



Integrating AWS S3 with File Access Manager

Version: 8.2 Revised: July 01, 2021

Copyright and Trademark Notices.

Copyright © 2021 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

“SailPoint,” “SailPoint & Design,” “SailPoint Technologies & Design,” “Identity Cube,” “Identity IQ,” “IdentityAI,” “IdentityNow,” “SailPoint Predictive Identity” and “SecurityIQ” are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. <https://www.sailpoint.com/patents>

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce's Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Contents

Contents	iii
Capabilities	5
Connector Overview	6
Crawler	6
Permission Collector	6
Identity Collection	6
Cross Account Access	8
Cross Account by Assume Roles	8
Block Public Access	9
Prerequisites for AWS	11
Software Requirements	11
Configuring an EC2 for File Access Manager Connector	11
Creating a Dedicated IAM User	18
Connector Installation Flow Overview	25
Collecting Data Stored in an External Application	26
Adding an AWS S3 Application	27
Select Wizard Type	27
General Details	27
Connection Details	27
Configuring and Scheduling the Permissions Collection	28
Scheduling a Task	29
Configuring and Scheduling the Crawler	30
Setting the Crawl Scope	31
Including and Excluding Paths by List	31
Excluding Paths by Regex for AWS S3 Buckets	31
The AWS Path Structure in File Access Manager	31
Setting Filters of Paths to Exclude in the Crawl Process for an Application Using Regex	32
Crawler Regex Exclusion Examples	32

Exclude all Folders Which Start With One or More Folder Names	32
Include ONLY Folders Which Start With One or More Folder Names	32
Excluding Top Level Resources	33
Special Consideration for Long File Paths in Crawl	34
Installing Services: Collector Installation	36
Verifying the AWS S3 Connector Installation	38
Installed Services	38
Log Files	38
Permissions Collection	38
Appendix A: Json Scripts	39
IdentityIQ_FileAccessManagerRole.json [EC2]	39
IdentityIQ_FileAccessManagerRole.json [Dedicated User]	39
IdentityIQ_FileAccessManager_AssumeRolePolicy.json	40
IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy.json	40

Capabilities

This connector enables you to use IdentityIQ File Access Manager to access and analyze data stored in AWS S3 and do the following:

- Analyze the structure of your stored data.
- Verify user permissions on the resources, and compare them against requirements.
- Identity collector – collect IAM users, groups and roles and the connections between them

See the IdentityIQ File Access Manager documentation for a full description.

Connector Overview

Accounts must be configured as described in [Prerequisites for AWS](#) , for them to be analyzed.

Crawler

The crawler analyzes the structure of the organization and builds the hierarchy tree

- Organization Root container
- Organization Units (OUs)
- AWS Accounts
- S3 Buckets
- S3 Folders

Analyze all Objects in S3 Buckets

If Analyze all Objects is checked, the crawler will get also the S3 Objects (files) under the buckets, their size and total size of the containing folder.

Permission Collector

The Permission collection will retrieve and analyze the following permissions:

- ACLs of buckets. If **Analyze ACLs** is checked, ACLs will be collected for the objects retrieved in the crawl.
- Bucket policies for the buckets and their objects.
- IAM policies which are relevant for the S3 buckets and Objects.
- Account and bucket level PublicAccessBlock configurations.
- Cross account permissions

Permission collection limitations and unsupported features:

- Permissions are analyzed for buckets and objects, not for folders since they are not an actual object in S3
- Permissions Boundary
- Policies Conditions
- Policies Variables
- Policies elements - NotPrincipal, NotAction, NotResource
- Only S3 related permissions are analyzed
- Access points and Jobs permissions are not analyzed

Identity Collection

The AWS identities will be collected by the permission collector at the beginning of the task.

- The following identities are collected:
 - AWS Accounts (root users)
 - IAM Users
 - IAM Groups
 - IAM Roles
- The AWS predefined groups are represented as the following groups:
 - <http://acs.amazonaws.com/groups/global/AllUsers>***
 - “Anonymous” with type “Everyone or Authenticated Users, or contains it”
 - <http://acs.amazonaws.com/groups/global/AuthenticatedUsers>***
 - “AwsAuthenticatedUsers” with type “Everyone or Authenticated Users, or contains it”
 - <http://acs.amazonaws.com/groups/s3/LogDelivery>***
 - “S3LogDelivery” with type “Local Group”.
- From each IAM Role, File Access Manager collects its trusted entities as members of the role.
- The AWS entities will be mapped to the following types:
 - IAM Users – will be saved as FAM “Local User” type.
 - IAM Groups – will be saved as FAM “Local Group” type.
 - IAM Roles – will be saved as FAM “Local Role” type.
 - AWS Account – will be saved as FAM “AWS Account” type.
 - AWS Service – will be saved as FAM “AWS Service” type.
 - All other types, including “Federated”, etc. , – will be saved as FAM “AWS External Account” type.
- IAM Role trusted Identity of type “*” is represented as “**Anonymous**” with type “Everyone, Authenticated Users, or contains it”.
- “Principal”: “*” in bucket policy is represented as “Anonymous” with type “Everyone, Authenticated Users, or contains it”.
- For each Collected identity, the primary ID will be their Arn and Alternative Ids will be collected as well:
 - For AWS Accounts – Id, root user Arn (“arn:aws:iam::{iamRootUser.Id}:root”) and canonical Id.
 - For other identities – Id.
- Additional information that is collected:
 - Name
 - Display Name
 - Description

- Domain – will be the AccountName(#AccountId)
- Email (Only for Aws Account)
- LastLogin (Only for IAM Users)

Cross Account Access

To achieve cross account access, and allow an AWS IAM Identity from Account A to access AWS resources in account B (S3 resource in our case) two conditions must be met:

1. The IAM Identity owner account A should give permission X on the S3 resource in account B.

In File Access Manager this permission will appear as **X-ByTrustedCrossAccount**

2. The S3 resource owner account B should give permission X on the resource to the IAM Identity from account A.

In File Access Manager this permission will appear as **X-ByTrustingCrossAccount**.

Permission X will be effective only if both permissions are granted to the user / group on the resource. Otherwise, the user / group will not be allowed to perform X on this resource.

