

AD FS implementacija i administracija

7. PREDAVANJE



Algebra

visoka škola za
primijenjeno računarstvo

Module Overview

- Overview of AD FS
- Deploying AD FS
- Implementing AD FS for a Single Organization
- Deploying AD FS in a Business-to-Business Federation Scenario
- Extending AD FS to External Clients



Algebra

visoka škola za
primijenjeno računarstvo

Lesson 1: Overview of AD FS

- What Is Identity Federation?
- What Is Claims-Based Identity?
- Web Services Overview
- What Is AD FS?
- How AD FS Enables SSO in a Single Organization
- How AD FS Enables SSO in a Business-to-Business Federation
- How AD FS Enables SSO with Online Services
- What Is New in Windows Server 2012 R2



Algebra

visoka škola za
primijenjeno računarstvo

Identity federation: *What Is Identity Federation?*

- Enables identification, authentication, and authorization across organizational and platform boundaries
- Requires a federated trust relationship between two organizations or entities
- Enables organizations to retain control over who can access resources
- Enables organizations to retain control of their user and group accounts

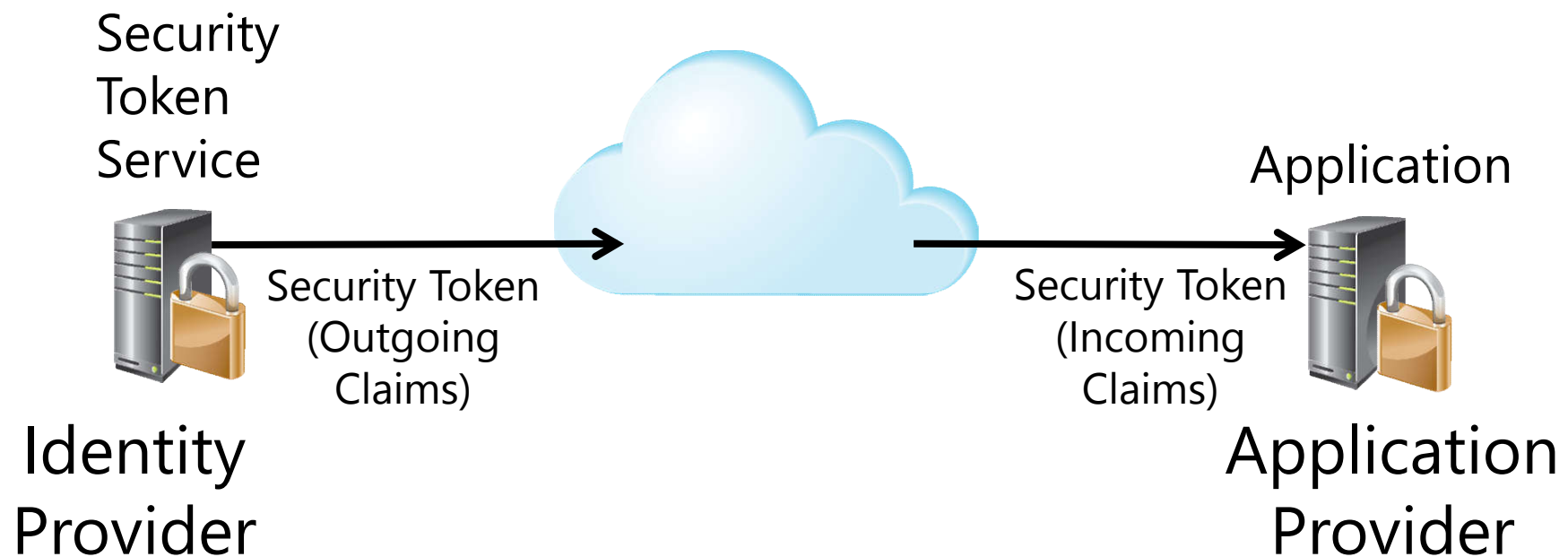


Algebra

visoka škola za
primijenjeno računarstvo

What Is Claims-Based Identity?

- Claims provide information about users
- Information is provided by the user's identity provider, and is accepted by the application provider



Algebra

visoka škola za
primijenjeno računarstvo

Web Services Overview

Web services are a standardized set of specifications used to build applications and services

Web services typically:

- Transmit data as XML
- Use SOAP to define the XML message format
- Use WSDL to define valid SOAP messages
- Use UDDI to describe available web services

SAML is a standard for exchanging identity claims



Algebra

visoka škola za
primijenjeno računarstvo

What Is AD FS?

AD FS is the Microsoft identity federation product that can use claim-based authentication

AD FS has the following features:

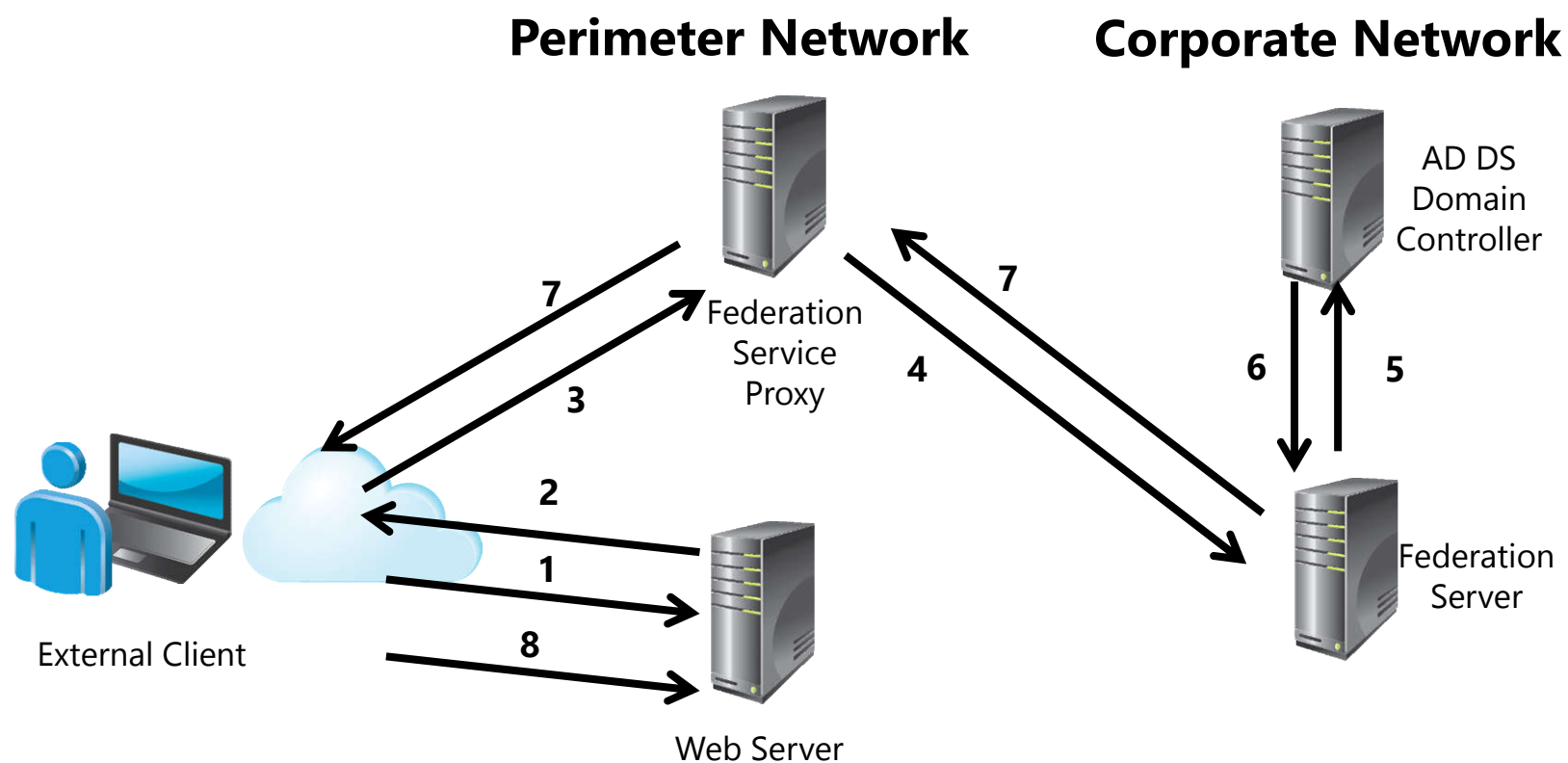
- SSO for web-based applications
- Interoperability with web services on multiple platforms
- Support for many clients, such as web browsers, mobile devices, and applications
- Extensibility to support customized claims from third-party applications
- Delegation of account management to the user's organization
- Integration with DAC
- Windows PowerShell cmdlets for administration



