title: Plan reports & monitoring deployment - Azure AD description: Describes how to plan and execute implementation of reporting and monitoring. services: active-directory author: BarbaraSelden manager: daveba ms.service: active-directory ms.topic: conceptual ms.workload: identity ms.subservice: report-monitor ms.date: 11/13/2018 ms.author: baselden ms.reviewer: plenzke

# Customer intent: As an Azure AD administrator, I want to monitor logs and report on access to increase security

## ms.collection: M365-identity-device-management

# Plan an Azure Active Directory reporting and monitoring deployment

Your Azure Active Directory (Azure AD) reporting and monitoring solution depends on your legal, security, and operational requirements and your existing environment and processes. This article presents the various design options and guides you to the right deployment strategy.

### Benefits of Azure AD reporting and monitoring

Azure AD reporting provides a comprehensive view and logs of Azure AD activity in your environment, including sign in events, audit events, and changes to your directory.

The provided data enables you to:

* determine how your apps and services are used.
* detect potential risks affecting the health of your environment.
* troubleshoot issues preventing your users from getting their work done.
* gain insights by seeing audit events of changes to your Azure AD directory.

[!IMPORTANT] Azure AD monitoring enables you to route your logs generated by Azure AD reporting to different target systems. You can then either retain it for long-term use or integrate it with third-party Security Information and Event Management (SIEM) tools to gain insights into your environment.

With Azure AD monitoring, you can route logs to:

* an Azure storage account for archival purposes.
* Azure Monitor logs, formerly known as Azure Log Analytics workspace, where you can analyze the data, create dashboards, and alert on specific events.
* an Azure event hub where you can integrate with your existing SIEM tools such as Splunk, Sumologic, or QRadar.

[!NOTE] We recently started using the term Azure Monitor logs instead of Log Analytics. Log data is still stored in a Log Analytics workspace and is still collected and analyzed by the same Log Analytics service. We are updating the terminology to better reflect the role of [logs in Azure Monitor](../../azure-monitor/platform/data-platform.md). See [Azure Monitor terminology changes](../../azure-monitor/terminology.md) for details.

[Learn more about report retention policies](./reference-reports-data-retention.md).

### Licensing and prerequisites for Azure AD reporting and monitoring

You’ll need an Azure AD premium license to access the Azure AD sign in logs.

For detailed feature and licensing information in the [Azure Active Directory pricing guide](https://azure.microsoft.com/pricing/details/active-directory/).

To deploy Azure AD monitoring and reporting you’ll need a user who is a global administrator or security administrator for the Azure AD tenant.

Depending on the final destination of your log data, you’ll need one of the following:

* An Azure storage account that you have ListKeys permissions for. We recommend that you use a general storage account and not a Blob storage account. For storage pricing information, see the [Azure Storage pricing calculator](https://azure.microsoft.com/pricing/calculator/?service=storage).
* An Azure Event Hubs namespace to integrate with third-party SIEM solutions.
* An Azure Log Analytics workspace to send logs to Azure Monitor logs.

## Plan an Azure reporting and monitoring deployment project

In this project, you’ll define the audiences that will consume and monitor reports, and define your Azure AD monitoring architecture.

### Engage the right stakeholders

When technology projects fail, they typically do so due to mismatched expectations on impact, outcomes, and responsibilities. To avoid these pitfalls, [ensure that you’re engaging the right stakeholders](https://aka.ms/deploymentplans). Also ensure that stakeholder roles in the project are well understood by documenting the stakeholders and their project input and accountabilities.

### Plan communications

Communication is critical to the success of any new service. Proactively communicate with your users how their experience will change, when it will change, and how to gain support if they experience issues.

### Document your current infrastructure and policies

Your current infrastructure and policies will drive your reporting and monitoring design. Ensure that you know

* What, if any, SIEM tools you’re using.
* Your Azure infrastructure, including existing storage accounts and monitoring being used.
* Your organizational retention policies for logs, including any applicable compliance frameworks required.

## Plan an Azure AD reporting and monitoring deployment

Reporting and monitoring are used to meet your business requirements, gain insights into usage patterns, and increase your organization’s security posture.

