# Microsoft - Managing trust relationships with multiple business identity providers (basics)

| | |
|---|---|
| **Code:** | 55091 |
| **Length:** | 3 days |
| **URL:** | View Online |

Decoupling cloud services from all the complexity by maintaining a direct relationship with all the identity providers is the topic of this course. Each identity provider can use its own authentication protocol and the authentication results will get normalized and once established will Access Control Services (ACS) care about authentication and authorization including provisioning of a UI for the user to choose among all the recognized identity providers. Claims will be accessible for the application developer as well as for SSO IT Pros to establish easy authentication and/or authorization without the necessity to know authentication protocols in detail. Management of different and multiple business identity providers will be handled in a unique fashion without the necessity to write different code. This relationships is called normalizing attributes and will be realized by you via the Azure Management APIs.

## Skills Gained

- Establish an organizational Enterprise Security Service Bus
- Create a Relying Party
- Establish ACS to delegate authentication
- Forward every request from unauthenticated users to ACS
- Broker authentication
- Change access rules in response to programmatic events
- Produce a securable resource
- Configure and code Input and Output claims transformation
- Broker Security Token Services from Yahoo and Microsoft
- Establish a tokenized communication between Azure Namespaces and WS-Federation sign-in endpoints
- Establish a Microsoft Azure Active Directory (MAAD) as an (additional) identity provider for any application associated/interfacing with their namespace
- Create an Azure Identity Provider via Namespace association
- Establish Azure Active Directory data streams into Name Space connected Applications
- Register a MAAD Graph Database as an additional identity provider for a namespace that controls global access and SSO
- Execute basic steps to establish MAAD as an SSO identity providers for web application

## Who Can Benefit

This course is intended for Architects, IT Professional (IT Pros) and Developers. IT Professional (IT Pros) who also create software applications, build or write computer code or develop Web sites or complex macros as a secondary responsibility and Developers who create software applications, develop web sites and create complex macros. Both should have a minimum of three months programming experience in C# and have basic Visual Studio 2010 or Visual Studio 2012 or Visual Studio 2013 navigation skills as well as Architects tasked with transitioning Identity and Access from classic on-Premise or non-Azure datacenters into Microsoft Azure Cloud or tasked to build secure IaaS/PaaS Hybrids between on-premise and Microsoft Azure Cloud.

### Prerequisites

- Knowledge and Skills to accomplish a given assignment in Visual Studio when using the General Development Settings collection in Visual Studio 2010 or Visual Studio 2012 or Visual Studio 2013. There is no prerequisite nor a requirement to use a credit card to establish a Microsoft Azure Account or to have a Microsoft Azure Account at all. Every student receives one or more than one dedicated cloud service(s) in VBICs cloud based virtual classroom. Students can be virtually anywhere and at different timezones and require only a Windows based OS device to utilize their Remote Desktop Connection tool, available on all Microsoft Windows Desktop operating systems > Windows XP.

## Course Details

### Outline

Module 1: Integration of traditional ASP.NET Web Sites into Enterprise Security Service Bus (ESSB) Decoupling cloud services from all the complexity by maintaining a direct relationship with all the identity providers is the topic of this module. Each identity provider can use its own authentication protocol and the authentication results will get normalized and once established will Access Control Services (ACS) care about authentication and authorization including provisioning of a UI for the user to choose among all the recognized identity providers. Claims will be accessible for the application developer as well as for SSO ITPros to establish easy authentication and/or authorization without the necessity to know authentication protocols in detail. Management of different and multiple business identity providers will be handled in a unique fashion without the necessity to write different code. This relationships is called normalizing attributes and will be realized by you via the Azure Management APIs. Lessons

- Establish first steps to build an organizational Enterprise Security Service Bus
- Create a Relying Party
- Establish ACS to delegate authentication
- Forwarding every request from unauthenticated users to ACS
- Broker authentication
- Change access rules in response to programmatic events

Lab 1: Logon with your VBIC OA

- For this Lab has a dedicated Cloud Service in VBICs virtual cloud classroom been issued
- Every student is using his dedicated developer environment and in addition has been granted Co-administrator access privileges in VBICs Enterprise Cloud Access Suite and every student has therefore been granted an organizational account and executes this training as organizational member of VBIC.

Lab 2: First step to establish an organizational Enterprise Security Service Bus

- Create a new Microsoft Azure Service Namespace
- Base this namespace inside of a selected region
- Scope this namespace global for planetary validity and reach

Lab 3: ACS to delegate authentication

- Removal of pre-COA (Cloud Oriented Architecture) pattern from a standard WEB Site project
- Apply standard procedures aimed to establish Access Control Services (ACS) as a broker service
- Design this service to handle authentication and authorization, including provisioning of a UI for the user to choose among all

the recognized identity providers

Lab 4: Relying Party

- Identity terms used in the ACS Management Portal referencing items in the Microsoft Azure Management Portal
- Binding and bridging IaaS/PaaS items from the Microsoft Azure Management Portal with PaaS/SaaS items from the ACS Management Portal
- Create an identity consuming Relying Party that is an identity term for a cloud service, a term in the Microsoft Azure Management Portal for a PaaS component encapsulating IaaS components
- Storage of identities and services capable to authenticate users
- Creation of Identity Provider
- Design ACS namespaces to interface with more than one storage or authentication services for users
- Reuse of pre-factored URIs to integrate multiple identity providers into your cloud service for authentication and authorization purposes

