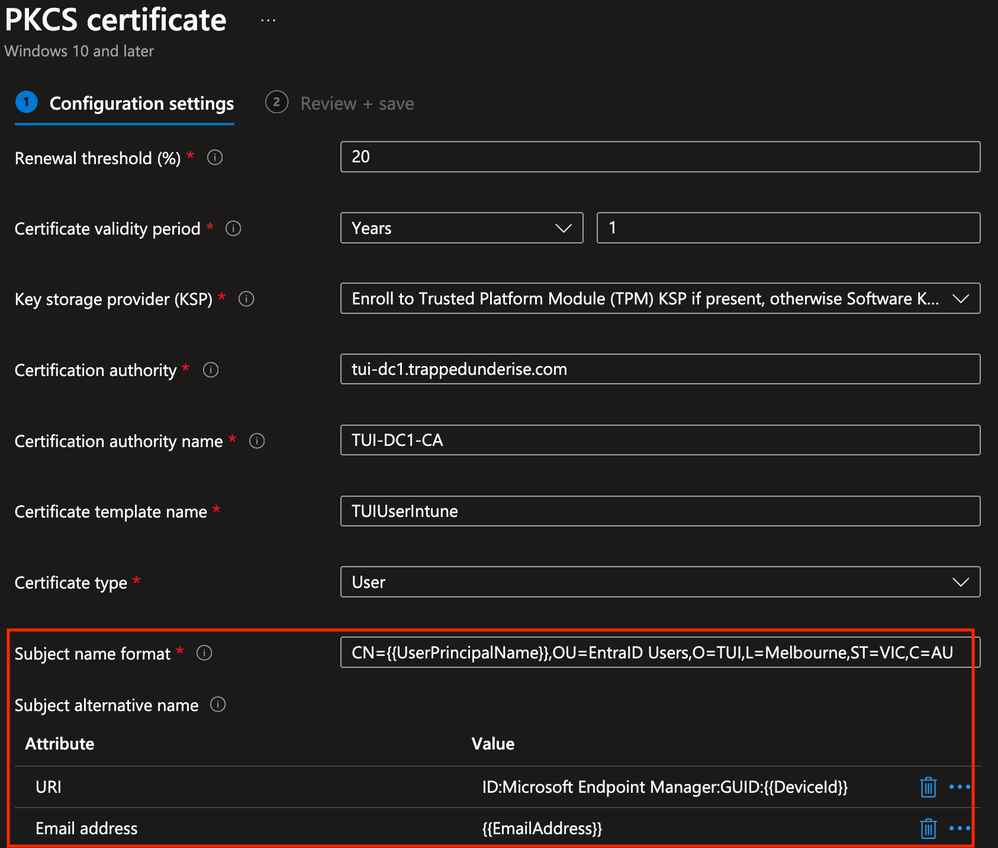


1. The Computer is registered with Entra ID and enrolled with Intune
2. The pre-configured Device Configuration Profiles assigned to the User and/or Computer are pushed from Intune to the endpoint; they include (among other attributes):
   * Certificate Profiles (PKCS, SCEP, or PKCS Imported)
   * Trusted Certificate Profiles (for the Root CA chain)
   * Wired and/or Wi-Fi network Profiles (used to configure the supplicant for 802.1x)
3. When the Certificate Profile (PKCS, in this example) is pushed to the endpoint, the enrolment is triggered
4. As Intune cannot natively enrol a certificate, it communicates to the Intune Certificate Connector to enrol a certificate with ADCS on behalf of the Computer and/or User
5. The Intune Certificate Connector provides the signed certificate(s) to Intune, which then pushes the certificate(s) to the endpoint, completing the enrolment

The combination of Intune and the Intune Certificate Connector is required in the flow described above as ADCS would otherwise have no knowledge of the Intune Device ID that must be inserted in the certificate as the GUID value.

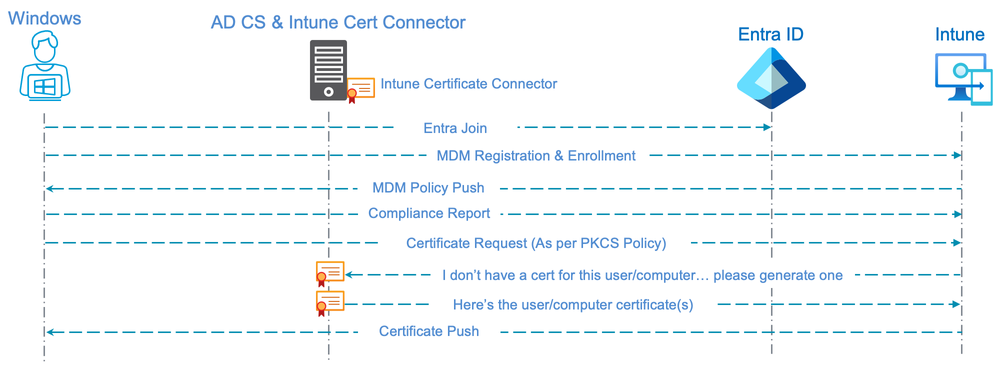
The following screenshot shows an example PKCS User Certificate Profile used by the flow described above. The resulting enrolled certificate will have the following attributes:

* Subject CN = User Principal Name (UPN) of the enrolled user
* Subject OU = EntraID Users (defined for use as a matching condition in ISE policies)
* SAN URI = GUID string value used to insert the Intune Device ID
* SAN Email address = Email address of the enrolled user



A similar certificate enrollment is also possible with Devices that are only Entra Joined (not a Computer joined to traditional AD). In that case, all components illustrated in the flow above would still be required except the traditional AD and Entra Connect.

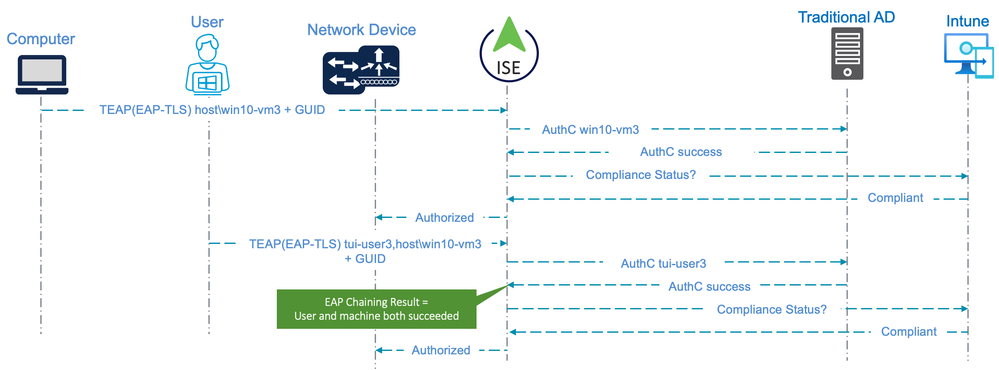
The diagram below illustrates the basic flow for an Entra Joined Device.



