

لوصول في مكحتل مئوق نيوكت ISE في مدختسم لكل يكيمانيدل

تايوتحمل

[عمدقمل](#)

[قيساسألابلطتمل](#)

[تابلطتمل](#)

[عمدختسمل تانوكمل](#)

[قيساسأ تامولعم](#)

[نيوكتل](#)

[ISE يلغ عمديج صصخم مدختسم عمس نيوكت](#)

[dACL ليل لوصول في مكحتل عمئاق نيوكت](#)

[قصصخمم عمسل عم يلخادم مدختسم باسح نيوكت](#)

[AD مدختسم باسح نيوكت](#)

[ISE ليل AD نم عمسلل داريتمل](#)

[نييخراخل او نييخراخل ني مدختسم ملل لي وختل في رعت تافل م نيوكت](#)

[لي وختل تاسايس نيوكت](#)

[حصلل نم ققحتل](#)

[اهجالص او عاطخال فاشكتسا](#)

عمدقمل

مدختسم لكل (dACL) يكيمانيدل لوصول في مكحت عمئاق نيوكت دنتمل اذه فصي
ة. وهل نزم عون في ني دوجومل ني مدختسم مل

قيساسألابلطتمل

تابلطتمل

Identity Services Engine (ISE) لعل سايسل نيوكتب ة فرعم كيدل نوكت نأب Cisco ي صوت

عمدختسمل تانوكمل

ة: لائل ة دامل تانوكمل او جماربلل تارادصل ل دنتمل اذه في ة دراوول تامولعمل دنتمت

- Identity Services Engine 3.0
- Microsoft Windows Active Directory 2016

ة صاخ ة لعم عم ة ئب في ة دوجومل ة زهجال نم دنتمل اذه في ة دراوول تامولعمل عاشن ا مت
تنك اذا. (يضا رتفا) حوسمم نيوكتب دنتمل اذه في عمدختسمل ة زهجال عمي مج ت ادب
رمأ يال لم تحملل ري ثاتلل كم هف نم دكأتف، لي غشتل دي قكتك بش

ةيساسأ تامولعم

ني دوجوملا ني مدختسم لابل صاخ مدختسم لكل يكي مانيدلا لوصولا يف مكحت ةمئاق نيوكت
يجراخ ةيوه نزخم وأ يلخادلا ISE ةيوه نزخم يف اما

نيوكتلا

يلخادلا نزخملا يف مدختسم يأل مدختسم لكل لوصولا يف مكحتلا ةمئاق نيوكت نكمي
نكمي، Active Directory (AD) ةمدخي يف مدختسم ل ةبسن لابل. ةصصخم مدختسم ةمس مدختسي
تامولعمل مسقلا اذه رفوي. عارجال س فن قي قحتل ةلس لس عونلا نم ةمس يأ مادختسا
لمعت يكل ISE لعل بولطملا نيوكتلا عم AD و ISE نم لك لعل تامسلا نيوكتلا ةبولطملا
ةزيمل اذه.

ISE لعل ةديج صصخم مدختسم ةمس نيوكت

حضم وه امك، + رزرقنا. ةصصخملا مدختسم تامس > تادادع > ةيوه ل اراد > اراد ل لقتنا
ةمسلا مسا، لاثملا اذه يف. تاريغيغتلا ظفحو ةديج ةصاخ ةفاضلا، ةروصولا يف
(ACL) لوصولا يف مكحتلا ةمئاق وه ةصصخملا

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration · Identity Management', and a warning for 'Evaluation Mode 27 Days' and 'License Warning'. The main content area is titled 'Settings' and contains a table of 'User Custom Attributes'. The table has columns for 'Mandatory', 'Attribute Name', and 'Data Type'. The attributes listed are: AllowPasswordChangeAfterLogin (String), Description (String), EmailAddress (String), EnableFlag (String), EnablePassword (String), Firstname (String), Lastname (String), Name (String, marked as mandatory with a green checkmark), and Password (Credential:Password) (String). Below the table, there is a section for 'User Custom Attributes' with a table showing 'ACL' as an attribute with a description 'Attribute for ACL per us', data type 'String', and parameters 'String Max length'. The 'Default Value Mandatory' column is empty. At the bottom right, there are 'Save' and 'Reset' buttons.

