# Authentification basée sur les attributs ISE et LDAP

## Contenu

Introduction Conditions préalables Conditions requises Components Used Configuration Diagramme du réseau Configurations Configurer LDAP Configuration du commutateur Configuration ISE Vérification Dépannage

#### Introduction

Ce document décrit comment configurer Cisco Identity Services Engine (ISE) et utiliser les attributs d'objets LDAP (Lightweight Directory Access Protocol) pour authentifier et autoriser dynamiquement les périphériques.

#### Note: Ce document est valide pour les configurations qui utilisent LDAP comme source d'identité externe pour l'authentification et l'autorisation ISE.

Contribué par Emmanuel Cano et Mauricio Ramos Ingénieur des services professionnels Cisco.

### Édité par Neri Cruz ingénieur TAC Cisco.

#### Conditions préalables

#### **Conditions requises**

Cisco vous recommande de connaître les sujets suivants :

- Connaissance de base des ensembles de politiques ISE, des politiques d'authentification et d'autorisation
- Protocole MAB (Mac Authentication Bypass)
- Connaissances de base du protocole Radius
- Connaissances de base du serveur Windows

#### **Components Used**

Les informations de ce document sont basées sur les versions logicielles et matérielles suivantes :

- Cisco ISE, correctif 11 de la version 2.4
- Microsoft Windows Server, version 2012 R2 x64
- Commutateur Cisco Catalyst 3650-24PD, version 03.07.05.E (15.2(3)E5)
- Ordinateur Microsoft Windows 7

**Note:** The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

#### Configuration

Cette section décrit comment configurer les périphériques réseau, l'intégration entre ISE et LDAP, et enfin configurer les attributs LDAP à utiliser dans la stratégie d'autorisation ISE.

#### Diagramme du réseau

Cette image illustre la topologie de réseau utilisée :



Voici le flux de trafic, comme illustré dans le schéma de réseau :

- 1. L'utilisateur connecte son ordinateur portable au port de commutation désigné.
- 2. Le commutateur envoie une requête d'accès Radius à l'ISE pour cet utilisateur
- 3. Lorsque l'ISE reçoit les informations, il interroge le serveur LDAP pour le fichier utilisateur spécifique, qui contient les attributs à utiliser dans les conditions de la stratégie d'autorisation.
- 4. Une fois que l'ISE a reçu les attributs (port de commutateur, nom de commutateur et adresse MAC de périphérique), il compare les informations fournies par le commutateur.
- 5. Si les informations d'attributs fournies par le commutateur sont identiques à celles fournies par LDAP, l'ISE envoie un ACCEPT RADIUS avec les autorisations configurées sur le profil d'autorisation.

#### Configurations

Utilisez cette section afin de configurer LDAP, le commutateur et l'ISE.

#### **Configuration LDAP**

Procédez comme suit pour configurer le serveur LDAP :

#### 1. Accédez à Gestionnaire de serveur > Tableau de bord > Outils > Modifier ADSI



2. Cliquez avec le bouton droit de la souris sur l'icône de modification ADSI et sélectionnez Se connecter à...

File Action	View Help	
♦	Q 📑 🚺	
📝 ADSI Edit		
⊿ 🗎 LDA	Connect to	
	View	•
	Refresh	
	Export List	
	Help	

3. Sous Paramètres de connexion, définissez un nom et sélectionnez le bouton **OK** pour démarrer la connexion.

Connection Settings
Name: Default naming context
Path: LDAP://WIN-8G7QAP9T36L.ciscoise.lab/Default naming context
Connection Point
O Select or type a Distinguished Name or Naming Context:
×
Select a well known Naming Context:
Default naming context 🗸
Computer
<ul> <li>Select or type a domain or server: (Server   Domain [:port])</li> </ul>
×
Default (Domain or server that you logged in to)
Use SSL-based Encryption
Advanced OK Cancel

4. Dans le même menu ADSI Edit, cliquez avec le bouton droit de la souris dans la connexion DC (DC=ciscodemo, DC=lab), sélectionnez Nouveau, puis sélectionnez l'option Objet

DC=Ial	h			
tin		New	•	Object
npute nain C		Rename		
eignSe tAndF		Properties		
naged )S Qui		Help		
gram Da	ata			
em				
1 Device	es			
rs				
Users				

