

وأداة شلالى إة دن تسملا ة قدا صملا نى وكت ISE ةرادال ةى كذلا ة قاطبلا

تاىوت حمللا

[ةمدقملا](#)

[ةىساسألا تاب لطلت ملا](#)

[تاب لطلت ملا](#)

[ةمدختسملا تانوك ملا](#)

[نى وكتلا](#)

[ةكبش للى طىطختلا مسرلا](#)

[ISE ب Active Directory طبر](#)

[للى دلل تا عومجم دى دحت](#)

[ىرادال لوصولل Active Directory رورم ةملك ىلا ةدن تسملا ة قدا صملا نى كمت](#)

[نى لوؤسملا تا عومجم ىلا ةى جراخلا ةى وهلا تا عومجم نى ىعت](#)

[اهب قوؤوم ةداهش دارىتسا](#)

[ةداهشلا ة قدا صم فى رع ت فلم نى وكت](#)

[للى معل ةداهش ىلا ةدن تسملا ة قدا صملا نى كمت](#)

[ةحصلا نم ققحتلا](#)

[اهال صاوا طخالل افاشكتسا](#)

ةمدقملا

ىلا لوصولل لى معل ةداهش ىلا ةدن تسملا ة قدا صملا نى وكت ةى فى ك دن تسملا اذه حضوى ةداهش لباقم ة قدا صملا ب ISE لوؤسم موقى، لا ثملا اذه فى (ISE) ةى وهلا تامدخ كرحم ةرادا ةصاخلا (GUI) ةى موسرلا مدختسملا ةهجاو ىلا لوؤسملا لوصو ىلع لوصحلل مدختسملا Cisco نم ةى وهلا تامدخ كرحم ةراداب

ةىساسألا تاب لطلت ملا

تاب لطلت ملا

ةىلاتلا عىضاوملاب ةفرعم كىدل نوكت نأب Cisco ىصوت:

- ةداهشلا و رورملا ةملك ة قدا صملا ISE نى وكت
- Microsoft Active Directory (AD)

ةمدختسملا تانوك ملا

ةىلاتلا ةى داملا تانوك ملا و اوجماربلا تارادصا ىلا دن تسملا اذه فى ةدراولل تامول عمل دن تسمت:

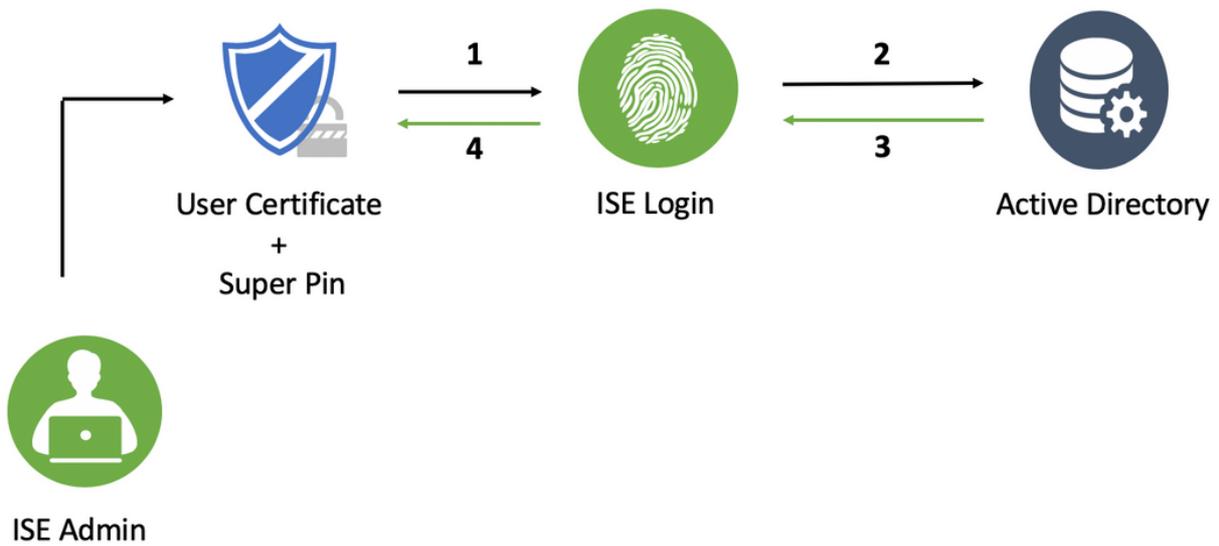
- Cisco Identity Services Engine (ISE)، رادصا 2.6
- Windows Active Directory (AD) Server 2008 رادصا 2
- ةداهش

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجالا نم دنتسملا اذه ي ف ةدراولما تامولعملما عاشنإ مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسملا ةزهجالا عيمج تادب ن.نيوكت يال لم تحملا ريثأتلما مهف نم دكأتف ،ةرشابم ةكبشلا