### Business use cases

* Required for solution to meet business needs
* Nice to have to meet business needs
* Not applicable

|  |  |
| --- | --- |
| Area | Description |
| Retention | **Log retention of more than 30 days**. ‎Due to legal or business requirements it is required to store audit logs and sign in logs of Azure AD longer than 30 days. |
| Analytics | **The logs need to be searchable**. ‎The stored logs need to be searchable with analytic tools. |
| Operational Insights | **Insights for various teams**. The need to give access for different users to gain operational insights such as application usage, sign in errors, self-service usage, trends, etc. |
| Security Insights | **Insights for various teams**. The need to give access for different users to gain operational insights such as application usage, sign in errors, self service usage, trends, etc. |
| Integration in SIEM systems | **SIEM integration**. ‎The need to integrate and stream Azure AD sign in logs and audit logs to existing SIEM systems. |

### Choose a monitoring solution architecture

With Azure AD monitoring, you can route your Azure AD activity logs to a system that best meets your business needs. You can then retain them for long-term reporting and analysis to gain insights into your environment, and integrate it with SIEM tools.

#### Decision flow chartAn image showing what is described in subsequent sections

#### Archive logs in a storage account

By routing logs to an Azure storage account, you can keep them for longer than the default retention period outlined in our [retention policies](./reference-reports-data-retention.md). Use this method if you need to archive your logs, but don’t need to integrate them with an SIEM system, and don’t need ongoing queries and analysis. You can still do on-demand searches.

Learn how to [route data to your storage account](./quickstart-azure-monitor-route-logs-to-storage-account.md).

#### Send logs to Azure Monitor logs

[Azure Monitor logs](../../azure-monitor/log-query/log-query-overview.md) consolidate monitoring data from different sources. It also provides a query language and analytics engine that gives you insights into the operation of your applications and use of resources. By sending Azure AD activity logs to Azure Monitor logs, you can quickly retrieve, monitor, and alert on collected data. Use this method when you don’t have an existing SIEM solution that you want to send your data to directly but do want queries and analysis. Once your data is in Azure Monitor logs, you can then send it to event hub and from there to a SIEM if you want to.

Learn how to [send data to Azure Monitor logs](./howto-integrate-activity-logs-with-log-analytics.md).

You can also install the pre-built views for Azure AD activity logs to monitor common scenarios involving sign in and audit events.

Learn how to [install and use log analytics views for Azure AD activity logs](./howto-install-use-log-analytics-views.md).

#### Stream logs to your Azure event hub

Routing logs to an Azure event hub enables integration with third-party SIEM tools. This integration allows you to combine Azure AD activity log data with other data managed by your SIEM, to provide richer insights into your environment.

Learn how to [stream logs to an event hub](/azure/active-directory/reports-monitoring/tutorial-azure-monitor-stream-logs-to-event-hub).

## Plan Operations and Security for Azure AD reporting and monitoring

Stakeholders need to access Azure AD logs to gain operational insights. Likely users include security team members, internal or external auditors, and the identity and access management operations team.

Azure AD roles enable you to delegate the ability to configure and view Azure AD Reports based on your role. Identify who in your organization needs permission to read Azure AD reports and what role would be appropriate for them.

The following roles can read Azure AD reports:

* Global Admin
* Security Admin
* Security Reader
* Report Reader

Learn More About [Azure AD Administrative Roles](../users-groups-roles/directory-assign-admin-roles.md).

*Always apply the concept of least privileges to reduce the risk of an account compromise*. Consider implementing [Privileged Identity Management](../privileged-identity-management/pim-configure.md) to further secure your organization.

## Deploy Azure AD reporting and monitoring

Depending on the decisions you have made earlier using the design guidance above, this section will guide you to the documentation on the different deployment options.

### Consume and archive Azure AD logs

[Find activity reports in the Azure portal](./howto-find-activity-reports.md)

[Archive Azure AD logs to an Azure Storage account](./quickstart-azure-monitor-route-logs-to-storage-account.md)

### Implement monitoring and analytics

[Send logs to Azure Monitor](./howto-integrate-activity-logs-with-log-analytics.md)

[Install and use the log analytics views for Azure Active Directory](./howto-install-use-log-analytics-views.md)

[Analyze Azure AD activity logs with Azure Monitor logs](./howto-analyze-activity-logs-log-analytics.md)

* [Interpret audit logs schema in Azure Monitor](./reference-azure-monitor-audit-log-schema.md)
* [Interpret sign in logs schema in Azure Monitor](./reference-azure-monitor-sign-ins-log-schema.md)
* [Stream Azure AD logs to an Azure event hub](./tutorial-azure-monitor-stream-logs-to-event-hub.md)
* [Integrate Azure AD logs with Splunk by using Azure Monitor](./howto-integrate-activity-logs-with-splunk.md)
* [Integrate Azure AD logs with SumoLogic by using Azure Monitor](./howto-integrate-activity-logs-with-sumologic.md)

## Next steps

Consider implementing [Privileged Identity Management](../privileged-identity-management/pim-configure.md)

Consider implementing [Azure role-based access control (Azure RBAC)](../../role-based-access-control/overview.md)