

# Funktionen und Anwendungsfälle unter ISE-Berichten

## Inhalt

[Einführung](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Navigation zwischen Berichten](#)

[Filter](#)

[Schnellfilter](#)

[Erweiterter Filter](#)

[Speichern unter "Meine Berichte"](#)

[Berichtsexporte](#)

[Geplante Berichte](#)

## Einführung

Dieses Dokument beschreibt die verschiedenen Funktionen und Anwendungsfälle im Abschnitt "Berichte" der Cisco Identity Services Engine (ISE). Diese Berichte dienen zur Überwachung und Fehlerbehebung der verschiedenen Funktionen der ISE und zur Analyse der Trends bei den Netzwerkaktivitäten von einem zentralen Administrationsknoten aus.

## Anforderungen

Cisco empfiehlt, dass Sie über die ISE verfügen.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ISE, Version 2.6.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Die Betriebsdaten sind die ISE DB mit den Kontextinformationen und Sitzungsinformationen aller authentifizierten Endpunkte und Benutzer, Audits von Backups im Prozess, Registrierung eines Knotens und ähnlicher Internode-Transaktionen, Admin-Anmeldungen, TACACS und Portal-Anmeldungen, Löschvorgänge usw. Diese Informationen werden ausschließlich auf den MNTs gespeichert und bei Bedarf in Form von Berichten auf den primären Admin-Knoten abgerufen. Die Berichte werden klassifiziert und organisiert, um eine einfache Diagnose zu ermöglichen.

**Hinweis:** Es wird empfohlen, die primären Admin- und primären MNT-Personas auf verschiedenen Knoten zu hosten, um eine Überlastung von admin-http-pool- und cpm-mnt-Threads auf demselben Knoten zu vermeiden.

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 | ✓           |

## Navigation zwischen Berichten

Navigieren Sie unter **Operations (Betrieb)** zu **Reports > ISE Reports (ISE-Berichte)**, im linken Bereich wird eine Liste der Berichtskategorien angezeigt, von denen jede weiter in Unterkategorien unterteilt ist, wie in diesem Bild gezeigt.

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        | Thu May 07 09:22:54 IST 2020 | SOTURN     | Logged At EQUALS today       | Queued | Cancel |
| RADIUS Subscribers | adminINTERNAL | No        | Thu May 07 09:22:52 IST 2020 | SOTURN     | Logged At CONTAINS last5days | Queued | Cancel |

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

Jeder Bericht verfügt über ein Informationssymbol **i**, wie in diesem Bild gezeigt, das die erforderlichen Beschreibungen und Protokollierungskategorien enthält.

**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.

Die meisten Berichte werden **heute** beim Zugriff automatisch für den Standardfilter ausgeführt.

Bestimmte Berichte wie die Statusübersicht erfordern eine Serverauswahl, klicken Sie auf **Go**, um auszuführen, und zeigen Sie den Bericht an.

Health Summary

Filters

- Server: server20
- Time Range: [Dropdown]

Go

## Filter

Mit der ISE können Sie die Ansicht jedes Berichts anpassen. Die beiden in ISE Reports verfügbaren Filter sind:

- Schnellfilter
- Erweiterter Filter

## Schnellfilter

Quick Filter ist für alle Berichte in einem Bereich verfügbar. Geben Sie den Suchtext in die Felder unter jeder Spalte ein. Der Schnellfilter verwendet Bedingungen wie "enthält", "beginnt", "endet mit", "beginnt" oder "endet mit" und mehrere Werte mit "OR-Operator", um die erforderlichen Protokolle abzurufen. Jede Kombination von Zeichenfolgen und Sternchen ist in diesen Feldern zulässig. Darüber hinaus ermöglicht die Option Einstellungen in der rechten Ecke dem Administrator, bestimmte Spalten auszuwählen, die in den Berichten angezeigt werden sollen.