نيوكتلا

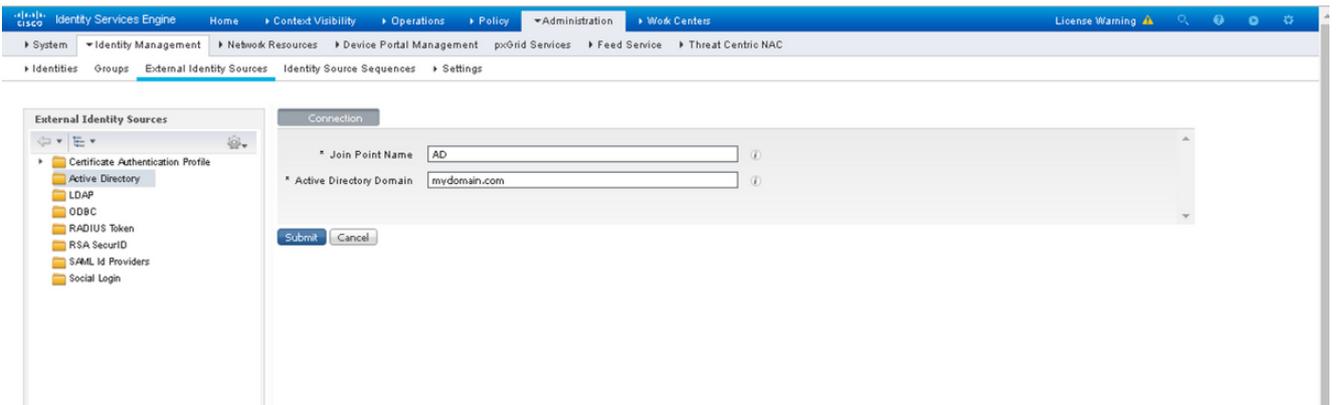
يرادلما لوصولل ةي جراخ ةي وهك ةي كذلا ةقاطبلا وأ لي عملما ةداهش نيوكتل مسقلا اذه مدختسأ Cisco ISE ةرادلما (GUI) ةي موسرلا مدختسملا ةهجاو ىلإ

ةكبشلا ل يطيختلا مسرلا

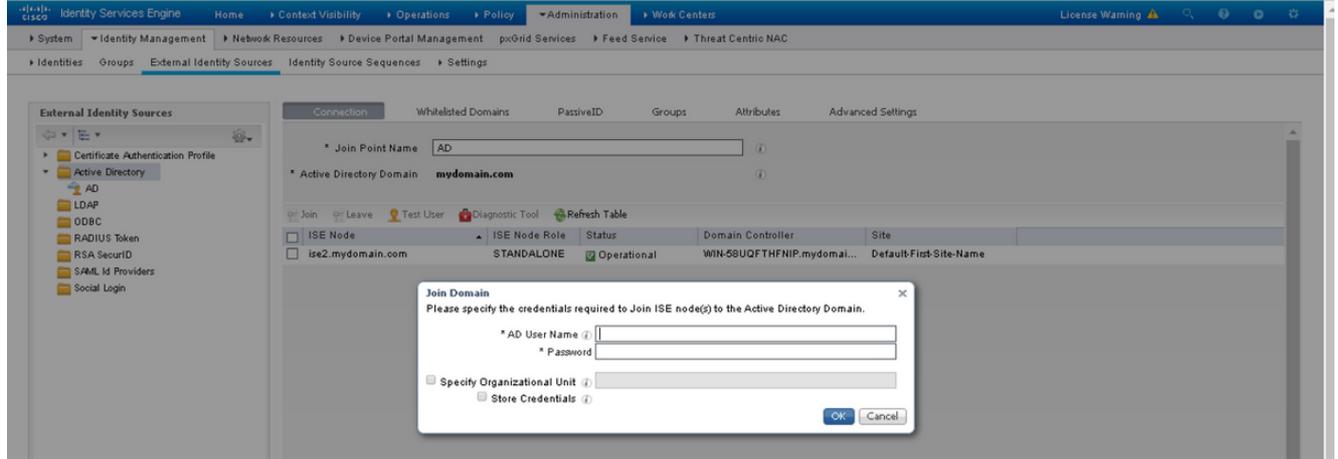


طبر Active Directory ب ISE طبر

1. Active Directory > ةي جراخلما ةي وهلا رداصم > ةي وهلا ةرادلما > ةرادلما رايختا.
2. Cisco ISE ي ف AD لاجم و طبرلا ةطقن مساب Active Directory لي ثم عاشناب مق .
3. لاسرا ىلع رقنا .



