MATRIX42

SMARTER WORKSPACE – BETTER LIFE

Matrix42 MyWorkspace

Getting Started with Amazon Web Services (AWS)

Version 1.0.0

22. April 2016

Copyright © 2000 - 2016 Matrix42 AG

This documentation is copyright protected. All rights are reserved by Matrix42 AG.

Any other use, in particular the disclosure to third parties, storage in a data system, dissemination, processing, presentation, performance and demonstration are prohibited. This applies to the entire document, as well as parts thereof.

Subject to change. Reprint, also in excerpts, is permitted only with the written consent of Matrix42 AG.

The software described in this document is subject to a permanent development due to which there may be differences in the documentation and the actual software. This documentation is not entitled to the actual functionality of the software.

Apple and **Mac OS X** are registered trademarks of Apple Inc.
Citrix® software or **Citrix® server** are Trademarks and Registered Trademarks of Citrix Systems, Inc. in the United States and other countries.
cygwin is copyrighted by Red Hat Inc. 1996-2003.
expat is copyrighted by Thai Open Source Software Center Ltd.
gSOAP is copyrighted by Robert A. van Engelen, Genivia, Inc. All rights reserved.
Iconv is copyrighted by 1999-2003 Free Software Foundation, Inc.
Iperf is copyrighted by the University of Illinois, except for the gnu_getopt.c, gnu_getopt_long.c, gnu_getopt.h files, and inet_aton.c, which are under the GNU General Public License.
Libmspack (C) 2003-2004 by Stuart Caie <kyzer@4u.net>.
OpenSSL This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
PuTTY is copyrighted by Simon Tatham. Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, and CORE SDI S.A.
RSA Data Security, Inc. MD5 Message-Digest Algorithm is copyrighted by RSA Data Security Inc. Created 1991. All rights reserved.
rsync is an open source utility that provides fast incremental file transfer. rsync is freely available under the GNU General Public License version 2.
runcontrol The Initial Developer of the Original Code is James Clark. Portions created by James Clark are Copyright (c) 1998 James Clark. All rights reserved.
SNMP++ Copyright (c) 1996 Hewlett-Packard Company.
VMware, the **VMware "boxes" logo and design, Virtual SMP, VMotion vSphere, vSphere Hypervisor (ESXi), ESX, View, ThinApp, vCenter** and **vCloud** are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
Windows, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and **Windows Server 2012** are registered trademarks of Microsoft Corporation.

Others, at this point not explicitly listed, company, brand and product names are trademarks or registered trademarks of their respective owners and are subject to trademark protection.

Getting Started with Amazon Web Services (AWS)

Getting Started with Amazon Web Services (AWS)

1. Summary

Amazon Web Services are used to manage many different cloud based elastic services of Amazon. The most popular example is Amazon EC2, S3 or Simple DB but also new business services like Amzon Work Mail is managed with the identity services of Amazon Web Services (AWS). This getting started guide describes how to integrate the identity services of Amazon Web Services with Matrix42 MyWorkspace.