Permissions Forensics 🔍 Saved Queries Global Options Apply ⚙️

Filters (2) Save Clear All

User Name	Equals	testAccessToAnotherResource	🔍 🗑️
Permission Type	Contains	GetBucketLocation	🔍 🗑️

View by: Groups & Users Direct Permissions Mark permissions unused for longer than 6 months 🔍

<input type="checkbox"/>	Business Resource Full Path	Application	User Name	User Domain	User Entity Type	Permission Type	ACL Type Allow?
<input type="checkbox"/>	Root/FAM-QA2(#98979385348)/s3-us-east-1.bucket1-fam-qa2-user1adminpriv	s3-1	FAMAdminUser1	FAM-QA1(#961222436048)	User	GetBucketLocation-ByTrustingCrossAccount	Allow
<input type="checkbox"/>	Root/FAM-QA2(#98979385348)/s3-us-east-1.bucket1-fam-qa2-user1adminpriv	s3-1	FAMAdminUser1	FAM-QA1(#961222436048)	User	GetBucketLocation-ByTrustedCrossAccount	Allow

In the example above, the user “FAMAdminUser1” from account “FA-QA1” has both “GetBucketLocation-ByTrustingCrossAccount” and “GetBucketLocation-ByTrustedCrossAccount” permission on bucket “bucket1-fam-qa2-user-1adminpriv” from account “FAM-QA2”.

Cross Account by Assume Roles

This scenario requires 4 conditions for user USER_A from account A to have permission X on resource RESOURCE_B from account B through role ASSUME_ROLE_B:

1. ASSUME_ROLE_B is defined in account B.
2. ASSUME_ROLE_B is attached to policy that gives permission X on RESOURCE_B.
3. USER_A should be a member of ASSUME_ROLE - a trusted entity of the role.
4. USER_A should have in account A, permission to assume ASSUME_ROLE_B in account B.

File Access Manager does not display this information in v8.2.

Connector Overview

Permissions Forensics 										Saved Queries	Global Options
<div> Filters (4) Save Clear All </div>											Apply
User Name	Equals	Ami@TestUser1									
Business Resource Full Path	Equals	Root/TEST/Test12/FAM-Dev-Public/*225054067900/s3-us-east-1-fam-dev-public-bucket1									
Permission Type	Equals	GetBucketPolicy									
Group Name	Equals	FAMConnectorRole									

In the example above, the role “FAMConnectorRole” allows “GetBucketPolicy” on bucket “fam-dev-public-bucket1”. The role and the bucket, both belong to account “FAM-Dev-Public”. The role has a member user (trusted entity) “AmirTestUser1” from account “Fam-Org”.

If in account FAM-Org, “AmirTestUser1” has a policy which allows it to assume the role “FAMConnectorRole” in account “FAM-Dev-Public” (Not supported in File Access Manager view in v8.2) – The permission will be active.

Block Public Access

The Amazon S3 Block Public Access feature provides settings for buckets and accounts to help manage public access to Amazon S3 resources. By default, new buckets and objects don't allow public access. However, users can modify bucket policies or object permissions to allow public access. S3 Block Public Access settings override these policies and permissions and enable to limit public access to these resources.

There are 4 settings both on the bucket level, and the account level, If the PublicAccessBlock settings are different between the bucket and the account, Amazon S3 uses the most restrictive combination of the bucket-level and account-level settings.

In File Access Manager these permissions appear with the suffix “Account-Disabled” for the account level settings and “Bucket-Disabled” for the bucket level settings. If one of these settings is turned off, the Permission Forensics view shows these permissions as “Allow”.

Permissions Forensics

Filters (2)

Save

Clear All

Permission Type

Contains

<-disabled

✎

🗑

Business Resource Full Path

Equals

Root/FAM-Dev1(#[REDACTED])/s3.ap-southeast-1.amazonaws.com/dev1

✎

🗑

View by: Groups & Users Direct Permissions

Mark permissions unused for longer than 6 months

⌵

<input type="checkbox"/> Resource Full Path	Application	User Name	User Domain	User Entity Type	Permission Type	ACL Type Allow?
<input type="checkbox"/> Root/FAM-Dev1(#[REDACTED])/s3.ap-southeast-1.amazonaws.com/dev1	s3-1				BlockPublicAcls-Bucket-Disabled	Deny
<input type="checkbox"/> Root/FAM-Dev1(#[REDACTED])/s3.ap-southeast-1.amazonaws.com/dev1	s3-1				BlockPublicPolicy-Bucket-Disabled	Deny
<input type="checkbox"/> Root/FAM-Dev1(#[REDACTED])/s3.ap-southeast-1.amazonaws.com/dev1	s3-1				IgnorePublicAcls-Bucket-Disabled	Deny
<input type="checkbox"/> Root/FAM-Dev1(#[REDACTED])/s3.ap-southeast-1.amazonaws.com/dev1	s3-1				RestrictPublicBuckets-Bucket-Disabled	Deny
<input type="checkbox"/> Root/FAM-Dev1(#[REDACTED])/s3.ap-southeast-1.amazonaws.com/dev1	s3-1				BlockPublicAcls-Account-Disabled	Allow
<input type="checkbox"/> Root/FAM-Dev1(#[REDACTED])/s3.ap-southeast-1.amazonaws.com/dev1	s3-1				BlockPublicPolicy-Account-Disabled	Allow
<input type="checkbox"/> Root/FAM-Dev1(#[REDACTED])/s3.ap-southeast-1.amazonaws.com/dev1	s3-1				IgnorePublicAcls-Account-Disabled	Allow
<input type="checkbox"/> Root/FAM-Dev1(#[REDACTED])/s3.ap-southeast-1.amazonaws.com/dev1	s3-1				RestrictPublicBuckets-Account-Disabled	Allow

In the admin client, in *Resources->Permissions->Simple View* they will appear with warnings.

The screenshot displays the SailPoint user interface. At the top, there's a navigation bar with links like Dashboard, Resources, My Tasks, Reports, Compliance, Forensics, Goals, Settings, and Admin. Below this, a secondary navigation bar includes Activities, Permissions (selected), Data, Alerts, and Owners.

