

Kenmerken en gebruiksgevallen onder ISE-rapporten

Inhoud

[Inleiding](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Navigatie tussen rapporten](#)

[Filters](#)

[Snel filter](#)

[Geavanceerd filter](#)

[Opslaan naar mijn rapporten](#)

[Uitvoer van rapporten](#)

[Geplande rapporten](#)

Inleiding

Dit document beschrijft de verschillende functies en gebruikerscases onder het gedeelte Rapporten van de Cisco Identity Services Engine (ISE). Deze rapporten worden gebruikt om de verschillende functies op ISE te controleren en problemen op te lossen en trends van de netwerkactiviteiten te analyseren vanuit een gecentraliseerd beheerknooppunt.

Vereisten

Cisco raadt u aan de kennis van ISE te hebben.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ISE, release 2.6.

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 live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Operationele gegevens zijn de ISE DB met de contextuele informatie en sessieinformatie van alle endpoints en gebruikers die als zodanig zijn geauthentiseerd, audits van back-ups in proces, registratie van een knooppunt en soortgelijke transacties tussen knooppunten, admin logins, TACACS en portal logins, zuiveringsoperaties, enz. Deze informatie wordt uitsluitend op zowel de MNTs opgeslagen en op bestelling opgehaald in de vorm van rapporten op het Primaire Admin-knooppunt. De rapporten zijn geclassificeerd en georganiseerd voor een gemakkelijke diagnose.

Opmerking: Het wordt aanbevolen de Primaire Admin en Primaire MNT-persoonlijkheden op verschillende knooppunten te huisvesten, om een overbelasting van **admin-http-pool** en **cpm-mnt** draden op hetzelfde knooppunt te voorkomen.

Deployment Nodes

Hostname	Personas	Role(s)	Services	Node Status
[Yellow Box]	Administration, Monitoring	SEC(A), PR2(M)	NONE	✓
[Yellow Box]	Administration, Monitoring	PR2(A), SEC(M)	NONE	✓
[Yellow Box]	Policy Service		SESSION_PROFILER, DEVICE ADMIN	✓

Navigatie tussen rapporten

Onder **Operations**, navigeer naar **Rapporten > ISE Rapporten**, heeft het linker deelvenster een lijst van de rapportcategorieën, die elk verder vertakt zijn in subcategorieën, zoals getoond in deze afbeelding.

Export Summary

Reports exported in last 7 days

Report Exported	Exported By	Scheduled	Triggered On	Repository	Filter Parameter(s)	Status	Action
AAA Diagnostics	adminINTERNAL	No	The May 07 09:22:54 IST 2020	SOTURN	Logged if EQUALS today	Quarant	Cancel
RADIUS Authentications	adminINTERNAL	No	The May 07 09:22:02 IST 2020	SOTURN	Logged if CONTAINS last5days	Quarant	Cancel

Last Updated: The May 07 2020 03:21:46 GMT+0530 (note Standard Time)

Elk rapport heeft een info-pictogram **i**, zoals in deze afbeelding te zien is, dat de vereiste beschrijving en registratiecategorieën bevat.

Data Purging Audit

The Data Purging Audit report records when the logging data is purged.

This report reflects two sources of data purging.

At 4AM daily, Cisco ISE checks whether there are any logging files that meet the criteria you have set on the Administration > Maintenance > Data Purging page. If so, the files are deleted and recorded in this report.

Additionally, Cisco ISE continually maintains a maximum of 50 percentage used storage space for the log files. Every hour, Cisco ISE verifies this percentage and deletes the oldest data until it reaches the 50 percentage threshold again. This information is also recorded in this report.

De meeste rapporten draaien automatisch voor het standaardfilter **vandaag** wanneer benaderd.

Bepaalde rapporten zoals het overzicht van de gezondheid vereisen serverselectie, klik op **Ga** om te lopen, en bekijk het rapport.

Health Summary

Filters

- Server: [Dropdown]
- Time Range: [Dropdown]

Go

Filters

Met ISE kunt u de weergave van elk rapport aanpassen. De twee filters die beschikbaar zijn in ISE Rapporten zijn:

- Snel filter
- Geavanceerd filter

Snel filter

Het snelfilter is beschikbaar voor alle enkelvoudige rapporten. Voer de zoektekst in de velden onder elke kolom in en het snelle filter gebruikt omstandigheden zoals bevat, start met, eindigt met, start met of eindigt met, en meerdere waarden met OR-operator om de vereiste logbestanden te krijgen. Elke combinatie van strings en sterretje is toegestaan in deze velden. Verder is het met de optie Instellingen op de rechterhoek mogelijk dat de beheerder specifieke kolommen selecteert die in de rapporten moeten worden weergegeven.