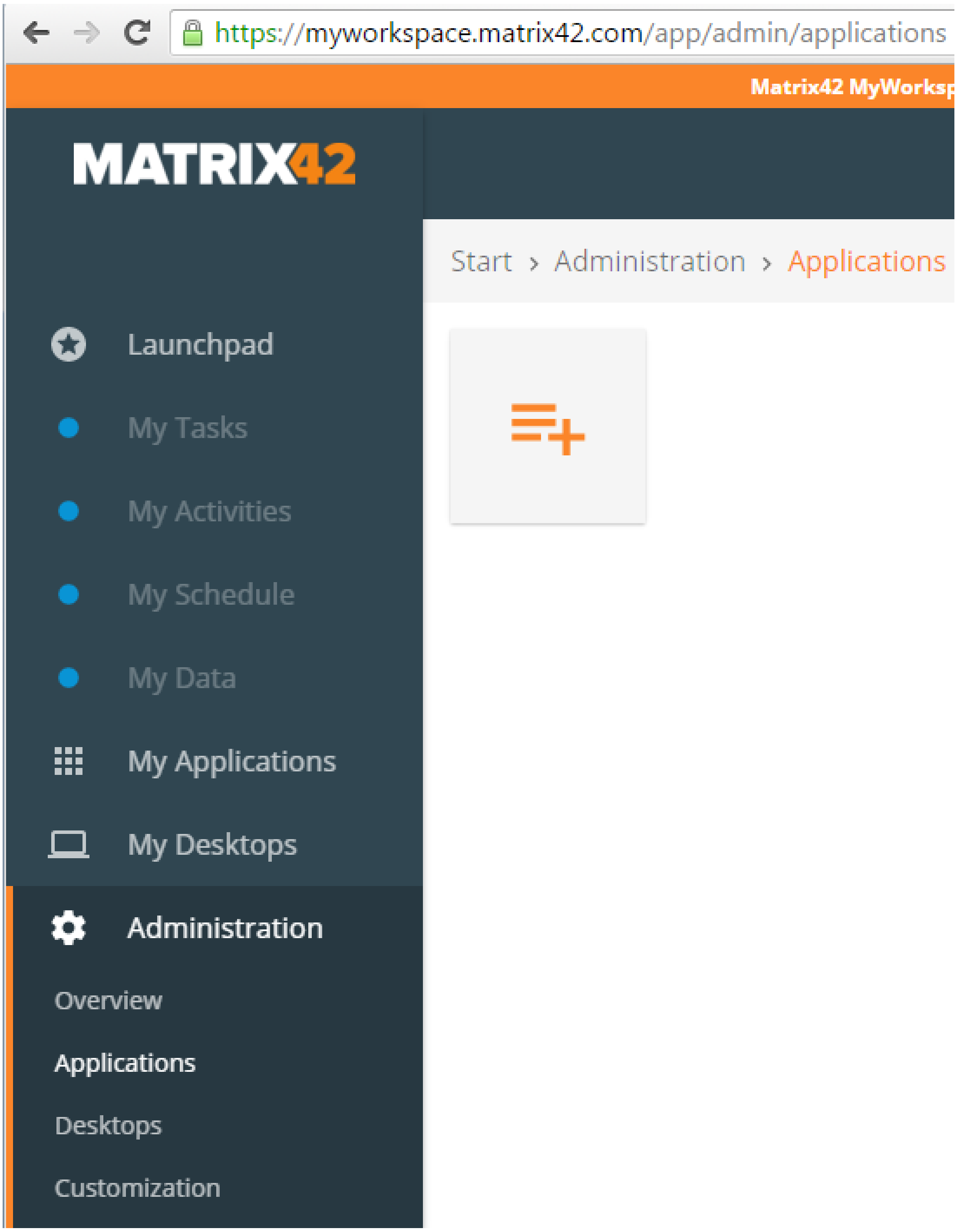
2. Goal

After completing this getting started guide you will be able to connect an existing or new Amazon Web Services account to Matrix42 MyWorkspace. This means it's possible to federate AWS with your existing on-premise or cloud based infrastructure, e.g. Active Directory, Azure Active Directory or Google Apps for Business.

2.1. Signup for Matrix42 MyWorkspace

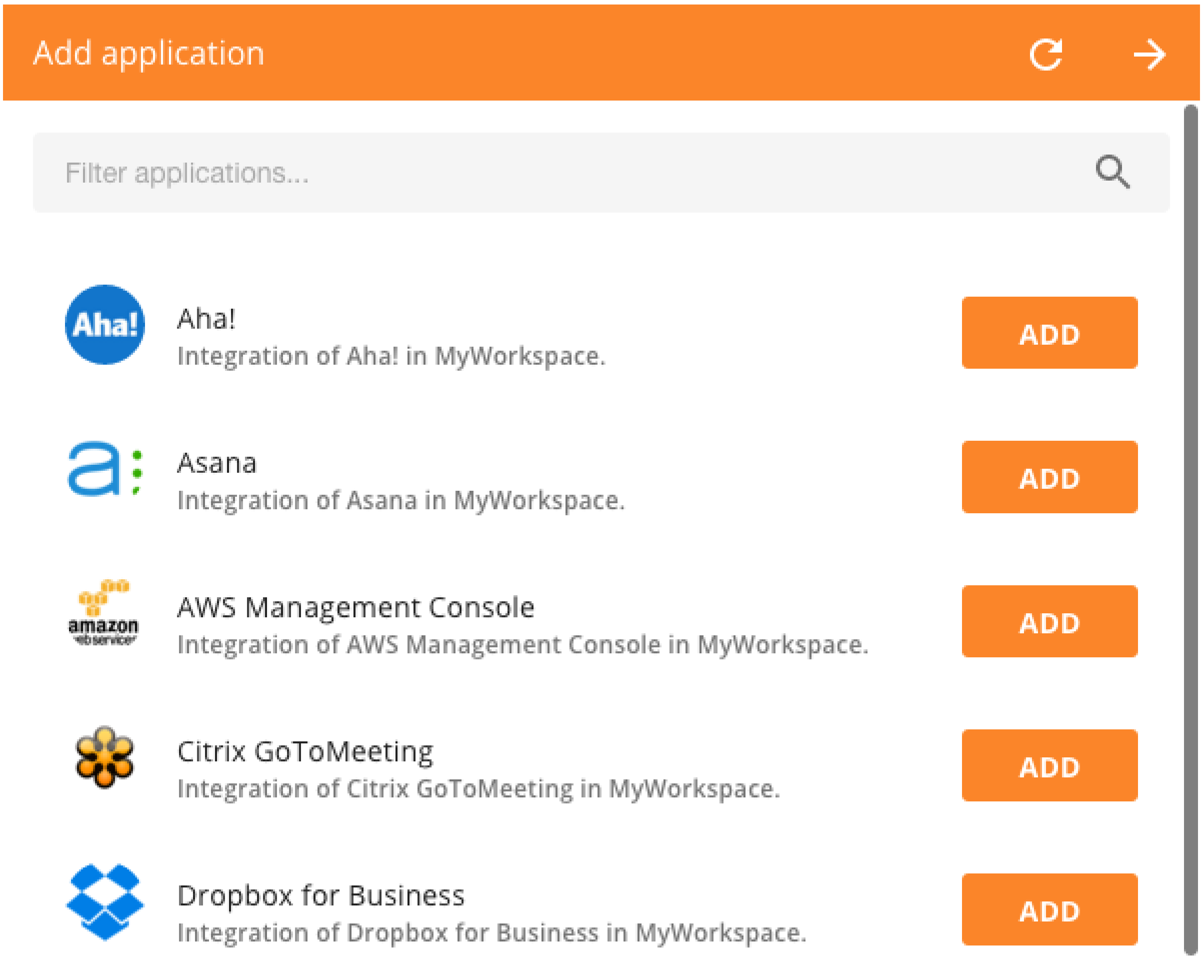
Visit the MyWorkspace welcome page https://myworkspace.matrix42.com/ and signup for a free new tenant our log into your existing MyWorkspace tenant. After that visit the applications section in the https://myworkspace.matrix42.com/app/admin/applications and click + orange tile to register Amazon Web Services as a new application.