The main content area is divided into two panels:

- Resources Tree (Left Panel):** Shows a hierarchical view of applications and resources. Under "All Applications", there's a folder "s3-1" containing a "Root" folder. Inside "Root", several resources are listed, including "Amir-Bucket3-Dev1", which is highlighted with a blue selection box.
- Permission Details (Right Panel):** Displays information for the selected resource "amir-bucket3-dev1". It shows the application as "s3-1" and the path as "Root/FAM-Dev1(60)/s3.us-east-1.amir-bucket3-dev1". The "Permissions Types" section lists various permissions such as OWNER (1), ALLS3PolicyActions (4), BlockPublicAcIs-Bucket-Disabled (0), BlockPublicPolicy-Bucket-Disabled (0), IgnorePublicAcIs-Bucket-Disabled (0), RestrictPublicBuckets-Bucket-Disabled (0), BlockPublicAcIs-Account-Disabled (0) (marked with a yellow warning triangle), BlockPublicPolicy-Account-Disabled (0) (marked with a yellow warning triangle), and IgnorePublicAcIs-Account-Disabled (0) (marked with a yellow warning triangle). A prominent orange alert banner states: "Alert! Everyone has BlockPublicAcIs-Account-Disabled access to this resource! View Details".

Prerequisites for AWS

This section describes the minimal set of permissions required to configure a File Access Manager AWS connector.

It is a step-by-step guide, including AWS Console Screens.

Make sure your system fits the descriptions below before starting the installation

There are two methods to configure the AWS File Access Manager connector, and the required configuration is different for each.

- EC2 instance to run File Access Manager (This is the recommended method)
- Dedicated IAM user

Software Requirements

IdentityIQ File Access Manager requires the latest ASP.NET Core 3.1.x Hosting Bundle. This bundle consists of .NET Runtime and ASP .NET Core Runtime. You can download the latest 3.1.x Hosting Bundle version from [here](#).

Configuring an EC2 for File Access Manager Connector

This is the recommended connection method for the File Access Manager connector.

Create a role and policies to enable running the File Access Manager activities on all accounts in the organization.

1. Sign into your AWS account.

aws

Sign in as IAM user

Account ID (12 digits) or account alias

012345678910

IAM user name

MyUserName

Password

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Amazon EventBridge

Connect SaaS apps and AWS services using events

aws

English

[Terms of Use Privacy Policy](#) © 1996-2021, Amazon Web Services, Inc. or its affiliates.

2. Create a new policy "IdentityIQ_FileAccessManager_AssumeRolePolicy".

This policy will allow the File Access Manager application, created in the next step, to perform an **Assume Role** on the roles that will be created in each account.

See [IdentityIQ_FileAccessManager_AssumeRolePolicy.json](#) in Appendix A.

Create policy

1 2 3

Review policy

Name* IdentityIQ_FileAccessManager_AssumeRolePolicy

Use alphanumeric and "+", "@", "-" characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and "+", "@", "-" characters.

Summary

Filter

Service

Access level

Resource

Request condition

Allow (1 of 276 services) [Show remaining 275](#)

STS

Limited: Write

RoleName | string like |
IdentityIQ_FileAccessManagerRole

None

Tags

Key

Value

No tags associated with the resource.

* Required

[Cancel](#)

[Previous](#)

[Create policy](#)

3. Create a new role

- Select **AWS Service** as the trusted entity type.
- Select EC2 as the service.

Create role

1 2 3 4

Select type of trusted entity



AWS service
EC2, Lambda and others



Another AWS account
Belonging to you or 3rd party



Web identity
Cognito or any OpenID provider



SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

4. Attach the role to the IdentityIQ_FileAccessManager_AssumeRolePolicy policy created above.

Create role 1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy ↺

Filter policies Showing 1 result

	Policy name ▼	Used as
<input checked="" type="checkbox"/>	IdentityIQ_FileAccessManager_AssumeRolePolicy	Permissions policy (3)

5. Give the role a name (e.g. IdentityIQ_FileAccessManager_EC2_Role) and create it.

Create role 1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name*
Use alphanumeric and '*+=, @-_' characters. Maximum 64 characters.

Role description
Maximum 1000 characters. Use alphanumeric and '*+=, @-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies IdentityIQ_FileAccessManager_AssumeRolePolicy [↗](#)

Permissions boundary Permissions boundary is not set

No tags were added.

6. If you are creating a **new** EC2 instance select the above role as the IAM role for the instance.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the low

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	<input type="text" value="vpc-d17ccbbb (default)"/>	Create new VPC
Subnet	<input type="text" value="No preference (default subnet in any Availability Zone)"/>	Create new subnet
Auto-assign Public IP	<input type="text" value="Use subnet setting (Enable)"/>	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<input type="text" value="Open"/>	
Domain join directory	<input type="text" value="No directory"/>	Create new directory
IAM role	<input type="text" value="IdentityIQ_FileAccessManager_EC2_Role"/>	Create new IAM role
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	<input type="text" value="Stop"/>	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring	Additional charges apply.
EBS-optimized instance	<input checked="" type="checkbox"/> Launch as EBS-optimized instance	
Tenancy	<input type="text" value="Shared - Run a shared hardware instance"/>	Additional charges will apply for dedicated tenancy.
Elastic Graphics	<input type="checkbox"/> Add Graphics Acceleration	Additional charges apply.
Credit specification	<input checked="" type="checkbox"/> Unlimited	Additional charges may apply

7. If you are using an **existing** EC2 instance, Modify the IAM role to the role above

In the option

EC2 > Instances > Actions > Security > Modify IAM role

EC2 > Instances > i-08905a3cda55f99f5 > Modify IAM role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

i-08905a3cda55f99f5

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

IdentityIQ_FileAccessManager_EC2_Role ▼

[Create new IAM role](#)

Cancel

Save

- Create a new policy for each organization account the connector is supposed to analyze

Create a new policy called “IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy” with all the required permissions for the connector.

See [IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy.json](#) in Appendix A.

Create policy

123

Review policy

Name* IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy

Use alphanumeric and '*-._@-' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '*-._@-' characters.

Summary

Q Filter

Service ▼	Access level	Resource	Request condition
Allow (3 of 284 services) Show remaining 281			
IAM	Limited: List, Read	All resources	None
Organizations	Limited: List	All resources	None
S3	Limited: List, Read	All resources	None

Tags

Key	Value
No tags associated with the resource.	