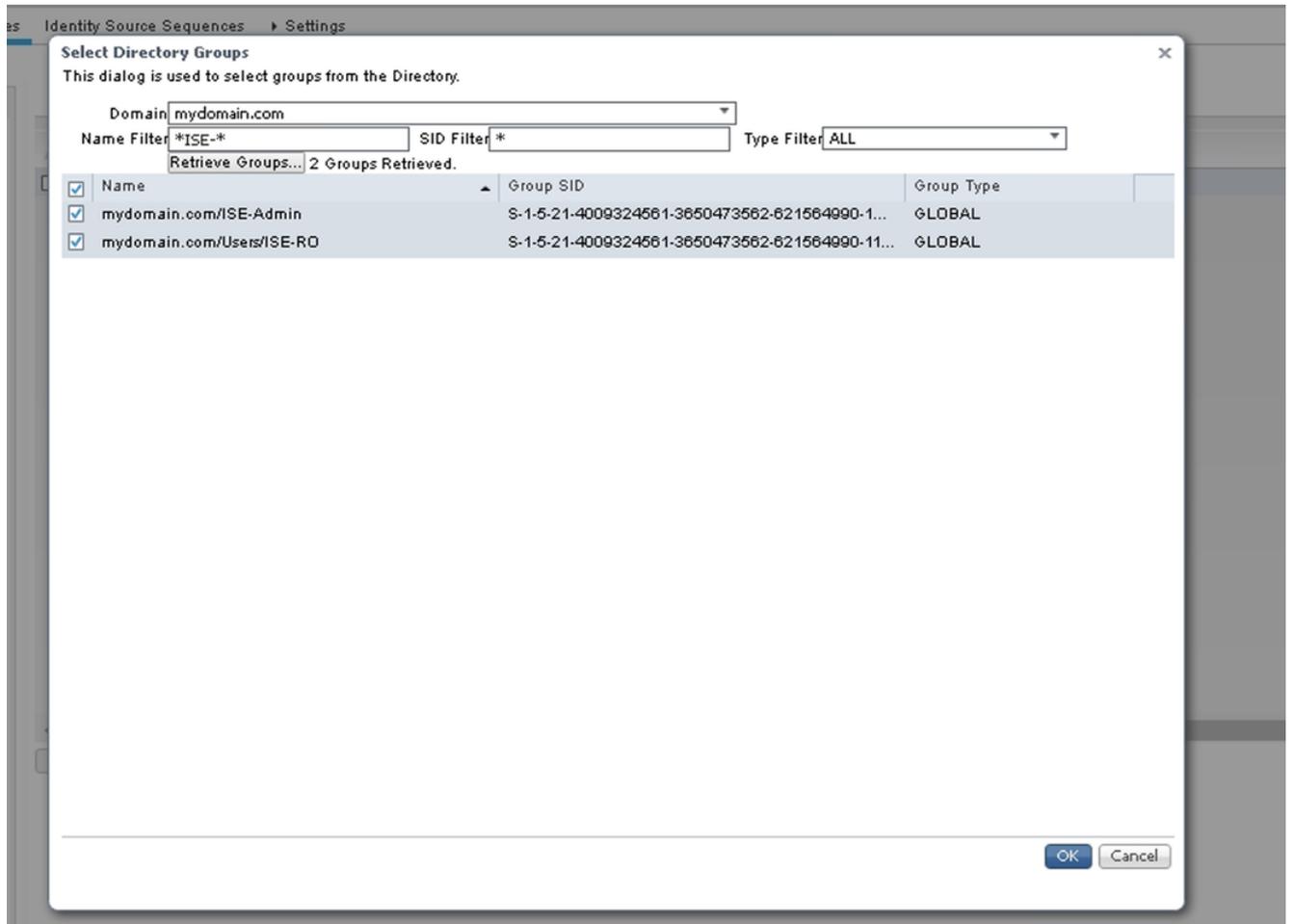
هجوم ينفذ من قبل رورملا عم لك وم دخت سمل مس امدخت ساب دق ع ل ا ع م ج ل ا م ضنا 4.
رمال.



5. طفق ق ط ق ط .

لي لدل ا ع و م ج م دي دحت

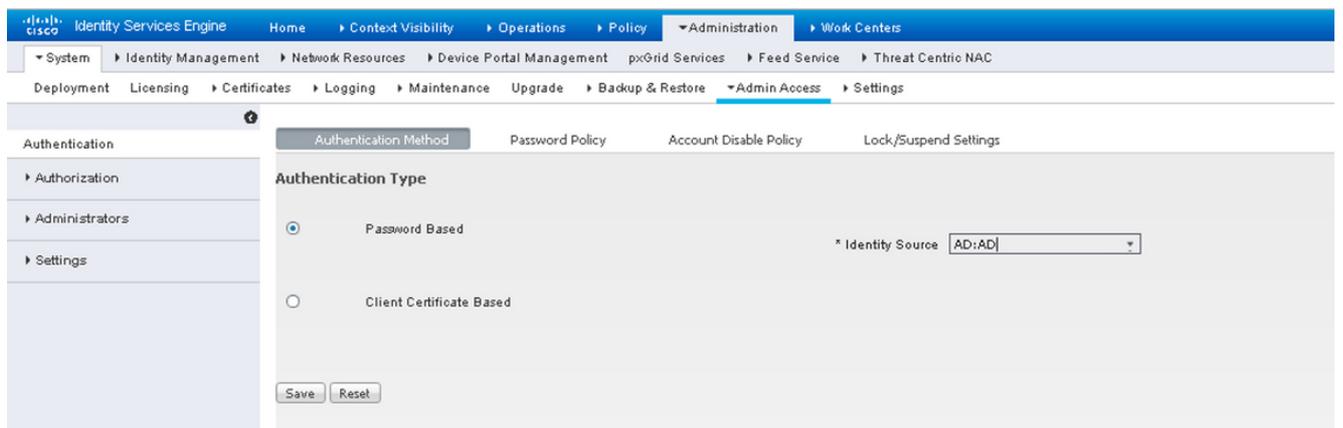
1. Active Directory ع و م ج م ل ا ا ه ن ي ع ت ب م ق و ع ي ج ر ا خ ل و و س م ع و م ج م ا ش ن ا ب م ق .
2. دي دحت > ا ع و م ج م > Active Directory > ع ي ج ر ا خ ل ا ع ي و ه ل ا ر د ا ص م > ع ي و ه ل ا ع ر ا د ا > ع ر ا د ا ر ت خ ا .
Directory ن م ا ع و م ج م
3. ل و و س م ل ا ا ه ل ا ي م ت ن ي ل ق ا ل ا ل ع ع د ح ا و AD ع و م ج م د ا د ر ت س ا .



4. ظفح ةق طقط.

يرادإلا لوصولل Active Directory رورم ةملك ىلإ ةدنتسملا ةقداصملا نيكمت

1. مضمنا رورملا ةملك ىلإ ةدنتسم ةقداصم بولسأك Active Directory لئثم نيكمتب مق قباس تقوي ف ISE ىلإ.
2. ةروصللا ف حضورم وه امك، ةقداصملا > لوؤسملا لوصولو > ماظن > ارادإرتخأ.



3. ظفح ةق طقط.