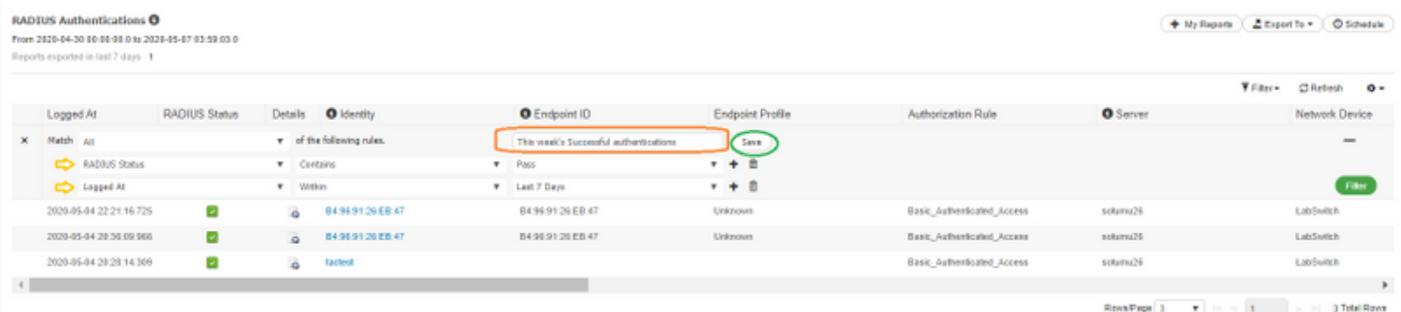


The screenshot shows the 'RADIUS Authentications' report in the ISE interface. The report is filtered for the last 7 days. A Quick Filter is applied to the 'Identity' column, showing the value '04-96-91-26-EB-47'. The table has columns for Logged At, RADIUS Status, Details, Identity, Endpoint ID, Endpoint Profile, Authorization Rule, and Server. A column order menu is open on the right, showing the current column order: Selected All, Logged At, RADIUS Status, Details, Identity, and Endpoint ID.

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

## Erweiterter Filter

Wie der Name schon sagt, ermöglicht Advanced Filter dem Administrator, logische und benutzerdefinierte Filter zu erstellen und die Vorlagen zu speichern. Wählen Sie im Dropdown-Menü **Match**-Regel entweder All (AND operation-match all criteria) oder Any (OR operation-match any one criteria) aus. Klicken Sie auf **Filter**, um den Bericht auszuführen und die Ergebnisse anzuzeigen, wie in diesem Bild gezeigt.



The screenshot shows the 'RADIUS Authentications' report with an Advanced Filter applied. The filter is set to 'Match: All' and 'of the following rules'. The rules are: 'RADIUS Status' contains 'Pass', 'Logged At' is within 'Last 7 Days', and 'Identity' is 'This week's Successful authentications'. The 'Filter' button is highlighted in green. The table shows the results of the filter, including columns for Logged At, RADIUS Status, Details, Identity, Endpoint ID, Endpoint Profile, Authorization Rule, Server, and Network Device.

| Logged At                          | RADIUS Status | Details | Identity          | Endpoint ID       | Endpoint Profile | Authorization Rule         | Server   | Network Device |
|------------------------------------|---------------|---------|-------------------|-------------------|------------------|----------------------------|----------|----------------|
| Match: All of the following rules. |               |         |                   |                   |                  |                            |          |                |
| RADIUS Status                      |               |         | Contains          | Pass              |                  |                            |          |                |
| Logged At                          |               |         | Within            | Last 7 Days       |                  |                            |          |                |
| 2020-05-04 22:21:16.725            | ✓             |         | 04-96-91-26-EB-47 | 04-96-91-26-EB-47 | Unknown          | Basic_Authenticated_Access | sikamu26 | LabSwitch      |
| 2020-05-04 20:36:09.966            | ✓             |         | 04-96-91-26-EB-47 | 04-96-91-26-EB-47 | Unknown          | Basic_Authenticated_Access | sikamu26 | LabSwitch      |
| 2020-05-04 20:28:14.309            | ✓             |         | factool           |                   |                  | Basic_Authenticated_Access | sikamu26 | LabSwitch      |

