

Beheer en RBAC-beleid op ISE begrijpen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verificatieinstellingen](#)

[Admin-groepen configureren](#)

[Admin-gebruikers configureren](#)

[Toestemmingen configureren](#)

[RBAC-beleid configureren](#)

[Instellingen instellen voor Admin Access](#)

[Admin Portal Access met AD-Credentials configureren](#)

[Doe mee met ISE naar AD](#)

[Map-groepen selecteren](#)

[Administratieve toegang voor AD inschakelen](#)

[De ISE Admin Group instellen op Toewijzing van AD-groepen](#)

[RBAC-toegangsrechten voor de Admin-groep instellen](#)

[Toegang tot ISE met AD-Credentials en controleer deze](#)

[Admin Portal Access met LDAP configureren](#)

[Doe mee met ISE aan LDAP](#)

[Administratieve toegang voor gebruikers van LDAP inschakelen](#)

[Stel de ISE Admin Group op LDAP groepjes in](#)

[RBAC-toegangsrechten voor de Admin-groep instellen](#)

[Toegang tot ISE met LDAP Credentials en controleer](#)

Inleiding

In dit document worden de functies van ISE beschreven om administratieve toegang op Identity Services Engine (ISE) te beheren.

Voorwaarden

Vereisten

Cisco raadt u aan om de kennis van deze onderwerpen te hebben:

- ISE
- Actieve map
- Lichtgewicht Directory Access Protocol (LDAP)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

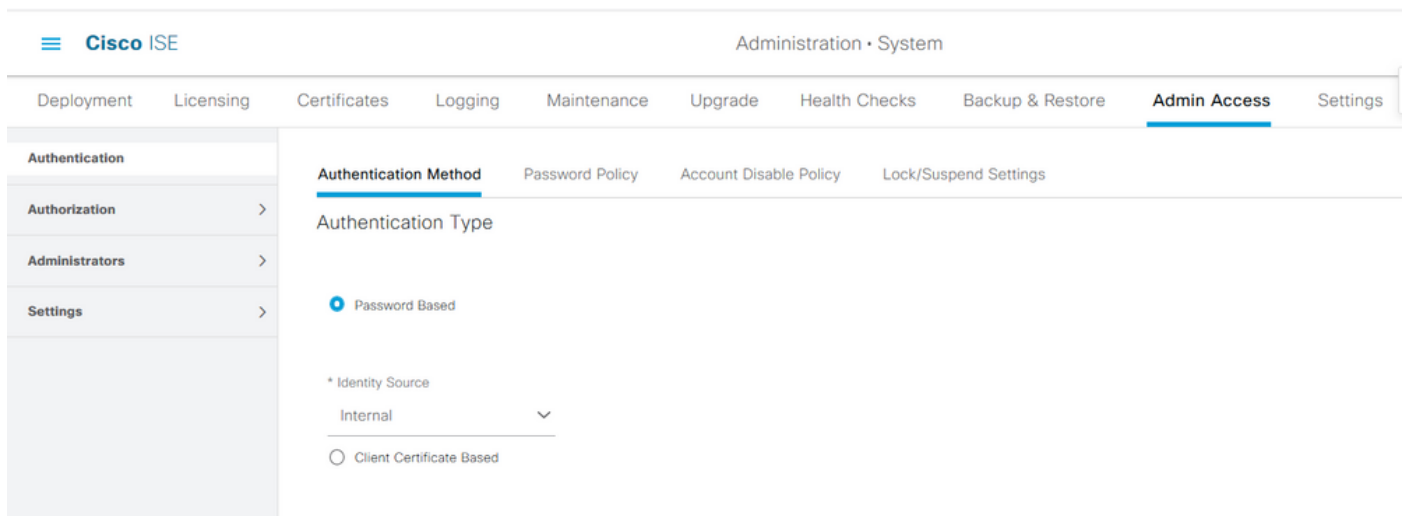
- Identity Services Engine 3.0
- Windows Server 2016

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Verificatieinstellingen

Admin-gebruikers moeten zichzelf authentiek verklaren om toegang tot om het even welke informatie op ISE te hebben. De identiteit van de beheerder kan worden geverifieerd met behulp van de ISE Interne Identity Store of een Externe Identity Store. De echtheid kan met een wachtwoord of met een certificaat worden geverifieerd. Om deze instellingen te configureren stuurt u naar **Beheer > Systeem > Toegang > Verificatie**. Selecteer het gewenste verificatietype onder het tabblad **Verificatiemethode**.



Opmerking: Op wachtwoord gebaseerde verificatie is standaard ingeschakeld. Als dit wordt gewijzigd in Clientverificatie op basis van certificaten, veroorzaakt dit een herstart van de toepassingsserver op alle implementatieknooppunten.

Identity Services Engine stelt niet in het wachtwoordbeleid voor Opdrachtlijn Interface (CLI) te configureren vanuit de CLI-indeling. Het beleid van het wachtwoord voor zowel de Graphical User Interface (GUI) als de CLI kan alleen worden ingesteld via de GUI van ISE. Om dit te configureren navigeer u naar **Beheer > Systeem > Admin Access > Verificatie** en navigeer naar het tabblad **Wachtwoordbeleid**.

Authentication

Authorization >

Administrators >

Settings >

GUI and CLI Password Policy

* Minimum Length: 4 characters (Valid Range 4 to 127)

Password must not contain:

- Admin name or its characters in reverse order
- *cisco* or its characters in reverse order
- This word or its characters in reverse order: _____
- Repeated characters four or more times consecutively
- Dictionary words, their characters in reverse order or their letters replaced with other characters ⓘ
 - Default Dictionary ⓘ
 - Custom Dictionary ⓘ No file selected.

The newly added custom dictionary file will replace the existing custom dictionary file.

Authentication

Authorization >

Administrators >

Settings >

Password must contain at least one character of each of the selected types:

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numeric characters
- Non-alphanumeric characters

Password History

- Password must be different from the previous 3 versions [When enabled CLI remembers only last 1 password irrespective of value configured]

* Cannot reuse password within 15 days (Valid Range 0 to 365)

Password Lifetime

Admins can be required to periodically change their password

If Admin user is also configured as a network user, an expired enable password can cause the admin account to become disabled

- Administrator passwords expire 45 days after creation or last change (valid range 1 to 3650)
- Send an email reminder to administrators 30 days prior to password expiration (valid range 1 to 3650)

ISE heeft een voorziening om een inactieve beheerder uit te schakelen. Om dit te configureren navigeer u naar **Beheer > Systeem > Admin Access > Verificatie** en navigeer naar **Account** tabblad **Policy**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', and 'Admin Access'. The left sidebar has 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Account Disable Policy' and shows a configuration option: 'Disable account after 30 days of inactivity. (Valid range 1 to 365)'. The checkbox is checked.

ISE biedt ook de mogelijkheid om een beheergebruikersaccount te vergrendelen of op te schorten op basis van het aantal mislukte inlogpogingen. Om dit te configureren navigeer u naar **Beheer > Systeem > Admin Access > Verificatie** en navigeer naar het tabblad **Lock/Suspend Settings**.

The screenshot shows the Cisco ISE Administration interface, specifically the 'Lock/Suspend Settings' configuration page. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled 'Lock/Suspend Settings' and shows the following configuration options: 'Suspend or Lock Account with Incorrect Login Attempts' (checked), 'Take action after 3 failed attempts (Valid Range 3 to 20)', 'Suspend account for 15 minutes (Valid Range 15 to 1440)' (selected), and 'Lock account' (unselected). There is also an 'Email remediation message' field with a text area containing the message: 'This account has been locked. For this account to become unlocked, please contact your IT helpdesk.'

Om de administratieve toegang te kunnen beheren, zijn er administratieve groepen, gebruikers en verschillende beleid/regels nodig om hun privileges te controleren en beheren.

Admin-groepen configureren

Navigeer naar **Beheer > Systeem > Admin Access > Beheerders > Admin Groepen** om beheerdersgroepen te configureren. Er zijn weinig groepen die standaard zijn ingebouwd en die niet kunnen worden verwijderd.