* Required

[Cancel](#)
[Previous](#)
[Create policy](#)

- Create a new role for the File Access Manager user to assume.

On each organization account the connector should analyze, create a new role called “IdentityIQ_FileAccessManagerRole” which the FAM user will assume. Select “Another AWS Account” and enter the account Id of the organization’s management account.

The role name should be kept as **IdentityIQ_FileAccessManagerRole**.

Create role 1 2 3 4

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* 012345678910 ⓘ

Options ☐ Require external ID (Best practice when a third party will assume this role)
☐ Require MFA ⓘ

10. Attach the IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy policy created above.

Create role 1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy ↻

Filter policies ▼ Showing 1 result

	Policy name ▼	Used as
<input checked="" type="checkbox"/>	IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy	None

11. Enter the role name - IdentityIQ_FileAccessManagerRole.

Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name* IdentityIQ_FileAccessManagerRole

Use alphanumeric and '+', '@', '-' characters. Maximum 64 characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Trusted entities The account 012345678910

Policies IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy

Permissions boundary Permissions boundary is not set

12. Edit the trust relationship of the new role.

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like Dashboard, Access management, Groups, Users, Roles (selected), Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled 'Roles > IdentityIQ_FileAccessManagerRole' and shows a 'Summary' tab. The summary includes details such as Role ARN (arn:aws:iam:012345678910:role/IdentityIQ_FileAccessManagerRole), Role description (with an 'Edit' link), Instance Profile ARNs, Path (/), Creation time (2021-04-06 21:25 UTC+0300), Last activity (Not accessed in the tracking period), and Maximum session duration (1 hour, with an 'Edit' link). Below this is a link to switch roles in the console. At the bottom, there are tabs for 'Permissions', 'Trust relationships' (selected), 'Tags', 'Access Advisor', and 'Revoke sessions'. The 'Trust relationships' tab shows a section for 'Trusted entities' with a table listing 'The account 012345678910'. There is also a 'Conditions' section on the right, which is currently empty.

13. Edit the json file

Replace “root” in the Principal section with

```
“assumed-role/{EC2 role name}/{EC2 instance ID}”
```

where “EC2 role name” is the name of the role created above (“IdentityIQ_FileAccessManager_EC2_Role” in this manual) and “EC2 instance ID” is the ID of the instance on which the FAM application is installed.

See [IdentityIQ_FileAccessManagerRole.json \[EC2\]](#) in Appendix A.

Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:sts::012345678910:assumed-role/IdentityIQ_FileAccessManager_EC2_Role/i-08f47a9c91225932e"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {}
11    }
12  ]
13 }
```

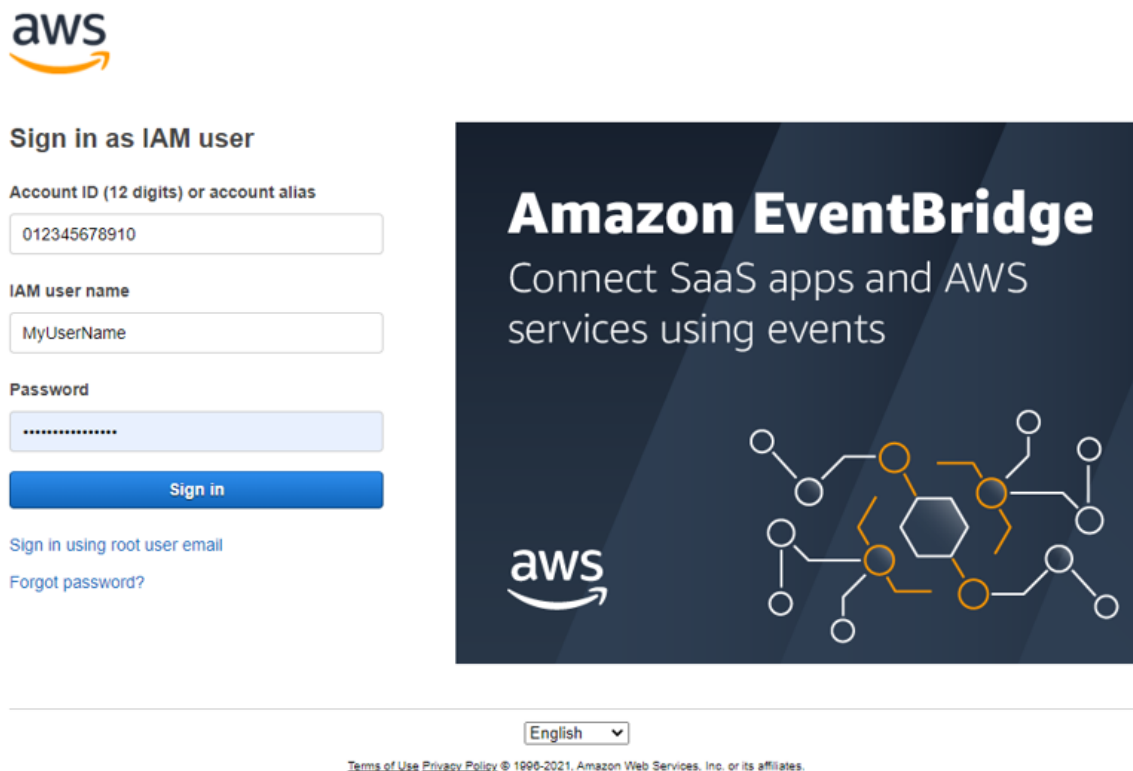
Cancel Update Trust Policy

Creating a Dedicated IAM User

The recommended method to install the File Access Manager connector is using the EC2 Login method. See [Configuring an EC2 for File Access Manager Connector](#). If you wish to use a dedicated IAM user login instead, follow this section:

To configure the connector, create dedicated users with the appropriate users and policies

1. Sign into your organization's management account.



The screenshot shows the AWS IAM console sign-in page. On the left, there is a form titled "Sign in as IAM user". It includes fields for "Account ID (12 digits) or account alias" (containing "012345678910"), "IAM user name" (containing "MyUserName"), and "Password" (masked with dots). A blue "Sign in" button is below the password field. Links for "Sign in using root user email" and "Forgot password?" are at the bottom left. On the right, there is a large banner for "Amazon EventBridge" with the text "Connect SaaS apps and AWS services using events" and a network diagram. At the bottom, there is a language dropdown set to "English" and a small link for "Terms of Use Privacy Policy © 1996-2021, Amazon Web Services, Inc. or its affiliates."

2. Create a new policy "IdentityIQ_FileAccessManager_AssumeRolePolicy". This policy will allow the File Access Manager user created in the next step to perform an **Assume Role** on the roles that will be created in each account.

See [IdentityIQ_FileAccessManager_AssumeRolePolicy.json](#) in Appendix A.

Create policy

1 2 3

Review policy

Name* IdentityIQ_FileAccessManager_AssumeRolePolicy

Use alphanumeric and '+', '@', '-' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Summary

Filter

Service	Access level	Resource	Request condition
Allow (1 of 276 services) Show remaining 275			
STS	Limited: Write	RoleName string like IdentityIQ_FileAccessManagerRole	None

Tags

Key	Value
No tags associated with the resource.	

* Required

Cancel

Previous

Create policy

3. Create an IAM User for File Access Manager and select Programmatic access. This access requires an access key and secret Key.

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* IdentityIQ_FileAccessManager_User

[Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Access type* ☒ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☐ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

4. Attach the policy IdentityIQ_FileAccessManager_AssumeRolePolicy policy created above to the new user

Search for services, features, marketplace products, and docs [Alt+S]

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	IdentityIQ_FileAccessManager_User
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	IdentityIQ_FileAccessManager_AssumeRolePolicy

Tags

No tags were added.

5. Save the generated Access Key and Secret Key in a secure place.

Add user

1 2 3 4 5

✓ **Success**

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://012345678910.signin.aws.amazon.com/console>

	User	Access key ID	Secret access key
▶	✓ IdentityIQ_FileAccessManager_User	AKIAIOSFODNN7EXAMPLE	***** Show

6. On each organization account the connector should analyze - Create new policy “*IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy*” with all the required permissions for the connector. See the code [IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy.json](#) in Appendix A.

Create policy

1 2 3

Review policy

Name* IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy

Use alphanumeric and '+,=, @, _' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+,=, @, _' characters.

Summary

Q Filter

Service ▾	Access level	Resource	Request condition
Allow (3 of 284 services) Show remaining 281			
IAM	Limited: List, Read	All resources	None
Organizations	Limited: List	All resources	None
S3	Limited: List, Read	All resources	None

Tags

Key	Value
-----	-------


No tags associated with the resource.


7. Create a new role “*IdentityIQ_FileAccessManagerRole*” which the File Access Manager user will assume on each organization account the connector should analyze. Select “**Another AWS Account**” and enter the user account ID.


Create role


1 2 3 4

Select type of trusted entity


AWS service
 EC2, Lambda and others


Another AWS account
 Belonging to you or 3rd party


Web identity
 Cognito or any OpenID provider


SAML 2.0 federation
 Your corporate directory

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* 012345678910 ⓘ

- Options
- ☐ Require external ID (Best practice when a third party will assume this role)
- ☐ Require MFA ⓘ

8. Attach the policy *IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy* created above.

Create role

1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Filter policies ▼
Showing 1 result

	Policy name ▼	Used as
<input checked="" type="checkbox"/>	IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy	None

- Enter the role name - *IdentityIQ_FileAccessManagerRole*.

This name cannot be changed.

Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name*
 Use alphanumeric and '+,=, @, _' characters. Maximum 64 characters.

Role description
 Maximum 1000 characters. Use alphanumeric and '+,=, @, _' characters.

Trusted entities The account 012345678910

Policies [IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy](#)

Permissions boundary Permissions boundary is not set

No tags were added.

- Edit the trust relationship of the new role.

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like Dashboard, Access management, Groups, Users, Roles (highlighted), Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled 'IdentityIQ_FileAccessManagerRole' and shows the 'Summary' tab. It displays metadata for the role, including its ARN, description, instance profile ARNs, path, creation time, last activity, and maximum session duration. Below this, there are tabs for Permissions, Trust relationships (selected), Tags, Access Advisor, and Revoke sessions. The 'Trust relationships' section shows a list of trusted entities, currently containing 'The account 012345678910'.

11. Edit the json file

Replace “root” in the Principal section with “user/{FAM IAM User username}” where “FAM IAM User username” is the user created above.

See [IdentityIQ_FileAccessManagerRole.json \[Dedicated User\]](#) in Appendix A.

Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::012345678910:user/IdentityIQ_FileAccessManager_User"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {}
11    }
12  ]
13 }
```


Connector Installation Flow Overview

To install the AWS S3 connector:

1. Configure all the prerequisites.
2. Add a new AWS S3 application in the Business Website.
3. Install the relevant services:
 - Permissions Collector

If you are using EC2 login, the collector should be installed on the EC2 instance.

Collecting Data Stored in an External Application

Connector / Collector terminology:

Connector

The collection of features, components and capabilities that comprise IdentityIQ File Access Manager support for an endpoint.

Collector

The “Agent” component or service in a Permission Collection architecture.

Engine

The core service counterpart of this architecture.

Identity Collector

A logical component used to fetch identities from an identity store and holds the configuration, settings for that identity store, and the relations between these identities.

The identity collector has no “physical” manifest.

- The actual work is done by the Collector Synchronizer.

The list below describes the high level installation process required to collect and analyze data from an external application. Most of these should already be set up in your IdentityIQ File Access Manager installation. See the server Installation guide for further details.

Install a Permission Collection central engine

One or more central engines, installed using the server installer

Create an Application in File Access Manager

From the Business Website. The application is linked to central engines listed above.

Install Permission Collectors (optional)

Optionally, you can install collectors that will run on a separate server and take some of the work from the central PC and DC engines (Where supported). When installing a collector, you attach it to an engine. If no collectors are installed, the central services act as both the engine and the collector.

To install a collector, you must have the **RabbitMQ** service installed for communication between the central engines and the collectors. RabbitMQ is installed

For further details, see section **Application > Central Service > Collector Relations** in the IdentityIQ File Access Manager Administrator Guide

Adding an AWS S3 Application

In order to integrate with AWS S3, we must first create an application entry in IdentityIQ File Access Manager. This entry includes the identification, connection details, and other parameters necessary to create the link.

To add an application, use the **New Application Wizard**.

1. Navigate to *Admin > Applications*
2. Click **Add New** to open the wizard.

Select Wizard Type

1. Click **Standard Application**
2. Click **Next** to open the **General Details** page.

General Details

Application Type

AWS S3

Application Name

Logical name of the application

Description

Description of the application

Tags

Select tags for the application from the dropdown menu, and / or type a new name, and press **Enter** to create a new tag. The dropdown list of tags filters out matching tags as you type and displays up to 50 tags.

The **tags** replace the **Logical container** field that was used when creating applications in releases before 8.2

Event Manager Server

This option is available if there are more than one event manager servers configured in the system.

Select an event manager from the drop down menu

Click **Next** to open the Connection Details page.

Connection Details

Management Account ID

The account ID of the AWS management account - This is required for collecting user details and permissions from different accounts.

Use Dedicated IAM User

Use this to select the login method. Leave unchecked to use the recommended method of EC2 login.

Check this box to use a dedicated IAM use account for login.

If selecting a Dedicated IAM User method, fill in the following fields:

- **Access Key Id**

The IAM user programmatic username of the File Access Manager user that was created in the pre-requisites.

- **Secret Access Key**

The IAM user programmatic password.

Click **Next**.

Configuring and Scheduling the Permissions Collection


Permissions can be analyzed to determine the application permissions of an out-of-the-box application, provided you have defined an identity store for File Access Manager to use in its analysis, and you have run a crawl for the application.

The permission collector is a software component responsible for analyzing the permissions in an application.

The Central Permission Collector Service is responsible for running the Permission Collector and Crawler tasks.

If the “IdentityIQ FAM Central Permission Collector” wasn’t installed during the installation of the server, this configuration setting will be disabled.

To configure the Permission Collection

- Open the edit screen of the required application
 - a. Navigate to **Admin > Applications**
 - b. Scroll through the list, or use the filter to find the application
 - c. Click the edit icon  on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

The actual entry fields vary according to the application type

When entering this page in edit mode, you can navigate between the various configuration windows using the **Next** and **Back** buttons.

Central Permissions Collection Service

Select a central permission collection service from the dropdown list. You can create permissions collection services as part of the service installation process. See section “Services Configuration” in the IdentityIQ File Access Manager Administrator Guide for further details.

Analyze all Objects in S3 Bucket

If checked – collect and analyze files in the buckets, and not only buckets and folders.

Default is unchecked.

Analyze ACL Permissions

Click to fetch and analyze ACL-type Permissions.

S3 ACLs is a legacy access control mechanism that predates IAM. AWS recommends using S3 bucket policies or IAM policies for access control.

If checked, ACLs will be collected for business resources, which will impact the performance of the Permission Collector. For cases with a large number of resources, skipping the ACL permission fetch can improve the service run time considerably .

This option is checked by default

If ACL is not supported by your server, make sure this field is unchecked.

Scheduling a Task

Create a Schedule

Click on this option to view the schedule setting parameters.

Schedule Task Name

A name for this scheduling task

When creating a new schedule, the system generates a default name in the following format:

{appName} - {type} Scheduler

You can override or keep this name suggestion.

Schedule

Select a scheduling frequency from the dropdown menu.

- **Schedule Types and Intervals**

Once

Single execution task runs.

Run After

Create dependency of tasks. The task starts running only upon successful completion of the first task.

Hourly

Set the start time.

Daily

Set the start date and time.

Weekly

Set the day(s) of the week on which to run.

Monthly

The start date defines the day of the month on which to run a task.

Quarterly

A monthly schedule with an interval of 3 months.

Half Yearly

A monthly schedule with an interval of 6 months.

Yearly

A monthly schedule with an interval of 12 months.

Date and time fields

Fill in the scheduling times. These fields differ, depending upon the scheduling frequency selected.


Active check box

Check this to activate the schedule.

Click **Next**.

Configuring and Scheduling the Crawler

To set or edit the Crawler configuration and scheduling

- Open the edit screen of the required application
 - a. Navigate to **Admin > Applications**
 - b. Scroll through the list, or use the filter to find the application
 - c. Click the edit icon  on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

The actual entry fields vary according to the application type

Calculate Resources' Size

Determine when, or at what frequency, File Access Manager calculates the resources' size.

Select one of the following:

- Never
- Always
- Second crawl and on (This is the default)

Exclude CloudTrail Logs

Check this box to exclude CloudTrail logs from being crawled and analyzed. There could be a very large number of these log files, and scanning them will have a negative impact on performance.

The default is checked.

Create a Schedule

Click to open the schedule panel. See [Scheduling a Task](#)


Setting the Crawl Scope

There are several options to set the crawl scope:

- Setting explicit list of resources to include and / or exclude from the scan.
- Creating a regex to define resources to exclude.

Including and Excluding Paths by List

To set the paths to include or exclude in the crawl process for an application

- Open the edit screen of the required application
 - a. Navigate to **Admin > Applications**
 - b. Scroll through the list, or use the filter to find the application
 - c. Click the edit icon  on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

The actual entry fields vary according to the application type

1. Scroll down to the Crawl configuration settings.
2. Click **Advanced Crawl Scope Configuration** to open the scope configuration panel.
3. Click Include / Exclude Resources to open the input fields.
4. To add a resource to a list, type in the full path to include / exclude in the top field and click **+** to add it to the list.
5. To remove a resource from a list, find the resource from the list, and click the **x** icon on the resource row.

When creating exclusion lists, excludes take precedence over includes.

Excluding Paths by Regex for AWS S3 Buckets

The AWS Path Structure in File Access Manager

File Access Manager uses a path name in the following structure:

Path Structure: Root/[OU]/[Account]/[Bucket Path]/[Folder]/[Filename]

Component structure: Root/[OU]/[OU2]/[Account name](#[Account ID])/s3.[region].[bucket name]/[folder]/[file name]

Example: Root/Example-OU/Example-Account(#420269343516)/s3.north-east-17.HR3InputDataBucket/Prospects/CVs/SueSmithPM.Docx

Root

All paths start with "Root/"

OU

The organizational unit. This could be empty, or include a string of one or more OUs, according to the BR hierarchical structure.

Account

Since account names are not unique under an organization, this string includes the account ID and the account name


```
[Account name] ([Account ID])
```

Bucket Path

The bucket section of the path starts with "s3." and includes the region

```
s3.[region].[bucket]
```

Setting Filters of Paths to Exclude in the Crawl Process for an Application Using Regex

- Open the edit screen of the required application
 - a. Navigate to **Admin > Applications**
 - b. Scroll through the list, or use the filter to find the application
 - c. Click the edit icon  on the line of the application
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

The actual entry fields vary according to the application type

1. Click **Exclude Paths by Regex** to open the configuration panel.
2. Type in the paths to exclude by Regex, See regex examples in the section below. Since the system does not collect BRs that match this Regex, it also does not analyze them for permissions. See the example below in section Business Resource Structure to better understand the business resource full path structure.

Crawler Regex Exclusion Examples

The following are examples of crawler Regex exclusions:

Exclude all Folders Which Start With One or More Folder Names

Starting with *bucket_name/folderName*

Regex: `bucket_name/folderName$`

Starting with *bucket_name/folderName* or *bucket_name/OtherFolderName*

Regex: `bucketName/(folderName|OtherFolderName)$`

Include ONLY Folders Which Start With One or More Folder Names

Starting with *bucket_name/shareName*

Regex: `^(?!bucket_name/shareName($|/.*)).*`

Starting with *bucket_name/folderName* or *bucket_name/OtherFolderName*

Regex: `^(?!bucket_name/(folderName|OtherFolderName)($|/.*)).*`

To write a backslash or a Dollar sign, add a backslash before it as an escape character.

To add a condition in a single command, use a pipe character “|”.

Excluding Top Level Resources

Use the top level exclusion screen to select top level roots to exclude from the crawl. This setting is done per application.

To exclude top level resources from the crawl process

1. Open the application screen

Admin > Applications

2. Find the application to configure and click the drop down menu on the application line. Select **Exclude Top Level Resources** to open the configuration panel.

3. **Run Task**

The Run Task button triggers a task that runs a short detection scan to detect the current top level resources.

Before running the task for the first time, the message above this button is:

"Note: Run task to detect the top-level resources"

If the top level resource list has changed in the application while you are on this screen, press this button to retrieve the updated structure.

Once triggered, you can see the task status in

Settings > Task Management > Tasks

This will only work if the user has access to the task page

When the task has completed, press **Refresh** to update the page with the list of top level resources.

4. Click the top level resource list, and select top level resources to exclude.
5. Click **Save** to save the change.
6. To refresh the list of top level resources, run the task again. Running the task will not clear the list of top level resources to exclude.

Top Level Resources Exclusion

s3-2

Last Successful Run 04-07-2021 3:35:18 PM

Run Task

View Task Status

Note: Refresh the list to view recently discovered resources

Refresh

Top Level Resources Exclusion List 2 Selected | Clear Selection

Top Level Resources Exclusion List

☐ Root/FAM-Org(#426259384505)/s3.us-east-1.test123456...
 ☒ Root/FAM-Dev1(#632879285990)/s3.ap-southeast-1.amir...
 ☐ Root/FAM-Dev1(#632879285990)/s3.sa-east-1.amir-buck...
 ☒ Root/FAM-Dev1(#632879285990)/s3.us-east-1.amir-buck...
 ☐ Root/FAM-Dev1(#632879285990)/s3.us-west-1.cf-templa...
 ☐ Root/FAM-Dev1(#632879285990)/s3.us-west-1.sp-cam-f...
 ☐ Root/AmirOU_A/Amir%2F\OU_A1/FAM-Dev2(#07325561...

Special Consideration for Long File Paths in Crawl

If you need to support long file paths above 4,000 characters for the crawl, set the flag

excludeVeryLongResourcePaths

in the Permission Collection Engine App.config file to true.

By default this value will be commented out and set to false.

This key ensures, when enabled, that paths longer than 4000 characters are excluded from the applications' resource discovery (Crawl), to avoid issues while storing them in the SQLServer database.

When enabled, business resources with full paths longer than 4000 characters, and everything included in the hierarchical structure below them, will be excluded from the crawl, and will not be collected by File Access Manager. This scenario is extremely rare.

You should not enable exclusion of long paths, unless you experience an issue.

Background

File Access Manager uses a hashing mechanism to create a unique identifier for each business resource stored in the File Access Manager database. The hashing mechanism in SQLServer versions 2014 and earlier, is unable to process (hash) values with 4,000 or more characters.

Though resources with paths of 4000 characters or longer are extremely rare, File Access Manager is designed to handle that limitation.

Identifying the Problem

When using an SQL Server database version 2014 and earlier

The following error message in the Permission Collection Engine log file:

```
System.Data.SqlClient.SqlException (0x80131904): String or binary data would be truncated.
```

In all other cases, this feature should not be enabled.

Setting the Long Resource Path Key

The Permission Collection Engine App.config file is `RoleAnalyticsServiceHost.exe.config`, and can be found in the folder