Getting Started with Amazon Web Services (AWS)



2.2. Register AWS as new application

Amazon Web Services can be registered as a new application in MyWorkspace. This process gives your end users who have permissions on the service seamless access. Start the registration process by pressing the "+" button in the upper right corner and selecting "AWS Management Console" from the applications catalog and click “Add” button.



Add application

Filter applications...

Aha!
Integration of Aha! in MyWorkspace.
ADD

Asana
Integration of Asana in MyWorkspace.
ADD

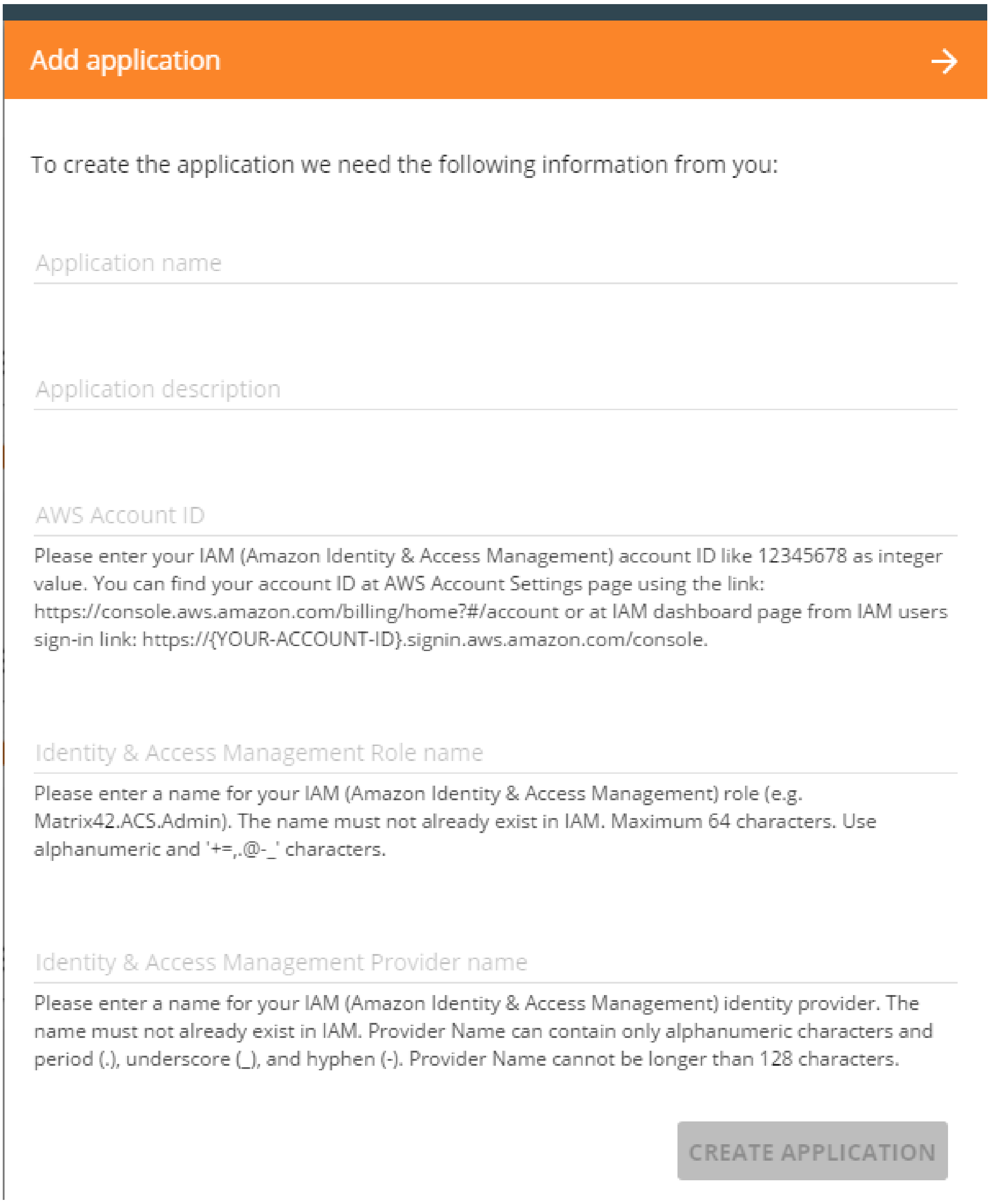
AWS Management Console
Integration of AWS Management Console in MyWorkspace.
ADD

