Contents

Introduction

This document describes how to configure Microsoft Active Directory Federated Services (ADFS) as an Identity Provider (IdP), which sends specific group details to the Cisco Cloud Web Security (CWS) service, rather than a full list of group memberships.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cloud Web Security configuration with the ScanCenter Portal
- Security Assertion Markup Language (SAML) authentication
- Administration of Microsoft ADFS server

Components Used

The information in this document is based on Microsoft ADFS version 2.0, that runs on Windows Server 2008 R2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

When the authentication process between a client browser occurs, the ADFS server (the IdP) and CWS (the Service Provider (SP)), all information is encrypted and added to the URL string in the client browser. This means the URL string is longer when more information is sent to CWS.

When you configure SAML authentication (with Microsoft ADFS) for use with the CWS service, you should configure a Relying Party Trust to provide the username and group information. Cloud Web Security: Configure user/group attributes with PingFederate and ADFS Whilst using SAML describes this step in more detail.

The number of groups a user is added to increases the URL size. If a user belongs to a large number of Active Directory (AD) groups, the URL grows to a size whereby the browser imposed URL limit is reached, and the authentication process fails.

Each browser might define their own maximum allowed URL length. RFC 2616 does not specify a maximum length, but practical limits are imposed by browser vendors.

> **Note**: It is not possible to explicitly define a maximum number of groups because a group does not have a fixed number of characters. For example, GroupA has less characters than Test_Group_A. To define a number of groups that stays below the URL limit depends on the character count of the Domain Name + Group Name.

Configure

You can configure the Microsoft ADFS server to include specific groups in the authentication process. Typically you would select only the groups used in the CWS Web Filtering rules. When you run an audit of policies that exist, it helps determine the groups that are already in use.

Both new and deployments that already exist should follow the best practice configuration that provides these benefits:

- Keeps URL size to a minimum
- Speeds up the authentication process between the IdP (ADFS) and the SP (CWS)
- Saves bandwidth on each authentication request

Best Practice Configuration

Open Claims Provider Trusts and create two Acceptance Transform Rules:

Use Claim rule template Send LDAP attributes as Claims

Attribute Store: AD;

LDAP Attribute: Token-groups - Unqualified Names;

Outgoing Claim Type: Group

Use Claim rule template Send LDAP attributes as Claims

Attribute Store: AD;

LDAP Attribute: SAM-Account-Name;

Outgoing Claim Type: Name

Create Issuance Transform Rules by opening Relying Part Trusts and creating two Transform Rules:

Use Transform an incoming claim template

Incoming Claim type: Name

Format: unspecified

Outgoing claim type: Name ID

Format: Unspecified

Select Pass through all claim values

Use Passthrough or Filter an incoming Claim

Incoming Claim type: Group

Select Pass through only claim values that start with a specific value:

Specify Your AD Group Names

Verify

Use this section to confirm that your configuration works properly.

- While logged in as the end user, browse to http://whoami.scansafe.net.
- The output should list only the groups specified in the previously mentioned procedure, rather than a full list of group memberships.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.