5. Sélectionnez l'option Unité d'organisation comme nouvel objet et sélectionnez Suivant.

Create Object	×
Select a class:	
msSFU30MailAliases msSFU30NetId msSFU30NetworkUser msTPM-InformationObjectsContainer nisMap nisNetgroup nisObject oncRpc	
organization organizationalUnit physicalLocation printOueue	~
< Back Next >	Cancel Help

6. Définissez un nom pour la nouvelle unité d'organisation et sélectionnez Suivant

	Create Object X
Attribute:	ou
Syntax:	Unicode String
Description:	Organizational-Unit-Name
Value:	AppleDevices
	Cancel Hala
	< baox Next > Cancel Help

7. Sélectionnez Terminer afin de créer la nouvelle unité d'organisation

Create Object	x
To complete the creation of this object, click Finish.	
To set more attributes, click More Attributes. More Attributes	
	_
< Back Finish Cancel Help	

8. Cliquez avec le bouton droit sur l'unité d'organisation qui vient d'être créée et sélectionnez Nouveau > Objet

CN=Builtin CN=Comput OU=Domain	Move New Connection from Here		
CN=Foreign	New	•	Object
CN=LostAnc	View		
📔 CN=Manage	VIEW	·	
CN=NTDS Q	Delete		
🦰 CN=Progran	Rename		
CN=System	Refresh		
📔 CN=TPM De			
CN=Users	Export List		
CN=VPNUse	Properties		
OU=Develop	Help		
📔 OU=AppleDe	help		

9. Sélectionnez le périphérique en tant que classe d'objet et sélectionnez suivant

Create Object	×
Select a class:	
builtinDomain classStore computer contact container country device dfsConfiguration domainDNS domainPolicy friendlyCountry group group crounOff IniqueNames	
< Back Next > Ca	incel Help

10.Définissez un nom dans le champ Valeur et sélectionnez Suivant

	Create Object X
Attribute:	an
Syntax:	Unicode String
Description:	Common-Name
Value:	LaptopTest
	< Back Next > Cancel Help

Create Object	x
To complete the creation of this object, click Finish.	
To set more attributes, click More Attributes. More Attributes	
< Back Finish Cancel Help	

11. Dans le menu déroulant, sélectionnez une propriété à afficher, sélectionnez l'option macAddress, puis définissez l'adresse MAC du point de terminaison qui sera authentifiée sous le champ Modifier l'attribut et sélectionnez Ajouter un bouton pour enregistrer l'adresse MAC du périphérique.

Remarque : utilisez deux-points au lieu de points ou un trait d'union entre les octets d'adresse MAC.

cn=L	aptopTest ×
Attributes	
Path: Class: device	
Select which properties to view:	Optional V
Select a property to view:	macAddress 🗸
Attribute Values	
Syntax: IA5String	
Edit Attribute:	
Value(s): 6C:B2:AE:3A:68	:6C
	Add Remove
	OK Cancel

12. Sélectionnez OK afin d'enregistrer les informations et continuer avec la configuration de l'objet du périphérique

13. Sélectionnez Terminer afin de créer le nouvel objet de périphérique

Create Object	x
To complete the creation of this object, click Finish.	
To set more attributes, click More Attributes. More Attributes	
< Back Finish Cancel Help	

14. Cliquez avec le bouton droit sur l'objet du périphérique et sélectionnez l'option Propriétés

ADSI Edit

	Name	Cla	355	Distinguished Name
	CN=LaptopTest	dev	vice	CN=LaptopTest,OU=AppleDevices,DC=ciscoise,DC=lab
		Move		
		Delete		
		Rename		
1		Properties		
		Help		

15. Sélectionnez **description** de l'option et **Modifier** afin de définir le nom du commutateur et le port de commutateur où le périphérique sera connecté.

ttribute Editor Security	
Attributes	
Attribute	Value
adminDescription	(not set)
adminDisplayName	(not set)
bootFile	(not set)
bootParameter	(not set)
cn	LaptopTest
description	<pre>(not set)</pre>
displayName	<not set=""></not>
displayNamePrintable	<not set=""></not>
distinguishedName	CN=Laptop Test.OU=AppleDevices.DC=cisc
dSASignature	<not set=""></not>
dSCorePropagationD	0x0 = ( )
extensionName	<not set=""></not>
flags	<not set=""></not>
fSMORoleOwner	<not set=""></not>
<	>
Edit	Filter
011	

16. Définissez le nom du commutateur et le port de commutateur. Veillez à utiliser une virgule pour séparer chaque valeur. Sélectionnez Ajouter, puis OK pour enregistrer les informations.