Logged At	RADIUS Status	Details	Identity	Endpoint ID	Endpoint Profile	Authorization Rule	Server
Last 7 Days			84-96-91-26-EB-47	Endpoint ID	Endpoint Profile	Authorization Rule	Server
2020-05-04 22:21:16.725	✓		84-96-91-26-EB-47	84-96-91-26-EB-47	Unknown	Basic_Authenticated_Access	sikamu26
2020-05-04 20:36:09.966	✓		84-96-91-26-EB-47	84-96-91-26-EB-47	Unknown	Basic_Authenticated_Access	sikamu26
2020-05-04 20:34:31.431	✗		84-96-91-26-EB-47	84-96-91-26-EB-47	Unknown	Default	sikamu26

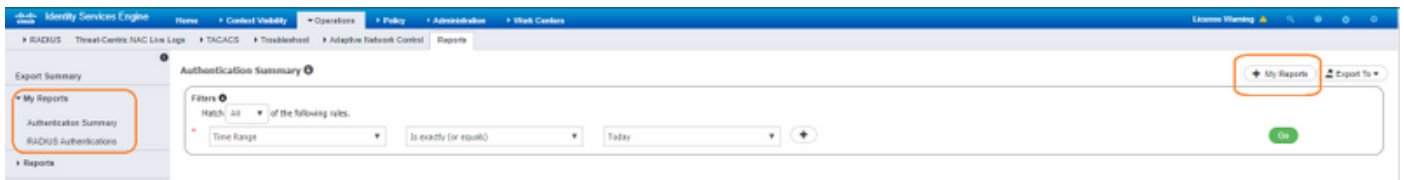
Geavanceerd filter

Zoals de naam al aangeeft, kan met Advanced Filter de beheerder logische en aangepaste filters maken en de sjablonen opslaan. Kies in de vervolgkeuzelijst **Match** of All (EN doe-mee aan alle criteria) of Any (of gebruik-match om een van de criteria). Klik op **filter** om het rapport te starten en de resultaten te bekijken, zoals in deze afbeelding.

Logged At	RADIUS Status	Details	Identity	Endpoint ID	Endpoint Profile	Authorization Rule	Server	Network Device
Match: All			of the following rules.	This week's Successful authentications	Save			
➤ RADIUS Status			Contains	Pass				
➤ Logged At			Within	Last 7 Days				
2020-05-04 22:21:16.725	✓		84-96-91-26-EB-47	84-96-91-26-EB-47	Unknown	Basic_Authenticated_Access	sikamu26	LabSwitch
2020-05-04 20:36:09.966	✓		84-96-91-26-EB-47	84-96-91-26-EB-47	Unknown	Basic_Authenticated_Access	sikamu26	LabSwitch
2020-05-04 20:28:14.369	✓		faulstul		Unknown	Basic_Authenticated_Access	sikamu26	LabSwitch