dACL لوصولا يف مكحتلا ةمئاق نيوكت

> ةسايسلا ل لقتنا، ليزنلل ةلباقلا (ACL) لوصولا يف مكحتلا ةمئاق نيوكتلا
ةلباقلا (ACL) لوصولا يف مكحتلا ةمئاق > ضيوفتلا > جئاتنلا > ةسايسلا رصانع
امك. تاريغيغتلا ظفحو dACL ل وتحمومسا ريفوتب مق. (Add) ةفاضلا قوف رزرقنا. ليزنلل
وه (dACL) ةيساسالا ةينبلل لوصولا يف مكحتلا ةمئاق مسا نإف، ةروصولا يف حضم وه
NotMuchAccess.

Dictionaryes Conditions **Results**

Downloadable ACL List > New Downloadable ACL

Downloadable ACL

* Name NotMuchAccess

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

1234567	permit ip any any
8910111	
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	
0414243	
4444444	

Check DACL Syntax ⓘ

Submit

ةصصخمللا ةمسلا عم يلخاد مدختسم باسح نيوكت

نيوكتو مدختسم ءاشنإب مق .ةفاضإ > ني مدختسم > تايوه > ةيوهلا ةرادإ > ةرادإ ىلإ لقتنا
 ذفنملا بةصاخلا لوصولا يف مكحتلا ةمئاق مسا مادختساب ةصصخمللا ةمسلا ةميقي
 مسا نوكي ،لاثلما اذه يف .دامتعالا دنعا هيلع لوصوللا ىلإ مدختسملا جاتحي يتلا (dACL)
 NotMuchAccess وه (dACL) ةيساسألا ةينبلل لوصولا يف مكحتلا ةمئاق