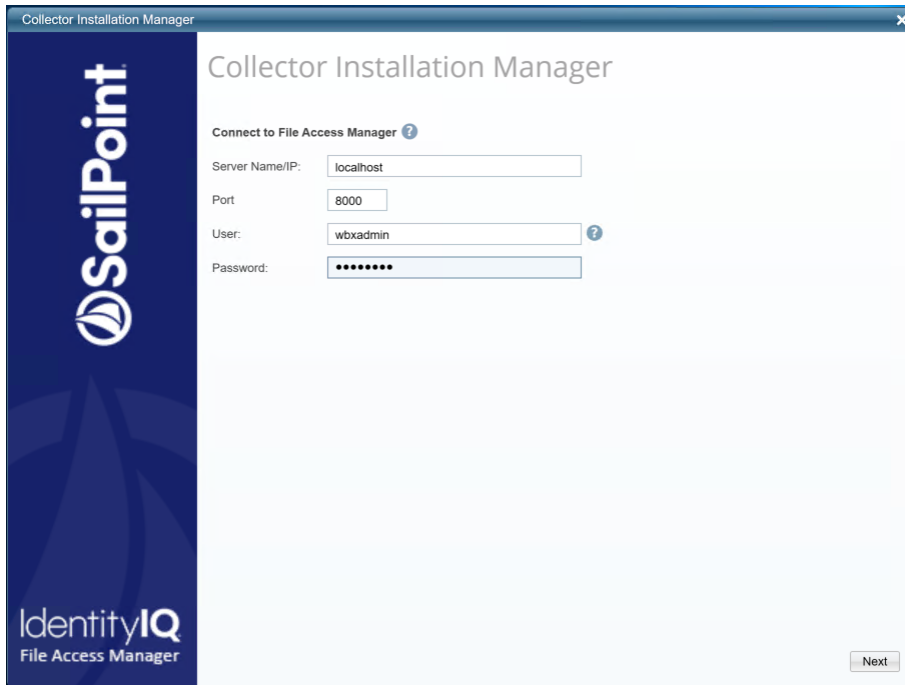
`%SailPoint_Home%\FileAccessManager\[Permission Collection instance]\`

Search for the key **`excludeVeryLongResourcePaths`** and correct it as described above.

Installing Services: Collector Installation

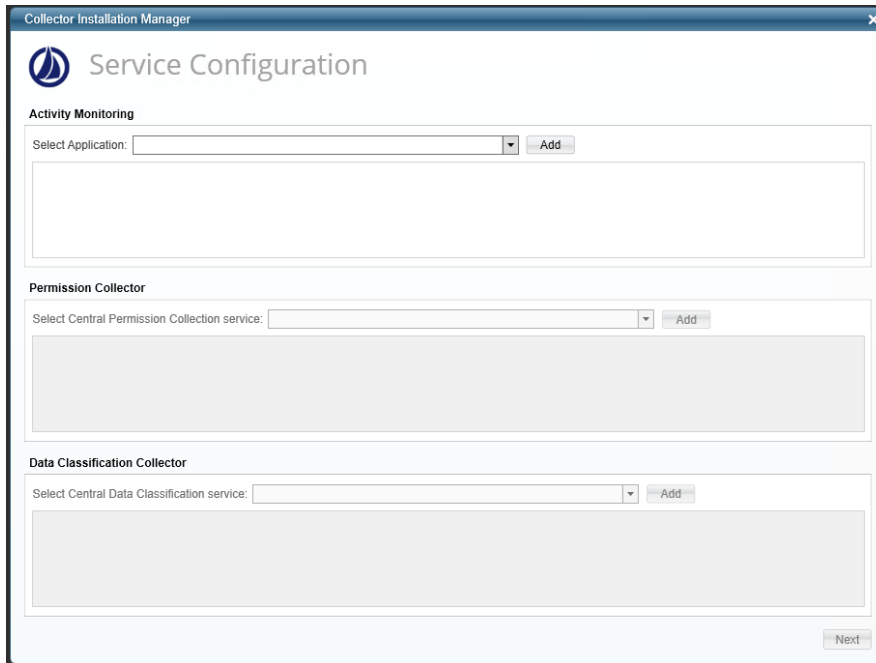
1. Run the **Collector Installation Manager** as an Administrator.
The installation files are in the installation package under the folder **Collectors**.

The Collector Installation Manager window displays.



2. Enter the credentials to connect to IdentityIQ File Access Manager.
 - a. ServerName/IP should be pointed to the Agent Configuration Manager service server.
 - b. An IdentityIQ File Access Manager user with Collector Manager permission (permission to install collectors). For Active Directory authentication, use the format domain\username.
3. Click **Next**.

The Service Configuration window displays.



4. In some applications, additional credentials may be required to allow granting elevated permission for activity monitoring collection.
5. If you are installing the Permission Collector, select the Central Permission Collector to which to connect this service, and click **Add**
6. Click **Next**.

The Installation Folder window displays.

If this is the first time you are installing collectors on this machine, you will be prompted to select an installation folder, in which all future collectors will also be installed.

7. Browse and select the location of the target folder for installation.
8. Browse and select the location of the folder for system logs.
9. Click **Next**.
10. The system begins installing the selected components.
11. Click **Finish**

The Finish button is displayed after all the selected components have been installed.

The *IdentityIQ File Access Manager Administrator Guide* provides more information on the collector services.

Verifying the AWS S3 Connector Installation

Installed Services

Verify that the services installed for the connector are available and active. Using windows Service manager, or other tool, look for the IdentityIQ File Access Manager services, and see that they are running.

for example:

- File Access Manager Central Permissions Collection - <Application_Name>

Log Files

Check the log files listed below for errors

- "%SAILPOINT_HOME_LOGS%\PermissionCollection_<Service_Name>.log"

Permissions Collection

1. Run the Crawler and Permissions Collector tasks (*Settings > Task Management > Scheduled Tasks*)
2. Verify that:
 - The tasks completed successfully
 - Business resources were created in the resource explorer (*Admin > Applications > [application column] > Manage Resources*)
 - Permissions display in the Permission Forensics page (*Forensics > Permissions*)

Appendix A: Json Scripts

This appendix includes the scripts required for creating the roles and policies mentioned in this guide.

Please make sure not to change the file names.

IdentityIQ_FileAccessManagerRole.json [EC2]

This is the version of the role to create for installation using an EC2 login

IdentityIQ_FileAccessManagerRole.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::{The EC2 instance account Id}:assumed-role/{EC2 instance
role name}/{EC2 instance Id}"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

IdentityIQ_FileAccessManagerRole.json [Dedicated User]

This is the version of the role to create for installation using a dedicated IAM user login

IdentityIQ_FileAccessManagerRole.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::{The user account ID}:user/{FAM IAM User username}"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

IdentityIQ_FileAccessManager_AssumeRolePolicy.json

IdentityIQ_FileAccessManager_AssumeRolePolicy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::*:role/IdentityIQ_FileAccessManagerRole"
    }
  ]
}
```

IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy.json

IdentityIQ_FileAccessManager_S3IAMReadOnlyAccessPolicy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",

```



```
        "iam:GetUserPolicy",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent"
    ],
    "Resource": "*"
}
]
```