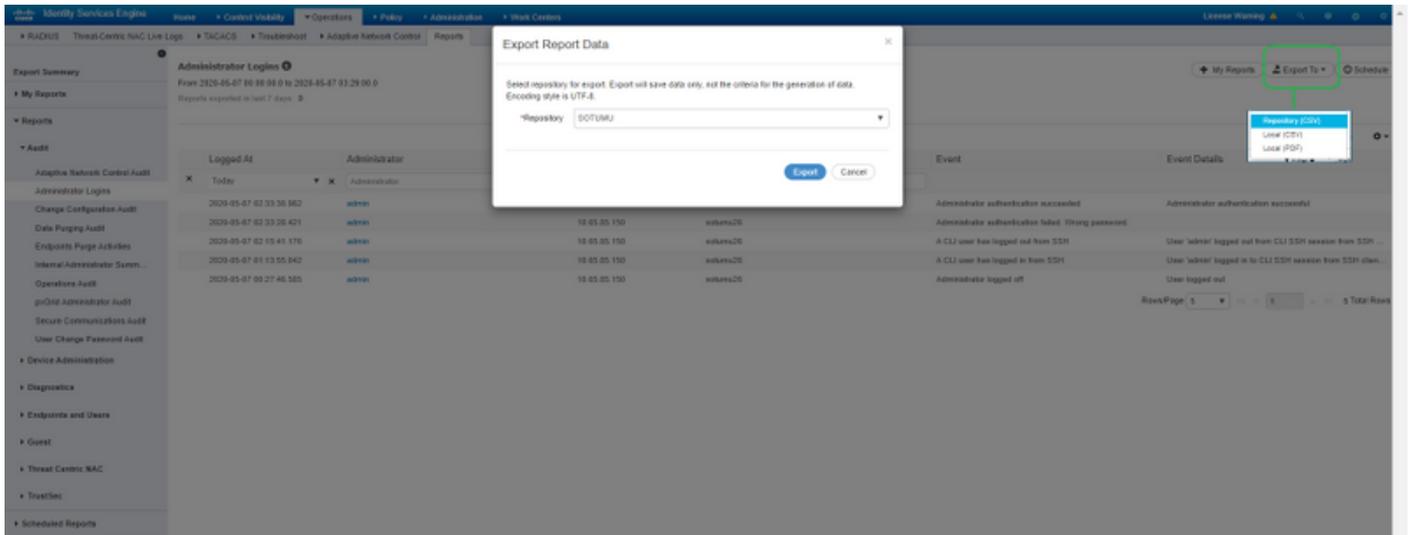
## Speichern unter "Meine Berichte"

In diesem Abschnitt auf der Registerkarte **Berichte** kann der Administrator die häufig besuchten Berichte speichern, um einen einfachen Zugriff zu ermöglichen. Die Suche nach den einzelnen Kategorien wird vereinfacht, und auf diese Berichte kann über **Meine Berichte** zugegriffen werden. Zusätzlich zur Standardansicht kann derselbe Bericht auf verschiedene Weise angepasst und jeder Iteration zu diesem Abschnitt hinzugefügt werden, um einen einfachen Zugriff zu ermöglichen.



## Berichtsexporte

Die Exportoption wird auf drei Optionen erweitert, wie in diesem Bild gezeigt.