ةقداصملا نيكمتل رورملا ةملك ىلإ ةدنتسملا ةقداصملا نيوكت مزلي: ةظحالام ةقداصملا ل حجنا نيوكت دعب نيوكتلا اذه سكع بجي. ةداهشلا ىلإ ةدنتسملا

عداهش لى لى عدنتس مل

نيلوؤس مل تاعومجم لى لى جراخ لى وه لى تاعومجم نى عت

ةىضارتف الة راد الة عومجم لى لى جراخ لى AD عومجم نى عت متى ، لى لى اذى ف

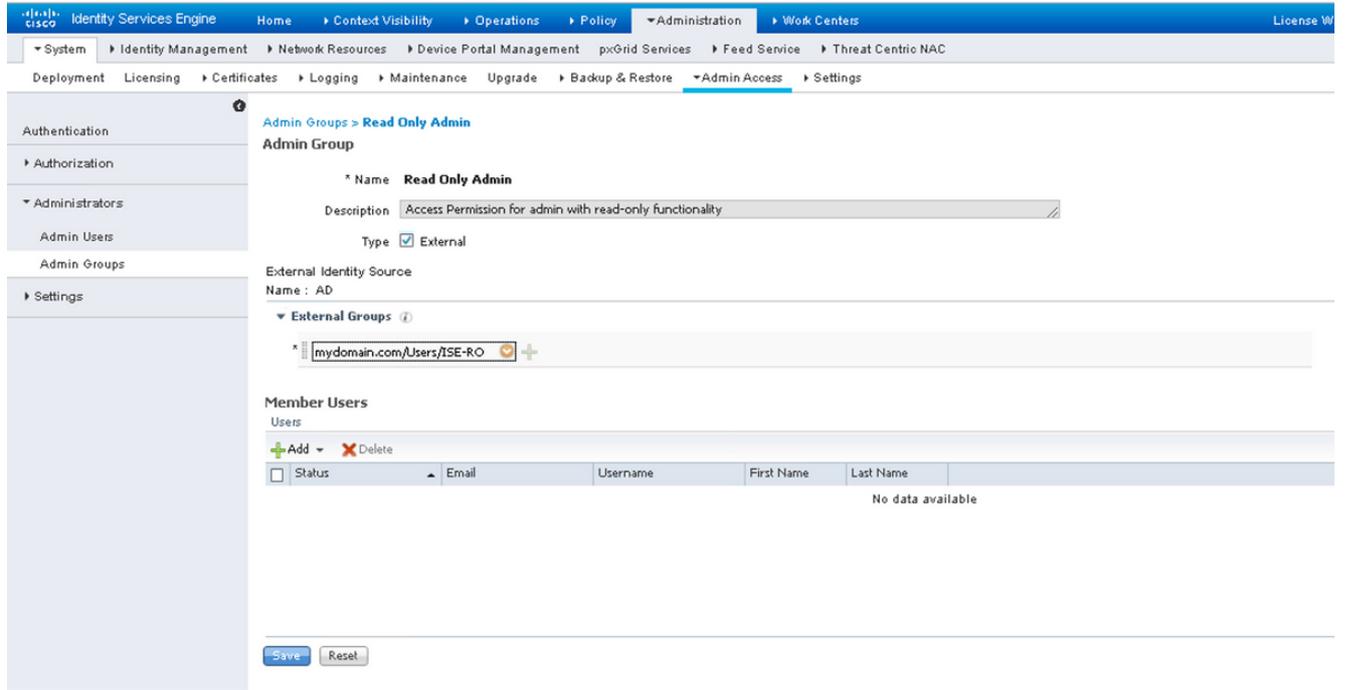
1. Super Admin > لوؤس مل تاعومجم > نولوؤس مل > لوؤس مل لوصو > ماظن لى > راد رتخأ
2. ةىجراخ تاعومجم نى لى AD عومجم ددحو جراخ عونك عون لى نى ققحت

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. The left sidebar shows a navigation tree with Authentication, Authorization, Administrators (Admin Users, Admin Groups), and Settings. The main content area is titled 'Admin Groups > System Admin' and shows the configuration for the 'System Admin' Admin Group. The 'Name' is 'System Admin' and the 'Description' is 'Access permission for Operations tab. Includes System and data access permission for Admin Groups.' The 'Type' is 'External'. The 'External Identity Source' is 'AD'. Under 'External Groups', there is a list with one entry: 'mydomain.com/ISE-Admin'. The 'Member Users' section is empty, showing 'No data available'. At the bottom, there are 'Save' and 'Reset' buttons.

3. ظفح ةق ققط

4. لوؤس مل طقف ةعارق > راد الة تاعومجم > نيلوؤس مل > لوؤس مل لوصو > ماظن لى > راد رتخأ

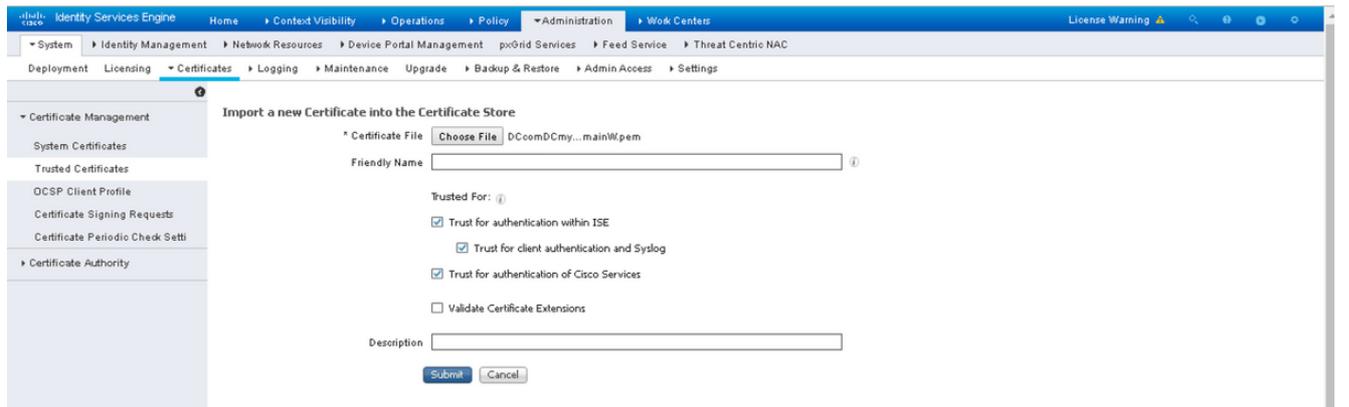
5. ةروصل لى ف حضوم وه امك ، ةىجراخ تاعومجم نى لى AD عومجم ددحو جراخ عون لى نى ققحت



6. ظفح ةق قوط.

