

InTune

Overview

InTune is Microsofts MDM Product. More information can be found at the Microsoft Documentation Library for InTune^[1]

InTune can be hosted in the cloud or on premis. All endpoint information is held on a Microsoft SQL database. This can be directly queried by ClearPass to determine if the device trying to connect to the network is a known device under InTune MDM management.

Configuration Steps

Define InTune as an authentication source

Type : SQL

Use for Authorization : Enabled

Server name : best practise to use FQN

Database name, username and password : You require a read-only database account. Every CPPM query in this authentication source will use these credentials

Port : 1433 by default for an SQL database

<https://arubapedia.arubanetworks.com/arubapedia/images/2/20/InTuneSummary.jpg>

Create an SQL filter that checks whether the device (by MAC address) is marked as a corporate device within the InTune database.

The use case is to only allow corporate devices onto the corporate wireless network covered by this Service.

Attribute filter :

SELECT Name0 DeviceName, wifimac00 DeviceMAC, deviceowner0 CorpOrPersonal

FROM device_wlan_data t1, system_disc t2

WHERE t1.machineid=t2.itemkey AND deviceowner0=1 AND
t1.WiFiMAC00='%{Connection:Client-Mac-Address-Hyphen}'

| Name | Alias Name | Data type | Enabled As |
|--------------------|-----------------|-----------|-----------------|
| 1. DeviceName | Phone | String | Role, Attribute |
| 2. CorpOrPersonal | CorporateDevice | Integer | Attribute |
| 3. DeviceMac | PhoneMAC | String | Attribute |
| 4. Click to add... | | | |

On calling this SQL it can return the following attributes:

1. Phone: this contains the InTune's device's name
2. CorporateDevice: this indicates ownership details

3. PhoneMAC

These attributes can then be referenced in the Service's Roles and Enforcement Policies.

Authorization Source

Add the InTune authentication source to the service's Authorization source tab:

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Authorization Details:

Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

| Authentication Source | Attributes Fetched From |
|---|--|
| 1. Active Directory BC [Active Directory] | Active Directory BC [Active Directory] |
| 2. [Local User Repository] [Local SQL DB] | [Local User Repository] [Local SQL DB] |

Additional authorization sources from which to fetch role-mapping attributes -

InTune [Generic SQL DB]

RemoveView DetailsModify

--Select to Add--

Role Mapping

Create a role mapping condition that verifies the device's MAC (PhoneMAC) address existing in InTune's

| | |
|--|-----------------------|
| (Authorization:InTune:PhoneMAC EXISTS) | |
| AND (Authentication:Status EQUALS User) | ROLE-CORPORATE-MOBILE |
| AND (Authorization:Active Directory BC:memberOf CONTAINS RESWIRELESSUSER01G) | |

This role mapping also checks whether the user is in an AD group. This is optional but a useful method of preventing some corporate mobile users access to the corporate network from these devices. In this use case the devices were not AD objects.

Enforcement Policy

Create an policy condition that uses the "ROLE-CORPORATE-MOBILE" to assign the appropriate Profile

| | |
|---|---|
| (Tips:Role EQUALS ROLE-LOCATION-SSC-WALSGRAVE) | PROFILE-WIFI-SSC-WALSGRAVE-MOBILE-WIFI |
| AND (Tips:Role EQUALS ROLE-CORPORATE-MOBILE) | |
| (Tips:Role EQUALS ROLE-LOCATION-SSC-HOLBORN) | PROFILE-WIFI-SSC-HOLBORN-MOBILE-WIFI |
| AND (Tips:Role EQUALS ROLE-CORPORATE-MOBILE) | |
| (Tips:Role EQUALS ROLE-LOCATION-SSC-MANCHESTER) | PROFILE-WIFI-SSC-MANCHESTER-MOBILE-WIFI |
| AND (Tips:Role EQUALS ROLE-CORPORATE-MOBILE) | |
| (Tips:Role EQUALS ROLE-LOCATION-SSC-ANSTY) | PROFILE-WIFI-SSC-ANSTY-MOBILE-WIFI |
| AND (Tips:Role EQUALS ROLE-CORPORATE-MOBILE) | |
| (Tips:Role EQUALS ROLE-LOCATION-SSC-LOCHSIDE) | PROFILE-WIFI-SSC-LOCHSIDE-MOBILE-WIFI |
| AND (Tips:Role EQUALS ROLE-CORPORATE-MOBILE) | |

This enforcement policy structure also checked the user location. This is optional but it allows CPPM to apply business requirement logic and prevent corporate mobile access in locations which have poor WAN links. Transaction data took a higher priority on these links than someone checking email on a corporate mobile!

References

[1] <https://technet.microsoft.com/en-us/library/jj676587.aspx>

Article Sources and Contributors

InTune *Source:* <https://arubapedia.arubanetworks.com/arubapedia/index.php?oldid=138023> *Contributors:* Carlos, Ctagg, Dmellor

Image Sources, Licenses and Contributors

File:InTune Attributes.jpg *Source:* https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:InTune_Attributes.jpg *License:* unknown *Contributors:* Dmellor
File:AuthorizeSource.jpg *Source:* <https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:AuthorizeSource.jpg> *License:* unknown *Contributors:* Dmellor
File:RoleCondition.jpg *Source:* <https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:RoleCondition.jpg> *License:* unknown *Contributors:* Dmellor
File:PolicyCondition.jpg *Source:* <https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:PolicyCondition.jpg> *License:* unknown *Contributors:* Dmellor