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Name testuserinternal

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password

* Login Password

Enable Password

> User Information

> Account Options

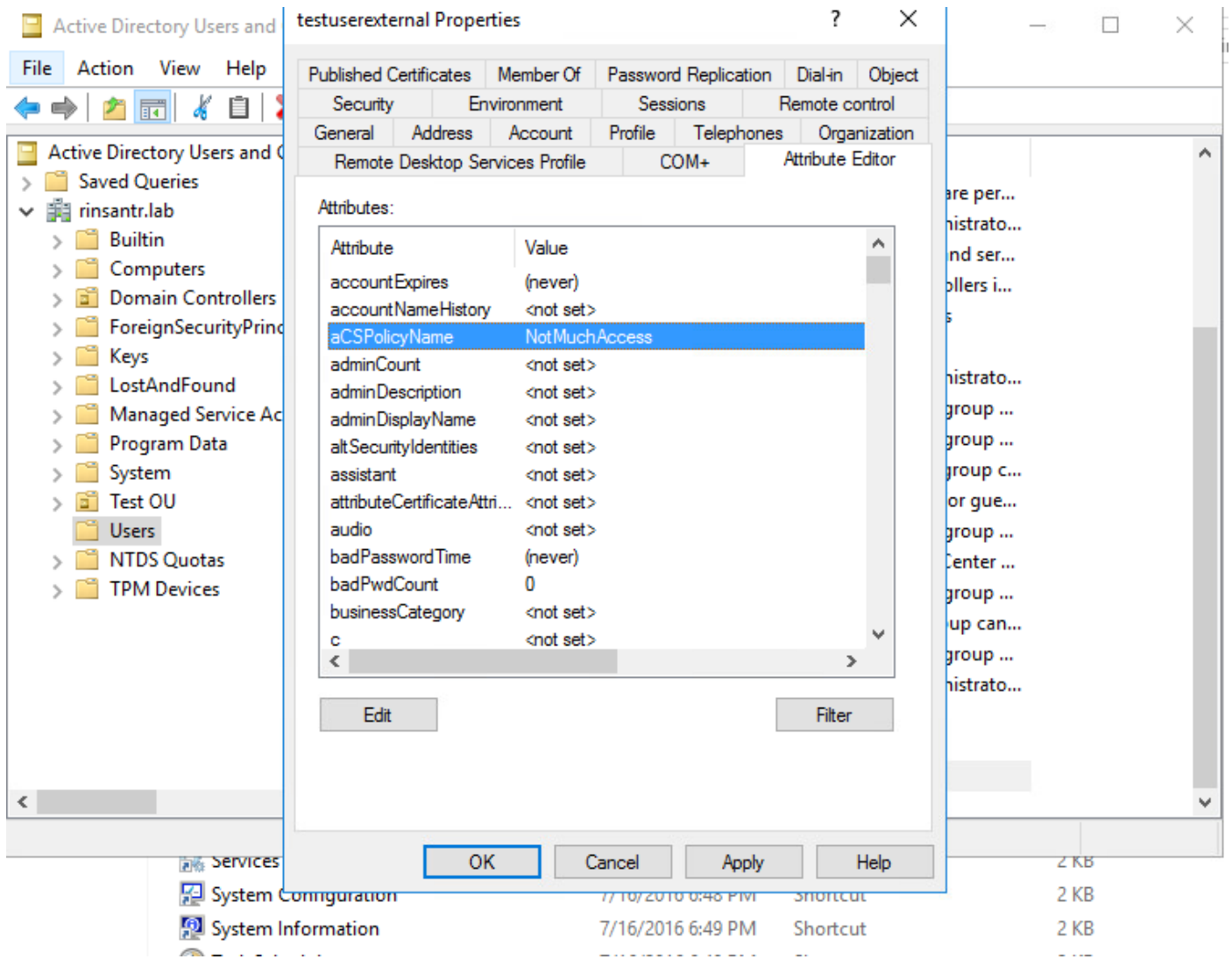
> Account Disable Policy

User Custom Attributes

ACL = NotMuchAccess

AD مَدْخَتْ سَمِ بَاسِحِ نِيوَكْتِ

رَحْمِ بِيوَبْتِ لَاقِ مَالِ عِ لَاقِ مِثْ مَدْخَتْ سَمِ لَاقِ بَاسِحِ صِئِاصِخِ لَاقِ لِقْتِ نَا، Active Directory يَفِ
 dACL مِ سَا دِي دَحْتِ لَاقِ مَدْخَتْ سَمِ لَاقِ مِ سَمِ لَاقِ يَهْ CSPolicyName، ةِ رِوَصِ لَاقِ يَفِ حِضُومِ وَهْ اَمِكِ. تَامِ سَمِ لَاقِ
 ةِ لَاقِ سَمِ لَاقِ لَاقِ لَاقِ نَا نَكَمِي ةِ مِ سَمِ يَأْ مَادِخَتْ سَمِ لَاقِ نَكَمِي، اَقِ بَسَمِ ةِ رَاشِ لَاقِ تَمْتِ اَمِكِ وَ، كِلْذِ عَمِ
 كِلْذِ كِ.



إلى ISE | AD نم ةمسلا داريتسإ

ةمسلا داريتسإ. اهداريتسإ إلى ISE جاتحي، AD إلى اهنيوكت مت يتلا ةمسلا مادختسإ، ةطقن نيوكت] > Active Directory > ةيجراخلا ةيوهلا رداصم > ةيوهلا ةرادا > ةرادا إلى لقتنا باسح مسا لخدأ. ليلدل نم تامس ددح مثة فاضا قوف رقنا. تامس بيوبتلا ةمالع > [طب رلا dACL، ل اهنيوكت مت يتلا ةمسلا ددح. تامسلا دادرستسإ قوف رقنا مثة AD إلى مدختسمل، ةيوهلا يف حضوره امك. ظفح قوف رقنا مثة قفاوم قوف رقنا ةمسلا.

Directory Attributes

Only attributes selected below will be available for use as policy conditions in policy rules.

* Sample User or Machine

Account

testuserexternal



Retrieve Attributes...

<input type="checkbox"/>	Name	Type	Example Value
<input checked="" type="checkbox"/>	aCSPolicyName	STRING	NotMuchAccess
<input type="checkbox"/>	accountExpires	STRING	9223372036854775807
<input type="checkbox"/>	badPasswordTime	STRING	0
<input type="checkbox"/>	badPwdCount	STRING	0
<input type="checkbox"/>	cn	STRING	testuserexternal
<input type="checkbox"/>	codePage	STRING	0
<input type="checkbox"/>	countryCode	STRING	0
<input type="checkbox"/>	dSCorePropagationData	STRING	16010101000000.0Z
<input type="checkbox"/>	displayName	STRING	testuserexternal
<input type="checkbox"/>	distinguishedName	STRING	CN=testuserexternal,CN=Users,DC=rinsantr,DC=lab

Cancel

OK

Click here to do visibility setup Do not show this again.