اهب قوٹوم ةداهش داريتسا

1. ليمعلا ةداهش عقوت يتلا (CA) قوصملا عجرملا ةداهش داريتسا.
2. داريتسا > اهب قوٹوم ةداهش > تاداهش > ماظن > ريدم راتخن.
3. قوصملا عجرملا ةداهش رتخاوح فصت رقنا.
4. ةروصل ي ف حوصوم وه امك، Syslog و ليمعلا ةقداصمب ةقثلا رايثخالا ةناخ ددح.



5. لاسرا يلع رقنا.

ةداهشلا ةقداصم فيرعت فلم نيوكت

1. قراد رتخا، ليمعلا ةداهش يل ةدنتسملا ةقداصملا ةداهشلا ةقداصم فيصوت عاشنل. ةفاض > ةداهشلا ةقداصم فيرعت فلم > ةيچراخلا ةيوهلا رداصم > ةيوهلا قرادا.

2. فيرعتل فل م سا فضا .

3. ةداهشل ةمس في لوؤسمل مدختسم سا يلع يوتحت يتل ةبسانملا ةمسلل ددح .

4. ةنراقم ديرو مدختسملا ةداهش يلع يوتحتي مدختسملاب صاخلا AD لچس ناك اذا ققحتف AD، في ةدوجوملا ةداهشل لباقم ضرعتسملا نم اهمالتسا متي يتل ةداهشل مت يذل Active Directory ليثم مسا ددحو، امئاد ةيئانث ةنراقم ذيفنت رايخالال ةناخ نم اقبس م هديدحت .

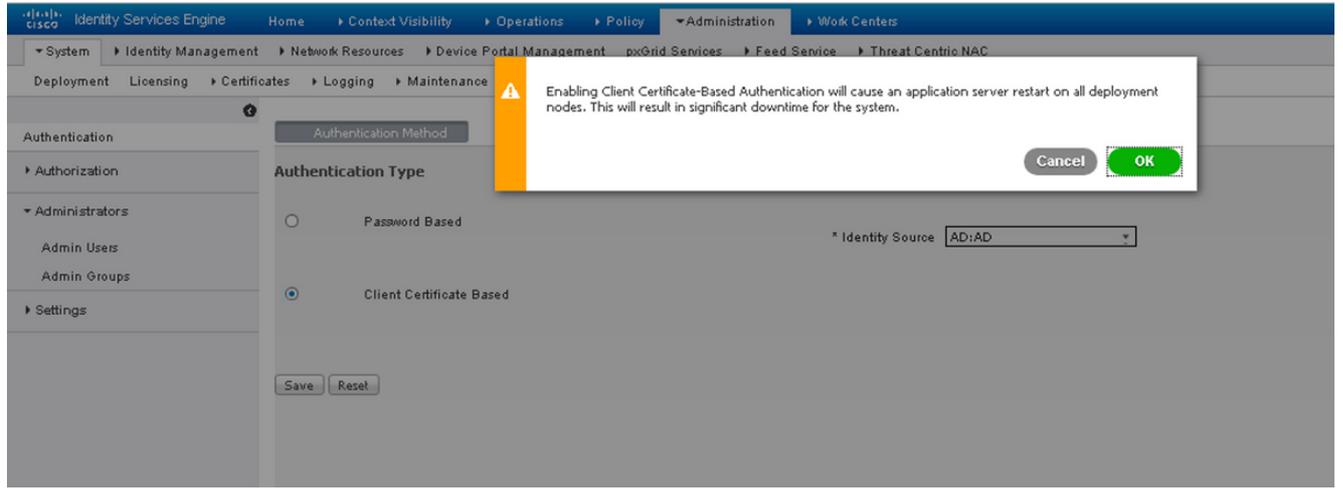
The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The left sidebar shows 'External Identity Sources' with a tree view containing 'Certificate Authentication Profile', 'Active Directory', 'AD', 'LDAP', 'ODBC', 'RADIUS Token', 'RSA SecurID', 'SAML Id Providers', and 'Social Login'. The main content area is titled 'Certificate Authentication Profiles List > New Certificate Authentication Profile'. The form fields are: 'Name' (CAC_Login_Profile), 'Description' (empty), 'Identity Store' (AD), 'Use Identity From' (Certificate Attribute, Subject Alternative Name - Other Name), and 'Match Client Certificate Against Certificate In Identity Store' (Always perform binary comparison). There are 'Submit' and 'Cancel' buttons at the bottom.

5. لاسرا يلع رقنا .