- Authentication
- Authorization >
- Administrators >
 - Admin Users
 - Admin Groups**
- Settings >

Admin Groups

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#) [Reset All Ext. groups](#)

<input type="checkbox"/>	Name	External Groups Mapped	Description
<input type="checkbox"/>	Customization Admin	0	Access Permission to Guest Menu and Device Portal Management.
<input type="checkbox"/>	ERS Admin	0	Full access permission to External RESTful Services (ERS) APIs. Admins ...
<input type="checkbox"/>	ERS Operator	0	Read-only access permission to the External RESTful Services (ERS) API...
<input type="checkbox"/>	Elevated System Admin	0	Access permission for Operations tab. Includes System and data access ...
<input type="checkbox"/>	Helpdesk Admin	0	Access permission for Operations tab.
<input type="checkbox"/>	Identity Admin	0	Access permission for Operations tab. Includes Identity Management and...
<input type="checkbox"/>	MnT Admin	0	Access permission for Operations tab.
<input type="checkbox"/>	Network Device Admin	0	Access permission for Operations tab. Includes Network Resources and ...
<input type="checkbox"/>	Policy Admin	0	Access permission for Operations and Policy tabs. Includes System and I...
<input type="checkbox"/>	RBAC Admin	0	Access permission for Operations tab. Includes System and data access ...
<input type="checkbox"/>	Read Only Admin	0	Access Permission for admin with read-only functionality
<input type="checkbox"/>	SPOG Admin	0	This is the group for SPOG Admin to use the APIs for export and import
<input type="checkbox"/>	Super Admin	0	Access permission for Operations, Policy and Administration tabs. Includ...
<input type="checkbox"/>	System Admin	0	Access permission for Operations tab. Includes System and data access ...

Nadat er een groep is gemaakt, selecteert u de groep en klikt u op Bewerken om administratieve gebruikers aan de groep toe te voegen. Er is een voorziening om externe identiteitsgroepen aan de Admin Groepen op ISE in kaart te brengen zodat een Externe Admin gebruiker de vereiste machtigingen krijgt. Om dit te configureren selecteert u het type als extern tijdens het toevoegen van de gebruiker.

- Authentication
- Authorization >
- Administrators >
 - Admin Users
 - Admin Groups**
- Settings >

Admin Groups > Super Admin

Admin Group

* Name

Description

Type External

External Identity Source
Name :

External Groups

* [+](#)

Member Users

Users

[+ Add](#) [Delete](#)

<input type="checkbox"/>	Status	Email	Username	First Name	Last Name
<input type="checkbox"/>	<input checked="" type="checkbox"/> Enabled		admin		

Admin-gebruikers configureren

Om Admin-gebruikers te configureren navigeer naar **Beheer > Systeem > Admin Access > Administrateurs > Admin Gebruikers**.

Cisco ISE Administration - System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication
Authorization >
Administrators >
Admin Users
Admin Groups
Settings >

Administrators

Edit + Add Change Status Delete Duplicate

<input type="checkbox"/>	Status	Name	Description	First Name	Last Name	Email Address	Admin Groups
<input type="checkbox"/>	Enabled	admin	Default Admin User				Super Admin

Klik op **Toevoegen**. Er zijn twee opties om uit te kiezen. De eerste is het toevoegen van een nieuwe gebruiker. De andere is om als ISE-beheerder een netwerktoegangsgebruiker (d.w.z. een door de gebruiker ingesteld interne gebruiker die toegang heeft tot het netwerk/de apparaten) te maken.

Cisco ISE Administration - System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication
Authorization >
Administrators >
Admin Users
Admin Groups
Settings >

Administrators

Edit + Add Change Status Delete Duplicate

<input type="checkbox"/>	Description	First Name	Last Name	Email Address	Admin Groups
<input type="checkbox"/>	Default Admin User				Super Admin

Create an Admin User
Select from Network Access Users >

Nadat u een optie hebt geselecteerd, moeten de gewenste gegevens worden verstrekt en moet de gebruikersgroep worden geselecteerd op basis waarvan de rechten en privileges aan de gebruiker worden verleend.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Administrators List > New Administrator

Authentication

Authorization >

Administrators >

Admin Users

Admin Groups

Settings >

Admin User

* Name Test_Admin

Status Enabled

Email testadmin@abcd.com Include system alarms in emails

External ⓘ

Read Only

Inactive account never disabled

Password

* Password ●●●●●●●● ⓘ

* Re-Enter Password ●●●●●●●● ⓘ

Generate Password

User Information

First Name

Last Name

Account Options

Description

Admin Groups

* ⓘ

Admin Groups

EQ

< ⓘ ⚙

Customization Admin ▲

ERS Admin

ERS Operator

Elevated System Admin

Helpdesk Admin

Identity Admin ▼

Toestemmingen configureren

Er zijn twee soorten permissies die voor een gebruikersgroep kunnen worden ingesteld:

1. Menu Access
2. Gegevenstoegang

Menu Access regelt het navigatie-zicht op ISE. Er zijn twee opties voor elk tabblad, Weergeven of verbergen, dat kan worden geconfigureerd. Een Menu Access-regel kan worden ingesteld om geselecteerde tabbladen te tonen of te verbergen.

Data Access controleert de mogelijkheid om de Identity Data op ISE te lezen/benaderen/te wijzigen. Toegangstoestemming kan alleen worden ingesteld voor Admin-groepen, gebruikersidentiteitsgroepen, Endpoint Identity Group en Network Apparaatgroepen. Er zijn drie opties voor deze entiteiten op ISE die kunnen worden geconfigureerd. Ze hebben volledige toegang, alleen-lezen toegang en geen toegang. Een gegevenstoegangsregel kan worden ingesteld om een van deze drie opties voor elk tabblad op ISE te kiezen.

Het beleid voor toegang tot het menu en toegang tot de gegevens moet worden gemaakt voordat ze op een willekeurige admin-groep kunnen worden toegepast. Er zijn een paar

beleidsmaatregelen die standaard zijn ingebouwd, maar ze kunnen altijd worden aangepast of er kan een nieuw beleid worden gecreëerd.

Om een Menu Access-beleid te configureren kunt u navigeren naar **Beheer > Systeem > Toegang > Toestemming > Toestemmingen > Menu-toegang**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration · System' and 'Admin Access'. The left sidebar shows a navigation menu with 'Permissions' expanded to 'Menu Access'. The main content area is titled 'Menu Access' and contains a table of permissions. Above the table are buttons for 'Edit', '+ Add', 'Duplicate', and 'Delete'.

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Super Admin Menu Access	Access permission for Operations tab, Policy tab, Guest Access tab, Mobile Device Management tab
<input type="checkbox"/>	Policy Admin Menu Access	Access permission for Operations tab, Policy tab, Guest Access tab, Mobile Device Management tab,
<input type="checkbox"/>	Helpdesk Admin Menu Access	Access permission for Operations tab.
<input type="checkbox"/>	Identity Admin Menu Access	Access permission for Operations tab and Identity Management.
<input type="checkbox"/>	Network Device Menu Access	Access permission for Operations tab and Network Resources.
<input type="checkbox"/>	System Admin Menu Access	Access permission for Operations tab and System.
<input type="checkbox"/>	RBAC Admin Menu Access	Access permission for Operations tab and System.
<input type="checkbox"/>	MnT Admin Menu Access	Access permission for Operations tab.
<input type="checkbox"/>	Customization Admin Menu Access	Access Permission to Guest Menu and Device Portal Management.
<input type="checkbox"/>	TACACS+ Admin Menu Access	Access Permission to Operations, Administration and Workcenter

Klik op **Toevoegen**. Elke navigatie optie in ISE kan worden ingesteld om te worden getoond/verborgen in een beleid.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access**

Menu Access List > New RBAC Menu Access

Create Menu Access Permission

* Name: Custom_Menu_Access

Description:

Menu Access Privileges

ISE Navigation Structure

- > Policy
- ▼ Administration
 - ▼ System
 - Deployment
 - Licensing
 - ▼ Certificates
 - Certificate Manage
 - System Certificates
 - Trusted Certificates

Permissions for Menu Access

Show

Hide

Om het beleid voor toegang tot gegevens te configureren dient u te navigeren naar **Administratie > Toegang tot beheersysteem > Toestemming > Toestemmingen > Toegang tot gegevens.**

Cisco ISE Administration • System Evaluation Mode ?