External Identity Sources

- Certificate Authentication F
- Active Directory
 - RiniAD
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

Attributes

Edit + Add Delete Attribute

<input type="checkbox"/>	Name	Type	Default	Internal Name
<input type="checkbox"/>	aCSPolicyName	STRING		aCSPolicyName

Save

Reset

نېي ج راخ لال او نېي ل خا دل ل نېي م د خ ت س م ل ل لې و خ ت ل ف ي ر ع ت ت ا ف ل م نېي و ك ت

> چئائ نل ل > ة س ا ي س ل ل ر ص ا ن ع > ة س ا ي س ل ل ي ل ل ق ت ن ا ، لې و خ ت ل ت ا ف ي ص و ت نېي و ك ت ل ة م ئ ا ق م س ا ر ت خ ا و م س ا ر ي ف و ت ب م ق . (Add) ة ف ا ض ا ق و ف ر ق ن ا . لې و خ ت ل ت ا ف ي ص و ت > لې و خ ت ل ل > ا ه ؤ ا ش ن ا م ت ي ت ل ل ة ص ص خ م ل ل ة م س ل ل م س ا < InternalUser ك (dACL) ل و ص و ل ا ب م ك ح ت ل ل

نېوكت متي، ځلځادلا مځختس ملل ؤبس نلاب، ؤروللا ي ف حضوم وه امك. ځلځادلا مځختس ملل ي تال (dACL) لولوللا ي ف مكحتلا ؤمئاق مځختساب InternalUserAttributeTest ف ي رعتلا فلم InternalUser:ACL ؤئيه ځل عاهنېوكت مت

Dictionaryes Conditions **Results**

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: InternalUserAttributeTest

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement: ⓘ

Agentless Posture: ⓘ

Passive Identity Tracking: ⓘ

Common Tasks

DACL Name: InternalUser:ACL

مساك <Join point name>: <attribute configure on AD> مځختسأ، ځراځلا مځختس ملل ؤبس نلاب دACL. ؤمئاق مځختساب ExternalUserAttributeTest ف ي رعتلا فلم نېوكت متي، لاثملا اذه ي ف ځي رنيAD:aCSPolicyName ؤئيه ځل عاهنېوكت مت ي تال طئاسولل لولوللا ي ف مكحتلا طبرلا ؤطقن مسا وه RiniAD نوكتي.

Dictionarys Conditions **Results**

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

DACL Name

ليوختال تاسايس نيوكت

تاعومجملا لى اذانتسا تاسايسلا تاعومجم > جهنلا في ضيوفتال تاسايس نيوكت نكمي
 نزم في مدختسملا مسا لى اذانتسا كلك و AD لى عي جراخل مدختسملا اه في دجاوتي يتال
 ةومجملا في دجوم مدختسم وه Testuserexternal، لالم اذه في ISE. ليخادلا ةي وهلا
 ل ليخادلا ةي وهلا نزم في دجوم مدختسم وه testuserInternal و rinsantr.lab/Users/Test Group
 ISE.

			Results	
Status	Rule Name	Conditions	Profiles	Security Groups
+	Search			
✓	Basic Authenticated Access Internal User	AND Network Access-AuthenticationStatus EQUALS AuthenticationPassed Radius-User-Name EQUALS testuserinternal	InternalUserAttributeTe... x	Select from list
✓	Basic Authenticated Access External User	AND Network Access-AuthenticationStatus EQUALS AuthenticationPassed RiniAD-ExternalGroups EQUALS rinsantr.lab/Users/Test Group	ExternalUserAttributeT... x	Select from list
✓	Default		DenyAccess x	Select from list

ةحصلا نم ققحتلا

نويوكتلا لمع نم ققحتلل مسقلا اذه مدختسأ

مدختسملا ةقداصم نم ققحتلل ةرشابملا RADIUS تالجس نم ققحت

يلخادلا مدختسملا

Jan 18, 2021 03:27:11.5...	✓	🔒	#ACSACL#-IP-...					
Jan 18, 2021 03:27:11.5...	✓	🔒	testuserinternal	B4:96:91:26:E0:2B	Intel-Device	New Polic...	New Polic...	InternalUs...