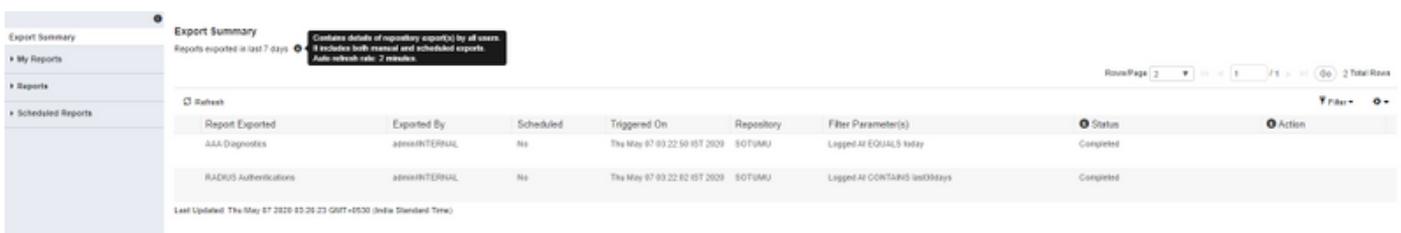


Es können maximal 5.000 Datensätze in .csv Excel-Datei (lokal gespeichert oder in ein vorkonfiguriertes Repository exportiert) und bis zu 1.000 Datensätze in eine PDF-Datei exportiert werden. Diese Berichte können nur als PDF-Dateien exportiert werden:

- Authentifizierungszusammenfassung
- Statuszusammenfassung
- Rollenbasierte Zugriffskontrollliste (RBACL) - Dropdown-Zusammenfassung (nur bei Cisco Catalyst Switches der Serie 6500 verfügbar)
- Zusammenfassung für Gastsponsor
- Änderungen am Endgeräteprofil
- Sitzungsstatus für Netzwerkgeräte

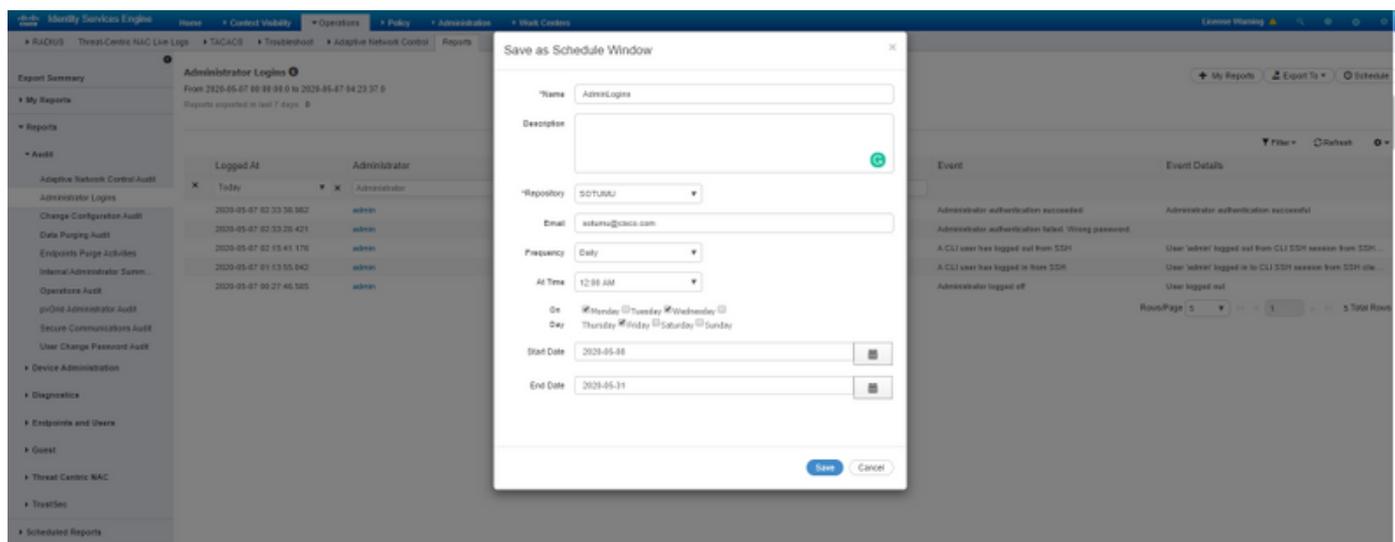
**Hinweis:** Stellen Sie sicher, dass die UTF-8-Codierung in Microsoft Excel aktiviert ist, um nicht englische Zeichen in den exportierten .csv-Dateien anzuzeigen.

Zusammenfassung exportieren:

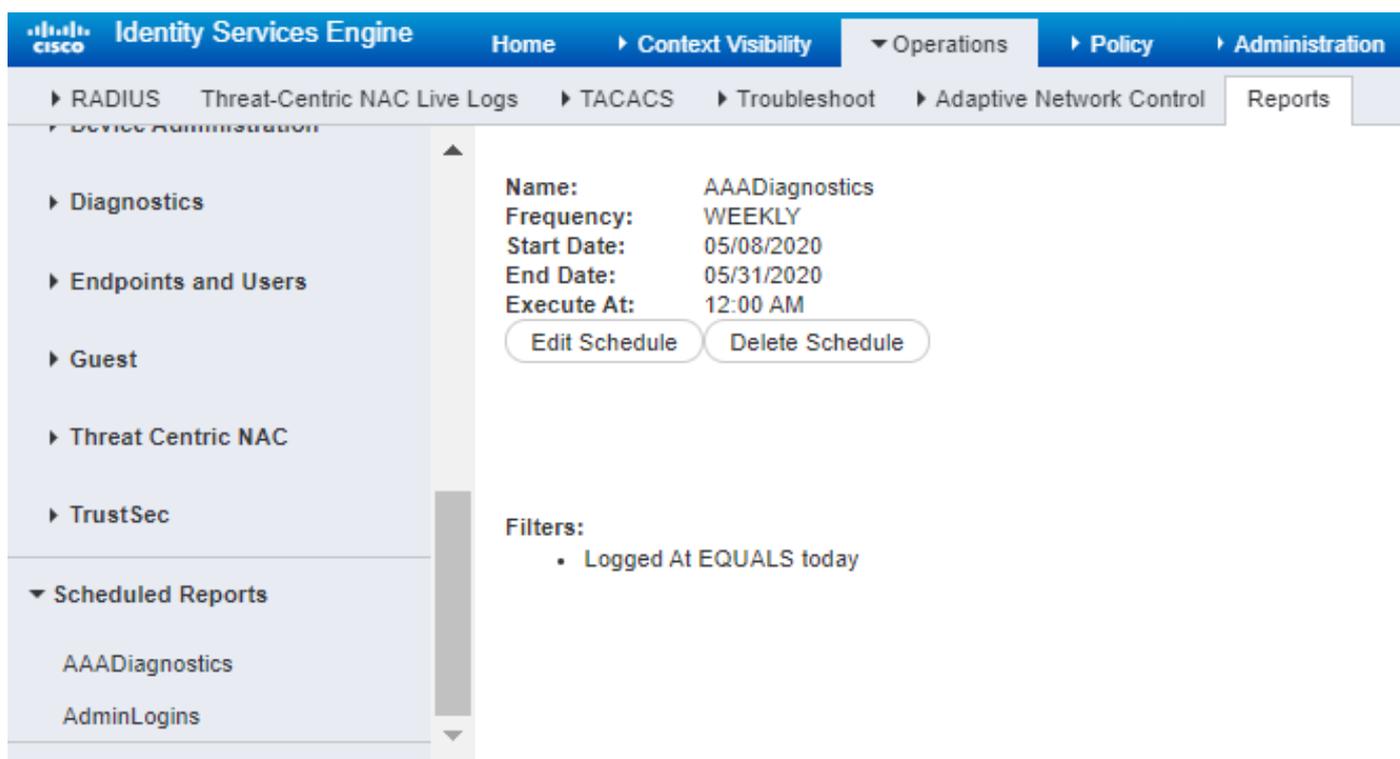


## Geplante Berichte

ISE-Berichte ermöglichen Ihnen die Anpassung, Speicherung, Ausführung der Berichte in festgelegten Intervallen und den Export in ein Remote-Repository. Für Benachrichtigungen über erfolgreich exportierte geplante Berichte können E-Mail-IDs hinzugefügt werden, wenn die ISE in einen SMTP-Server integriert ist (navigieren Sie zu **Administration > System > Settings**).



Auf geplante Berichte können Sie später zugreifen, um die Einstellungen zu bearbeiten, wie in diesem Bild gezeigt.



Weitere Informationen zur Überwachung und Fehlerbehebung der ISE finden Sie [im Administratorhandbuch](#).