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Data Access

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Super Admin Data Access	Access permission for Admin Groups, User Identity Groups, Endpoint Identity Groups, All Locations and All Device Types.
<input type="checkbox"/>	Policy Admin Data Access	Access permission for User Identity Groups and Endpoint Identity Groups.
<input type="checkbox"/>	Identity Admin Data Access	Access permission for User Identity Groups and Endpoint Identity Groups.
<input type="checkbox"/>	Network Admin Data Access	Access permission for All Locations and All Device Types.
<input type="checkbox"/>	System Admin Data Access	Access permission for Admin Groups.
<input type="checkbox"/>	RBAC Admin Data Access	Access permission for Admin Groups.
<input type="checkbox"/>	Customization Admin Data Access	
<input type="checkbox"/>	TACACS+ Admin Data Access	Access permission for All Locations and All Device Types, User Identity groups and End point identity groups.
<input type="checkbox"/>	Read Only Admin Data Access	Access permission for All Locations and All Device Types, User Identity groups and End point identity groups.

Klik op **Add** om een nieuw beleid en configureerbare rechten te maken voor toegang tot Admin/User Identity/Endpoint Identity/Network Group.

Authentication

Authorization ▾

Permissions ▾

Menu Access

Data Access

RBAC Policy

Administrators >

Settings >

Create Data Access Permission

* Name

Description

Data Access Privileges

- > Admin Groups
- > User Identity Groups
- ▾ Endpoint Identity Groups
 - Blacklist
 - GuestEndpoints
 - RegisteredDevices
 - Unknown
 - > Profiled
 - > Network Device Groups

Permissions for Data Access

Full Access

Read Only Access

No Access

RBAC-beleid configureren

RBAC staat voor rollengebaseerde toegangscontrole. Rol (Admin Group) waartoe een gebruiker behoort, kan worden ingesteld om het gewenste menu- en gegevenstoegangsbeleid te gebruiken. Er kunnen meerdere RBAC-beleid worden ingesteld voor één rol OF meerdere rollen kunnen worden ingesteld in één beleid voor toegang tot menu en/of gegevens. Al deze toepasbaar beleid wordt beoordeeld wanneer een beheerder een actie probeert uit te voeren. Het uiteindelijke besluit is het geheel van alle beleidsmaatregelen die op die rol van toepassing zijn. Indien er tegenstrijdige regels bestaan die tegelijkertijd toestaan en ontkennen, wordt de ontkenningsovertreden door de vergunningsregel. Om dit beleid te configureren klikt u op **Beheer > System > Toegang > autorisatie > RCB Beleid**.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Se

Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (identity group data element). Multiple Menu/Data Access permissions are not allowed on a single policy. You can copy the default policies shown below, then modify them as needed. Note that system-created and default policies cannot be deleted. For decision making, all applicable policies will be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy (policies are displayed in alphabetical order of the policy name).

Authentication

Authorization

Permissions

RBAC Policy

Administrators

Settings

RBAC Policies

Rule Name	Admin Groups	Permissions
<input checked="" type="checkbox"/> Customization Admin Policy	If Customization Admin	+ then Customization Admin Menu ... + Actions
<input checked="" type="checkbox"/> Elevated System Admin Policy	If Elevated System Admin	+ then System Admin Menu Access ... + Actions
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin	+ then Super Admin Data Access + Actions
<input checked="" type="checkbox"/> ERS Operator Policy	If ERS Operator	+ then Super Admin Data Access + Actions
<input checked="" type="checkbox"/> ERS Trustsec Policy	If ERS Trustsec	+ then Super Admin Data Access + Actions
<input checked="" type="checkbox"/> Helpdesk Admin Policy	If Helpdesk Admin	+ then Helpdesk Admin Menu Access + Actions
<input checked="" type="checkbox"/> Identity Admin Policy	If Identity Admin	+ then Identity Admin Menu Access ... + Actions
<input checked="" type="checkbox"/> MnT Admin Policy	If MnT Admin	+ then MnT Admin Menu Access + Actions
<input checked="" type="checkbox"/> Network Device Policy	If Network Device Admin	+ then Network Device Menu Access... + Actions
<input checked="" type="checkbox"/> Policy Admin Policy	If Policy Admin	+ then Policy Admin Menu Access a... + Actions
<input checked="" type="checkbox"/> RBAC Admin Policy	If RBAC Admin	+ then RBAC Admin Menu Access a... + Actions

Klik op **Handelingen** om beleid te dupliceren/invoegen/verwijderen.

Opmerking: Systeemgecreëerd en standaard beleid kan niet worden bijgewerkt en standaard beleid kan niet worden verwijderd.

Opmerking: De toegangsrechten van meerdere menu's/data kunnen niet in één regel worden ingesteld.

Instellingen instellen voor Admin Access

Naast het RBAC-beleid zijn er een aantal instellingen die gemeenschappelijk zijn voor alle beheergebruikers.

Om het aantal maximaal toegestane sessies te configureren, vooraf inloggen en achteraf inlogbanners voor GUI en CLI, **navigeer** naar **Administratie > Systeem > Admin Access > Instellingen > Toegang**. Configureer deze onder het tabblad **Session**.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access**

Authentication
 Authorization >
 Administrators >
 Settings ▾
 Access
 Session
 Portal Customization

Session IP Access MnT Access

GUI Sessions

Maximum Concurrent Sessions: 10 (Valid Range 1 to 20)

Pre-login banner
 Welcome to ISE

Post-login banner

CLI Sessions

Maximum Concurrent Sessions: 5 (Valid Range 1 to 10)

Pre-login banner

Om de lijst met IP-adressen te configureren waartoe de GUI en de CLI toegang hebben, navigeer naar **Beheer > Systeem > Admin Access > Instellingen > Toegang** en navigeer naar het **IP Access** tabblad.

Cisco ISE Administration • System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access**

Authentication
 Authorization >
 Administrators >
 Settings ▾
 Access
 Session
 Portal Customization

Session **IP Access** MnT Access

Access Restriction
 Allow all IP addresses to connect
 Allow only listed IP addresses to connect

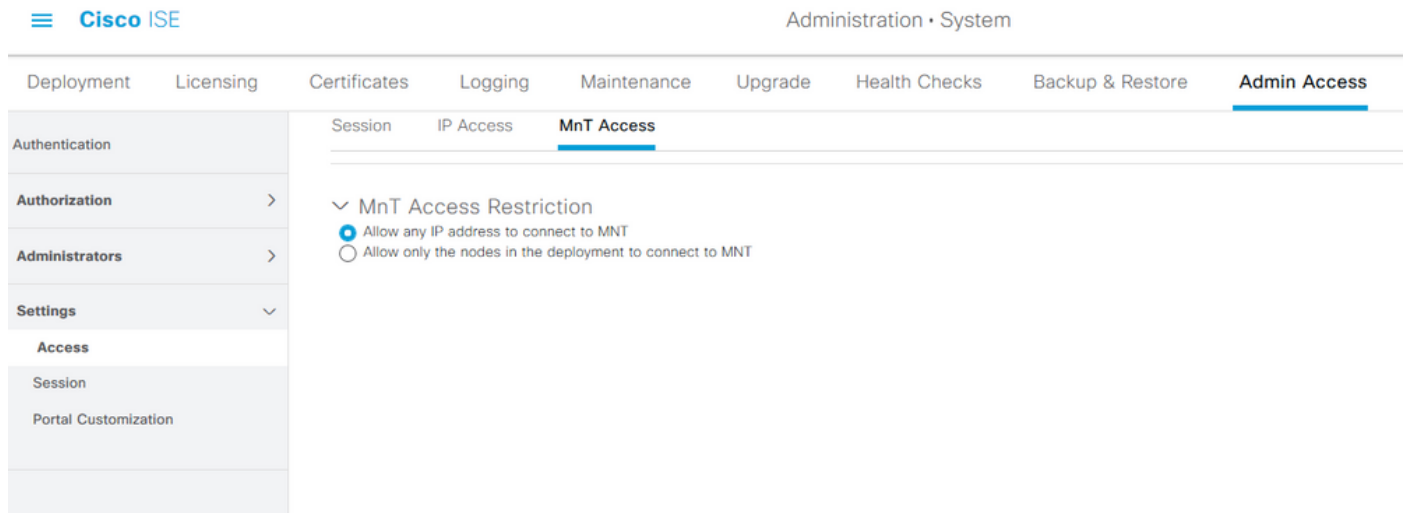
Configure IP List for Access Restriction
 IP List
 + Add Edit Delete

IP	MASK
<input type="checkbox"/> 10.9.8.0	<input type="checkbox"/> 24

Om een lijst van knooppunten te vormen waarvan de beheerders tot de sectie MnT in Cisco ISE kunnen toegang hebben, navigeer naar **Administratie > Systeem > Toegang > Instellingen > Toegang > Toegang** en navigeer naar het tabblad **MnT Access**.