Multi-valued String Editor		x
Attribute: description		
Value to add:		_
switchapflexconnect,GigabitEthemet1/0/6	Add	
Values:		
	Remove	
		_
OK	Cancel	

- Switchapflexconnect est le nom du commutateur.
- GigabitEthernet1/0/6 est le port de commutation auquel le point d'extrémité est connecté.

Note: Il est possible d'utiliser des scripts afin d'ajouter des attributs à un champ spécifique, cependant, pour cet exemple, nous définissons les valeurs manuellement

Note: L'attribut AD est sensible à la casse, si vous utilisez toutes les adresses Mac dans ISE en minuscules convertis en majuscules au cours de la requête LDAP. Afin d'éviter ce comportement, désactivez la recherche d'hôte de processus sous les protocoles autorisés. Vous trouverez des détails sur ce lien : <u>https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin\_guide/b\_ISE\_admin\_3\_0.pdf</u>

## Configuration du commutateur

La section suivante décrit la configuration de la communication 802.1x entre ISE et le commutateur.

aaa new-model ! aaa group server radius ISE server name ISE deadtime 15 ! aaa authentication dot1x default group ISE aaa authorization network default group ISE aaa accounting update newinfo aaa accounting dot1x default start-stop group ISE ! aaa server radius dynamic-author client 10.81.127.109 server-key XXXXabc ! aaa session-id common switch 1 provision ws-c3650-24pd ! dot1x system-auth-control dot1x critical eapol diagnostic bootup level minimal spanning-tree mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level 3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127 switchport mode access authentication event fail action next-method authentication event server dead action authorize vlan 127 authentication event server alive action reinitialize authentication host-mode multi-domain authentication open authentication order dot1x mab authentication priority dot1x mab authentication port-control auto authentication periodic authentication timer reauthenticate server authenticator timer inactivity server dynamic authentication violation restrict mab dot1x pae authenticator dot1x timeout tx-period 10 spanning-tree portfast ! radius server ISE address ipv4 10.81.127.109 auth-port 1812 acct-port 1813 automate-tester username radiustest idle-time 5 key XXXXabc !

Note: Il se peut que la configuration globale et la configuration d'interface doivent être ajustées dans votre environnement

#### **Configuration ISE**

Les éléments suivants décrivent la configuration sur ISE pour obtenir les attributs du serveur LDAP et configurer les stratégies ISE.

1. Sur ISE, accédez à Administration->Gestion des identités->Sources d'identité externes et sélectionnez le dossier LDAP et cliquez sur Ajouter afin de



2. Sous l'onglet Général, définissez un nom et sélectionnez l'adresse MAC comme attribut Nom du sujet

LDAP Identity Sources List > Ide	p_mab				•	
LDAP Identity Source						
General Conn	ection Directory Organizatio	n Groups	Attributes	Advanced Settings		
* Name	ldap_mab					
Description						
- Schema	Custom .					
* Subject Objectclass	device	* Group Objectclass	Group			
* Subject Name Attribute	macAddress	* Group Map Attribute	member			
* Group Name Attribute	distinguishedName	Certificate Attribute				
O Rubiard Objects Cont	ain Balamana To Comuna					
Oracita Objects Conta	an Reference to Groups					
<ul> <li>Group Objects Contain</li> </ul>	n Reference to subjects					
	Subjects In Groups Are Stored	In Member Attribute As	Distinguished Name			
User Info Attributes ()						
First Name		Department				
Last Name		Organizational Unit				
Job Title		Locality				
Email		State or Province				
Telephone		Country				
Charles & Charles		county)				
Street Address						

3. Sous l'onglet **Connexion**, configurez l'adresse IP, le nom de domaine d'administration et le mot de passe du serveur LDAP pour obtenir une connexion réussie.