Lab 5: Forwarding every request from unauthenticated users to ACS

- Establish WS-Federation Metadata endpoints
- Create a document interface describing the WS-Federation STS that ACS exposes in a Microsoft Azure namespace
- Program that every authentication request will be forwarded to Azure ACS and to return to the application you currently program, e.g. a Web Site
- Execution of a combination of tasks shared between ITPro and Developer
- Design functional workflows between Microsoft Azure IaaS and Microsoft Azure PaaS

Lab 6: Brokering authentication

- Configure the ACS management portal to provide a variety of multiple identity provider (IP)
- Configuration of multiple and parallel IP interfaces to ACS
- Establish management and direct binding between Users, Azure Cloud Services and Identity provider Interface
- Provide public brokering services between IPs and Cloud Services
- Add Identity providers as IaaS via Microsoft Azure Management Portals well as PaaS programmatically via Visual Studio (VSTO) while both are brokered by Azure Access Control Services
- Configure transformation of Claims input before it reaches the final recipient; the relying application.
- Create and edit rule groups manually using the ACS Management Portal and programmatically via (VST)

Lab 7: Change access rules in response to programmatic events

- Create and edit rule groups no longer manually using the ACS Management Portal but programmatically
- Reapply steps learned by utilizing configuration in ACS Management Portal now via code and programming the ACS Management Service
- Create a dedicated interface for a programmatic approach and secure it with a password

After completing this module, students will be able to:

- Hands on create first steps in order to establish an organizational Enterprise Security Service Bus
- Create a Relying Party
- Establish ACS to delegate authentication
- Forward every request from unauthenticated users to ACS
- Broker authentication

- Change access rules in response to programmatic events

Module 2: Integration of public identity provider into Enterprise Security Service Bus (ESSB) Advanced procedures aimed to decouple cloud service from all the complexity while maintaining a direct relationship with a multiplicity of identity providers is the core learning unit of this module. Any identity provider can use its own authentication protocol and the authentication results will get normalized and once established will Access Control Services ACS care about authentication and authorization, including providing a UI for the user of this multiple identity SSO system enabling them to choose among all the Azure recognized identity providers. Claims will be accessible for the developer to establish easy authorization without the necessity to know authentication protocols in detail. Management of different and multiple business identity providers will be handled in a unique fashion without the necessity to write different code. This relationship is called normalizing attributes and will be realized by you via the Microsoft Azure Portal and the management API. In addition to the exercise already executed that did provide know how to integrate business directories into a Federate Identity meshwork will you now do a selection of the very same steps to task Microsoft Azure to serve users coming from Facebook or Microsoft Live ID if they want to use your web site. Lessons

- Hands-on establish advanced steps to create an organizational Enterprise Security Service Bus
- Create a Relying Party
- Establish ACS to delegate authentication
- Forwarding every request from unauthenticated users to ACS

Lab 1: Produce a securable resource

- Create a simple cloud service
- Interface a cloud service with multiplicity of identity provider
- Decoupled a cloud service from all the complexity of having to maintaining a direct relationship with a multiplicity of identity provider

Lab 2: Logon with your VBIC OA

- For this Lab has a new dedicated Cloud Service in VBICs virtual cloud classroom been issued
- Every student is using his dedicated developer environment and in addition has been granted Co-administrator access privileges in VBICs Enterprise Cloud Access Suite and every student has therefore been granted an organizational account and executes this training as organizational member of VBIC.

Lab 3: Input and Output claims transformation

- Configure claims input coming from Yahoo and Microsoft IDs into ACS
- Transformed input to output claims
- Configure delivery of transformed output claims towards your relying party application

Lab 4: Brokering Security Token Services from Yahoo and Microsoft

- Establish trust relationship between your claims-aware application and the Azure Access Control Services
- Establish ACS as a trusted Brokering Service between Microsoft Azure, Yahoo and Microsoft

After completing this module, students will be able to:

- First step to establish an organizational Enterprise Security Service Bus
- Create a Relying Party
- Establish ACS to delegate authentication
- Forwarding every request from unauthenticated users to ACS

Module 3: Develop and publish applications that integrate with Microsoft Azure Active Directory (MAAD) In this module a pre-existing Microsoft Azure Active Directory (MAAD) repository is available in VBICs virtual classroom, consisting of users to be interfaced to a namespace and released for application to be linked to this Access Control namespace. As a result will the Microsoft Azure Active Directory be available as an (additional) identity provider for any application associated/interfacing with this namespace. Applications that are connected to your access control namespace become interfaced with the VBIC provided Microsoft Azure Active Directory (MAAD). MAAD generated tokens will be transformed into ACS tokens, available for authentication and authorization purposes for user identities, application identities and data identities. Youll define the recipient for the success token, signaling a positive authentication event, as a URL address, parameterized as an App. Youll further define countermeasure preventing man-in-the-middle attacks by defining the App ID URI, by utilizing a control parameter that has to be delivered with the MAAD token. The MAAD user token must be delivered in conjunction with the entityID of the Access Control namespace, otherwise ACS would interpret it as a token reused from a man-in-the-middle attack. As ACS does not call the Graph API is there no SSO with read or write access to MAAD at all, just MAAD providing additional identities via token, based on a fixed selection in ACS. Calling MAAD Graph API and establishing a global SSO and a multitenant Single Sign-Up read or write access to MAAD is covered in Course 55086AC - Enterprise SSO - cloud audited deployment for distributed onsite-offsite development. Lessons