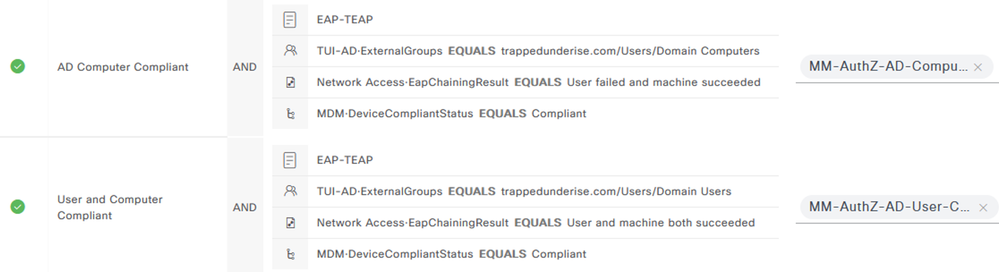
**ISE Authentication Flow with Traditional AD & Intune MDM Compliance**

With a Computer that is joined to traditional AD and enrolled with Intune (including the certificate enrolment with the GUID inserted), ISE can perform an MDM Compliance check as a condition for authorization. As the Compliance check requires the GUID as a Device Identifier, the authentication must use EAP-TLS to provide the GUID to ISE via the certificate. Either the traditional EAP-TLS, TEAP with an inner method of EAP-TLS [TEAP(EAP-TLS)], or EAP-FAST (Cisco Secure Client Network Access Manager) with an inner method of EAP-TLS [EAP-FAST(EAP-TLS)] can be used for the authentication.

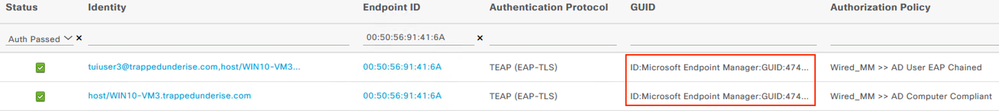
The following diagram illustrates the flow for a Hybrid Entra Joined Computer using TEAP(EAP-TLS) and configured for ‘User or Computer authentication’ mode with EAP Chaining. The flow includes both an EAP Chaining result of ‘User and computer both succeeded’ and an MDM Compliance check against Intune as conditions for Authorization.



The screenshot below shows an example of ISE Authorization Policies related to the flow illustrated above. The policies are for a Wired endpoint using TEAP(EAP-TLS) with ‘User or Computer authentication’ mode and EAP-TLS and include the MDM Compliance check. Active Directory Group membership is also used as an Authorization condition for both the Computer and User sessions.



The following screenshot shows the ISE RADIUS Live Logs related to the above flow. The logs indicate authentication via TEAP(EAP-TLS) and include the GUID presented to ISE within both the Computer and User certificates.



**Authentication/Authorization with ISE and Entra ID**

When authenticating a User or Computer against traditional AD, ISE performs the lookups using traditional methods such as LDAP or Kerberos (depending on how ISE is configured to integrate with AD). Entra ID, however, does not directly support these traditional protocols. Due to these limitations, ISE can only integrate with Entra ID to authenticate and/or authorize a User using two methods (at the time of this writing); REST ID (supported from ISE 3.0) or EAP-TLS (supported from ISE 3.2).

**User Authentication with Entra ID via REST ID**

ISE REST ID functionality is based on the new service introduced in ISE 3.0 - REST Auth Service. This service is responsible for communication with Entra over Open Authorization (OAuth) ROPC exchanges in order to perform user authentication and group retrieval.

For more information on how to configure ISE authentication against Entra ID using REST ID, see the following link.  
[Configure ISE 3.0 REST ID with Azure Active Directory](https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216182-configure-ise-3-0-rest-id-with-azure-act.html)

Authentication using REST ID is supported for Wired, Wireless, and Remote Access VPN connectivity. The authentication is performed using EAP-TTLS with an inner method of PAP and this option has the following caveats/limitations.

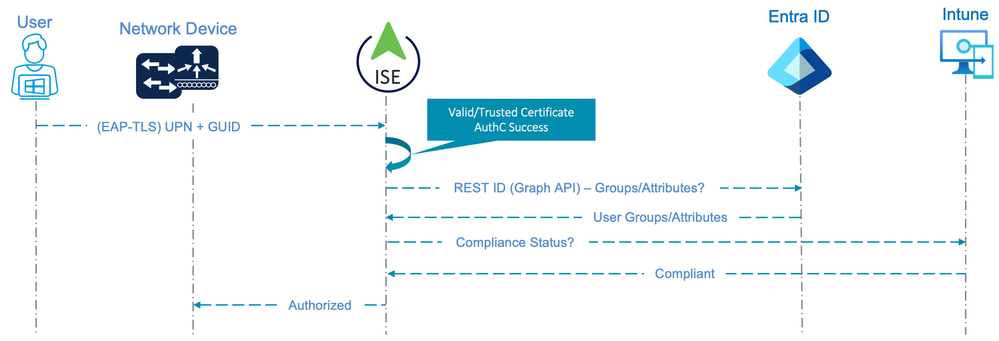
* Computer authentication is not possible as there is no Device credential/password concept in Entra ID
* The User is prompted for their credentials when connecting to the network; this can adversely impact the user experience, especially for Wired and Wireless connections
* Intune MDM Compliance checks are not possible since there is no certificate presented to ISE with the GUID
* As per Microsoft, ROPC is not compatible with MFA. To use this flow, MFA must be disabled for users using this App Registration using Conditional Access or other methods.  
  <https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth-ropc>
* Unlike PEAP(MSCHAPv2), EAP-TTLS(PAP) has no built-in mechanism to facilitate password changes. If the User's password expires or an Administrator forces a password change in Entra ID, the User will need to perform the password change from another network or device that has internet access before they can authenticate via 802.1x using EAP-TTLS(PAP) again. This is a limitation of the protocol that cannot be overcome and one of the many downsides to using password-based authentication methods.

**User Authorization with Entra ID and EAP-TLS**

ISE 3.2 introduced a new feature in which ISE can perform Authorization for an EAP-TLS User session using Entra ID user group membership as a condition. The ISE REST ID Service described above is also used to perform the lookup of group membership and other attributes associated with the Entra ID user using the Microsoft Graph API. Since the endpoint is authenticating via EAP-TLS using the User certificate, the GUID can be presented to ISE and MDM Compliance status can be used as a condition for Authorization.