يجراخلا مدختسملا

Jan 18, 2021 03:39:33.3...	✓	🔒	#ACSACL#-IP-...					
Jan 18, 2021 03:39:33.3...	✓	🔒	testuserexternal	B4:96:91:26:E0:2B	Intel-Device	New Polic...	New Polic...	ExternalUs...

تناك اذا امم ققحتلل ةحجانلا مدختسملا ةقداصم يلع ةربكملا ةسدعلا زمر قوف رقنا ةرشابملا تالجسلا يف ةماعلا ةرظنلا مسق يف ةحيحصلا جهنلا يل لصت تابلللا ةيلصفتلا.


يلخادلا مدختسملا

Overview

Event	5200 Authentication succeeded
Username	testuserinternal
Endpoint Id	B4:96:91:26:E0:2B 
Endpoint Profile	Intel-Device
Authentication Policy	New Policy Set 1 >> Authentication Rule 1
Authorization Policy	New Policy Set 1 >> Basic Authenticated Access Internal User
Authorization Result	InternalUserAttributeTest

يخراخال المدخستسمل:

Overview

Event	5200 Authentication succeeded
Username	testuserexternal
Endpoint Id	B4:96:91:26:E0:2B 
Endpoint Profile	Intel-Device
Authentication Policy	New Policy Set 1 >> Authentication Rule 1
Authorization Policy	New Policy Set 1 >> Basic Authenticated Access External User
Authorization Result	ExternalUserAttributeTest

دادرتسإ نم ققحتلل ةلصفملا ةرشابملا تالجلسلا يف ىرخألا تامسلا مسق نم ققحت
مدخستسمل تامس.

يلخادل المدخستسمل:

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

يخرج راخال مدختس مل:

aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

نم ققحتلل ليليصفتلل ةرشابملا ليغشتلل تالچسب صاخلا "چئاتنلا" مسق نم ققحت لوصولا لوبق نم عزجك dACL ةمس لاسلا

cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-NotMuchAccess-60049cbb
---------------	--

لوصولا يف مكحتلا ةمئاق ليزنت نم ققحتلل ةرشابملا RADIUS تالچس نم اضيأ ققحت لوصولا ةقداصم دعب (dACL) ةساسألا ةينبلل

Jan 18, 2021 03:39:33.3...



#ACSACL#-IP-NotMuchAccess-60049cbb

ةينبلل لوصولاب مكحتلا ةمئاق ليزنت لچس لعل ةربكملا ةسدعلا ةنوقيأ رقنا مكحتلا ةمئاق ليزنت ديكأتل ةماعلا ةرظنلا مسق نم ققحت مئحجانلا (dACL) ةساسألا (dACL) ةساسألا ةينبلل لوصولاب

Overview

Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-NotMuchAccess-60049cbb
Endpoint Id	
Endpoint Profile	
Authorization Result	

ةمئاق تايوتحم نم ققحتلل يليصفتلا ريرقتلا اذه في "جئاتنلا" مسق نم ققحت (dACL) ةيساسألا ةينبلل لوصولا في مكحتلا

cisco-av-pair

ip:inacl#1=permit ip any any

اهحالصإو ءاطخألا فاشكتسا

ليكشت اذه ىرحتي نأ رفوتي ةدحم ةمولعم نم ام ايلاح كانه

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك ة ق م ق د ن و ك ت ن ل ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر م . ة ص ا خ ل م ه ت غ ل ب
Cisco مچرت م ا م د ق م م ي ت ل ا ة م ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا م ا د ع و چ ر ل ا ب م ص و ت و ت ا مچرت ل ا ه ذ ه ق د ن ع ا ه ت م ل و ئ س م Cisco
Systems م (ر ف و ت م ط ب ا ر ل ا) م ل ص ا ل ا م ي ز م ل چ ن ل ا دن ت س م ل ا