Algebra

visoka škola za
primijenjeno računarstvo

How AD FS Enables SSO in a Single Organization



Algebra
visoka škola za
primijenjeno računarstvo

visoka škola za
primijenjeno računarstvo

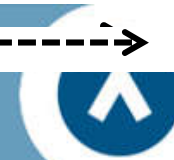
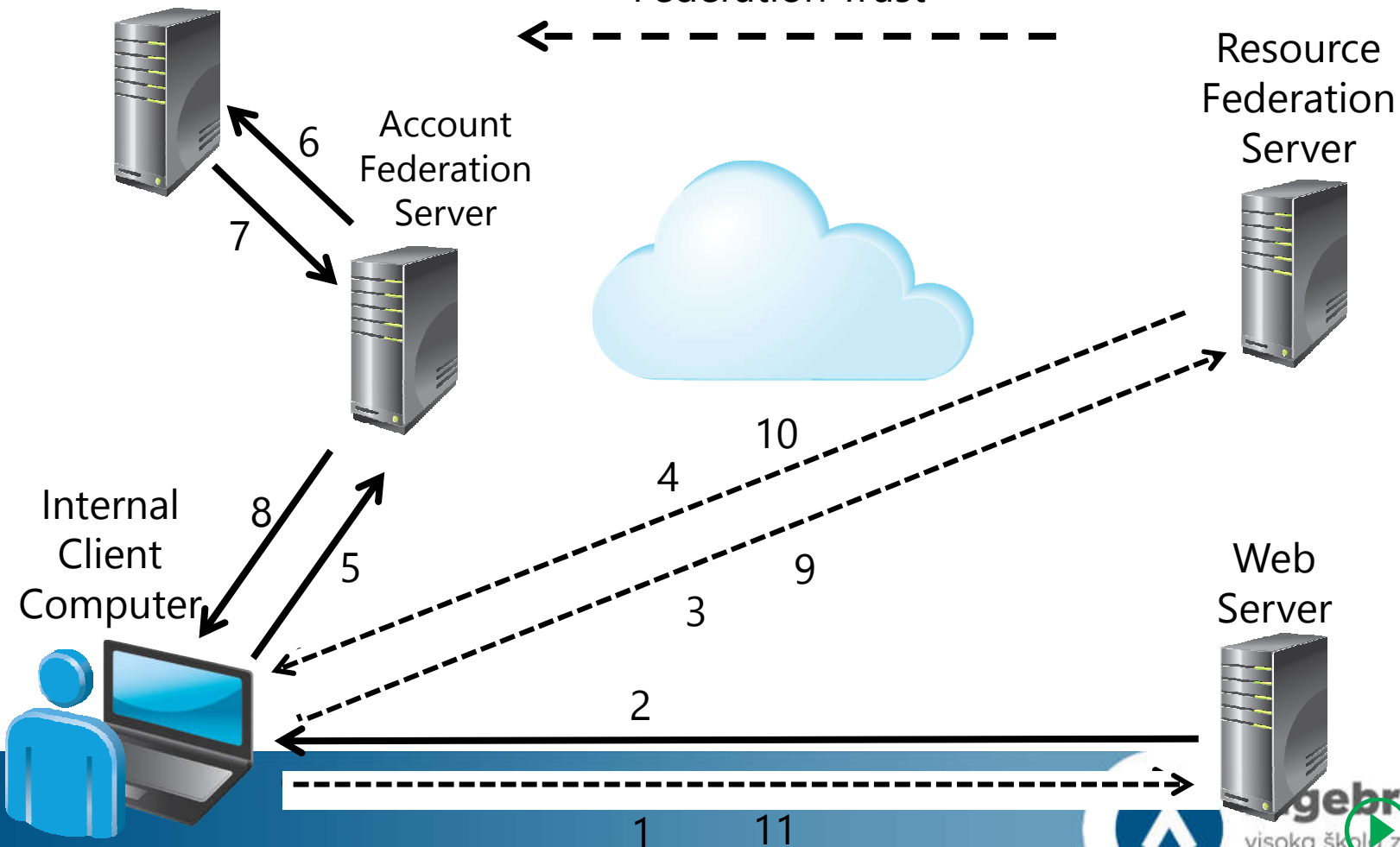
How AD FS Enables SSO in a Business-to-Business Scenario