General Connection	Directory Organization	Groups	Attributes	Advanced Settings	
Primar	y Server			Se	econdary Server
					Enable Secondary Server
* Hostname/IP 10.81	.127.111			Hostname/IP	x.
* Port 389				Port 3	89
Specify server for each ISE node					
Access	Anonymous Access			Aco	ess 💿 Anonymous Access
	<ul> <li>Authenticated Access</li> </ul>				Authenticated Access
Admin DN	* cn=administrator, cn=users, dc=	c		Admin I	DN
Password	• •••••			Passwo	ord
Caston Authoritanian	C Enable Service Authentication			Passing & the strent set	Enable Serves Authoritization
Secure Authentication	Enable Server Identity Check			Secure Authenticat	Enable Server Identity Check
LDAP Server Root CA	Certificate Services Root CA - *	æ		LDAP Server Root	CA Certificate Services Root CA - *
		Th.		Issuer CA of ISE Certificat	Calant H manipud (antiant) * (1)

Note: Le port 389 est le port par défaut utilisé.

4. Sous l'onglet Attributs, sélectionnez les attributs macAddress et description. Ces attributs seront utilisés dans la stratégie d'autorisation

#### LDAP Identity Sources List > Idap\_mab

#### **LDAP Identity Source**

General Conr	nection	Directory Organization	Groups	Attributes	Advanced Settings
/ Edit 🕂 Add 👻 🗙 Delete	e Attribute				
Name	🔺 Туре	Default	Internal Name		
description	STRING		description		
distinguishedName	STRING		distinguishedName		
macAddress	STRING		macAddress		

5. Pour créer un protocole autorisé, accédez à **Policy->Policy Elements->Results->Authentication->Allowed Protocols.** Définissez et sélectionnez Process Host Lookup et Allow PAP/ASCII comme les seuls protocoles autorisés. Enfin, sélectionnez **Enregistrer** 

cisco Identity Services Engine	Home  + Context Visibility  + Operations	Policy Administration
Policy Sets Profiling Posture C	nt Provisioning    Policy Elements	
Dictionaries  Conditions Result		
Authentication	Allowed Protocols Services List > MAB_MacAddres Allowed Protocols	•
Allowed Protocols	Name MA8_MacAddress	]
Authorization	Description	
Profiling		
Posture	<ul> <li>Allowed Protocols</li> </ul>	
Client Provisioning	Authentication Bypass	
	Process Host Lookup (2)	
	Authentication Protocols	
	Allow PAP/ASCII	

6. Pour créer un profil d'autorisation, accédez à **Policy->Policy Elements->Results->Authorization->Authorization Profiles.** Sélectionnez **Ajouter** et définissez les autorisations qui seront attribuées au point de terminaison.

dentity Services Engine	Home	s  Policy  Administration	<ul> <li>Work Centers</li> </ul>
Policy Sets    Policy Elements			
Dictionaries  Conditions  Results			
0			
Authentication	Standard Authorization Profiles		
- Authorization	For Policy Export go to Administration > Sy	stem > Backup & Restore > Policy Expo	ort Page
Authorization Profiles	/ Edit 🕂 Add 🕞 Duplicate 🗙 Delete		
Dowoloodoble ACLs	Name	Profile	
Downloadable ACLS	Blackhole_Wireless_Access	🚓 Cisco 🕀	
Profiling	Cisco_IP_Phones	🗰 Cisco 🕀	
→ Posture	Cisco_Temporal_Onboard	💏 Cisco 🕀	

dentity Services Engine	Home	ns  Policy  Administration	Work Centers
Policy Sets    Policy Elements			
Dictionaries + Conditions - Resul	8		
Authentication	Authorization Profiles > New Authorization Authorization Profile	Profile	
- Authorization	* Name MACPORTSWI	<b>ICHLDAP</b>	
Authorization Profiles	Description		At
Downloadable ACLs	* Access Type ACCESS_ACCE	т т	
Profiling	Network Device Profile 🛛 🗮 Cisco 👻	Ð	
→ Posture	Service Template		
Client Provisioning	Track Movement		
	Passive Identity Tracking 🗌 🕧		
	<ul> <li>Common Tasks</li> </ul>		
	DACL Name	PERMIT_ALL_IPV4_TRAFFIC	

7.Accédez à Policy-> Policy Set et créez un jeu de stratégies à l'aide de la condition prédéfinie Wired\_MAB et du protocole autorisé créé à l'étape 5.