Citrix GoToMeeting
Integration of Citrix GoToMeeting in MyWorkspace.
ADD

Dropbox for Business
Integration of Dropbox for Business in MyWorkspace.
ADD

2.3. Fill AWS Application mandatory fields

Fill AWS application mandatory fields like Application Name, Description, AWS Account ID, Identity & Access Management Role name, Identity & Access Management Provider name.
Please pay attention at fields description for AWS Account ID, Role name and Provider name.



To create the application we need the following information from you:

Please enter your IAM (Amazon Identity & Access Management) account ID like 12345678 as integer value. You can find your account ID at AWS Account Settings page using the link: https://console.aws.amazon.com/billing/home?#/account or at IAM dashboard page from IAM users sign-in link: https://{YOUR-ACCOUNT-ID}.signin.aws.amazon.com/console.

Please enter a name for your IAM (Amazon Identity & Access Management) role (e.g. Matrix42.ACS.Admin). The name must not already exist in IAM. Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Please enter a name for your IAM (Amazon Identity & Access Management) identity provider. The name must not already exist in IAM. Provider Name can contain only alphanumeric characters and period (.), underscore (_), and hyphen (-). Provider Name cannot be longer than 128 characters.

2.4. Create application

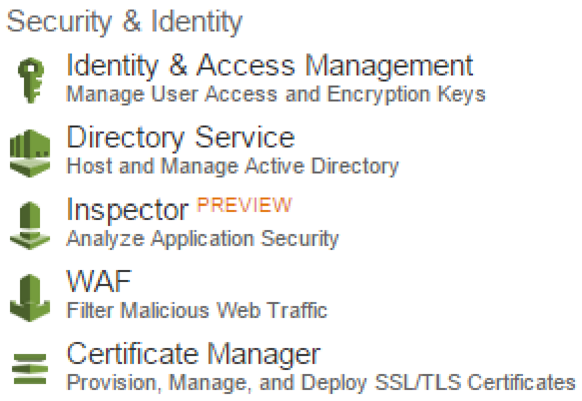
Click “Create application” button. Application will be created and now you need to configure the AWS Management Console and its Identity provider. For this you can use the “Integration Guide” button for created application or follow this document.

2.5. Go to AWS management console

Go to https://console.aws.amazon.com and sign in with your AWS Management Console administrator account.

2.6. Navigate to "Security & Identity" section

Navigate to "Security & Identity" section and click on the "Identity & Access Management" item.



Security & Identity

Identity & Access Management
Manage User Access and Encryption Keys

Directory Service
Host and Manage Active Directory

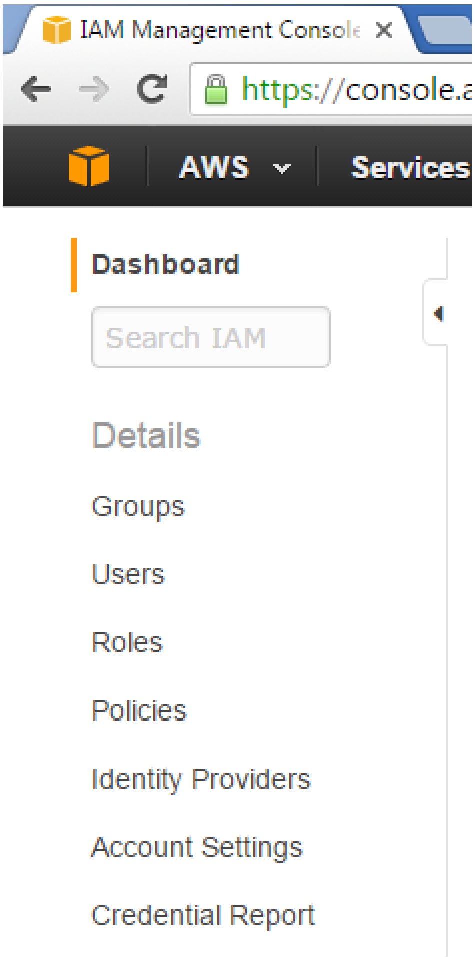
Inspector PREVIEW
Analyze Application Security

WAF
Filter Malicious Web Traffic

Certificate Manager
Provision, Manage, and Deploy SSL/TLS Certificates

2.7. Identity Providers

In the left vertical menu click "Identity Providers"

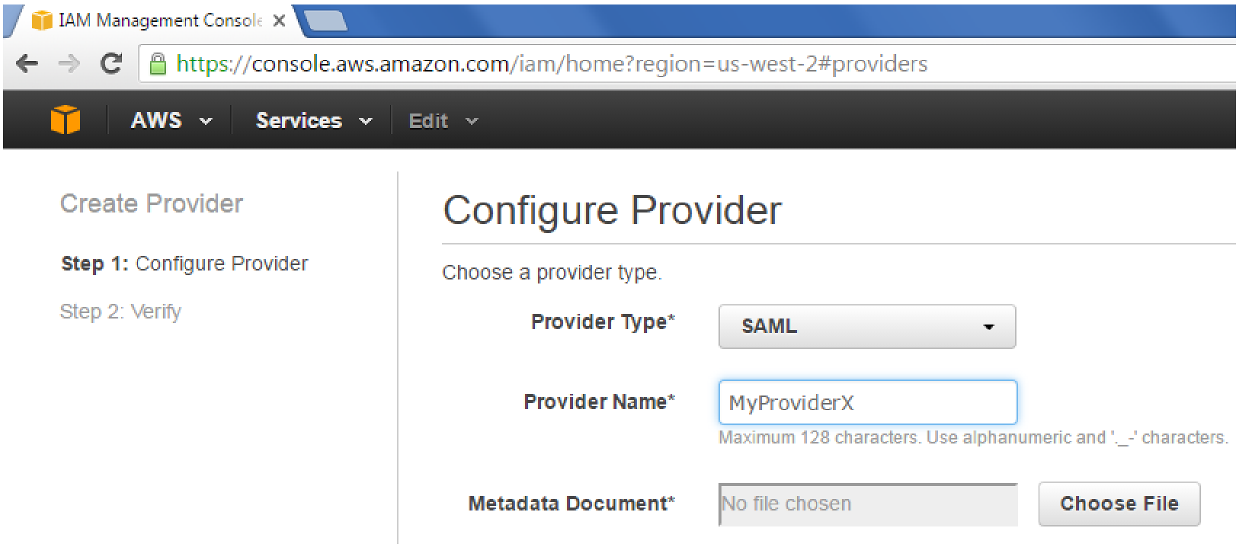


2.8. Create Provider

On the top menu click "Create Provider" button

2.9. Configure your provider

On the "Configure Provider Page" in "Provider Type" dropdown box choose "SAML" and in "Provider Name" field input your Identity Provider Name you used in MyWorkspace during AWS application creation. You can find it in MyWorkspace application Integration Guide, step 5.



https://console.aws.amazon.com/iam/home?region=us-west-2#providers

Configure Provider

Choose a provider type.

Provider Type* SAML

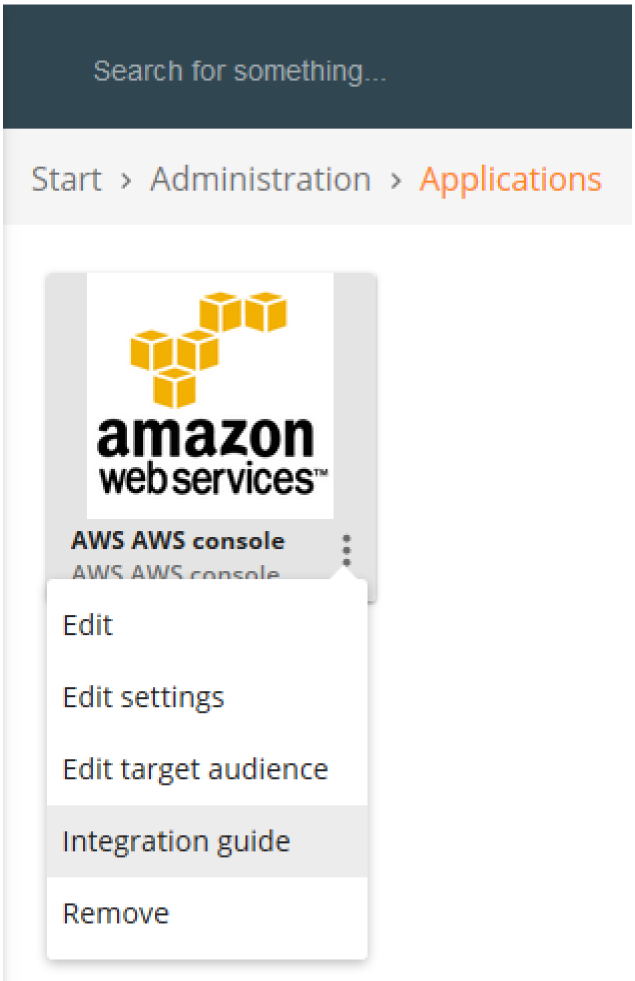
Provider Name* MyProviderX

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

Metadata Document* No file chosen

2.10. Download MyWorkspace metadata document

Choose your newly created AWS application and press ⋮ button in the right bottom corner of your application tile. Then in opened menu choose the “Integration Guide” menu item.



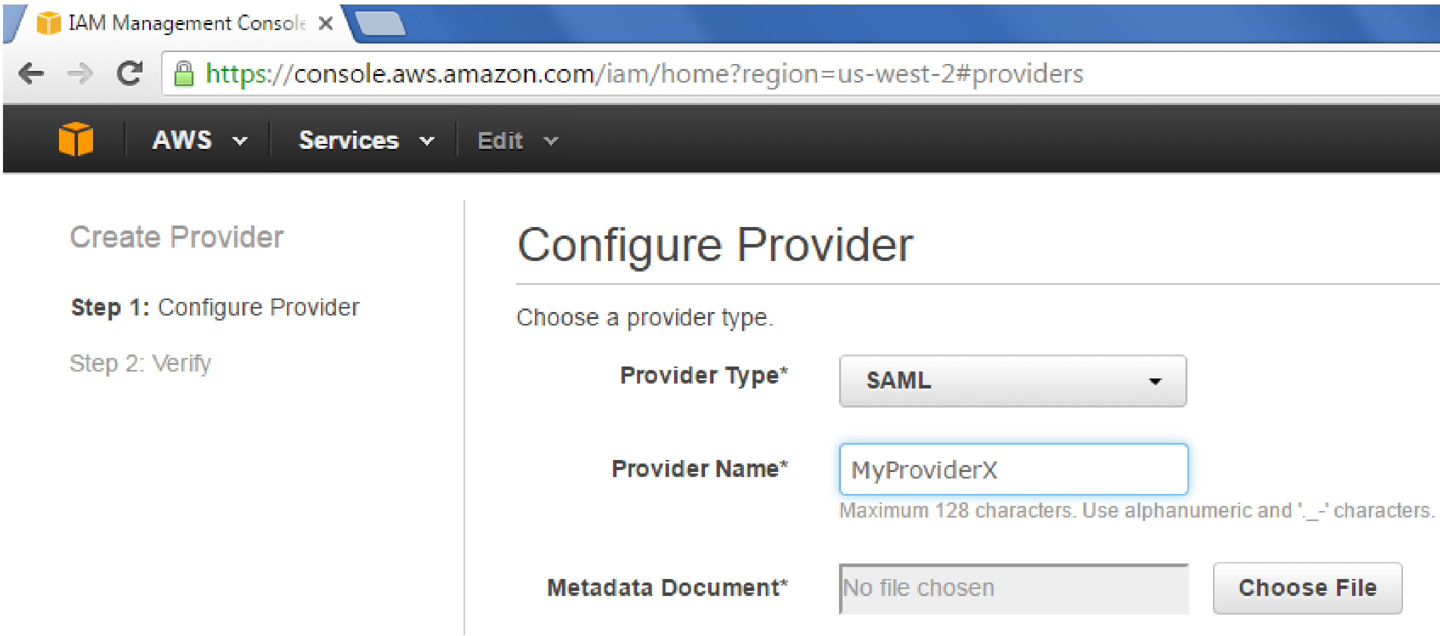
The panel with Integration Guide will be opened, then navigate to the Step 6 where you can find the dynamically generated link to the metadata document in the format:
https://accounts.matrix42.com/issue/{some-id}/saml2/metadata
Open a new browser tab and navigate by that URL to download your MyWorkspace Identity Provider application specific Metadata document (special for your AWS application).

2.11. Save metadata document

Save your application specific Metadata document on your local drive. You can do this via browser file menu, or using the option "View Source" from browser context menu.
Be careful: open saved Metadata document in any text editor and check that it doesn't contain any html styles like padding, etc. or html specific tags like div, span etc. This document should have an XML valid structure.

2.12. Upload your metadata document for AWS Identity Provider

Navigate back to your AWS Management Console.
For "Metadata Document" upload field click the button "Choose File" and choose your previously saved to your local drive Metadata document.



https://console.aws.amazon.com/iam/home?region=us-west-2#providers

Configure Provider

Choose a provider type.

Provider Type*: SAML

Provider Name*: MyProviderX

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

Metadata Document*: No file chosen

2.13. Click Next

Click "Next Step" button in the right bottom corner.

2.14. Create AWS Identity Provider

On the "Verify Provider Information" page click "Create" button. Then your provider will be created and you will see it at providers list.