Trey Research

A. Datum

AD DS

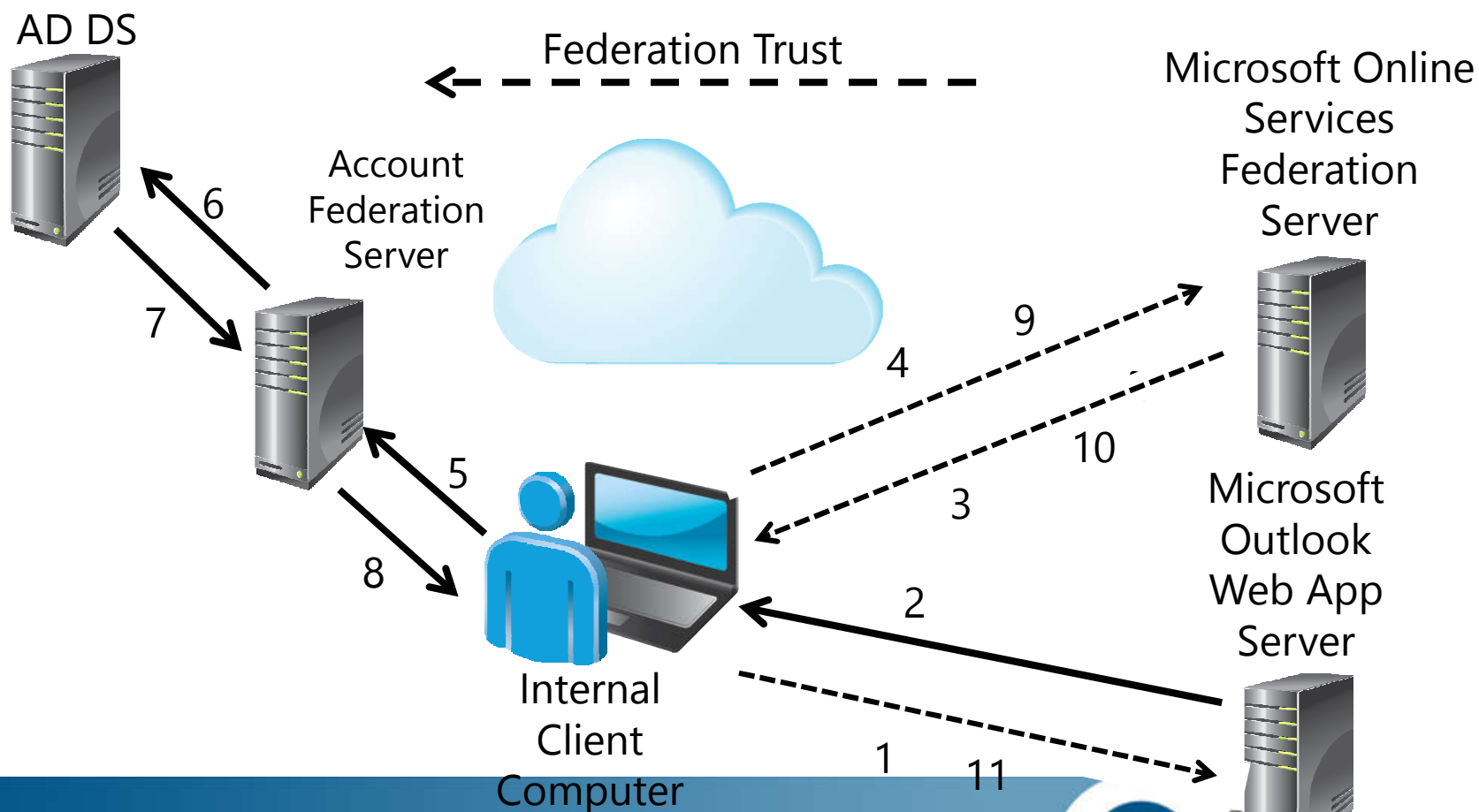
Federation Trust



How AD FS Enables SSO with Online Services

On-Premises

Microsoft Exchange Online



AMRI
visoka škola za
primijenjeno računarstvo

What Is New in Windows Server 2012 R2

- Installation:
 - No IIS 8.5 required
 - Can install on domain controllers
- Enhanced authentication:
 - Authentication policies with scope
 - Multifactor authentication
- New claims types:
 - Mostly device and certificate related
- Web Application Proxy:
 - Provides secure remote access to web-based applications
 - Replaces AD FS proxy



Algebra

visoka škola za
primijenjeno računarstvo

Lesson 2: Deploying AD FS

- AD FS Components
- AD FS Prerequisites
- PKI and Certificate Requirements
- Federation Server Roles
- Demonstration: Installing the AD FS Server Role



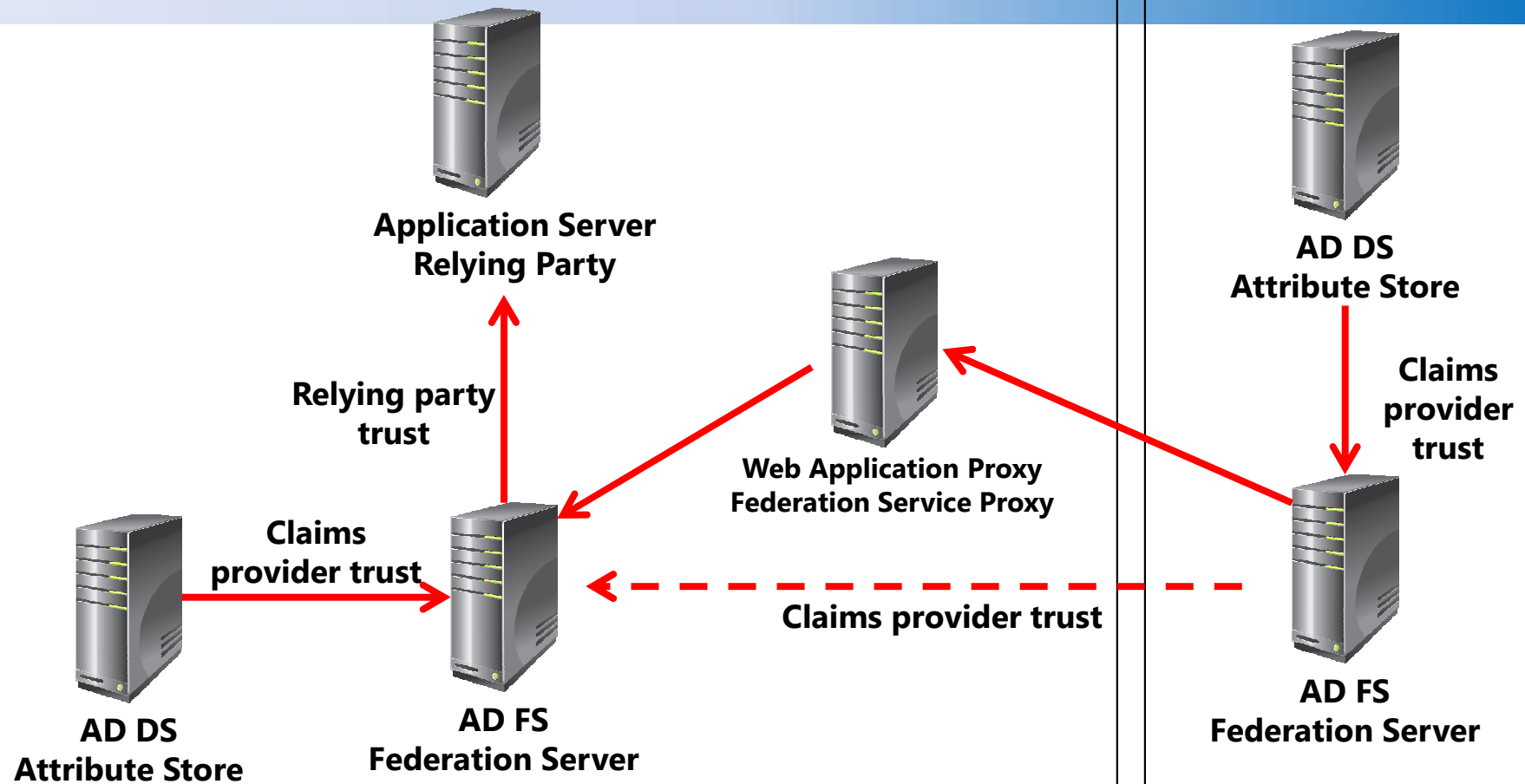
Algebra

visoka škola za
primijenjeno računarstvo

AD FS Components

Internal Network

Partner Network



AD FS Prerequisites

Successful AD FS deployment includes the following critical infrastructure:

- TCP/IP network connectivity
- AD DS
- Attribute stores
- DNS
- Compatible operating systems

Installation changes in Windows Server 2012 R2:

- IIS is not required
- No AD FS stand-alone server option



Algebra

visoka škola za
primijenjeno računarstvo

PKI and Certificate Requirements

Certificates used by AD FS:

- Service communication certificates
- Token-signing certificates
- Token-decrypting certificates

When choosing certificates, ensure that the service communication certificate is trusted by all federation partners and clients

If you use an internal CA then users must have access to certificate revocation information



Algebra

visoka škola za
primijenjeno računarstvo

Federation Server Roles

Claims provider federation server:

- Authenticates internal users
- Issues signed tokens containing user claims

Relying party federation server:

- Consumes tokens from the claims provider
- Issues tokens for application access

Federation server proxy:

- Is deployed in a perimeter network
- Provides a layer of security for internal federation servers



Algebra

visoka škola za
primijenjeno računarstvo

Demonstration: Installing the AD FS Server Role

- In this demonstration, you will see how to install and configure the AD FS server role



Algebra

visoka škola za
primijenjeno računarstvo



Algebra

visoka škola za
primijenjeno računarstvo

Lesson 3: Implementing AD FS for a Single Organization

- What Are AD FS Claims?
- What Are AD FS Claim Rules?
- What Is a Claims-Provider Trust?
- What Is a Relying-Party Trust?
- Demonstration: Configuring Claims Provider and Relying Party Trusts
- What Are Authentication Policies?
- What Is Multifactor Authentication?



Algebra

visoka škola za
primijenjeno računarstvo

What Are AD FS Claims?

Claims provide information about users from the claims provider to the relying party

AD FS:

- Provides a default set of built-in claims
- Enables the creation of custom claims
- Requires that each claim have a unique URI

Claims can be:

- Retrieved from an attribute store
- Calculated based on retrieved values
- Transformed into alternate values



Algebra

visoka škola za
primijenjeno računarstvo

What Are AD FS Claim Rules?