Policy Sets - MAB_LDAP			Reset Policyset Hitcounts Reset	Save
Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Search				
Ø MAB_LDAP		Wired_MAB	MAB_MacAddress x v +	0

8. Sous le nouveau jeu de stratégies créé, créez une stratégie d'authentification à l'aide de la séquence de source d'identité externe de la bibliothèque Wired\_MAB prédéfinie et de la connexion LDAP

Autor	incereor i	romy (z)							
•	Status	Rule Name	Con	Rions		Use		Hits	Actions
earch									
						idap_mab	x v		
						♥ Options			
						If Auth fail			
	0	Auth_MAB_LDAP		Wired_MAB		REJECT	× *	0	۰
			_			If User not found			
						REJECT	× *		
						If Process fail			
						DROP	**		
						DenyAccess			
	0	Default			¢,	> Options		0	•

9. Sous Stratégie d'autorisation, définissez un nom et créez une condition composée à l'aide de la description de l'attribut LDAP, de l'ID de port NAS Radius et de NetworkDeviceName. Enfin, ajoutez le profil d'autorisation créé à l'étape 6.

C	onditions Studio									0	$\times$
Lib	brary		Editor								
\$	Search by Name										00
9		9 t †		Ê.	Click to act	- an awn	Allebude uniture			-	
	EAP-TLS	Ø			Equais	Attribute value				-	0
1	Guest_Flow	0	AND ¥	Ŀ	Click to add an attribute						
	MAC_in_SAN	Ø		3	Equals	•	Attribute value				
1	Network_Access_Authentication_Passed	Ø					- New AND	OP			
Ī	Non_Cisco_Profiled_Phones	0									2
	Non_Compliant_Devices			Set to 'Is not' Duplicate					Duplicate	Save	
	Switch_Local_Web_Authentication	Ø									
	Switch_Web_Authentication	0									
1	Wired_802.1X	Ø									
1	Wired_MAB	0									
							Results				
Rul	le Name Conditions						Profiles	Security Groups		Hits	Action
Rul	le Name Conditions	ion CONTAINS R	dius NAS-Port-Id twork Access Netw	orkDeviceName			Profiles (+ MACPORTSWITCHLDAP) +	Security Groups		Hits	Action.

Après avoir appliqué la configuration, vous devez pouvoir vous connecter au réseau sans intervention de l'utilisateur.

## Vérification

Une fois connecté au port de commutateur désigné, vous pouvez taper show authentication session interface GigabitEthernet X/X/X pour valider l'état d'authentification et d'autorisation du périphérique.

Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID: 0x103DFC000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir: both Session timeout: N/A Restart timeout: N/A Common Session ID: 0A517F65000013DA87E85A24 Acct session ID: 0x000015D9 Handle: 0x9300005C Current Policy: Policy\_Gi1/0/6 Local Policies: Service Template: DEFAULT\_LINKSEC\_POLICY\_SHOULD\_SECURE (priority 150) Security Policy: Should Secure Security Status: Link Unsecure Method status list: Method State mab Authc Success Sur ISE, vous pouvez utiliser Radius Live Logs pour confirmer.

C F	Refresh O Reset Repeat Counts 💆 Export To -											
	Time Status Details Repeat Id		Identity	Endpoint ID	Endpoint P Authentication Policy	Server	Authorization Profiles					
×		•			Identity	Endpoint ID	Endpoint Prof Authentication Policy	Server	Authorization Profiles			
	Jan 20, 2020 06:21:47.825 PM	•	0	0	employee1@ciscodemo.lab	6C:B2:AE:3A:68:6C	Unknown	ise23-1	MACPORTSWITCHLDAP			
	Jan 20, 2020 06:21:47.801 PM		0		employee1@ciscodemo.lab	6C:82:AE:3A:68:6C	Unknown	ise23-1	MACPORTSWITCHLDAP			

# Dépannage

Sur le serveur LDAP, vérifiez que l'adresse MAC, le nom de commutateur approprié et le port de commutateur du périphérique créé sont configurés.