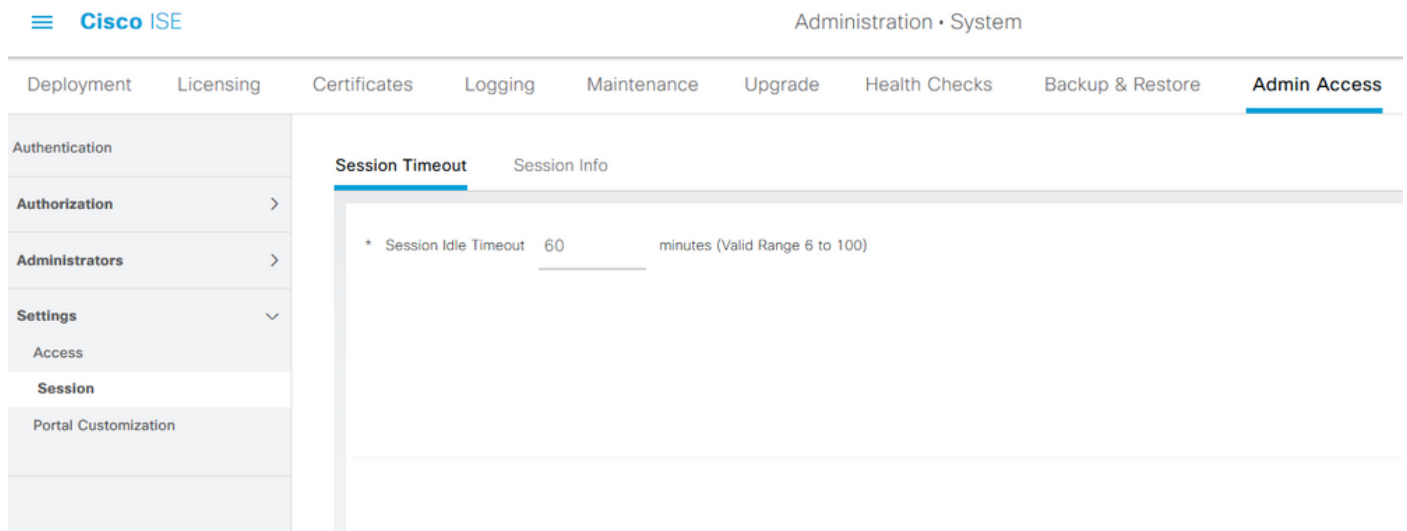
Als u knooppunten of entiteiten binnen of buiten de implementatie wilt toestaan om syslogs naar

MnT te verzenden, klik dan op het **IP-adres toestaan om verbinding te maken met de radioknop MNT**. Als u alleen knooppunten of entiteiten binnen de implementatie wilt toestaan om syslogs naar MnT te verzenden, klikt u op **Alleen de knooppunten in de implementatie toestaan om verbinding te maken met de radioknop MNT**.

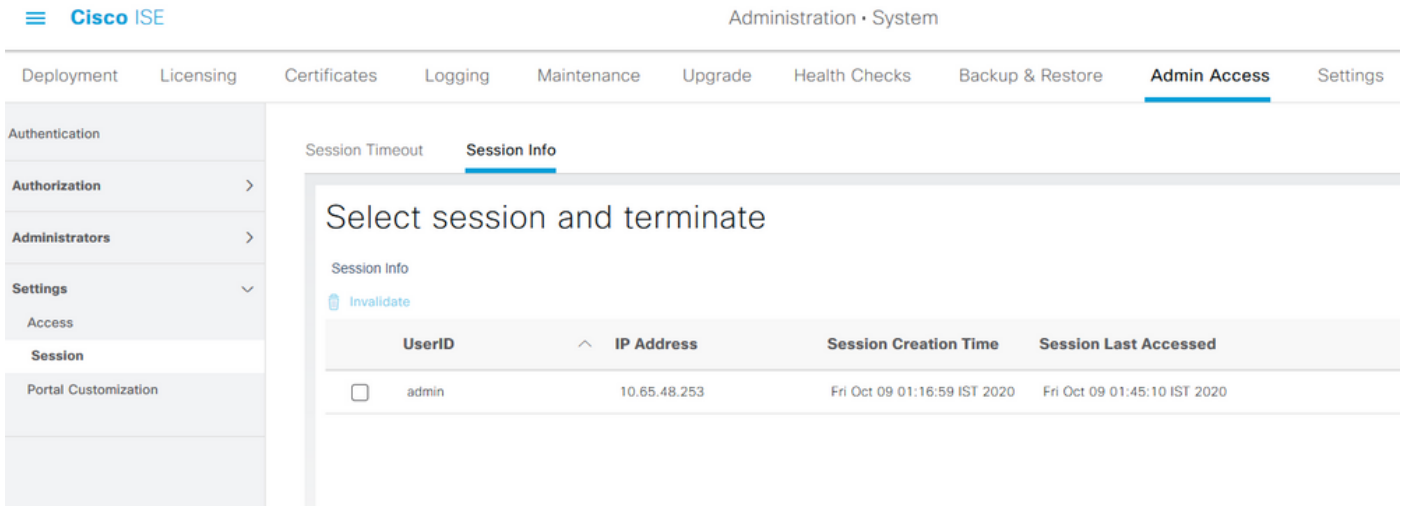


Opmerking: Voor ISE 2.6-patches 2 en later, *gebruik "ISE Messaging Service" voor levering van UDP-systemen aan MnT* is standaard ingeschakeld waardoor niet alle syslogs van andere entiteiten buiten de implementatie kunnen komen.

Om een timeout waarde te configureren door de inactiviteit van een sessie, navigeer dan naar **Administratie > Systeem > Admin Access > Instellingen > Sessie**. Stel deze waarde in onder het tabblad **Time-out voor sessie**.