2.15. Create new Role

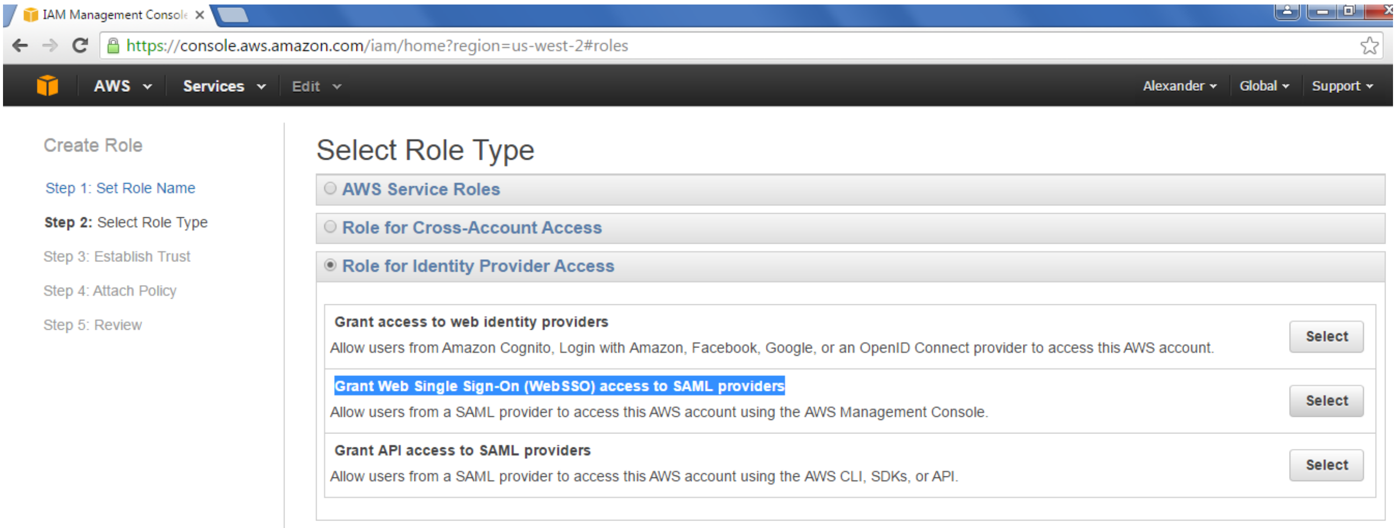
At AWS Management Console in the left navigation menu click "Roles" menu item. Then click "Create New Role" button.

2.16. Fill Role name

On the "Set Role Name" page input your Role name you used in MyWorkspace during AWS application creation. You can find exact Role Name using Integration Guide button, look at Step 12.

2.17. Select Role Type

On the "Select Role Type" page choose the "Role For Identity Provider Access" item and click "Select" button for "Grant Web Single Sign-On (WebSSO) access to SAML providers" item.



IAM Management Console
https://console.aws.amazon.com/iam/home?region=us-west-2#roles
AWS
Services
Edit
Alexander
Global
Support

Create Role

Step 1: Set Role Name

Step 2: Select Role Type

Step 3: Establish Trust

Step 4: Attach Policy

Step 5: Review

Select Role Type

○ AWS Service Roles

○ Role for Cross-Account Access

● Role for Identity Provider Access

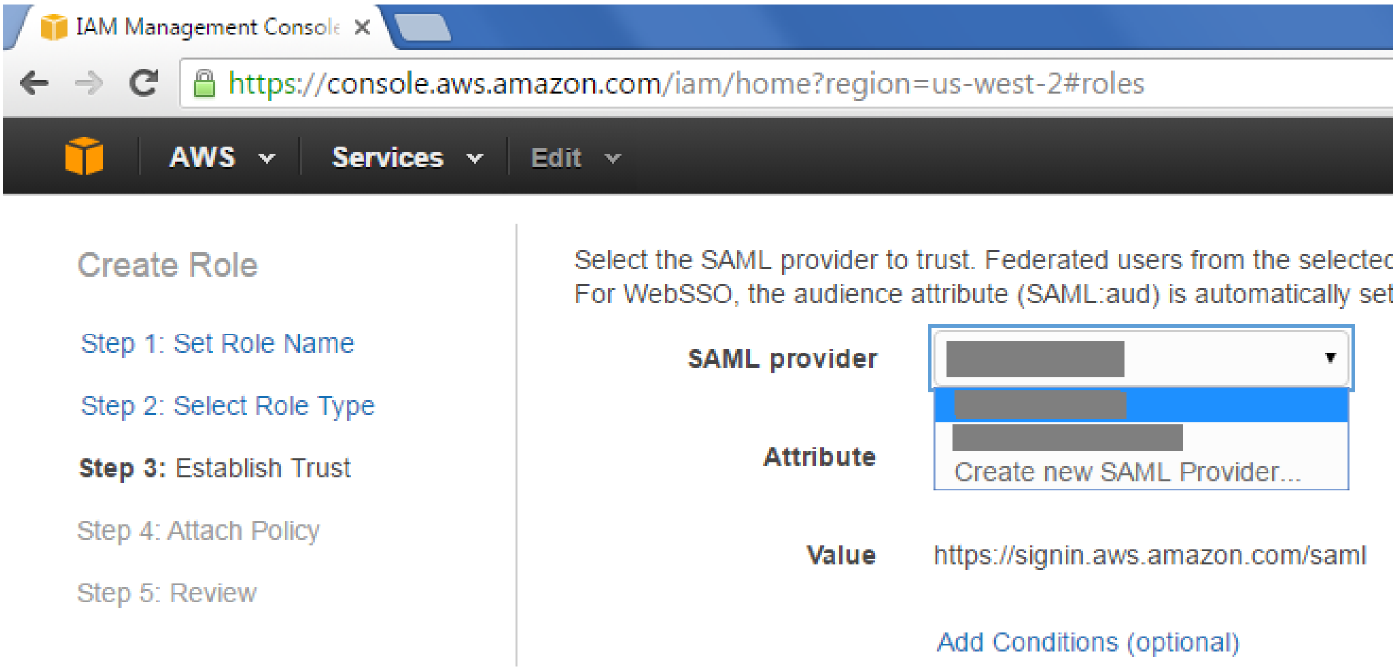
Grant access to web identity providers
Allow users from Amazon Cognito, Login with Amazon, Facebook, Google, or an OpenID Connect provider to access this AWS account. Select