- Claim rules define how claims are sent and consumed by AD FS servers
- Claims provider rules are acceptance transform rules
- Relying party rules can be:
 - Issuance transform rules
 - Issuance authorization rules
 - Delegation authorization rules
- AD FS servers provide default claim rules, templates, and a syntax for creating custom claim rules



Algebra

visoka škola za
primijenjeno računarstvo

What Is a Claims-Provider Trust?

Claims provider trusts:

- Are configured on the relying party federation server
- Identify the claims provider
- Configure the claim rules for the claims provider

In a single-organization scenario, a claims provider trust called Active Directory defines how AD DS user credentials are processed

Additional claims provider trusts can be configured by:

- Importing the federation metadata
- Importing a configuration file
- Configuring the trust manually



Algebra

visoka škola za
primijenjeno računarstvo

What Is a Relying-Party Trust?

Relying party trusts:

- Are configured on the claims provider federation server
- Identify the relying party
- Configure the claim rules for the relying party

In a single-organization scenario, a relying party trust defines the connection to internal applications

Additional relying party trusts can be configured by:

- Importing the federation metadata
- Importing a configuration file
- Manually configuring the trust



Algebra

visoka škola za
primijenjeno računarstvo

Demonstration: Configuring Claims Provider and Relying Party Trusts

- In this demonstration, you will see how to:
 - Configure a claims provider trust
 - Configure a certificate for a web-based app
 - Configure a WIF application for AD FS
 - Configure a relying party trust



Algebra

visoka škola za
primijenjeno računarstvo



Algebra

visoka škola za
primijenjeno računarstvo



Algebra

visoka škola za
primijenjeno računarstvo



Algebra

visoka škola za
primijenjeno računarstvo

What Are Authentication Policies?

Authentication methods can be configured for the intranet or extranet

- Windows authentication
- Forms authentication
- Certificate authentication



Algebra

visoka škola za
primijenjeno računarstvo

What Is Multifactor Authentication?

Multifactor authentication requires an additional factor for authentication

- Certificate authentication or third-party vendors

Multifactor authentication can apply to:

- Specific users or groups
- Registered or unregistered devices
- Intranet or extranet

Windows Azure Multi-Factor Authentication uses the following:

- Phone calls
- Text messages
- Mobile App



Algebra

visoka škola za
primijenjeno računarstvo

Lab A: Implementing AD FS

- Exercise 1: Installing and Configuring AD FS
- Exercise 2: Configuring an Internal Application for AD FS

Logon Information

Virtual machines: 20412D-LON-DC1,
20412D-LON-SVR1, 20412D-LON-CL1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Estimated Time: 30 minutes



Algebra

visoka škola za
primijenjeno računarstvo

Lab Scenario

A. Datum Corporation has set up a variety of business relationships with other companies and customers. Some of these partner companies and customers must access business applications that are running on the A. Datum network. The business groups at A. Datum want to provide a maximum level of functionality and access to these companies. The Security and Operations departments want to ensure that the partners and customers can access only the resources to which they require access, and that implementing the solution does not increase the workload for the Operations team significantly. A. Datum also is working on migrating some parts of its network infrastructure to Microsoft Online Services, including Windows Azure and Office 365.



Algebra

visoka škola za
primijenjeno računarstvo

Lab Scenario

To meet these business requirements, A. Datum plans to implement AD FS. In the initial deployment, the company plans to use AD FS to implement SSO for internal users who access an application on a Web server.

As one of the senior network administrators at A. Datum, it is your responsibility to implement the AD FS solution. As a proof-of-concept, you plan to deploy a sample claims-aware application, and you will configure AD FS to enable internal users to access the application.



Algebra

visoka škola za
primijenjeno računarstvo

Lab Review

- Why was it important to configure adfs.adatum.com to use as a host name for the AD FS service?
- How can you test whether AD FS is functioning properly?



Algebra

visoka škola za
primijenjeno računarstvo

Lesson 4: Deploying AD FS in a Business-to-Business Federation Scenario

- Configuring an Account Partner
- Configuring a Resource Partner
- Configuring Claims Rules for Business-to-Business Scenarios
- How Home Realm Discovery Works
- Demonstration: Configuring Claim Rules



Algebra

visoka škola za
primijenjeno računarstvo

Configuring an Account Partner

An account partner is a claims provider in a business to business federation scenario

To configure an account partner:

1. Implement the physical topology
2. Add an attribute store
3. Configure a relying party trust
4. Add a claim description
5. Prepare client computers for federation



Algebra

visoka škola za
primijenjeno računarstvo

Configuring a Resource Partner

A resource partner is a relying party in a business-to-business federation scenario

To configure an relying partner:

1. Implement the physical topology
2. Add an attribute store
3. Configure a claims provider trust
4. Create claim rule sets for the claims provider trust



Algebra

visoka škola za
primijenjeno računarstvo

Configuring Claims Rules for Business-to-Business Scenarios

Business to business scenarios may require more complex claims rules

You can create claims rules by using the following templates:

- Send LDAP Attributes as Claims
- Send Group Membership as a Claim
- Pass Through or Filter an Incoming Claim
- Transform an Incoming Claim
- Permit or Deny Users Based on an Incoming Claim

You can also create custom rules by using the AD FS claim rule language



Algebra

visoka škola za
primijenjeno računarstvo

How Home Realm Discovery Works

Home realm discovery identifies the AD FS server responsible for providing claims about a user

There are two methods for home realm discovery:

- Prompt users during their first authentication
- Include a WHR string in the application URL

SAML applications can use a preconfigured profile for home realm discovery



Algebra

visoka škola za
primijenjeno računarstvo

Demonstration: Configuring Claim Rules

- In this demonstration, you will see how to configure claim rules



Algebra

visoka škola za
primijenjeno računarstvo



Algebra

visoka škola za
primijenjeno računarstvo

Lesson 5: Extending AD FS to External Clients

- What Is Web Application Proxy?
- Publishing an Application in Web Application Proxy
- Web Application Proxy and AD FS
- Demonstration: Installing and Configuring Web Application Proxy
- What Is Workplace Join?
- The Workplace Join Process
- Performing a Workplace Join



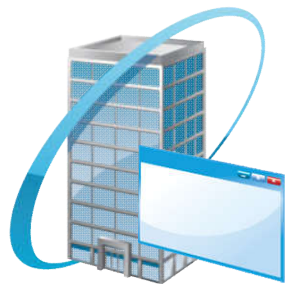
Algebra

visoka škola za
primijenjeno računarstvo

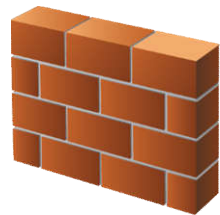
What Is Web Application Proxy?