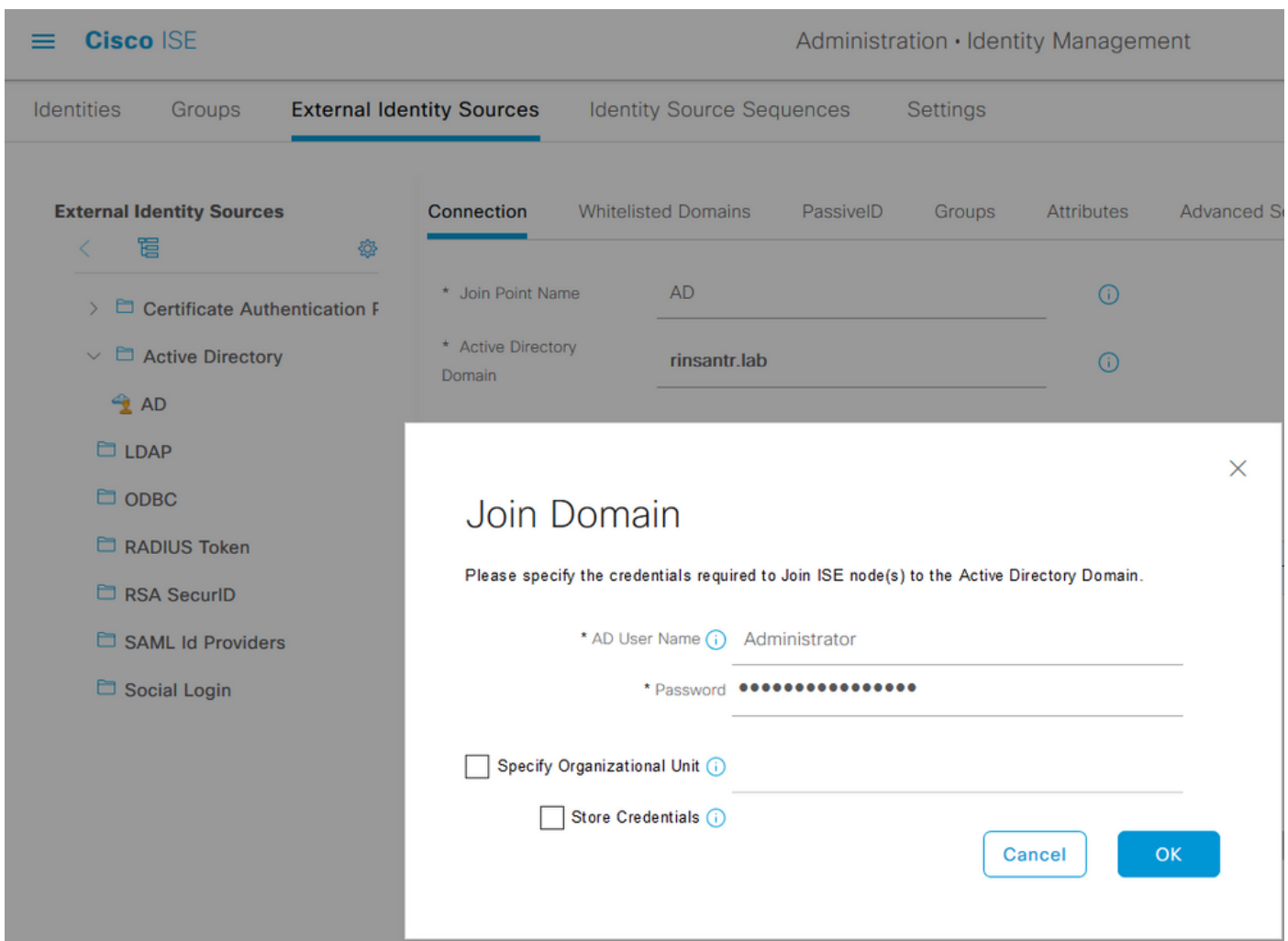
Om de huidige actieve sessies te bekijken/ongeldig te maken, navigeer dan naar **Beheer > Admin Access > Instellingen > Sessie** en klik op het tabblad **Sessieinfo**.



Admin Portal Access met AD-Credentials configureren

Doe mee met ISE naar AD

Om zich bij ISE aan een extern domein aan te sluiten, navigeer naar **Beheer > Identity Management > Externe Hulpbronnen > Active Directory**. Geef het nieuwe aansluitpunt naam en actief folder domein op. Voer de aanmeldingsgegevens in van de AD-account die wijzigingen in computerobjecten kunnen toevoegen en aanbrengen, en klik op **OK**.



Connection Whitelisted Domains PassiveID Groups Attributes Advanced Settings

* Join Point Name AD ⓘ

* Active Directory Domain rinsantr.lab ⓘ

+ Join + Leave 👤 Test User 🔧 Diagnostic Tool ↻ Refresh Table

<input type="checkbox"/>	ISE Node	ISE Node R...	Status	Domain Controller	Site
<input type="checkbox"/>	rini-ise-30.gce.iselab.local	STANDALONE	✔ Operational	WIN-5KSMPOHEP5A.rinsantr.l...	Default-First-Site-Name

Map-groepen selecteren

Navigeer naar **Administratie > identiteitsbeheer > Externe Bronnen > Actieve Map**. Klik op de gewenste naam aan punt toevoegen en navigeer naar het tabblad **Groepen**. Klik op **Add > Selecteer groepen uit Map > Retouregroepen**. Importeer minimaal één AD-groep waartoe de beheerder behoort, en klik op **OK** en klik vervolgens op **Opslaan**.

Identity Sources

Connection

Edit +

Na

No data available

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain rinsantr.lab

Name Filter * SID Filter * Type Filter ALL

50 Groups Retrieved.

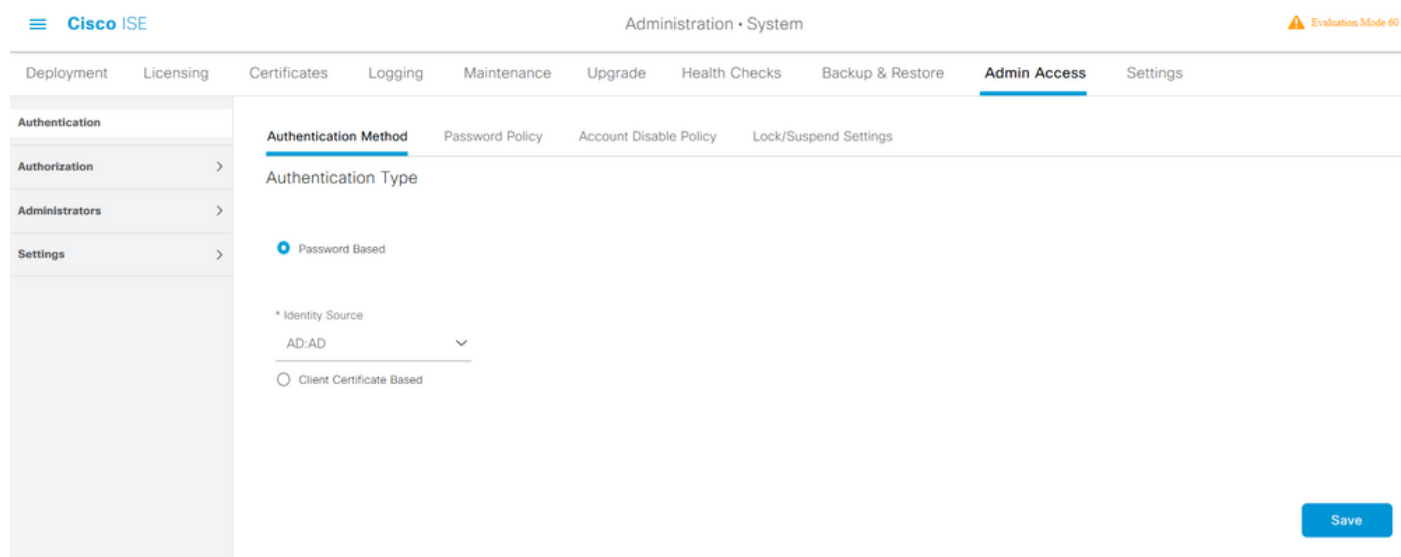
<input type="checkbox"/>	Name	Group SID	Group Type
<input type="checkbox"/>	rinsantr.lab/Users/Enterprise Key Admins	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input type="checkbox"/>	rinsantr.lab/Users/Enterprise Read-only Domain ...	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input type="checkbox"/>	rinsantr.lab/Users/Group Policy Creator Owners	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/Key Admins	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/Protected Users	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/RAS and IAS Servers	S-1-5-21-1977851106-3699455990-29458652...	DOMAIN LOCAL
<input type="checkbox"/>	rinsantr.lab/Users/Read-only Domain Controllers	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/Schema Admins	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input checked="" type="checkbox"/>	rinsantr.lab/Users/Test Group	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL

[Edit](#) [+ Add](#) [Delete Group](#) [Update SID Values](#)

<input type="checkbox"/>	Name	SID
<input type="checkbox"/>	rinsantr.lab/Users/Test Group	S-1-5-21-1977851106-3699455990-2945865208-1106

Administratieve toegang voor AD inschakelen

Om op wachtwoord gebaseerde verificatie van ISE met behulp van AD mogelijk te maken, navigeer naar **Administratie > Systeem > Admin Access > Verificatie**. Selecteer in het tabblad **Verificatiemethode** de optie **Wachtwoord gebaseerd**. Selecteer **AD** in het vervolgkeuzemenu **Identity Source** en klik op **Save**.