ةدنتسملا ةقداصلل ةداهشل ةقداصم فيرعت فل م سفن كالهتسا نكمي : ةظحالم اضيا ةيانهنلا ةطقن ةيوه يل

ليمعل ةداهش يل ةدنتسملا ةقداصل ني كمت

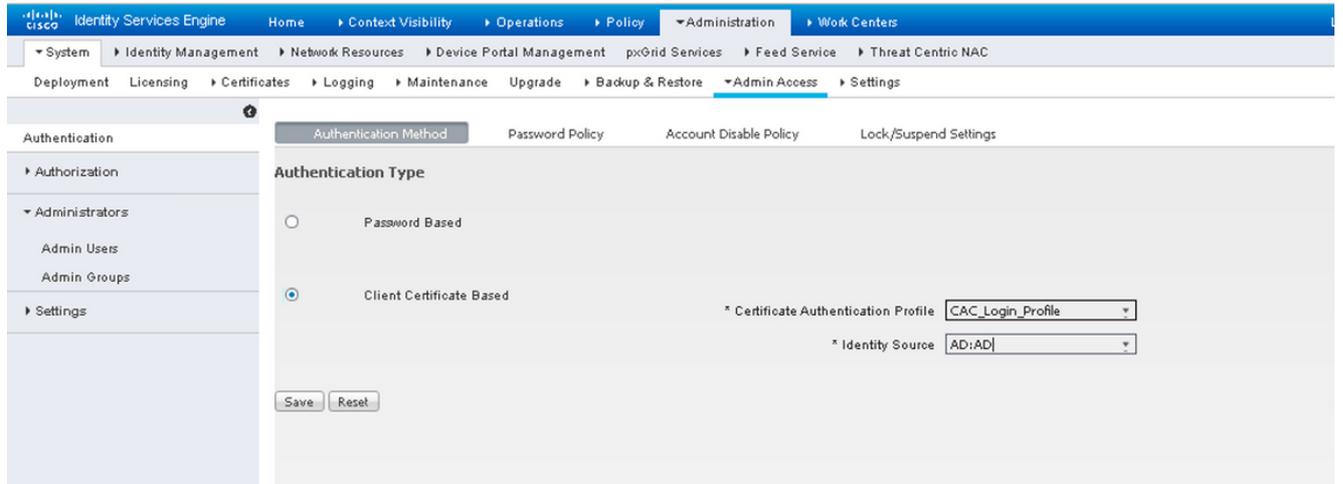
1. ليمعل ةداهش ةقداصل بولسا > ةقداصلملا > لوؤسمل لوصو > ماظنلا > ةرادال راتخن . يل ةدنتسملا



2. OK قوف رقناو.

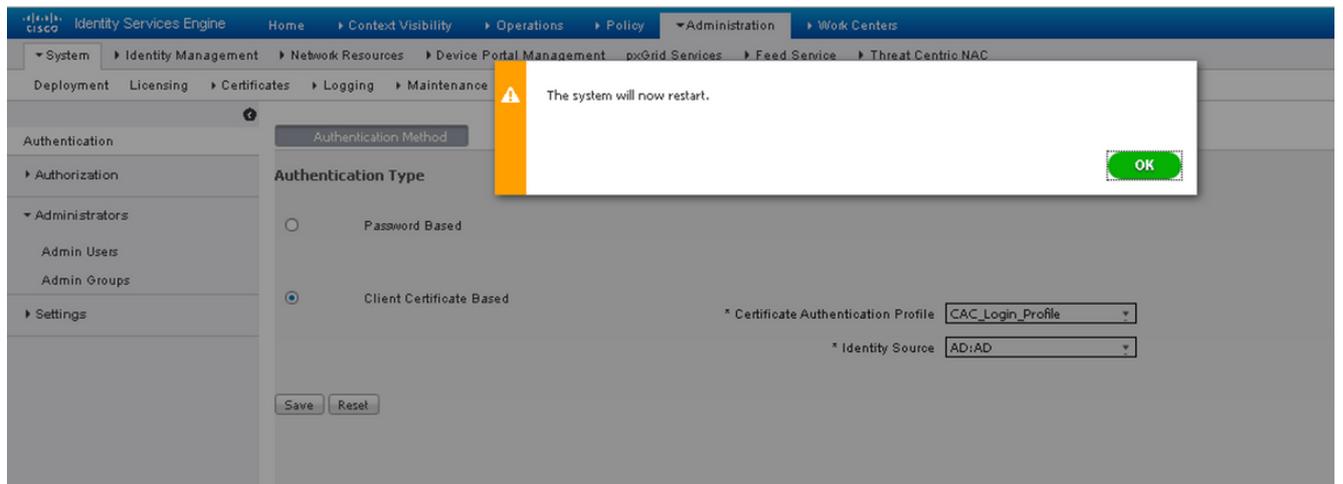
3. اق بس م هنيوكت مت يذلا ةداهشلا ةقداصم فيرعت فلم رتخأ.

4. دح Active Directory ليثم مسا دح.



5. ظفح ةق طقط.