Web Application Proxy:

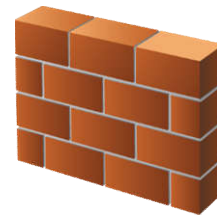
- Increases security for web-based applications and AD FS
- Is placed in a perimeter network
- Drops invalid requests
- Is independent of the web server software being used
- Is new in Windows Server 2012 R2



Intranet Application



Web Application Proxy



Internet



Algebra

visoka škola za
primijenjeno računarstvo

Publishing an Application in Web Application Proxy

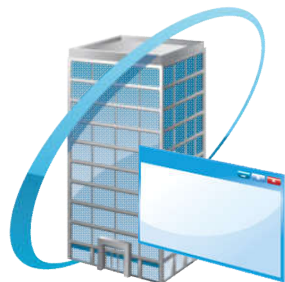
- Preauthentication options:

- Pass-through
- AD FS

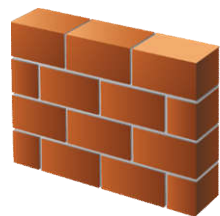
- URLs:

- External
- Backend server

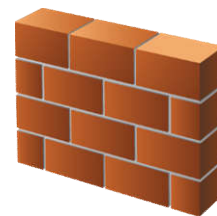
- Certificates



Intranet Application



Web Application Proxy



Internet



Algebra

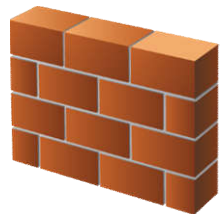
visoka škola za
primijenjeno računarstvo

Web Application Proxy and AD FS

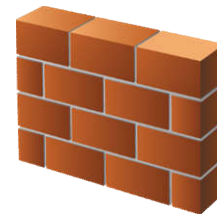
- Web Application Proxy includes federation service proxy functionality
- The same certificate is used on the AD FS server and Web Application Proxy
- Split DNS allows the same name to resolve to different IP addresses



AD FS Server
adfs.adatum.com
172.16.0.21



Web Application Proxy
adfs.adatum.com
10.10.0.100



Internet



Algebra

visoka škola za
primijenjeno računarstvo

Demonstration: Installing and Configuring Web Application Proxy

- In this demonstration, you will see how to:
 - Install Web Application Proxy
 - Export the certificate from the AD FS server
 - Import the certificate to the Web Application Proxy server
 - Configure Web Application Proxy



Algebra

visoka škola za
primijenjeno računarstvo



Algebra

visoka škola za
primijenjeno računarstvo



Algebra

visoka škola za
primijenjeno računarstvo



Algebra

visoka škola za
primijenjeno računarstvo

What Is Workplace Join?

Workplace Join:

- Creates an object in AD DS for non-domain joined devices
- Works with Windows 8.1 and iOS devices
- Can control access to claims-aware applications
- Enables SSO for application access

Enabling Workplace Join

1. Enable-AdfsDeviceRegistration –PrepareActiveDirectory
2. Enable-AdfsDeviceRegistration
3. Enable Device Authentication in AD FS



Algebra

visoka škola za
primijenjeno računarstvo

The Workplace Join Process

To perform a Workplace Join the service communication certificate for AD FS must be trusted by devices

Devices running Windows:

- Require a UPN for authentication
- Access by using enterpriseregistration.upndomainname.com

Devices running iOS use Safari to install a configuration profile

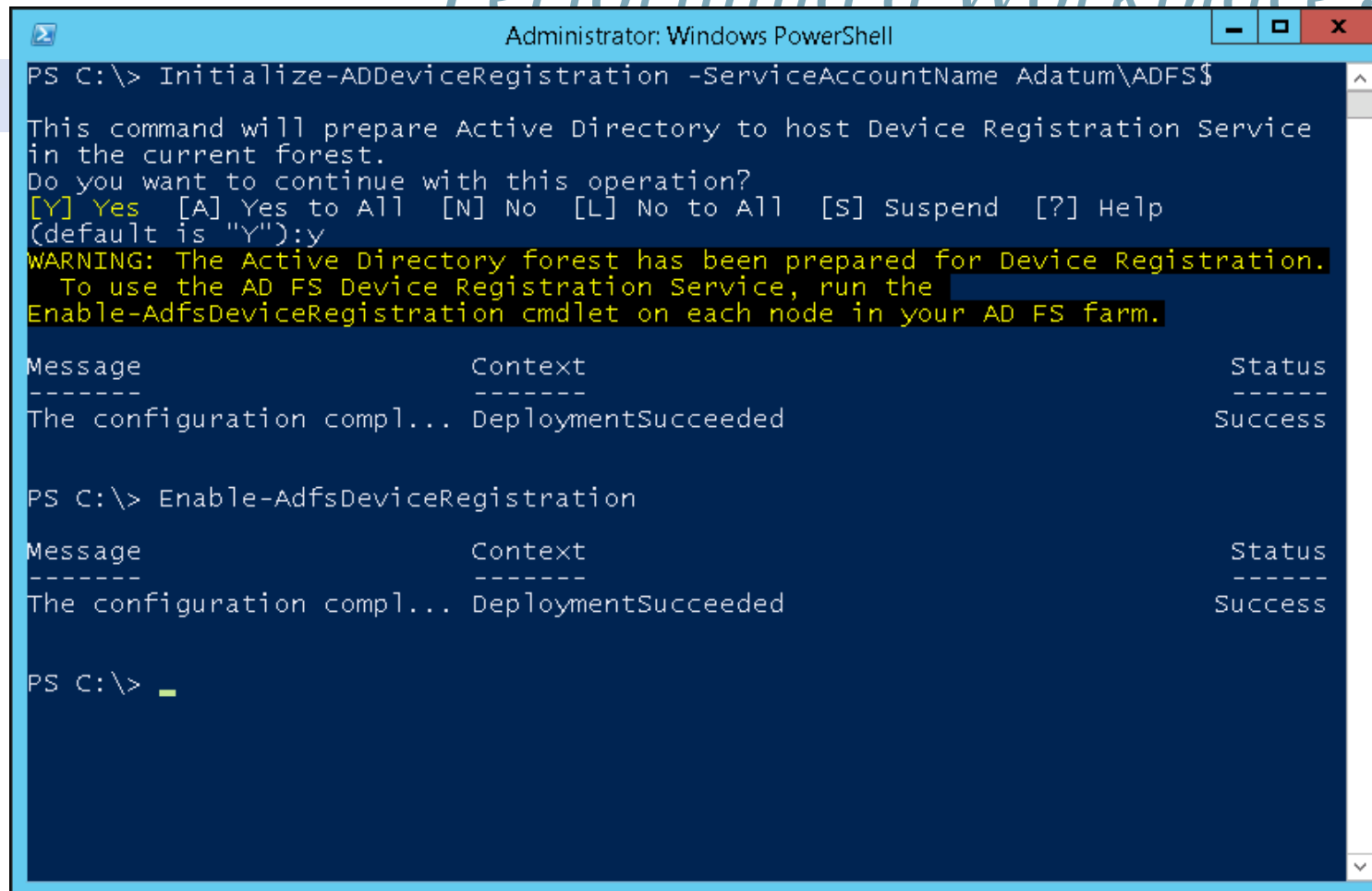
A certificate is placed on the device for authentication



Algebra

visoka škola za
primijenjeno računarstvo

Performing a Workplace Join



```
Administrator: Windows PowerShell
PS C:\> Initialize-ADDeviceRegistration -ServiceAccountName Adatum\ADFS$

This command will prepare Active Directory to host Device Registration Service
in the current forest.
Do you want to continue with this operation?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):y
WARNING: The Active Directory forest has been prepared for Device Registration.
To use the AD FS Device Registration Service, run the
Enable-AdfsDeviceRegistration cmdlet on each node in your AD FS farm.

Message                Context                Status
-----                -
The configuration compl... DeploymentSucceeded Success

PS C:\> Enable-AdfsDeviceRegistration

Message                Context                Status
-----                -
The configuration compl... DeploymentSucceeded Success

PS C:\> _
```

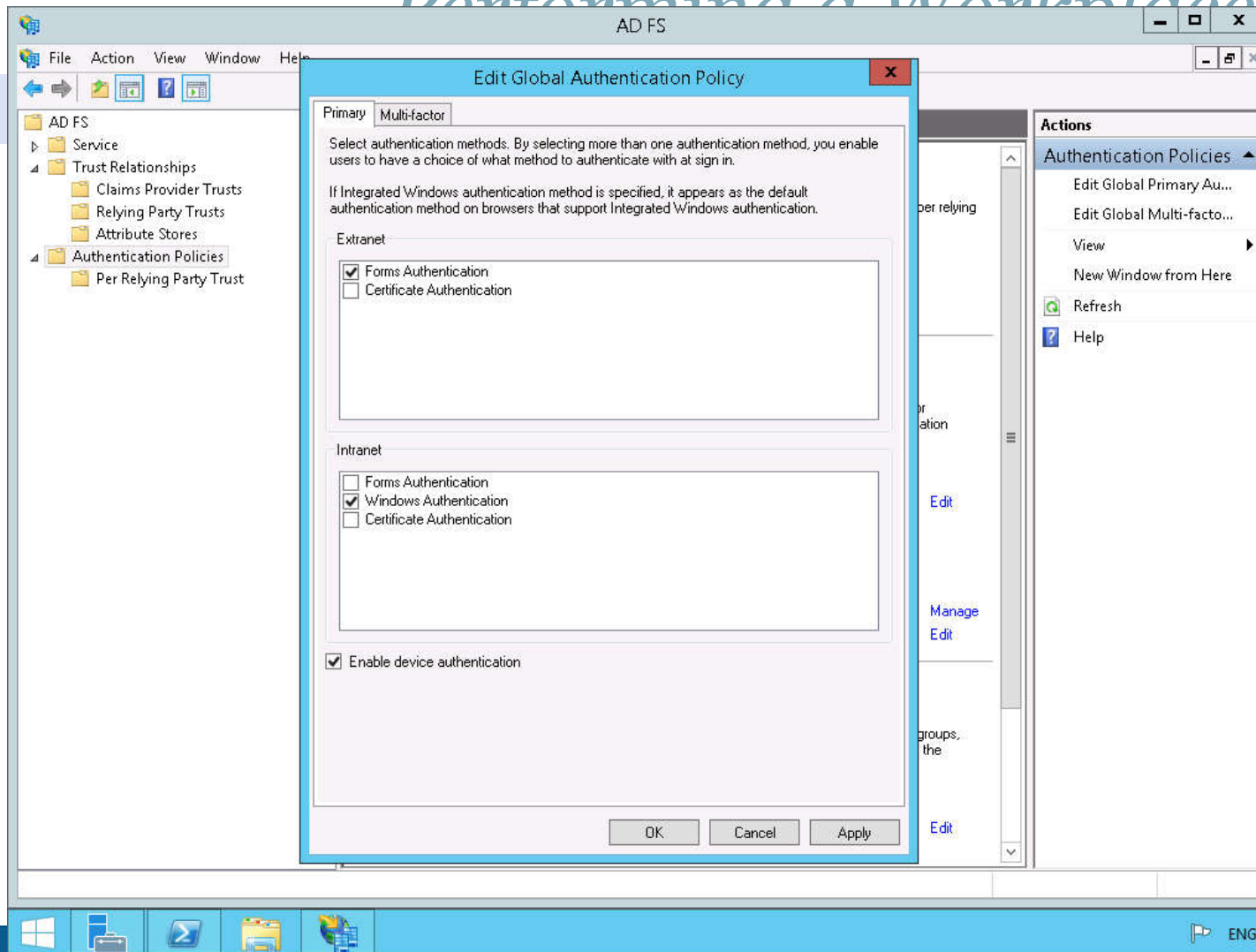
Enable Device Registration



Algebra

visoka škola za
primijenjeno računarstvo

Performing a Workplace Join



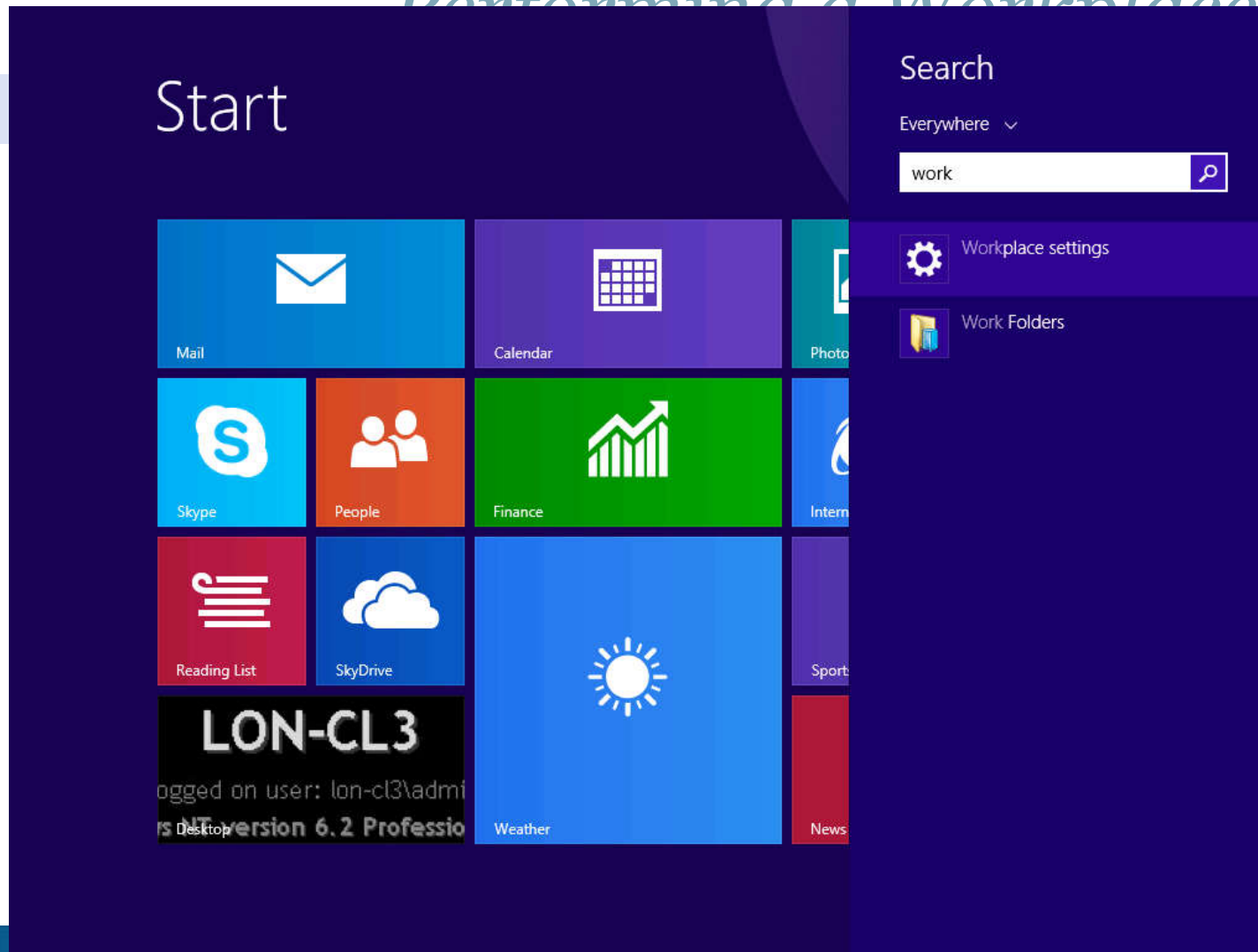
Enable device authentication in AD FS



Algebra

visoka škola za
primijenjeno računarstvo

Performing a Workplace Join



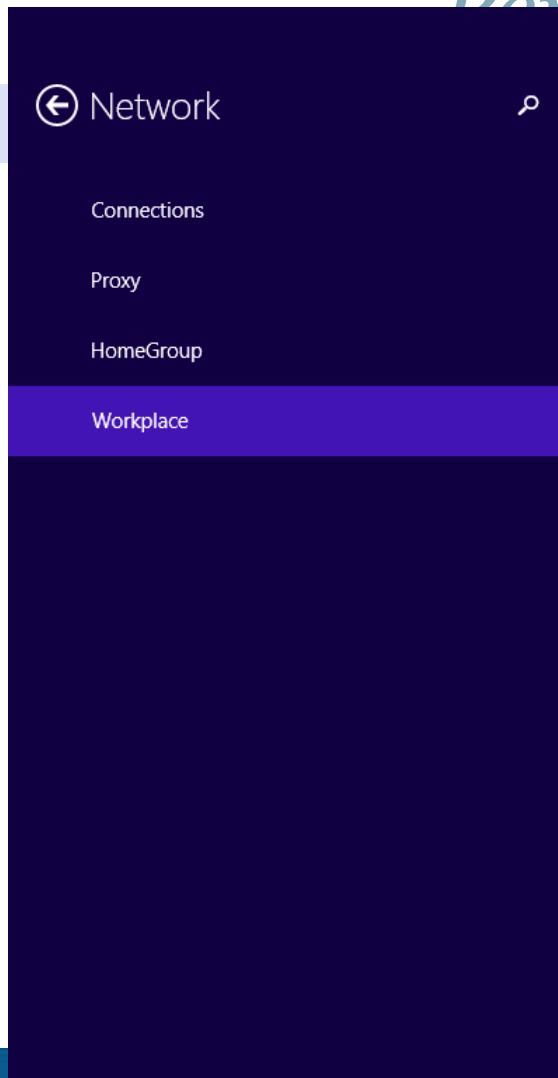
Go to Workplace settings on the client



Algebra

visoka škola za
primijenjeno računarstvo

Performing a Workplace Join



Workplace

Enter your user ID to get workplace access or turn on device management

Join your workplace network so that you can use network resources like internal websites and business apps

Join

With device management turned on, your IT admin can set up apps and services for you

Turn on

Enter the email address/UPN



Algebra

visoka škola za
primijenjeno računarstvo

Join

← Network



Workplace

Enter your user ID to get workplace access or turn on device management

← Connecting to A. Datum Corporation