For more detail on configuring ISE and Entra ID for authorization against Entra ID (not including the Intune integration), see the following link.  
[Configure ISE 3.2 EAP-TLS with Microsoft Azure Active Directory](https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/218197-configure-ise-3-2-eap-tls-with-azure-act.html)

The following diagram illustrates the flow for an endpoint configured for EAP-TLS with ‘User authentication’ mode. Both the Entra ID group membership and Intune Compliance status are used as conditions for Authorization.

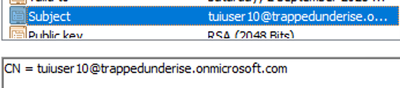


In this flow, it is important to understand that ISE is **not** capable of performing Authentication against Entra ID. The Authentication in this case is only based on the client presenting a valid User certificate that is trusted by ISE. The User credential provided within the certificate is not checked against any Identity Store, which could raise security concerns with some organizations.

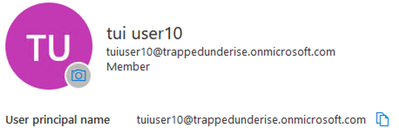
This flow has the following caveats and limitations:

* A minimum of ISE 3.2 is required to perform the Group/Attribute lookup using REST ID as a condition for authorization
* Computer authentication is not possible as there is no Device credential/password concept in Entra ID
* The User Principal Name (UPN) must be used in either the Certificate ‘Subject – Common Name’ or ‘Subject Alternative Name’ field
* The ISE Certificate Authentication Profile (CAP) used for Authentication must be configured to use the field with the UPN for the identity
* TEAP(EAP-TLS) and EAP-FAST(EAP-TLS) with EAP Chaining are supported for this flow from ISE 3.2 patch 5 and ISE 3.3 patch 1 due to the fix implemented by bugID [CSCwd34467](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwd34467)

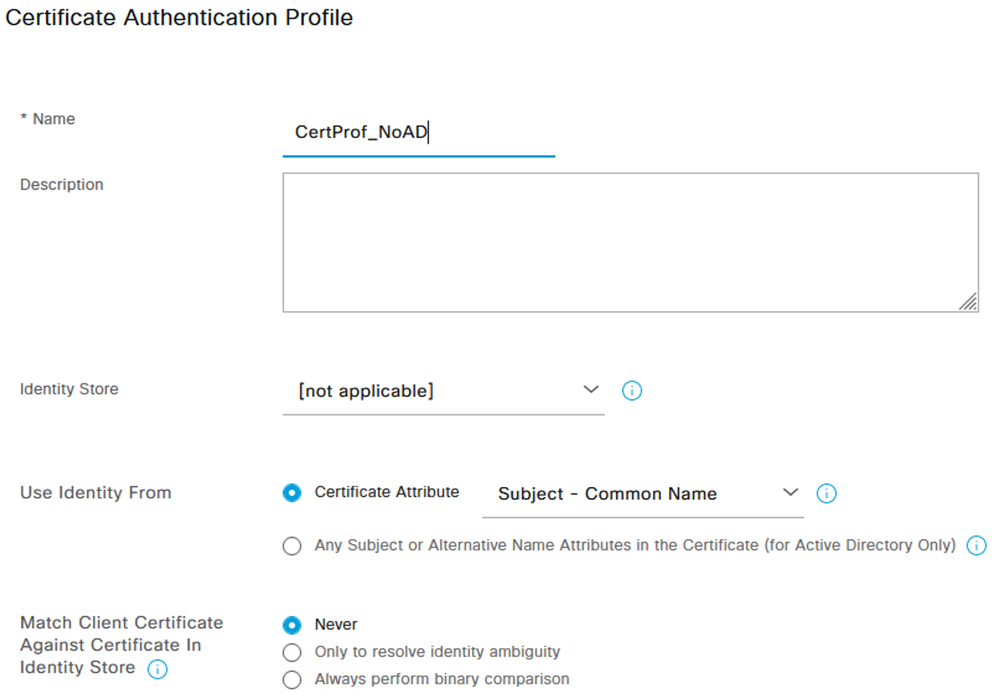
*Example User Certificate with the UPN in the ‘Subject – Common Name’ field:*



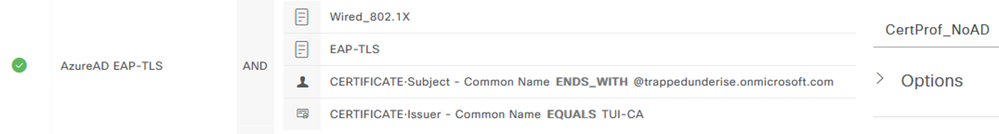
*Example Entra ID User with UPN:*



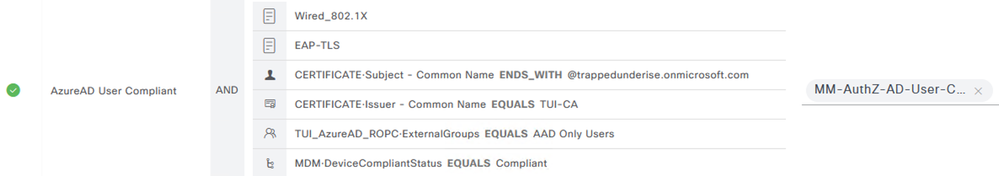
The following screenshot shows an example of a Certificate Authentication Profile configuration used for the above flow.



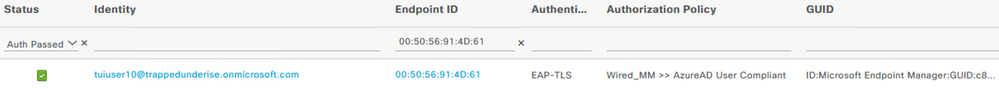
The following screenshot shows an example Authentication Policy used for this flow. This policy uses values in the Certificate ‘Subject – CN’ and ‘Issuer – CN’ as matching conditions to differentiate from sessions using other Authentication methods. The ‘Subject – CN’ is matching on the suffix used by the User UPN (@trappedunderise.onmicrosoft.com).



The following screenshot shows an example Authorization Policy used for this flow. The policy uses similar matching conditions to those used in the Authentication Policy in addition to the Entra ID group membership and MDM Compliance status conditions.



The following screenshot shows the ISE RADIUS Live Logs related to the above flow.



User Attributes from Entra ID

As of ISE 3.2 patch 4 (at the time of this writing), the following 44 Entra ID User Attributes can be added in ISE to be used in Authorization conditions for the 'User Authorization with Entra ID and EAP-TLS' flow described above.

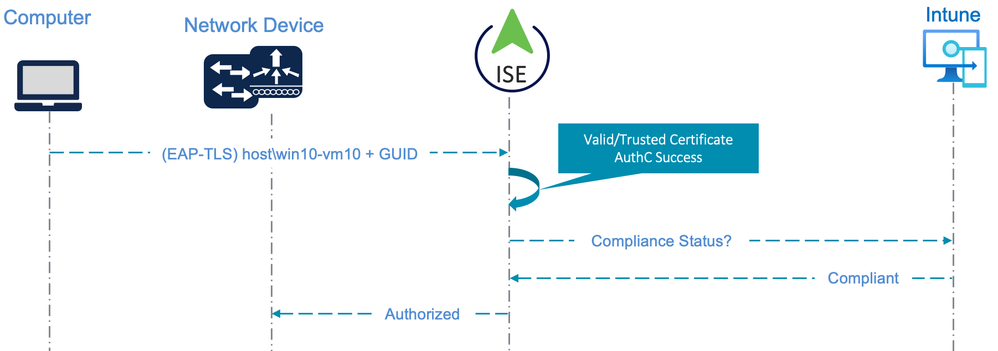
|  |  |
| --- | --- |
| country | passwordPolicies |
| onPremisesDistinguishedName | state |
| preferredLanguage | preferredName |
| mySite | department |
| isResourceAccount | showInAddressList |
| mail | userPrincipalName |
| city | mailNickname |
| displayName | givenName |
| companyName | employeeId |
| jobTitle | ageGroup |
| postalCode | onPremisesSecurityIdentifier |
| legalAgeGroupClassification | creationType |
| preferredDataLocation | employeeType |
| accountEnabled | mobilePhone |
| aboutMe | streetAddress |
| externalUserState | onPremisesImmutableId |
| onPremisesSyncEnabled | onPremisesDomainName |
| onPremisesUserPrincipalName | faxNumber |
| officeLocation | securityIdentifier |
| surname | usageLocation |
| deviceEnrollmentLimit | userType |
| onPremisesSamAccountName | consentProvidedForMinor |

More details on configuring and troubleshooting the REST ID integration leveraged by this use case can be found in the following document.  
[Configure Cisco ISE 3.2 EAP-TLS with Microsoft Azure Active Directory](https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/218197-configure-ise-3-2-eap-tls-with-azure-act.html)

**Authentication/Authorization of an Entra Joined Device using EAP-TLS**

Since first publishing this article, I've been asked by multiple peers and customers if similar flows can be used to authenticate/authorize a pure Entra Joined Device using EAP-TLS and a certificate enrolled by Intune.

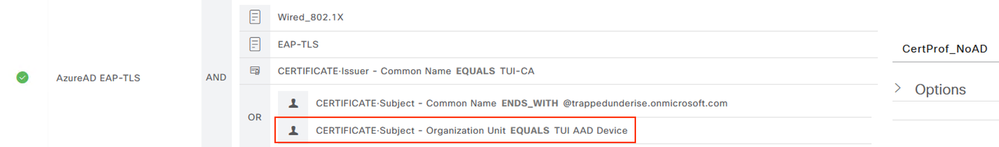
The following diagram illustrates the flow that can be used to authenticate and authorize an Entra Joined Device when it is in the Computer state.



This flow has the following caveats and limitations:

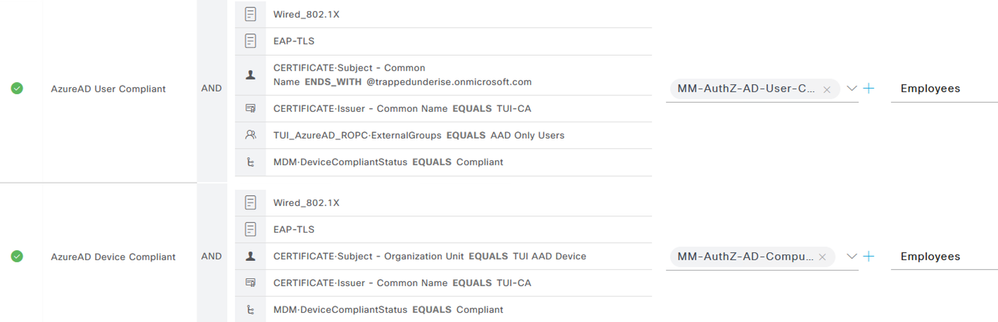
* Authentication is based purely on a valid/trusted certificate presented by the client
* The Device credential is not Authenticated against any Identity Store
* TEAP(EAP-TLS) and EAP-FAST(EAP-TLS) with EAP Chaining are supported for this flow from ISE 3.2 patch 5 and ISE 3.3 patch 1 due to the fix implemented by bugID [CSCwd34467](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwd34467)
* Authorization is based only on the trusted certificate and (optional) Intune compliance
* For Intune compliance (optional), the certificate used for the Computer state must be enrolled via an Intune Configuration Profile (Device certificate) so the GUID is present in the SAN field.
* As there is no interaction with Entra ID, this specific flow can technically be used with ISE version 3.1 and above.

The following screenshot shows an example Authentication Policy used for this flow. This policy uses values in the Certificate ‘Subject – OU’ and ‘Issuer – CN’ as matching conditions to differentiate from sessions using other Authentication methods or EAP-TLS flows not involving Entra ID. The ‘Subject – OU’ attribute is a unique static value defined in the Intune Configuration Profile to provide this differentiation. The same Certificate Authentication Profile described above was used for this flow, so a single Authentication Policy will serve both the User and Computer (Device) flows.

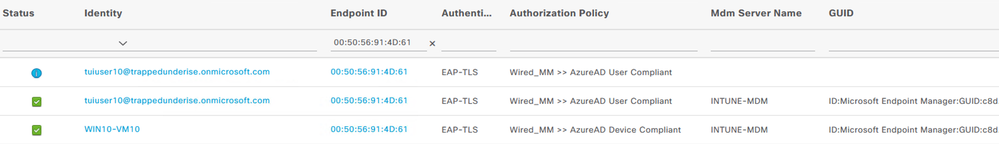


*Example Intune Device PKCS Profile with OU:  
*

The following screenshot shows an example Authorization Policy used for this flow as well as the above User flow. The policy uses similar matching conditions to those used in the Authentication Policy in addition to the MDM Compliance status conditions.



The following image shows example Live Logs from ISE 3.2 for an Entra Joined Device that is configured for EAP-TLS with 'User or computer authentication' using the User and Device Entra ID flows described above.



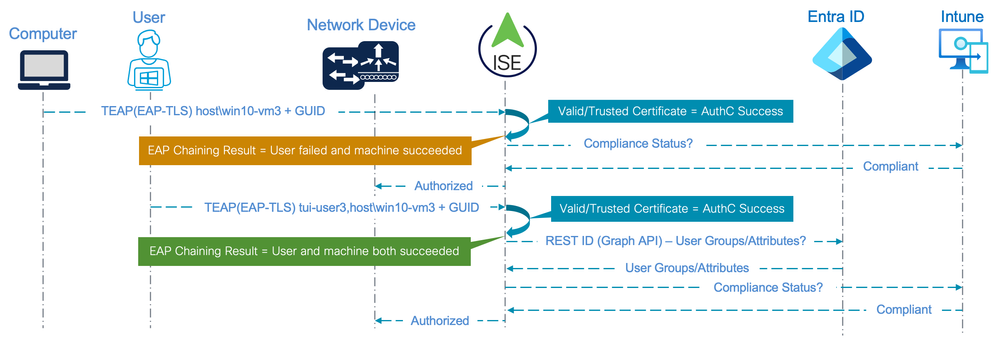
It is important to reiterate that the Device credential is **not** validated by any Identity Store and the Compliance state is checked using the GUID presented in the Device certificate.

If the Device certificate is somehow compromised, the GUID will also be compromised. This could allow a threat actor to gain network access using the certificate. In the event of a lost device and/or a compromised certificate, the Device should be retired or deleted from Intune immediately and the certificate should be revoked.

**Entra Joined Device and Entra User with TEAP(EAP-TLS) and EAP Chaining**

Due to the fix implemented by bugID [CSCwd34467](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwd34467) in ISE 3.2 patch 5 and 3.3 patch 1, it is now possible to use the TEAP and EAP-FAST protocols and EAP Chaining feature described above for **authorization** of sessions involving Entra Joined Devices (not joined to Traditional AD) and Entra ID user accounts. The EAP Chaining results can be combined with other conditions described above (i.e. User Group/Attribute matches, Intune Registration/Compliance status) in the Authorization Policy.

The following diagram illustrates the flow that can be used for both the Device and User sessions in this use case.

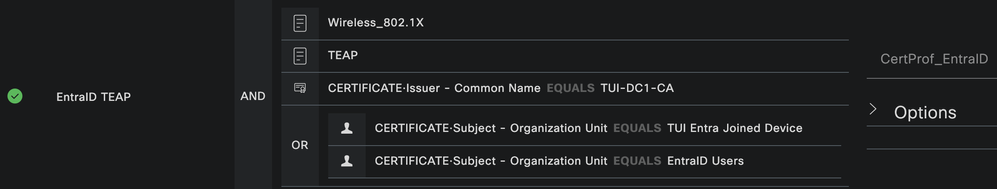


As with the use cases described above, it is important to understand that ISE is **not** capable of performing Authentication against Entra ID for either the Device or User. The Authentication in this case is only based on the client presenting a valid User and Device certificate that is trusted by ISE. The User credential provided within the certificate is not checked against any Identity Store, which could raise security concerns with some organizations.  
For the User session, the same Group and Attribute match conditions are supported as per the above use case with EAP-TLS

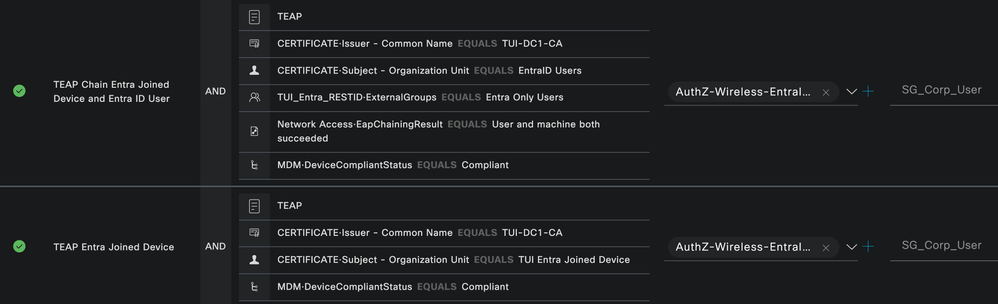
This flow has the following characteristics, caveats, and limitations:

* A minimum of ISE 3.2 patch 5 or 3.3 patch 1 is required for support of the REST ID lookup and the bug fix
* Either the Windows supplicant is configured for 'User or Computer Authentication' with the necessary TEAP(EAP-TLS) protocol settings **or**the Cisco Secure Client Network Access Manager (NAM) supplicant is configured for 'Machine and User Connection' with the necessary EAP-FAST(EAP-TLS) protocol settings
* Use of Intune Registration/Compliance status as a condition of Authorization for either the Device and/or User session (which is optional) requires those certificates to be enrolled via an Intune Configuration Profile (Device/User certificate) so the GUID is present in the SAN field
* If User Group/Attribute conditions are used in the Authorization Policy (which is optional), the User Principal Name (UPN) must be used in either the Certificate ‘Subject – Common Name’ or ‘Subject Alternative Name’ field for the User certificate and the ISE Certificate Authentication Profile (CAP) used for User Authentication must be configured to use the field with the UPN for the identity

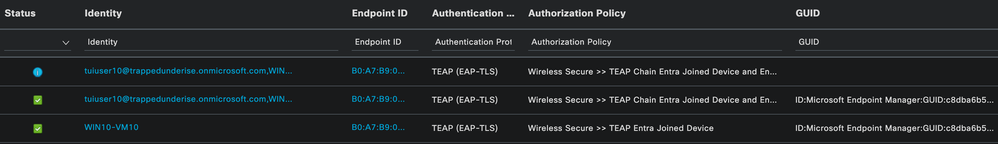
The following screenshot from ISE 3.3 patch 2 shows an example Authentication Policy used for this flow. This policy uses values in the Certificate ‘Subject – OU’ as a matching condition to differentiate from sessions using TEAP(EAP-TLS) with Traditional AD. The ‘Subject – OU’ attribute is a unique static value defined in the Intune Configuration Profile for both the Device and User certificate to provide this differentiation.



The following screenshot shows example Authorization Policies used for the User and Device sessions. The policy uses similar matching conditions to those used in the Authentication Policy in addition to the (optional) MDM Compliance status conditions for both the User and Device as well as a Group match for the User account in Entra ID (also optional).



The following image shows example Live Logs from ISE 3.3 patch 2 for the flow described in this use case.



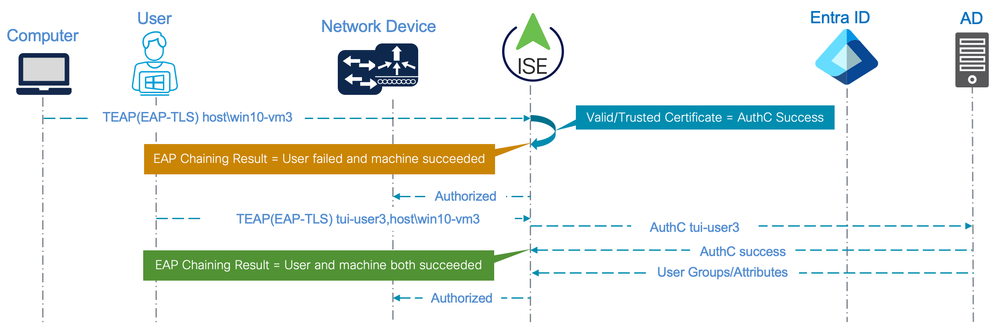
As with the above examples, it is important to reiterate that neither the Device nor User credential is **not** authenticated by any Identity Store and the Compliance state is checked using the GUID presented in the certificate.

If the certificate is somehow compromised, both the Entra ID UPN and the GUID will also be compromised. This could allow a threat actor to gain network access using the certificate. In the event of a lost device and/or a compromised certificate, the Device should be retired or deleted from Intune immediately and the certificates should be revoked.

**Entra Joined Device and AD User with TEAP(EAP-TLS) and EAP Chaining**

Due to the fix implemented by bugID [CSCwd34467](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwd34467) in ISE 3.2 patch 5 and 3.3 patch 1, it is also now possible to use the TEAP and EAP-FAST protocols and EAP Chaining feature described above for **authorization** of sessions involving Entra Joined Devices (not joined to Traditional AD) and Traditional Active Directory User accounts using TEAP(EAP-TLS) or EAP-FAST(EAP-TLS). The EAP Chaining results can be combined with other conditions described above (i.e. User Group/Attribute matches, Intune Registration/Compliance status) in the Authorization Policy.

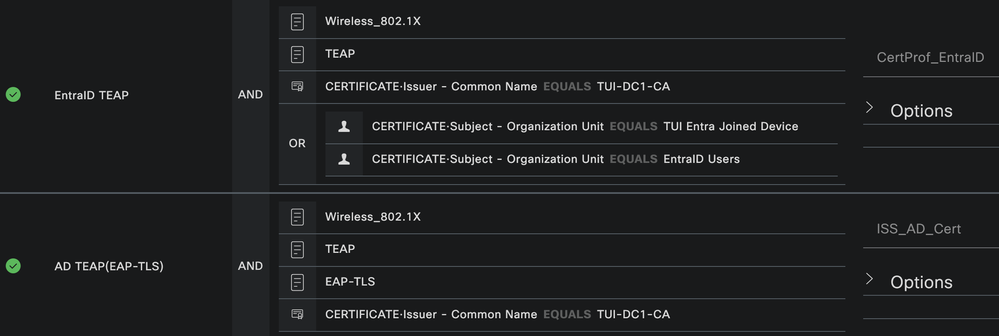
The following diagram illustrates the flow that can be used for both the Device and User sessions in this use case.



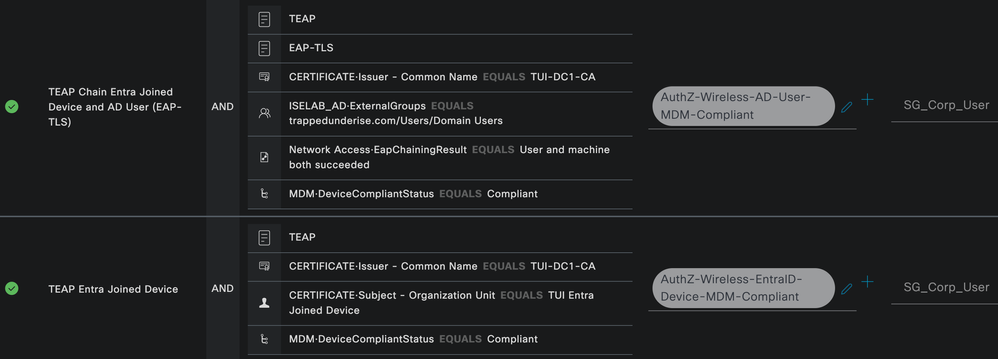
This flow has the following characteristics, caveats, and limitations:

* A minimum of ISE 3.2 patch 5 or 3.3 patch 1 is required for the bug fix
* Either the Windows supplicant is configured for 'User or Computer Authentication' with the necessary TEAP(EAP-TLS) protocol settings **or**the Cisco Secure Client Network Access Manager (NAM) supplicant is configured for 'Machine and User Connection' with the necessary EAP-FAST(EAP-TLS) protocol settings
* While not shown in this example, use of Intune Registration/Compliance status as a condition of Authorization is also supported as reflected in the above use cases

 The following screenshot from ISE 3.3 patch 2 shows example Authentication Policies used for this flow. For the User session, and Identity Source Sequence (ISS\_AD\_Cert) is used to capture the AD Username from the certificate Subject Common Name to use for identity and check that Username against Active Directory.



The following screenshot shows example Authorization Policies used for the User and Device sessions. The policy uses similar matching conditions to those used in the Authentication Policy in addition to the (optional) MDM Compliance status conditions for both the User and Device as well as a Group match for the User account in AD.



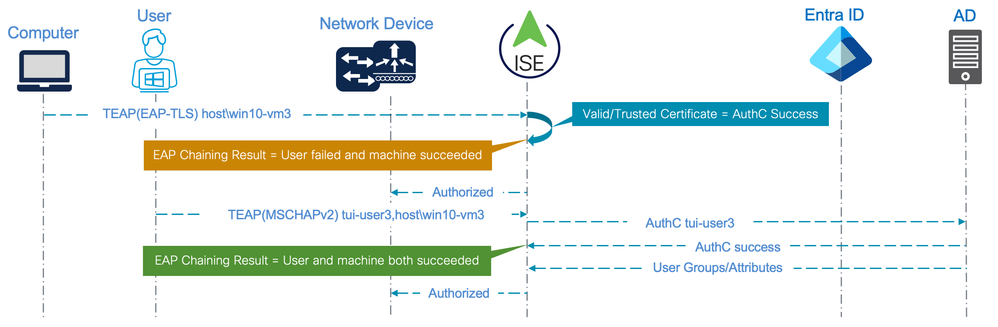
As with the above examples, the Device credential is **not** validated by any Identity Store and the Compliance state is checked using the GUID presented in the Device certificate.

If the Device certificate is somehow compromised, the GUID will also be compromised. This could allow a threat actor to gain network access using the certificate. In the event of a lost device and/or a compromised certificate, the Device should be retired or deleted from Intune immediately and the certificate should be revoked.

**Entra Joined Device with TEAP(EAP-TLS) and AD User with TEAP(MSCHAPv2) and EAP Chaining**

Due to the fix implemented by bugID [CSCwd34467](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwd34467) in ISE 3.2 patch 5 and 3.3 patch 1, it is also now possible to use the TEAP and EAP-FAST protocols and EAP Chaining feature described above for **authorization** of sessions involving Entra Joined Devices (not joined to Traditional AD) and Traditional Active Directory User accounts using a combination of either TEAP(EAP-TLS) and TEAP(EAP-MSCHAPv2) **or** EAP-FAST(EAP-TLS) and EAP-FAST(EAP-MSCHAPv2). The EAP Chaining results can be combined with other conditions described above (i.e. User Group/Attribute matches, Intune Registration/Compliance status) in the Authorization Policy.

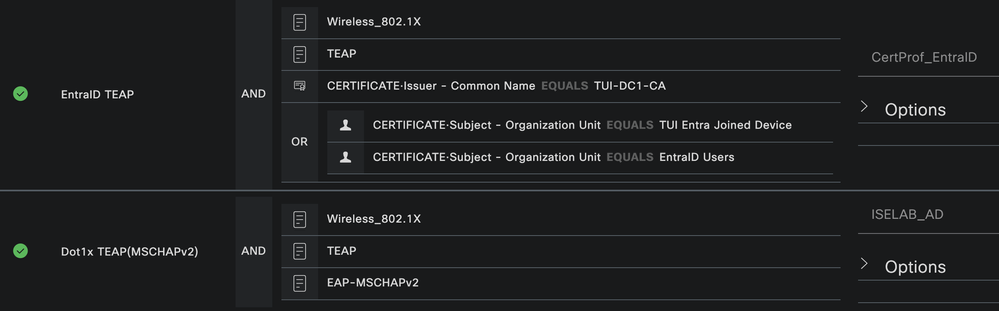
The following diagram illustrates the flow that can be used for both the Device and User sessions in this use case.



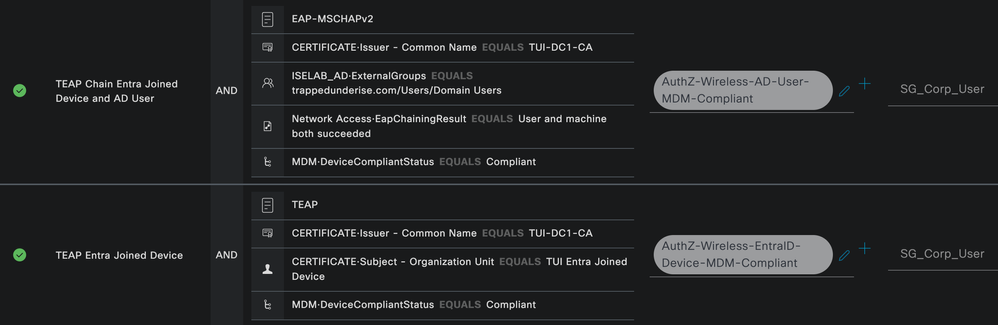
This flow has the following characteristics, caveats, and limitations:

* A minimum of ISE 3.2 patch 5 or 3.3 patch 1 is required for the bug fix
* Either the Windows supplicant is configured for 'User or Computer Authentication' with the necessary TEAP(EAP-TLS) protocol settings **or**the Cisco Secure Client Network Access Manager (NAM) supplicant is configured for 'Machine and User Connection' with the necessary EAP-FAST(EAP-TLS) protocol settings
* While not shown in this example, use of Intune Registration/Compliance status as a condition of Authorization is also supported as reflected in the above use cases
* Use of MSCHAPv2 (in the User session for this example) requires disabling [Credential Guard](https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/considerations-known-issues)
* The user **must** login to Windows using their AD password; they **cannot** use Windows Hello logins with MSCHAPv2 authentication as ISE needs the username and password from the Windows supplicant to authenticate the User against AD.

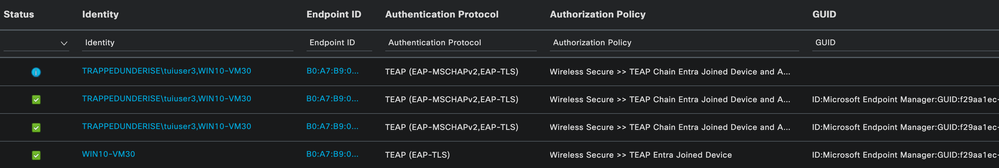
The following screenshot from ISE 3.3 patch 2 shows example Authentication Policies used for this flow.



The following screenshot shows example Authorization Policies used for the User and Device sessions. The policy uses similar matching conditions to those used in the Authentication Policy in addition to the (optional) MDM Compliance status conditions for both the User and Device as well as a Group match for the User account in AD.



The following image shows example Live Logs from ISE 3.3 patch 2 for the flow described in this use case.



As with the above examples, the Device credential is **not** validated by any Identity Store and the Compliance state is checked using the GUID presented in the Device certificate.

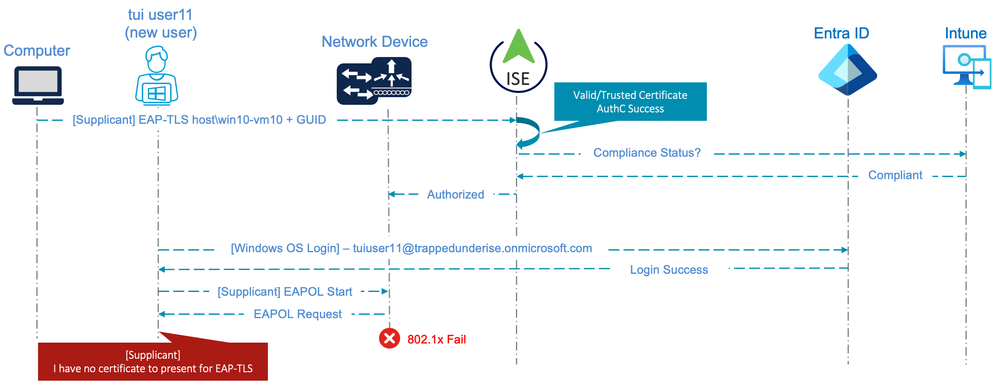
If the Device certificate is somehow compromised, the GUID will also be compromised. This could allow a threat actor to gain network access using the certificate. In the event of a lost device and/or a compromised certificate, the Device should be retired or deleted from Intune immediately and the certificate should be revoked.