Grant Web Single Sign-On (WebSSO) access to SAML providers
Allow users from a SAML provider to access this AWS account using the AWS Management Console. Select

Grant API access to SAML providers
Allow users from a SAML provider to access this AWS account using the AWS CLI, SDKs, or API. Select

2.18. Choose your Identity Provider

On the opened "Establish Trust" page choose your Identity Provider from the "SAML Provider" dropdown box and click "Next Step" button.



IAM Management Console
https://console.aws.amazon.com/iam/home?region=us-west-2#roles
AWS
Services
Edit

Create Role

Step 1: Set Role Name

Step 2: Select Role Type

Step 3: Establish Trust

Step 4: Attach Policy

Step 5: Review

Select the SAML provider to trust. Federated users from the selectec
For WebSSO, the audience attribute (SAML:aud) is automatically set

SAML provider [redacted] ▾
[redacted]
[redacted]
Create new SAML Provider...

Attribute

Value https://signin.aws.amazon.com/saml

Add Conditions (optional)

2.19. Click Next

Click "Next Step" button.

2.20. Choose the policy

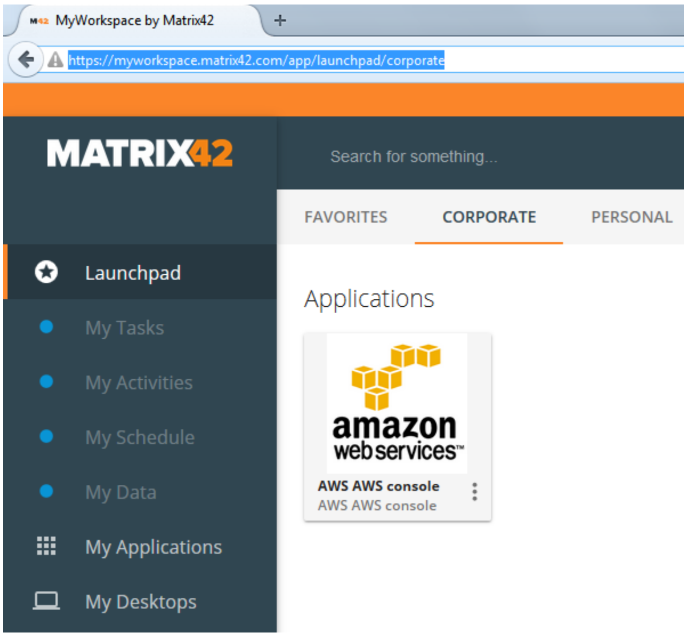
On the "Attach Policy" page attach the needed policy to that role or you can do it afterwards and for now just skip that step. Click "Next Step" button.

2.21. Role Review Page

On the "Review Page" click "Create Role" button.

2.22. Everything is completed

Everything is configured now. To test, if SSO works correctly, sign out from your AWS Management Console account and navigate to the MyWorkspace Launchpad area for Corporate applications: https://myworkspace.matrix42.com/app/launchpad/corporate and click your AWS application tile or use the launch URL provided for your application in the MyWorkspace Application Integration Guide – last step.



Matrix42 AG
Elbinger Str. 7
60487 Frankfurt
Germany

Tel.:	+49 (0)6102 - 816-0
Fax:	+49 (0)6102 - 816-100
E-Mail:	info@matrix42.com
Web:	http://www.matrix42.com