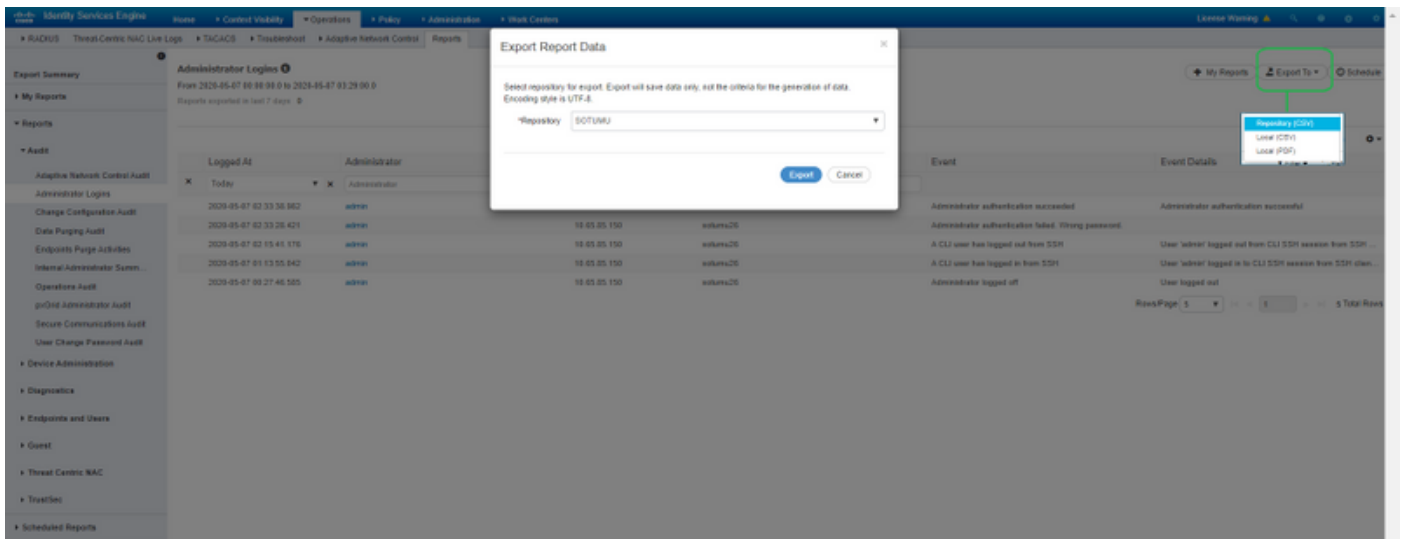
Opslaan naar mijn rapporten

In dit gedeelte van het tabblad **Rapporten** kunt u de beheerder toestaan de veelbezochte rapporten op te slaan zodat deze makkelijk te bereiken zijn. Het vermindert elke keer de zoektocht naar de categorieën en deze verslagen kunnen worden geraadpleegd via **mijn verslagen**. Naast de standaardweergave kunt u hetzelfde rapport op verschillende manieren aanpassen en elke iteratie aan deze sectie toevoegen voor een eenvoudige toegang.



Uitvoer van rapporten

De exportoptie wordt naar drie keuzes uitgebreid, zoals in deze afbeelding.



Er kunnen maximaal 5000 records worden geëxporteerd naar **.csv** Excel-bestand (kan lokaal worden opgeslagen of geëxporteerd naar een vooraf ingestelde opslagplaats) en maximaal 1000 records naar een PDF-bestand. Deze rapporten kunnen alleen worden geëxporteerd als PDF-bestanden:

- Verificatieoverzicht
- Gezondheidssamenvatting
- Rollend-Based Access Control List (RBACL) Drop Summary (alleen beschikbaar met Cisco Catalyst 6500 Series-switches)
- Samenvatting van Guest Sponsor
- Profielwijzigingen van endpoints
- Sessiestatus voor netwerkapparaat

Opmerking: Zorg ervoor dat UTF-8-codering is ingeschakeld op Microsoft Excel om tekens die geen Engels zijn, in de geëxporteerde **.csv**-bestanden te bekijken.

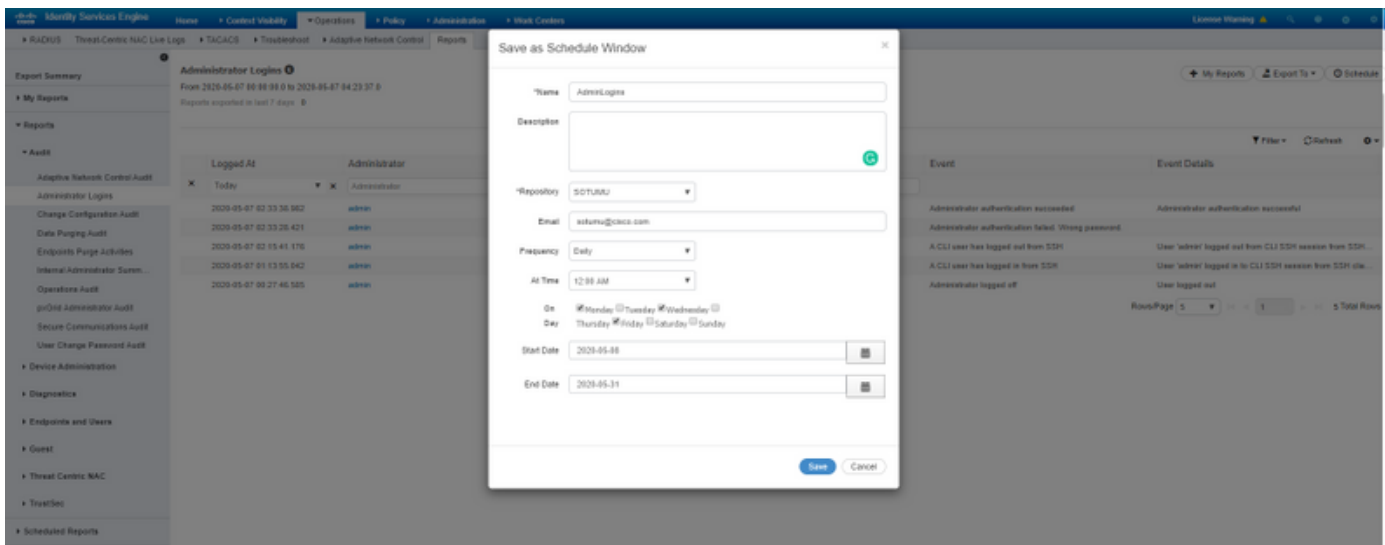
Exportoverzicht:

Report Exported	Exported By	Scheduled	Triggered On	Repository	Filter Parameter(s)	Status	Action
AAA Diagnostics	admin@TERMINAL	No	The May 07 09:22:50 IST 2020	SOTUMU	Logged At EQUALS today	Completed	
RADIUS Authentications	admin@TERMINAL	No	The May 07 09:22:02 IST 2020	SOTUMU	Logged At CONTAINS last5days	Completed	

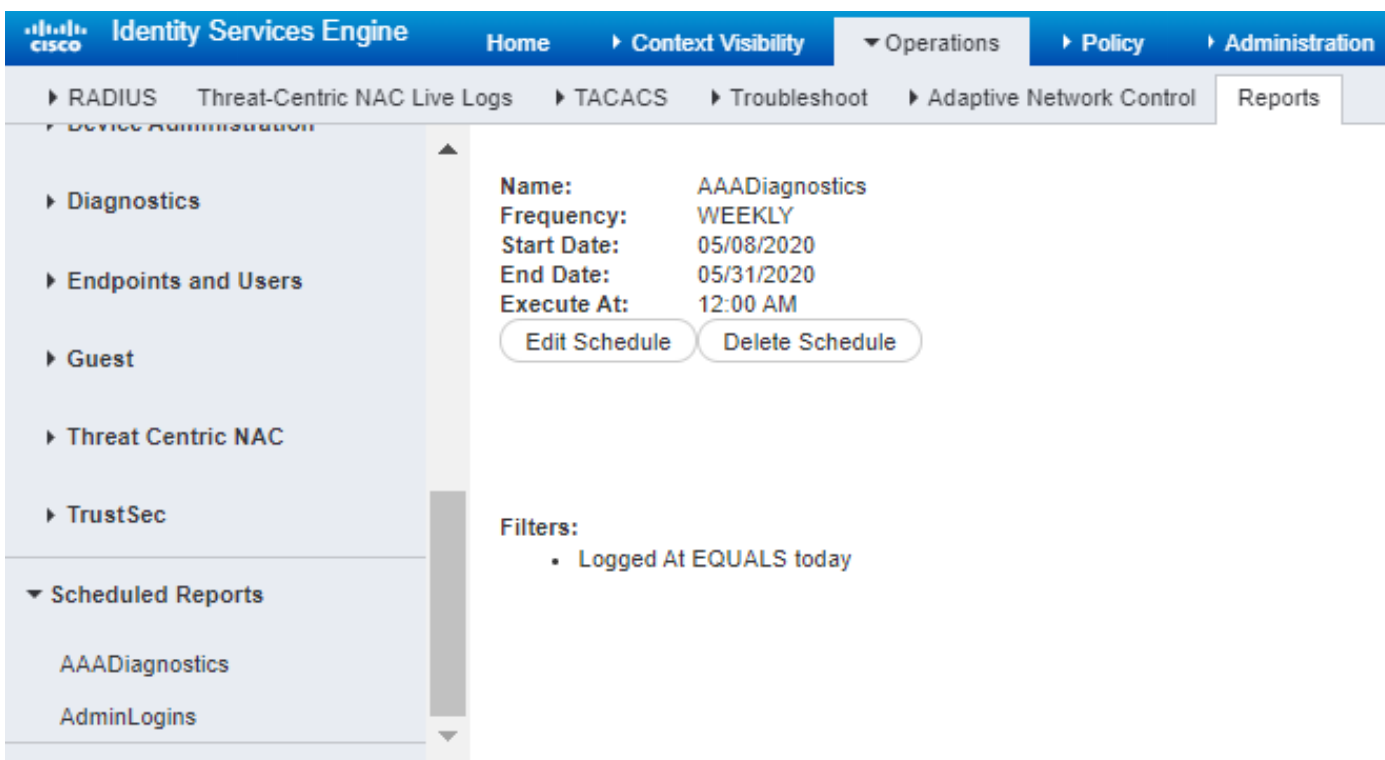
Last Updated: The May 07 2020 03:20:23 GMT+0530 (India Standard Time)

Geplande rapporten

Met ISE-rapporten kunt u de rapporten aanpassen, opslaan, uitvoeren met tussenpozen van een tijdstip en exporteren naar een externe opslagplaats. E-mail-ID's kunnen worden toegevoegd voor kennisgevingen van succesvol uitgevoerde geplande rapporten als de ISE is geïntegreerd met een MTP-server (navigeer naar **Administratie > Systeem > Instellingen**).



Geplande rapporten kunnen later worden geraadpleegd om de instellingen te bewerken, zoals in deze afbeelding wordt weergegeven.



Raadpleeg de [Admin Guide](#) voor meer informatie over het bewaken en oplossen van problemen.