CN=	LaptopTest Properties ? ×
Attribute Editor Security	
Attributes:	
Attribute	Value 🔨
lastKnownParent	<not set=""></not>
macAddress	6C:B2:AE:3A:68:6C
manager	<not set=""></not>
mS-DS-ConsistencyC	<not set=""></not>
mS-DS-ConsistencyG	<not set=""></not>
msDS-LastKnownRDN	<not set=""></not>
msDS-NcType	<not set=""></not>
msSFU30Aliases	<not set=""></not>
msSFU30Name	<not set=""></not>
msSFU30NisDomain	<not set=""></not>
name	LaptopTest
nisMapName	<not set=""></not>
0	<not set=""></not>
objectCategory	CN=Device,CN=Schema,CN=Configuration, [ 🗸
< 111	>
Edit	Filter
ОК	Cancel Apply Help

CN=	LaptopTest Properties ? ×						
Attribute Editor Security							
Attributes:							
Attribute	Value ^						
adminDescription	<not set=""></not>						
adminDisplayName	<not set=""></not>						
bootFile	<not set=""></not>						
bootParameter	<not set=""></not>						
cn	Laptop Test						
description	switchapflexconnect,GigabitEthemet1/0/6						
displayName	<not set=""></not>						
displayNamePrintable	<not set=""></not>						
distinguishedName	CN=LaptopTest,OU=AppleDevices,DC=cisc						
dSASignature	<not set=""></not>						
dSCorePropagationD	0x0 = ( )						
extensionName	<not set=""></not>						
flags	<not set=""></not>						
fSMORoleOwner	<not set=""></not>						
<							
Edit	Filter						
ОК	Cancel Apply Help						

Sur ISE, vous pouvez prendre une capture de paquets (Accédez à **Opérations->Dépannage->Outil de diagnostic->Dumps TCP**) afin de valider que les valeurs sont envoyées de LDAP à ISE

27	124,204090	18.81.127.189	18,81,127,111	Line	201	searchinguest121 "Rongpladevices,80-classeen,80-lat" whilefalletime	
28	124,308017	38.40.127.111	38.81.127.300	LOW	202	searchiesExtry(2) *OH-Laptophert,00-Applatencies,80-clacations,00-clat*   searchiesDenci2) secons	
29	324.303231	18.81.127.189	38,81,127,113	LEHP	233	sear-thepast131 "Bodgstebectors,30-classion,30-fait" whitebattree	
10	124, 128283	18.81.127.111	18,81,127,189	1.010	110	unard/Andistry(3) "Objaging/ext, Objaging/ext, St-ciacadess, St-cial"   unard/Andisectation -	4
31	124, 101079	18.81.107.189	18,81,127,111	LENP	100	overthinguestial "Budgpielewices, Dicissione, Dicist" wholeholdree	
32	124,305384	14.41.127.111	18,81,127,199	LEMP	- 64	searchicologiai accoss (2 results)	
33	121.404145	10.01.117.108	38.82.107.111	1.5.00	100	searching as (15) "Riska lefectors, Nuclearabae, Mulat" statisfications	
					-	constant accepted accepted accepted	
	* attribu	tes: 3 items					
	<ul> <li>Parts</li> </ul>	aAUV/IbAstist its	<ul> <li>description</li> </ul>				
	19	pel description					
	7.14	fail 1 sham					
		Annohulation and	tchop/Texcomect_Gigab	at the rest is	1.1		
	<ul> <li>Parts</li> </ul>	INTERNAL INCOME.	#1stinguisheddane				
	14	per distinguished an					
	1.14	fact 1 liters					
		Anto-DutaWalters (Sec.	apteralizat, Minkaplathey	term. Most tax	-	n, Novian	
	<ul> <li>Barili</li> </ul>	addentributed but item	and Maliness				
	1.	call machiness					
	7.10	fact 1 them					
		Anteritational and Mini-	12-AP-34-AP-07				
			11 - 12 - 2-1 - 12 - 17 - 17 - 17 - 17 -				