De ISE Admin Group instellen op Toewijzing van AD-groepen

Dit staat een vergunning toe om de Rol Based Access Control (RBAC) machtigingen voor de beheerder te bepalen op basis van groepslidmaatschap in AD. Om een Cisco ISE Admin Group te definiëren en die aan een AD groep toe te wijzen, navigeer naar **Beheer > Systeem > Admin Access > Administrators > Admin Groepen**. Klik op **Toevoegen** en voer een naam voor de nieuwe Admin-groep in. Controleer in het veld Type het vakje **Externe** controle. Selecteer in het vervolgkeuzemenu **Externe Groepen** de AD-groep waaraan deze Admin-groep moet worden toegewezen (zoals gedefinieerd in het bovenstaande gedeelte Map Group selecteren). **Breng** de wijzigingen in.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access**

Authentication

Authorization >

Administrators >

Admin Users

Admin Groups

Settings >

Admin Groups > ISE AD Admin Group

Admin Group

* Name: ISE AD Admin Group

Description:

Type: External

External Identity Source
Name: AD

External Groups

* +

Member Users

Users

+ Add Delete

<input type="checkbox"/>	Status	Email	Username	First Name	Last Name
No data available					

RBAC-toegangsrechten voor de Admin-groep instellen

Als u RBAC-toestemming wilt toewijzen aan de Admin Group die in de vorige sectie is gemaakt, navigeer dan naar **Administratie > Systeem > Admin Access > autorisatie > RBAC Policy**. Selecteer in het vervolgkeuzemenu **Handelingen** rechts de optie **Nieuw beleid invoegen**. Stel een nieuwe regel in, stel deze in kaart met de Admin Group die in de bovenstaande sectie is gedefinieerd en wijs deze toe met de gewenste gegevens en menu-toegangsrechten en klik vervolgens op **Opslaan**.

Cisco ISE Administration • System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (identity group data elements) and other c allowed on a single policy. You can copy the default policies shown below, then modify them as needed. Note that system-created and default policies cannot be updated, and default policies cannot be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy. Permit overrides Deny. (The policies are displayed in alphabetical order of the policy name).

RBAC Policies

Rule Name	Admin Groups	Permissions
<input checked="" type="checkbox"/> Customization Admin Policy	If Customization Admin +	then Customization Admin Men... + Actions
<input checked="" type="checkbox"/> RBAC Policy 1	If ISE AD Admin Group +	then Super Admin Menu Acces... X Actions
<input checked="" type="checkbox"/> Elevated System Admin Poli	If Elevated System Admin +	then
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin +	then
<input checked="" type="checkbox"/> ERS Operator Policy	If ERS Operator +	then

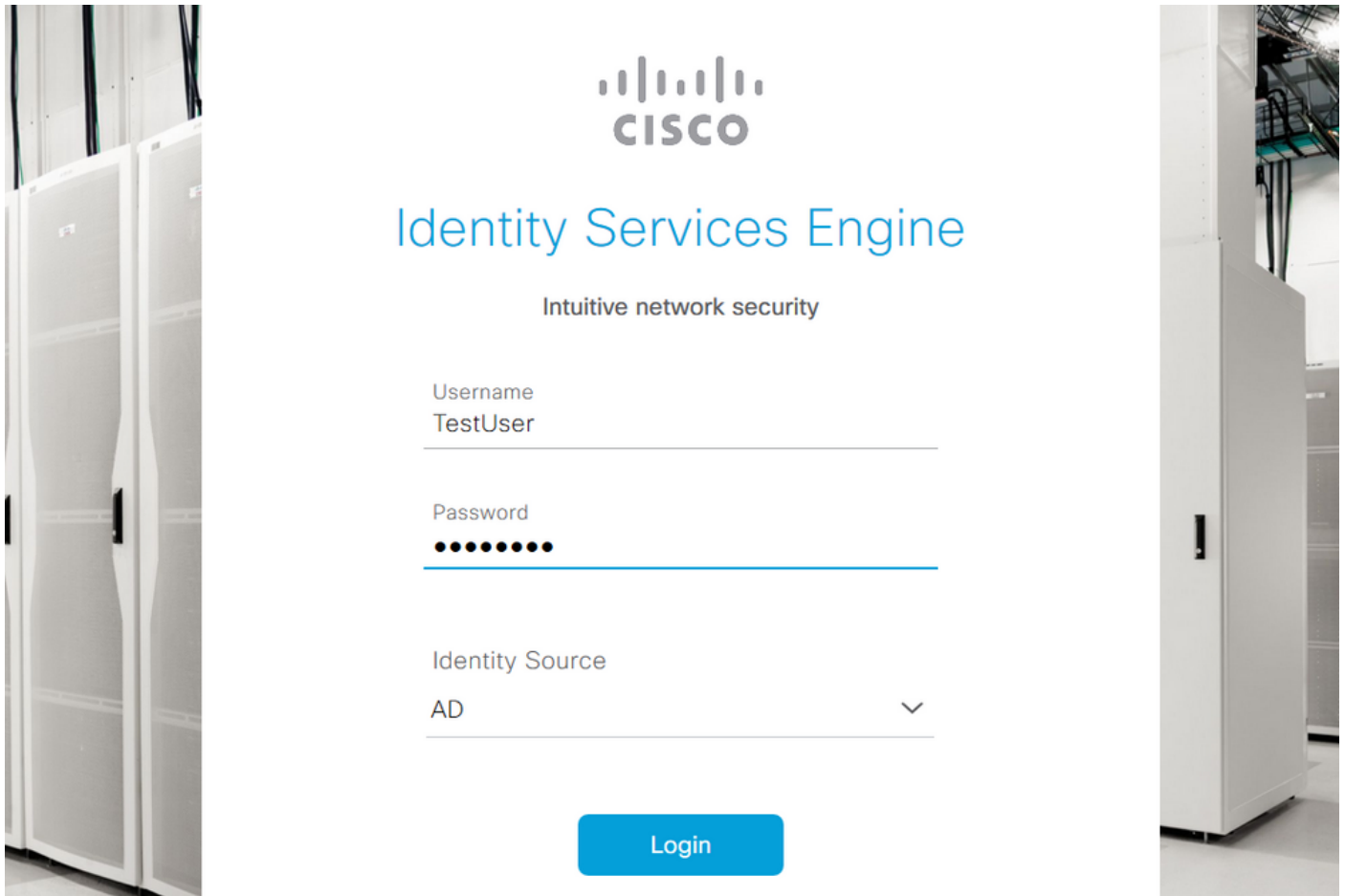
Super Admin Menu Access +

Super Admin Data Access +

Toegang tot ISE met AD-Credentials en controleer deze

Uitloggen van de administratieve GUI. Selecteer de optie **Punt** samenvoegen in het vervolgkeuzemenu **Identity Source**. Voer de gebruikersnaam en het wachtwoord in uit de AD-

database en log in.



The image shows a login interface for the Cisco Identity Services Engine (ISE). At the top center is the Cisco logo, consisting of a stylized signal icon above the word "CISCO". Below the logo is the title "Identity Services Engine" in a large blue font, followed by the tagline "Intuitive network security" in a smaller black font. The login form includes three fields: "Username" with the text "TestUser", "Password" with a masked password of ten dots, and "Identity Source" with a dropdown menu currently showing "AD". A blue "Login" button is positioned at the bottom center of the form. The background of the page is a light gray, and the entire interface is flanked by two vertical panels showing server racks in a data center.

Om te bevestigen dat de configuratie correct werkt, verifieert u de geauthenteerde gebruikersnaam van het pictogram **Settings** in de rechterbovenhoek van de ISE GUI. Navigeer naar **serverinformatie** en controleer de gebruikersnaam.

Server Information

Username: TestUser

Host: rini-ise-30

Personas: Administration, Monitoring, Policy
Service (SESSION,PROFILER)

Role: STANDALONE

System Time: Oct 27 2020 01:23:21 AM
Asia/Kolkata

FIPS Mode: Disabled

Version: 3.0.0.458

Patch Information: none












OK

Admin Portal Access met LDAP configureren

Doe mee met ISE aan LDAP

Navigeer naar **Administratie > identiteitsbeheer > Externe identiteitsbronnen > Actieve Map > LDAP**. Typ onder het tabblad **Algemeen** een naam voor de LDAP en kies het schema als **actieve map**.

External Identity Sources

- <  
- >  Certificate Authentication F
- ▼  Active Directory
 -  AD
 -  LDAP
 -  ODBC
 -  RADIUS Token
 -  RSA SecurID
 -  SAML Id Providers
 -  Social Login

[LDAP Identity Sources List](#) > New LDAP Identity Source

LDAP Identity Source









General Connection Directory Organization Groups Attribut

* Name

Description

▶ Schema ▼

Daarna, om het connectietype te configureren navigeer naar het tabblad **Connection**. Stel hier de Hostname/IP van de Primaire LDAP-server in samen met poort 389 (LDAP)/636 (LDAP-Secure). Voer het pad van de Admin-naam (DN) in met het Admin-wachtwoord van de LDAP-server.

- ▼  Active Directory
 -  AD
 -  LDAP
 -  ODBC
 -  RADIUS Token
 -  RSA SecurID
 -  SAML Id Providers
 -  Social Login

General **Connection** Directory Organization Groups Attributes Advanced Settings

	Primary Server		Secondary Server
			<input type="checkbox"/> Enable Secondary Server
* Hostname/IP	<input type="text" value="10.127.196.131"/> ⓘ	Hostname/IP	<input type="text"/>
* Port	<input type="text" value="389"/>	Port	<input type="text" value="389"/>
<input type="checkbox"/> Specify server for each ISE node			
Access	<input type="radio"/> Anonymous Access <input checked="" type="radio"/> Authenticated Access	Access	<input checked="" type="radio"/> Anonymous Access <input type="radio"/> Authenticated Access
Admin DN	<input type="text" value="* CN=Administrator,CN=Users,DC"/>	Admin DN	<input type="text" value="admin"/>
Password	<input type="text" value="*"/>	Password	<input type="text"/>
Secure Authentication	<input type="checkbox"/> Enable Secure Authentication	Secure Authentication	<input type="checkbox"/> Enable Secure Authentication

Klik vervolgens op het tabblad **Map Organisatie** en klik op **Namen** om de juiste organisatiegroep van de gebruiker te kiezen, gebaseerd op de hiërarchie van gebruikers die opgeslagen zijn in de LDAP server.

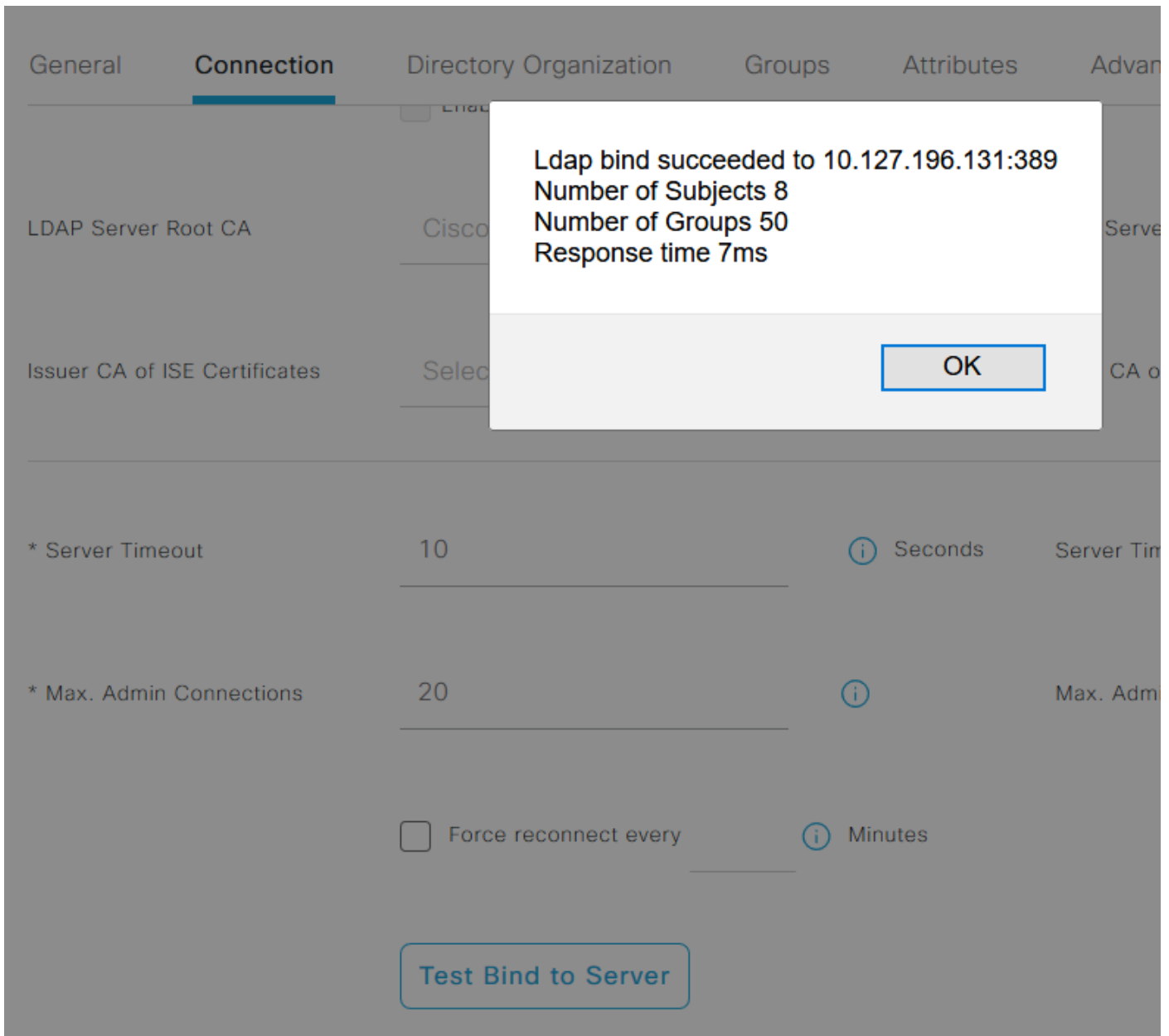
External Identity Sources

[Certificate Authentication F](#)[Active Directory](#)[AD](#)[LDAP](#)[ODBC](#)[RADIUS Token](#)[RSA SecurID](#)[SAML Id Providers](#)[Social Login](#)[LDAP Identity Sources List](#) > LDAPExample

LDAP Identity Source

General Connection **Directory Organization** Groups Attributes Advanced Settings* Subject Search Base DC=rinsantr,DC=lab [Naming Contexts...](#) ⓘ* Group Search Base DC=rinsantr,DC=lab [Naming Contexts...](#) ⓘSearch for MAC Address in Format ▼ Strip start of subject name up to the last occurrence of the separator Strip end of subject name from the first occurrence of the separator

Klik op **Test Bind to Server** onder het **tabblad Connection** om de bereikbaarheid van de LDAP server vanaf ISE te testen.



Blader nu naar het tabblad **Groepen** en klik op **Toevoegen > Groepen uit map > Groepen ophalen**. Als u ten minste één groep importeert waartoe de beheerder behoort, klikt u op **OK** en vervolgens klikt u op **Opslaan**.

Select Directory Groups

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.

Filter: * Retrieve Groups... Number of Groups Retrieved: 50 (Limit is 100)

<input type="checkbox"/>	Name
<input type="checkbox"/>	CN=Server Operators,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Storage Replica Administrators,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=System Managed Accounts Group,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Terminal Server License Servers,CN=Builtin,DC=rinsantr,DC=lab
<input checked="" type="checkbox"/>	CN=Test Group,CN=Users,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Users,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Windows Authorization Access Group,CN=Builtin,DC=rinsantr,DC=lab

Cancel OK

Internal Identity Sources

- <
- > Certificate Authentication F
- > Active Directory
- ✓ LDAP
 - LDAPExample
 - ODBC
 - RADIUS Token
 - RSA SecurID

LDAP Identity Sources List > LDAPExample

LDAP Identity Source

General Connection Directory Organization **Groups** Attributes Advanced Settings

Edit Add Delete Group

<input type="checkbox"/>	Name
<input type="checkbox"/>	CN=Test Group,CN=Users,DC=rinsantr,DC=lab

Administratieve toegang voor gebruikers van LDAP inschakelen

Om op wachtwoord gebaseerde verificatie van ISE met behulp van LDAP mogelijk te maken, navigeer naar **Administratie > Systeem > Admin Access > Verificatie**. Selecteer in het tabblad **Verificatiemethode** de optie **Wachtwoord gebaseerd**. Selecteer **LDAP** in het vervolgkeuzemenu **Identity Source** en klik op **Save**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE' and 'Administration - System'. The main navigation menu has 'Admin Access' selected. The left sidebar shows 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Authentication Method' and 'Authentication Type'. Under 'Authentication Method', 'Password Based' is selected. Under 'Authentication Type', 'Identity Source' is set to 'LDAP:LDAPExample' and 'Client Certificate Based' is unselected. A 'Save' button is located at the bottom right.

Stel de ISE Admin Group op LDAP groepjes in

Hierdoor krijgt de geconfigureerde gebruiker toegang tot de beheerder op basis van de toestemming van het RBAC-beleid, dat op zijn beurt gebaseerd is op het lidmaatschap van de LeerP-groep van de gebruiker. Om een Cisco ISE Admin Group te definiëren en in kaart te brengen aan een LDAP groep, navigeer naar **Beheer > Systeem > Admin Access > Administrators > Admin Groepen**. Klik op **Toevoegen** en voer een naam voor de nieuwe Admin-groep in. Controleer in het veld Type het vakje **Externe** controle. Selecteer in het vervolgkeuzemenu **Externe Groepen** de LDAP-groep waaraan deze Admin-groep moet worden toegewezen (zoals eerder opgehaald en gedefinieerd). **Breng** de wijzigingen in.

The screenshot shows the 'New Admin Group' form in the Cisco ISE Administration interface. The 'Name' field contains 'ISE LDAP Admin Group'. The 'Description' field is empty. The 'Type' field has the 'External' checkbox checked. The 'External Identity Source' section shows 'Name : LDAPExample'. The 'External Groups' section is expanded, showing a list of groups with 'CN=Test Group,CN=Users,DC=' selected. A 'Save' button is visible at the bottom right.

RBAC-toegangsrechten voor de Admin-groep instellen

Als u RBAC-toestemming wilt toewijzen aan de Admin Group die in de vorige sectie is gemaakt, navigeer dan naar **Administratie > Systeem > Admin Access > autorisatie > RBAC Policy**. Selecteer in het vervolgkeuzemenu **Handelingen** rechts de optie **Nieuw beleid invoegen**. Stel een nieuwe regel in, stel deze in kaart met de Admin Group die in de bovenstaande sectie is

gedefinieerd en wijs deze toe met de gewenste gegevens en menu-toegangsrechten en klik vervolgens op **Opslaan**.

The screenshot shows the Cisco ISE Administration System interface. The top navigation bar includes 'Administration · System' and an 'Evaluate' button. The main menu on the left includes 'Authentication', 'Authorization', 'Permissions', 'RBAC Policy', 'Administrators', and 'Settings'. The 'RBAC Policy' section is active, displaying a table of policies. A dropdown menu is open for the 'Super Admin Menu Access' policy, showing options like 'Super Admin Menu Access' and 'Read Only Admin Data Access'.

Rule Name	Admin Groups	Permissions
Customization Admin Policy	Customization Admin	Customization Admin Menu ...
RBAC Policy 2	ISE LDAP Admin Group	Super Admin Menu Access a...
Elevated System Admin Poli	Elevated System Admin	
ERS Admin Policy	ERS Admin	
ERS Operator Policy	ERS Operator	
ERS Trustsec Policy	ERS Trustsec	Super Admin Data Access
Healthcheck Admin Policy	Healthcheck Admin	Healthcheck Admin Menu Access

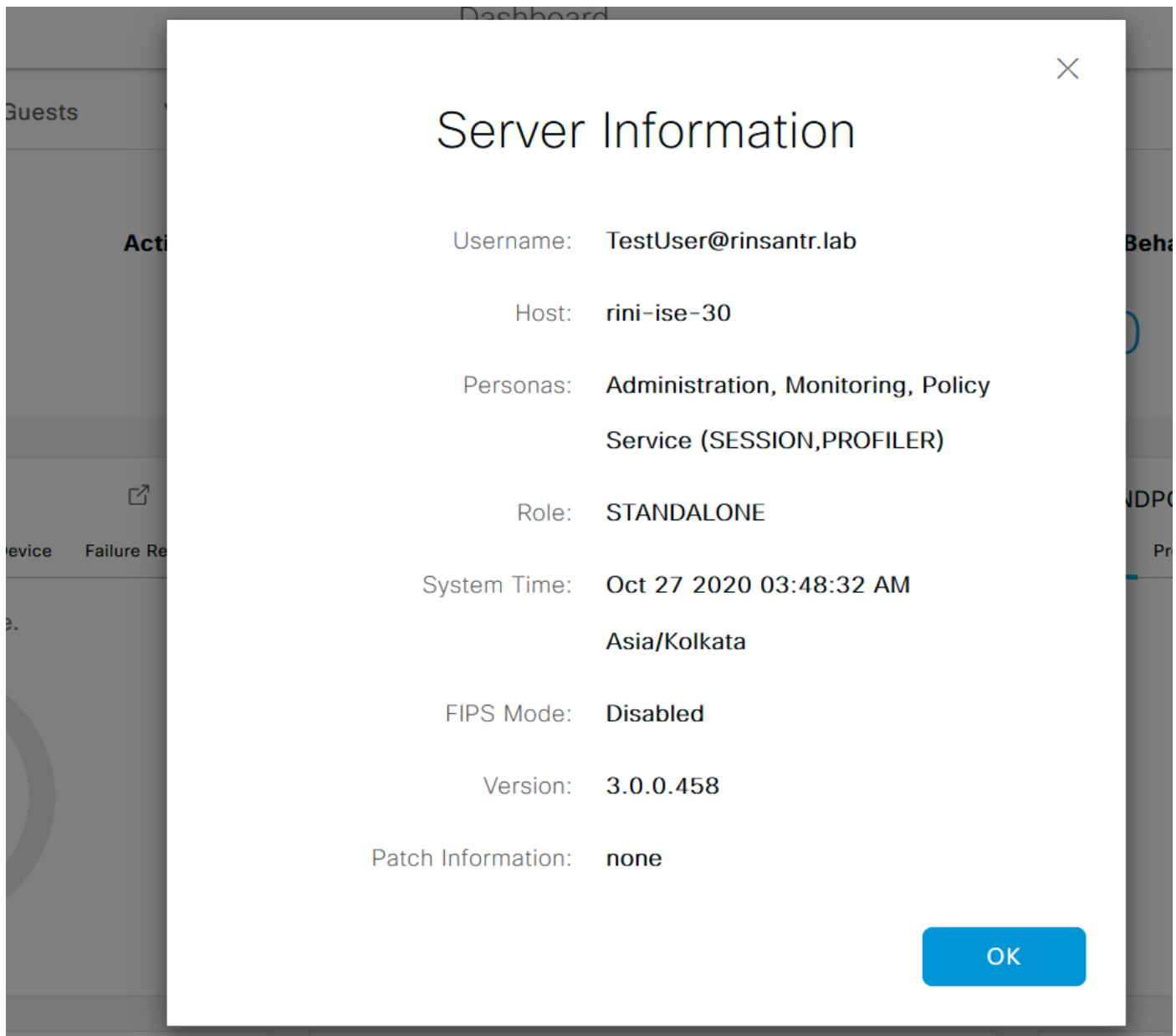
Toegang tot ISE met LDAP Credentials en controleer

Uitloggen van de administratieve GUI. Selecteer de LDAP naam in het vervolgkeuzemenu **Identity Source**. Voer de gebruikersnaam en het wachtwoord in uit de LDAP-database en log in.

The screenshot shows the Cisco Identity Services Engine login page. The page features the Cisco logo and the text 'Identity Services Engine' and 'Intuitive network security'. The login form includes fields for 'Username' (TestUser@rinsantr.lab), 'Password' (masked with dots), and 'Identity Source' (LDAPExample). A blue 'Login' button is at the bottom.

Om te bevestigen dat de configuratie correct werkt, verifieert u de geauthenticeerde

gebruikersnaam van het pictogram **Instellingen** in de rechterbovenhoek van de ISE GUI. Navigeer naar **serverinformatie** en controleer de gebruikersnaam.



The screenshot shows a 'Server Information' dialog box overlaid on the ISE GUI. The dialog contains the following information:

- Username: TestUser@rinsantr.lab
- Host: rini-ise-30
- Personas: Administration, Monitoring, Policy Service (SESSION,PROFILER)
- Role: STANDALONE
- System Time: Oct 27 2020 03:48:32 AM Asia/Kolkata
- FIPS Mode: Disabled
- Version: 3.0.0.458
- Patch Information: none

An 'OK' button is located at the bottom right of the dialog.