- Establish a tokenized communication between Azure Namespaces and WS-Federation sign-in endpoints
- Establish a Microsoft Azure Active Directory (MAAD) as an (additional) identity provider for any application associated/interfacing with your namespace

Lab 1: Logon with your VBIC OA

- For this Lab has a new dedicated Cloud Service in VBICs virtual cloud classroom been issued
- Every student is using his dedicated developer environment and in addition has been granted Co-administrator access privileges in VBICs Enterprise Cloud Access Suite and every student has therefore been granted an organizational account and executes this training as organizational member of VBIC.

Lab 2: Azure Identity Provider via Namespace association

- Interface with a pre-existing Microsoft Azure Active Directory (MAAD) repository
- Bind users of MAAD to a namespace
- Released binding as an application to be linked to this Access Control namespace
- Configure Microsoft Azure Active Directory as an (additional) identity provider for any application associated/interfacing with this namespace

Lab 3: Establish Azure Active Directory data streams into Name Space connected Applications

- Program and configure a generic interface aimed that all applications developed so far connect to your access control namespace and become interfaced with the VBIC provided Microsoft Azure Active Directory (MAAD)
- Transform MAAD generated tokens into ACS tokens, available for authentication and authorization purposes for user identities, application identities and data identities
- Define the recipient for the success token, signaling a positive authentication event, as a URL address, parameterized as an App
- Define countermeasures preventing man-in-the-middle attacks by defining the App ID URI and by utilizing a control parameter that has to be delivered with the MAAD token
- Configure and code man-in-the-middle countermeasures
- Design MAAD to provide additional identities via token based on a fixed selection in ACS as an alternative to complex SSO setups

Lab 4: MAAD Graph Database registration as an additional identity provider for your namespace that controls global access and SSO

- Configure a customized selection
- Establish an additional security token service (STS) as an additional Identity Provider
- Bind a custom STS to MAAD
- Bind MAAD to a custom STS and establish a customized STS selection as MAAD claims identity

Lab 5: MAAD identity providers as SSO for web application

- Use MAAD as part of all other registered identity provider for the Access Control namespace
- Utilize operational standard procedures to execute and showcase MAAD selection during development of a web app
- Execute operational procedures for Key Management required between Azure and Visual Studio in order to associate the app with your Access Control namespace

After completing this module, students will be able to:

- Establish a tokenized communication between Azure Namespaces and WS-Federation sign-in endpoints
- Establish Microsoft Azure Active Directory (MAAD) as an (additional) identity provider for any application associated/interfacing with their namespace

Module 4: Assessment (if time permits): Add French, German, English and Italian as a multilingual integration of traditional ASP.NET Web Sites into your Enterprise Security Service Bus (ESSB) Add French, German, English and Italian as a multilingual integration of traditional ASP.NET Web Sites into your Enterprise Security Service Bus (ESSB) Lessons

- Code a multilingual Enterprise Security Service Bus (ESSB)

Lab 1: Logon with your VBIC OA

- For this Lab has a new dedicated Cloud Service in VBICs virtual cloud classroom been issued
- Every student is using his dedicated developer environment and in addition has been granted Co-administrator access privileges in VBICs Enterprise Cloud Access Suite and every student has therefore been granted an organizational account and executes this training as organizational member of VBIC.

Lab 2: Repeat Module 1 from Step 1 until step 146

- Repeat Module 1 from Step 1 until step 146

Lab 3: Modify Module 1 so your ESSB becomes multilingual and supports local STS claims originating from Italian, French, German and English office locations or customers in these countries.

- Modify Module 1 so your ESSB becomes multilingual and supports local STS claims originating from Italian, French, German and English office locations or customers in these countries.

Lab 4: Task 4: Inform your instructor and VBIC Help Desk (info@vbic.net) if you have reached step 146 while accomplished Lab 3. Logout and close your RDP session.

- Task 4: Inform your instructor and VBIC Help Desk (info@vbic.net) if you have reached step 146 while accomplished Lab 3. Logout and close your RDP session.

After completing this module, students will be able to:

- The Assessment is only optional, only if time permits, voluntary at the discretion of the student and does not have a solution folder as there are many ways to achieve the to be assessed target of evaluation and is subject of evaluation by instructor or VBIC staff
- If assessment is taken by students will student receive either an assessment from instructor about assessment passing during class or will receive a follow up email for assessment validation result from/by VBIC staff, 5 days after last day of class.