**Entra ID Multi-User Scenario**

After some additional discussions with customers, it was determined that the above flow for "Authentication/Authorization of an Entra Joined Device using EAP-TLS" would be relevant for a scenario in which multiple Entra ID Users needed to login to the same Entra Joined Device. When a new Entra ID User logs into an Entra Joined Device, the Windows OS (not the supplicant) must authenticate the credentials against Entra ID. This process happens during the Windows Computer state, therefore network connectivity in this state is required.

Upon successful authentication of the new user, the User's profile is loaded and the desktop is presented. It is important to note, however, that the Intune User Certificate Profiles are not installed immediately as part of the Windows User Profile. If the supplicant is configured for 'User or Computer Authentication' it will attempt to initiate an 802.1x session for the new User. Since there is no User certificate installed yet, this will result in an authentication failure. This results in a 'catch-22' scenario in which there is no network connectivity due to the lack of User certificate, and the User certificate cannot be enrolled due to lack of network connectivity.

The following diagram illustrates the flow and 802.1x failure described in this scenario.

****

As such, the supplicant should be configured for 'Computer Authentication' for this multi-user scenario to mitigate the User authentication failure. However, this will result in the inability to provide differentiated authorization for the users using this Computer. As the User credential is not being provided by the supplicant, this will also result in no visibility of the User associated with this session.

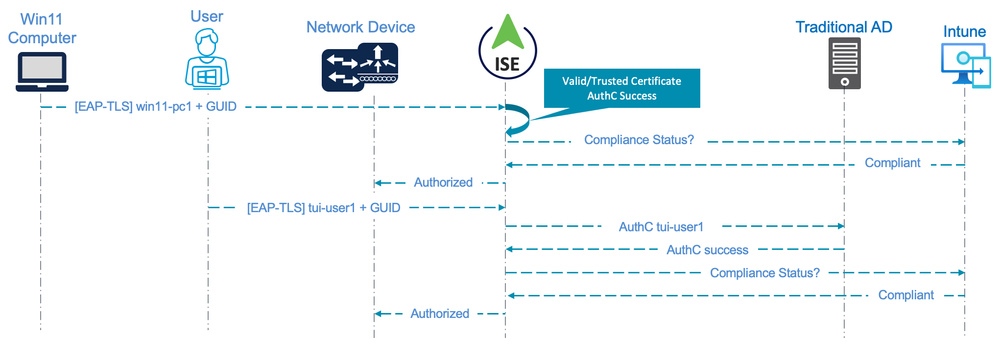
* From ISE 3.2 patch 5 or 3.1 patch 1, this scenario can be mitigated using TEAP(EAP-TLS) to provide network connectivity based on the 'User failed and machine succeeded' EAP Chaining result. This could allow the time and network connectivity necessary for the User certificate profile (and any other required Intune Configuration Profiles) to be pushed to the device.
* This would be a similar scenario to [EAP-TEAP: First time user login/chicken & egg scenario](https://community.cisco.com/t5/network-access-control/eap-teap-first-time-user-login-chicken-amp-egg-scenario/td-p/4475351)

**Mixed Entra Joined Device & Traditional AD User Scenario with EAP-TLS**

Depending on the current state of the Entra ID and Traditional AD environment, a combination of the above flows is also possible. Take the following scenario, for example:

* Windows 10 PCs joined to the organisation's Traditional AD domain
  + Currently using TEAP(EAP-TLS) with EAP Chaining
  + Certificates enrolled using Group Policy
* Corporate AD User accounts synchronised with Entra ID
* Windows 11 PCs being deployed
  + Entra ID Joined (not Hybrid or joined to Traditional AD)
  + Intune Managed
  + Certificates enrolled using Intune; unique Subject OU used in the template to provide differentiation in ISE policies

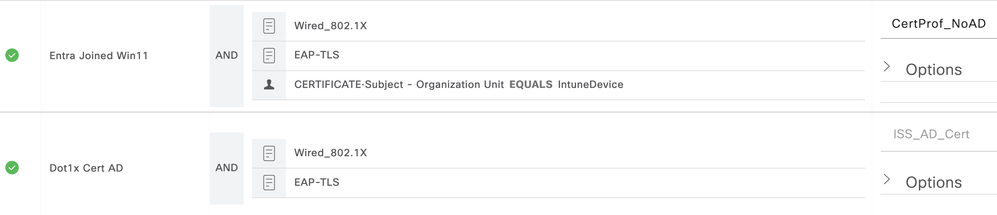
The following diagram illustrates the flow used for this scenario.



This flow has the following caveats and limitations:

* Windows supplicant configured for EAP-TLS with 'User or Computer' authentication
* Device Authentication is based purely on a valid/trusted certificate presented by the endpoint
* User Authentication is performed against the organisation's Traditional AD
* Device Authorization is based only on the trusted certificate (with Subject OU = IntuneDevice) and (optional) Intune compliance
* User Authorization is based on AD Group membership, the certificate Subject OU (IntuneUser) and (optional) Intune compliance
* For Intune compliance, the certificate used for the both the User and Computer state must be enrolled via an Intune Configuration Profile so the GUID is present in the SAN field.
* As there is no interaction with Entra ID, this specific flow can technically be used with ISE version 3.1 and above.

The following screenshot shows an example Authentication Policy used for this flow. This policy uses values in the Certificate ‘Subject – OU’ as a matching condition to differentiate from the current Windows 10 sessions using TEAP(EAP-TLS). The ‘Subject – OU’ attribute is a unique static value defined in the Intune Configuration Profile to provide this differentiation.



The following screenshot shows an example Authorization Policy used for this flow. The policy uses similar matching conditions to those used in the Authentication Policy in addition to the MDM Compliance status conditions.



The Intune compliance check is used for both the Computer and User session. This was done to provide for the scenario in which a User is already logged in when the Windows 11 endpoint is connected to the network. In that scenario, there would be no Computer session involved unless/until the User logs out.

**Additional Use Cases**

The following links provide additional use cases for User and/or Device authentication in relation to Entra ID.

[ISE BYOD Flow Using Entra ID](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675)

**Summary**

The following table summarises the available options at the time of this writing for Computer/User Authentication and Intune MDM Compliance with ISE when using Traditional AD versus Entra ID.

The EAP-FAST references below require the use of the Cisco Secure Client Network Access Manager (NAM) supplicant and were validated using Secure Client version 5.1.4.74.