A. Datum Corporation

Sign in with your organizational account

brad@adatum.com

••••••••



Sign in

© 2013 Microsoft

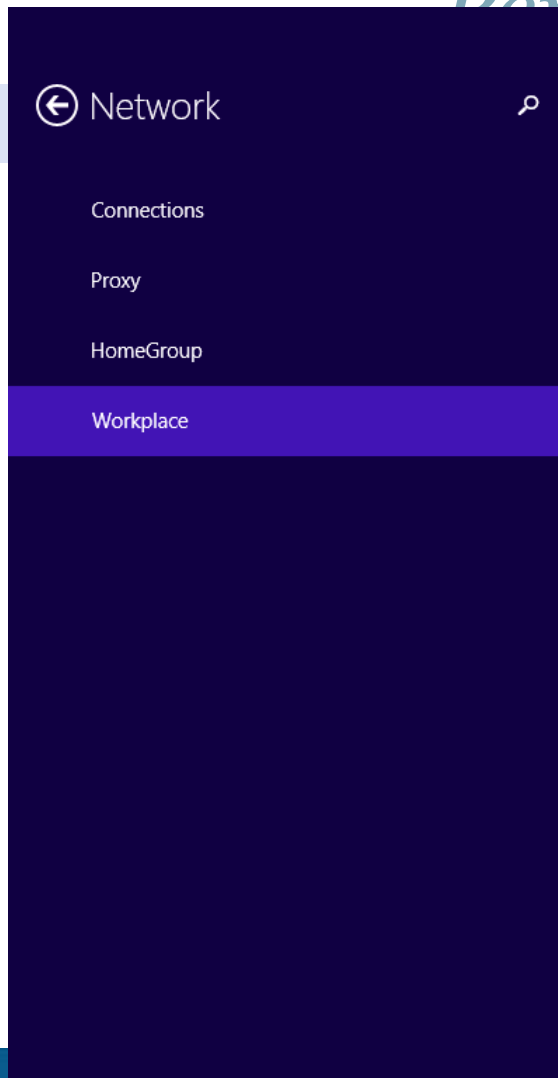
Enter credentials



Algebra

visoka škola za
primijenjeno računarstvo

Performing a Workplace Join



Workplace

Enter your user ID to get workplace access or turn on device management

brad@adatum.com

Join your workplace network so that you can use network resources like internal websites and business apps

Join

Connecting to workplace

With device management turned on, your IT admin can set up apps and services for you

Turn on

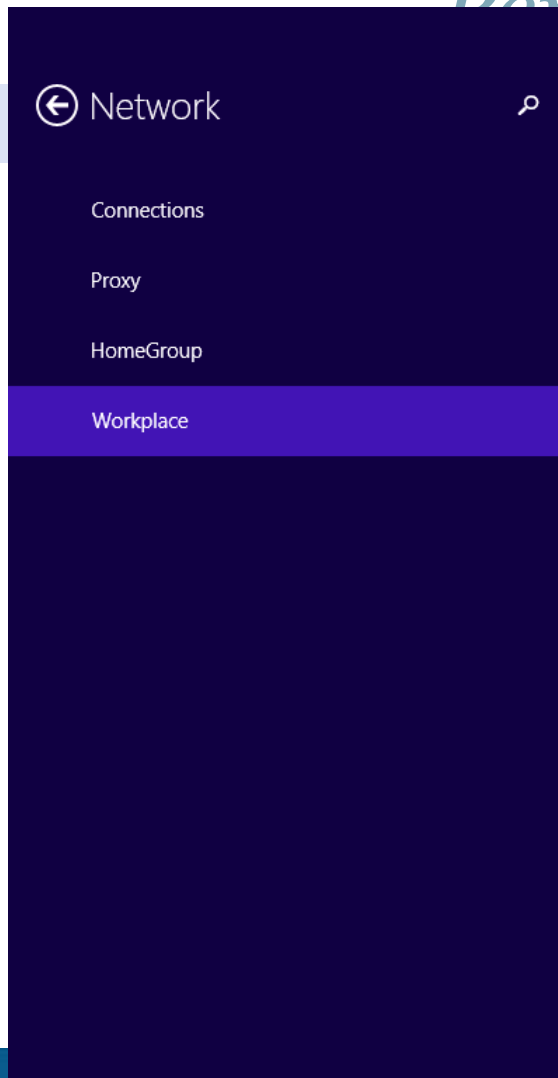
Wait a few moments while connecting



Algebra

visoka škola za
primijenjeno računarstvo

Performing a Workplace Join



Workplace

Enter your user ID to get workplace access or turn on device management

brad@adatum.com

This device has joined your workplace network

Leave

With device management turned on, your IT admin can set up apps and services for you

Turn on

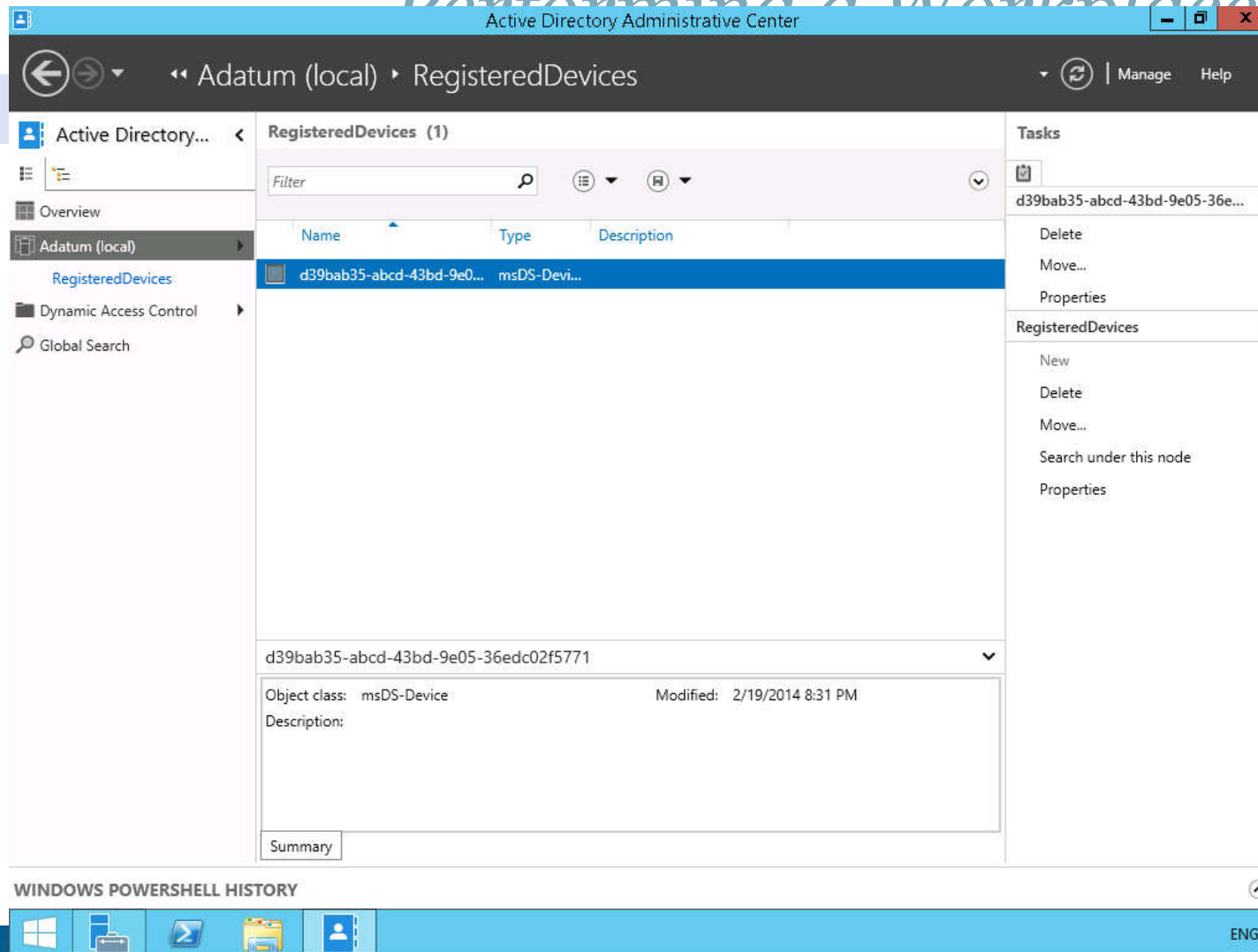
Workplace join completed successfully



Algebra

visoka škola za
primijenjeno računarstvo

Performing a Workplace Join



An object is created in AD DS for the device



Algebra

visoka škola za
primijenjeno računarstvo

Performing a Workplace Join

The screenshot displays the Active Directory Administrative Center interface. The main window shows the 'RegisteredDevices' container for 'Adatum (local)'. A specific device is selected, identified by its GUID: d39bab35-abcd-43bd-9e05-36edc02f5771. The 'Attribute Editor' tab is active, showing a list of attributes and their values. The 'displayName' attribute is highlighted, showing the value 'LON-CL3'. The 'Security' tab is also visible. The right-hand pane shows the 'Tasks' for the selected device, including 'Delete', 'Move...', 'Properties', and 'New'. The bottom of the window shows the 'WINDOWS POWERSHELL HISTORY' pane and the system tray with the Windows logo, taskbar icons, and the language 'ENG'.

Active Directory Administrative Center

Adatum (local) RegisteredDevices

Active Directory Administrative Center

Overview

Adatum (local)

RegisteredDevices

Dynamic Access Control

Global Search

Tasks

d39bab35-abcd-43bd-9e05-36e...

Delete

Move...

Properties

RegisteredDevices

New

Delete

Move...

Search under this node

Properties

General

Protect from accidental deletion

Extensions

Security Attribute Editor

Attributes:

Attribute	Value
adminDescription	<not set>
adminDisplayName	<not set>
altSecurityIdentities	X509.<SHA1-TP-PUBKEY>EA2288E98EE2
cn	d39bab35-abcd-43bd-9e05-36edc02f5771
description	<not set>
displayName	LON-CL3
displayNamePrintable	<not set>
distinguishedName	CN=d39bab35-abcd-43bd-9e05-36edc02f57
dSASignature	<not set>
dSCorePropagationD...	0x0 = { }
extensionName	<not set>
flags	<not set>
fSMORoleOwner	<not set>
instanceType	0x4 = { WRITE }

More Information

OK Cancel

WINDOWS POWERSHELL HISTORY

ENG

Properties of the registered device



Algebra

visoka škola za
primijenjeno računarstvo

Performing a Windows Join

Windows Identity Foundation...

https://lon-svr1.adatum.com/AdatumTestApp/

Welcome : Brad Sutton
Values from IIdentity

IsAuthenticated:True Name:Brad Sutton

Claims from IClaimsIdentity

Claim Type	Claim Value	Value Type
http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname	ADATUM\Brad	string
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	Brad@adatum.com	string
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	brad@adatum.com	string
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Brad Sutton	string
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ADATUM\Brad	string
http://schemas.microsoft.com/2012/01/devicecontext/claims/displayname	LON-CL3	string
http://schemas.microsoft.com/2012/01/devicecontext/claims/ostype	Windows	string
http://schemas.microsoft.com/2012/01/devicecontext/claims/osversion	6.3.9600.0	string
http://schemas.microsoft.com/2012/01/devicecontext/claims/ismanaged	false	boolean
http://schemas.microsoft.com/2012/01/devicecontext/claims/isregistereduser	true	boolean
http://schemas.microsoft.com/2012/01/devicecontext/claims/identifier	2733927a-bf38-45e8-ba92-b80142a8e6af	string
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/windows	string
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	2014-02-20T04:54:20.144Z	dateTime

ENG

Claims presented to an application



Algebra

visoka škola za
primijenjeno računarstvo

Lab B: Implementing AD FS for External Partners and Users

- Exercise 1: Configuring AD FS for a Federated Business Partner
- Exercise 2: Configuring Web Application Proxy

Logon Information

Virtual machines: 20412D-LON-DC1, 20412D-LON-SVR1, 20412D-LON-SVR2, 20412D-TREY-DC1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Estimated Time: 45 minutes



Algebra

visoka škola za
primijenjeno računarstvo

Lab Scenario

A. Datum Corporation has set up a variety of business relationships with other companies and customers. Some of these partner companies and customers must access business applications that are running on the A. Datum network. The business groups at A. Datum want to provide a maximum level of functionality and access to these companies. The Security and Operations departments want to ensure that the partners and customers can access only the resources to which they require access, and that implementing the solution does not increase the workload for the Operations team significantly. A. Datum also plans to migrate some parts of its network infrastructure to Microsoft Online Services, including Windows Azure and Office 365.



Algebra

visoka škola za
primijenjeno računarstvo

Lab Scenario

Now that you have deployed AD FS for internal users, the next step is to enable access to the same application for external partner organizations and for external users. A. Datum Corporation has entered into a partnership with Trey Research. You need to ensure that Trey Research users can access the internal application. You also need to ensure that A. Datum Corporation users working outside the office can access the application.

As one of the senior network administrators at A. Datum, it is your responsibility to implement the AD FS solution. As a proof-of-concept, you are deploying a sample claims-aware application, and configuring AD FS to enable both Trey Research users and external A. Datum Corporation users to

Lab Review

- Why does using certificate from a trusted provider on the Internet negate the need to configure certificate trusts between organizations?
- Could you have created authorization rules in Adatum.com and achieved the same result if you had instead created authorization rules in TreyResearch.net?



Algebra

visoka škola za
primijenjeno računarstvo

Module Review and Takeaways

➤ Review Questions



Algebra

visoka škola za
primijenjeno računarstvo



Algebra

visoka škola za
primijenjeno računarstvo



Algebra

visoka škola za
primijenjeno računarstvo