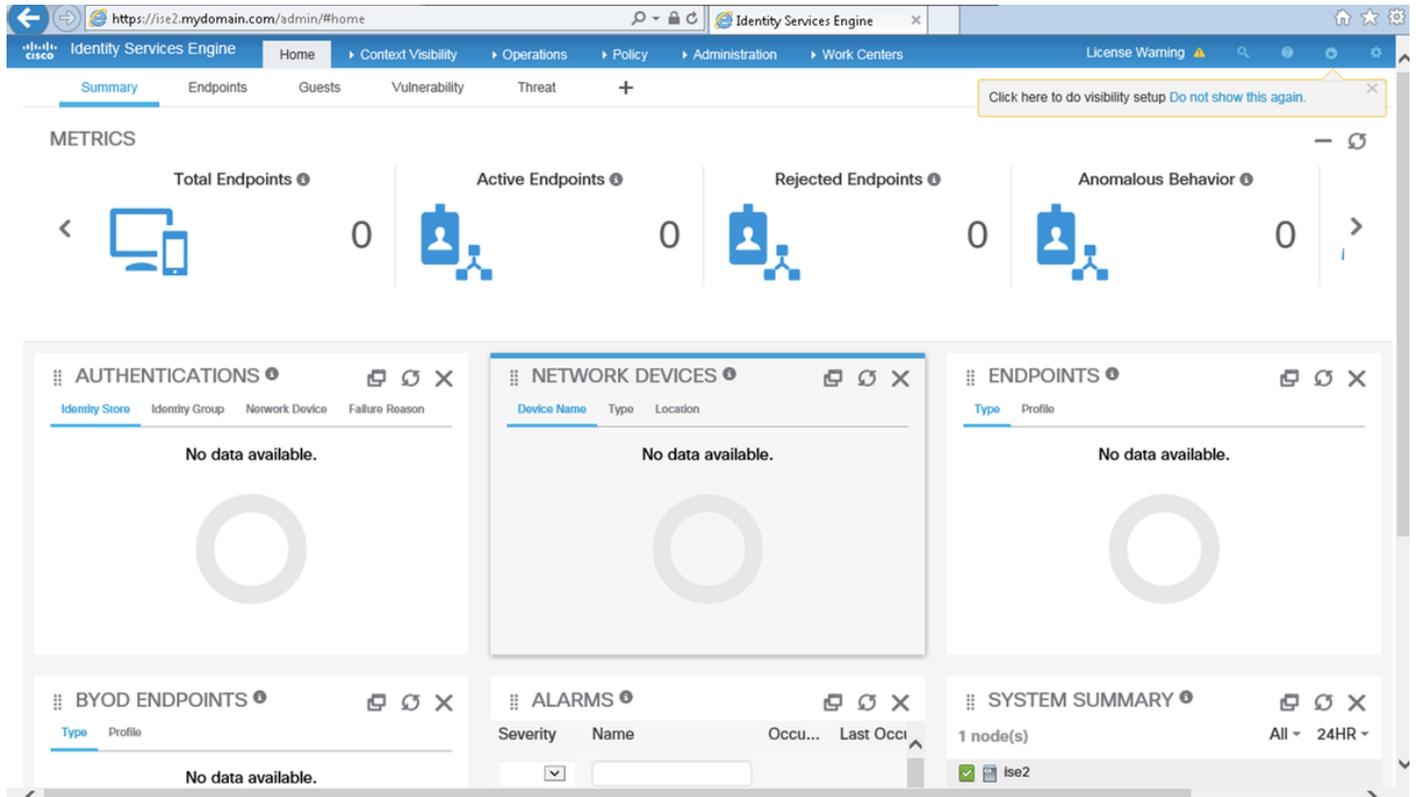
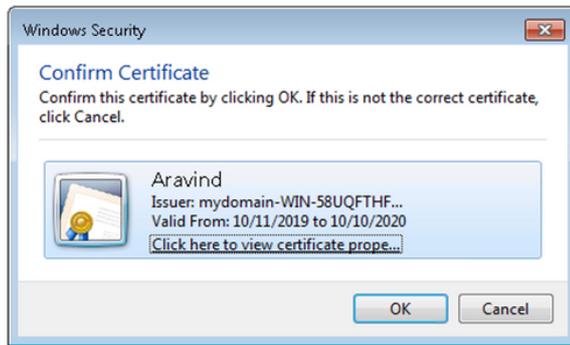
6. رشنلا ليغشت ةداعإ تايلمع يف دقعلا ةفاك لىع ISE تامدخ.



ةحصلال نم ققحتال

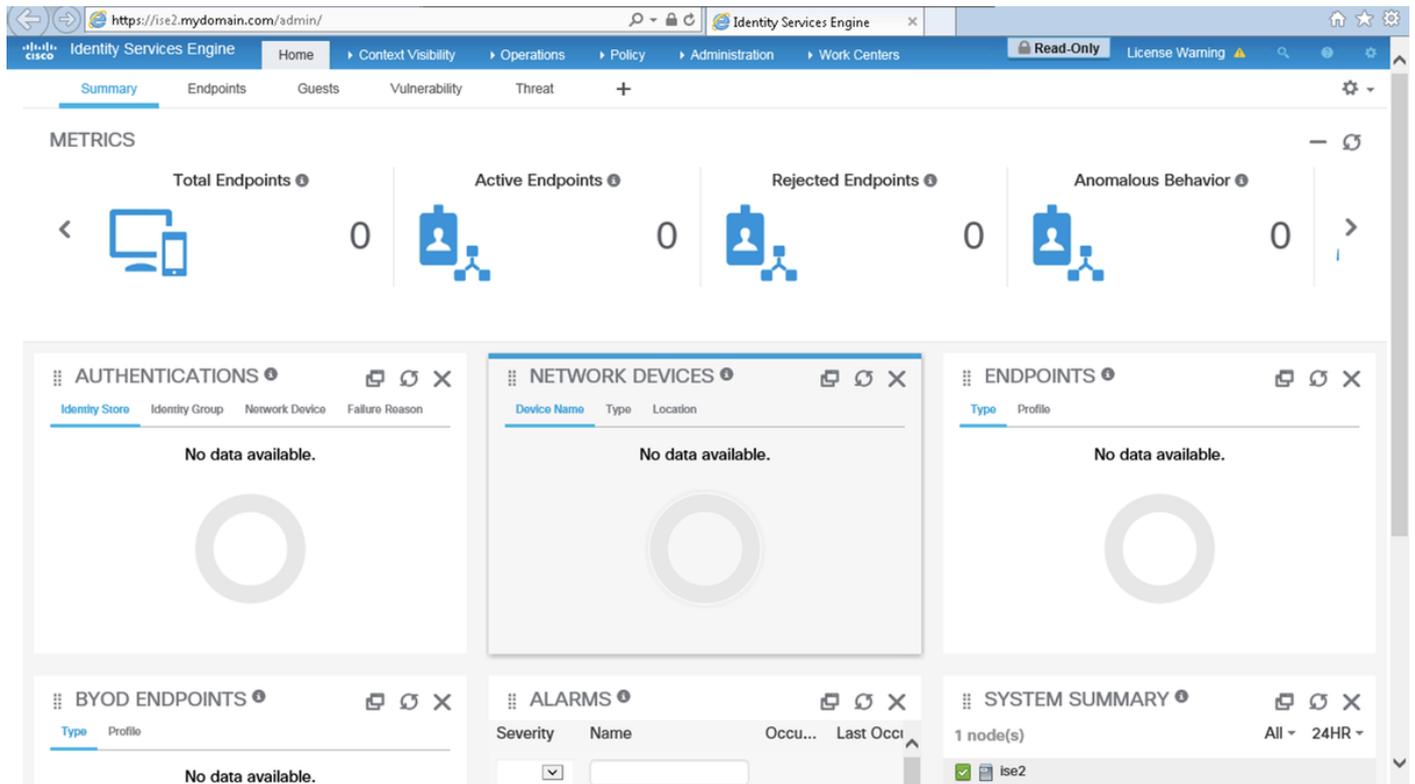
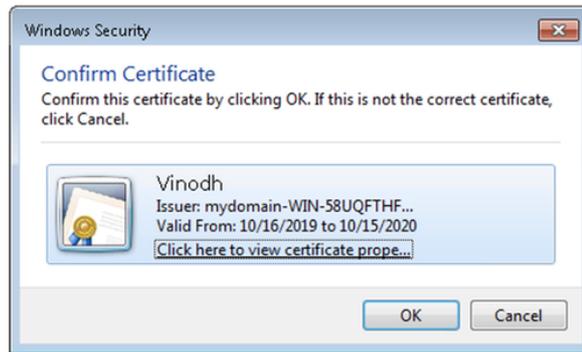
ةمدخ ةلأح ربيغت دعب ISE ب ةصاخال (GUI) ةيموسرللا مدختسمللا ةهجالل لوصولال نم ققحتل
لليغشلال ديق لىل اقايبطلال مداخ.

للىل لولذل ليجستل ةداهش رايختأب مدختسمللا ةبلاطم نم ققحتل **Super Admin** مدختسمل
عز نم ةداهشلال تناك اذ **Super Admin** تازايتمه ائاطعوا (ISE) ةيموسرللا مدختسمللا ةهجالل
زيمتملل لوؤسملل ةيجراخلال ةيوهلال ةومجم يف مدختسمل.



ةبلاطم متت هنا نم ققحتل: (طقف ةعارقلل لوؤسمل مدختسمل) **Read-Only Admin User**

هحنم متي و (ISE) ةيموسرللا مدختسمللا ةهجاو ىلإ لوخدلا ليحستل ةداهش راي تخاب مدختسمللا ةيوهلا ةعومجم يف مدختسمللا عزم ةداهشلا تناك اذا "طقف ةءارقللا لوؤسم" تازاي تما طقف ةءارقللا لوؤسمل ةيخراخللا



ءداهش Smartcard مدقت (CAC) كرتشمللا لوصولا ةقاطب مادختسا ةلاح يف: ةظحالم لصفألا (PIN) ي صخشلا فيرعتلا زمر مدختسمللا لخدي نأ دعب ISE ىلإ مدختسمللا حلصللا

اهحالصوا ءاطخألا فاشكتسا

1. ف م ك ح ت ل ل ل ي ط ع ت ب ح م س ي ن م آ ع ض و ي ف Cisco ISE ع د ب ل **start ise safe** ر م أ ل م د خ ت س أ . ISE ت ا م د خ ل ي غ ش ت ة د ا ع إ و ن ي و ك ت ل ا ح ي ح ص ت و ل و و س م ل ل خ د م ي ل ا ا ت ق و م ل و و ص و ل ا ق ي ب ط ت ل ا ع د ب ه ع ب ت ي ي ذ ل ا **stop ise** ر م أ ل م ا د خ ت س ا ب .
2. ل خ د م ي ل ل ل و و ص و ل ا ن ي م أ ت ب ل و و س م ل ا م ا ق ا ذ ا د ا د ر ت س ا ل ل ة ل ي س و ن م أ ل ا ر ا ي خ ل ل ر ف و ي . ل و و س م ل ا م ا ق ا ذ ا ث د ح ل ا ا ذ ه ث د ح ي د ق . د ص ق ن و د ن ي م د خ ت س م ل ا ع ي م ج ل Cisco ISE ل و و س م ة ح ف ص > ت ا د ا د ع | > ل و و س م ل ا ل و و ص و > ة ر ا د ا ل ا ي ف ة ح ي ح ص ر ي غ IP ل و و ص و ة م ئ ا ق ن ي و ك ت ب م س ا ي ل ل ع ج ر ي و ة د ا ه ش ل ل ا ي ل ل ة د ن ت س م ل ا ة ق د ا ص م ل ا ن م أ ل ا ر ا ي خ ل ل ز و ا ج ت ي ا م ك . ل و و ص و ل ا Cisco ل و و س م ل ل خ د م ي ل ل ل و و خ د ل ل ل ي ج س ت ل ر و ر م ل ا ة م ل ك ة ق د ا ص م و ي ض ا ر ت ف ا ل ا م د خ ت س م ل ا ISE .

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل متهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل