



TOOLS TO CREATE YOUR OWN IDENTITY MANAGEMENT SYSTEM

ERIC KREBILL

Technology Director

Tri County Area Schools

The goal of this session

- ▶ Overall understanding of what makes an Identity Management System work
- ▶ Basic familiarity with several tools available to make your own Identity Management System
- ▶ Provide scripts that I use at Tri County to manage student identities

One of the most frustrating feelings in the world is being smart enough to know there's a better way to do something, but not smart enough to create a way to do it.

Tools

- ▶ WinSCP
- ▶ PowerShell
- ▶ GAM
- ▶ GCDS
- ▶ GSPS
- ▶ Active Directory
- ▶ IIS
- ▶ ADFS
- ▶ Clever

K-5 Students

- ▶ Students are assigned 8 character password
- ▶ 3-letter word + 5-letter word = 8 characters
- ▶ Word list stolen from scrabble website
- ▶ Sanitized for use with elementary students
- ▶ K-2 students use Clever for Chromebook login



File

Home

Insert

Page Layout

Formulas

Data

Review

View

Tell me what you want to do...



Cut

Copy

Paste

Format Painter

Clipboard

Calibri

11

A A

**B** *I* U

A

Font

Wrap Text

Merge & Center

Alignment

General

\$ % ,

Number



Conditional Formatting



Table

Normal

Neutral

V1



fx

A

B

C

D

E

F

G

H

I

J

K

L

1 3letters 5letters

2 ace about

3 act above

4 add abuse

5 age actor

6 ago acute

7 aid admit

8 aim adopt

9 air adult

10 ale after

11 all again

12 alt agent

13 amp agree

14 and ahead

Clever

- ▶ Only using for login, no portal
- ▶ Elementary secretaries handle badges
- ▶ 2 badges per student
 - ▷ 1 for classroom
 - ▷ 1 for computer lab
- ▶ Nightly exports from Synergy

How do your teachers get new student passwords?



One Developer Army

@OneDeveloperArmy

Follow



Programming today is a race between software engineers striving to build bigger and better idiot-proof programs, and the universe trying to produce bigger and better idiots. So far, the universe is winning.

11:55 AM - 17 Jul 2018

How my teachers get student passwords!

- ▶ Custom web form!
- ▶ Teacher logs in (Active Directory credentials)
- ▶ Enters student ID
- ▶ Password displayed on screen
- ▶ Password stored in Active Directory
- ▶ No separate database, everything stored in AD



Student Password Lookup Tool

Welcome to the Student Password Lookup Tool.

To access this site, enter the Username and Password that you use to login to your computer.

Log In	
User Name:	<input type="text"/>
Password:	<input type="password"/>
<input type="button" value="Log In"/>	

If you have any problems with this site, please enter a work order.



Student Password Lookup Tool

[Logout](#) ekrebill

Please type in the Student ID (number):

Student ID:

Lookup Password

If you have any problems with this site, please enter a work order.



Student Password Lookup Tool

[Logout](#) ekrebill

Please type in the Student ID (number):

Password for test student is **ITWORKS**

Lookup Another

If you have any problems with this site, please enter a work order.

Decrypting AD passwords?

- ▶ Not decrypting passwords
- ▶ Passwords for K-5 stored in hidden AD field
 - ▷ Stored in plain text
 - ▷ Same field holds placeholder for 6-12
 - ▷ Using custom AD fields for sensitive data
- ▶ Passwords for 6-12 not stored
- ▶ Someone good enough to hack AD doesn't care about the password of a 9 yr old

"PROGRAMMING IS NOT STRESSFUL AT ALL"

ARTHUR, 25

6-12 Students

- ▶ Students are assigned a default password
- ▶ Same password for all new students
- ▶ Students are sent a welcome email
- ▶ Web-based password change form
 - ▷ 100% chromebooks
 - ▷ Active Directory still in charge!

Web-based password change?

- ▶ ADFS Password Change portal
- ▶ Part of Server 2016
 - ▶ Just needs enabled
- ▶ No extra cost / licensing
- ▶ Use PowerShell to customize page
- ▶ Could use NAT to make public
- ▶ Needs certificate!
- ▶ 101% CHROMEBOOK FRIENDLY!!!



Tri County Area Schools

Tradition • Character • Achievement • Success

Update Password

Do not enter your email address as username, only enter your username (ex. 123456)

HOW USERS SEE PROGRAMMERS



HOW PROGRAMMERS SEE USERS



What do you do if a student forgets their password?

We are fortunate that farts aren't as sudden, violent, and difficult to suppress as sneezes.

What I do if a student forgets their password!

- ▶ Custom web form!
- ▶ Teacher logs in (Active Directory credentials)
- ▶ Enters student ID
- ▶ Confirm student name
- ▶ Instructions displayed on screen
- ▶ Default PW set in Active Directory instantly
- ▶ Default PW set in Google instantly (GSPS)
- ▶ Email sent to student with change instructions



Student Password Reset Tool

Welcome to the Student Password Reset Tool.

To access this site, enter the Username and Password that you use to login to your computer.

Log In	
User Name:	<input type="text"/>
Password:	<input type="password"/>
<input type="button" value="Log In"/>	

If you have any problems with this site, please enter a work order.



Student Password Reset Tool

[Logout](#) ekrebill

Please type in the Student ID of the student you would like to reset the password for:

Student ID:

Reset Password

If you have any problems with this site, please enter a work order.



Student Password Reset Tool

[Logout](#) ekrebill

Please type in the Student ID of the student you would like to reset the password for:

Are you sure you want to reset **test student's** password?

Yes

No / Cancel

If you have any problems with this site, please enter a work order.



Student Password Reset Tool

[Logout](#) [ekrebill](#)

Password was reset successfully.

Please tell test student that their new password is They will receive an email with instructions on how to change their password.

Please type in the Student ID of the student you would like to reset the password for:

Student ID:

Reset Password

If you have any problems with this site, please enter a work order.



Mail ▾



More ▾

1 of 1



COMPOSE

Inbox

Starred

Sent Mail

Drafts

More ▾

Password Change Information

Inbox x



admin@tricountyschools.com

Aug 2 (10 days ago)



to me ▾

Your password has been changed. Reminder: you have 2 weeks to change your password or your account will automatically be locked. Follow this link for information on how to change your password: <https://goo.gl/iSiASB>



Click here to [Reply](#) or [Forward](#)

Using 0 GB

[Manage](#)

[Program Policies](#)

Powered by Google™

Last account activity: Jul 26

[Details](#)



Tri County Area Schools

Tradition • Character • Achievement • Success

Password Change Instructions

Grades 6-12

You are here because one of your teachers reset your password back to default. Upon resetting the password, students have 2 weeks to change their password before their account is locked.

To change your password, simply follow this link: <http://pw.tricountyschools.com>

Update Password

Example: 123456

In the 1st box: your student number

Old password

In the 2nd box: your old password (the one your teacher gave you)

New password

In the 3rd box: your new password (minimum 8 characters)

Confirm new password

In the 4th box: repeat your new password to ensure it's correct

Submit

Cancel

Click the Submit button and you're all set. The chromebook will log you out automatically and you'll need to log in again using your new password.

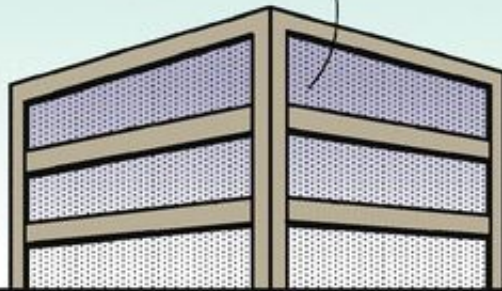
WAS IT
HUMAN
ERROR?

I
DOUBT
IT



Dilbert.com DilbertCartoonist@gmail.com

NO HUMAN WOULD
BE THAT STUPID. MY
BEST GUESS IS THAT
A CABBAGE GOT ACCESS
TO YOUR COMPUTER.



5:20-10 ©2010 Scott Adams, Inc./Dist. by UFS, Inc.

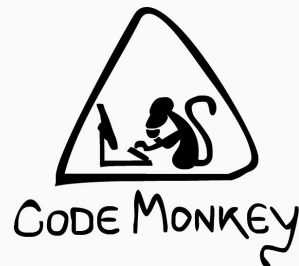
CABBAGES
CAN'T USE
COMPUTERS.

CAN THEY
TELL WHEN
THEY'RE
BEING
MOCKED?




Key points - PowerShell

- ▶ Not just for super nerds and code monkeys
- ▶ Useful for all kinds of tasks
 - ▷ Formatting data
 - ▷ Doing *anything* with Active Directory
 - ▷ Working with GUI-less Windows Servers
 - ▷ Almost any repetitive task on a Windows Server
- ▶ If you aren't using PowerShell now, look into it



Key points - GAM

- ▶ GAMADV > Original GAM
- ▶ GAM + PowerShell = 
 - ▷ So awesome it doesn't even need more cowbell
- ▶ Pulling all data directly from Active Directory
- ▶ Only running GAM commands on new students
 - ▷ Using if whencreated < 1
- ▶ GAM + PowerShell works slower than batch files

Key points - GCDS / GSPS

- ▶ Google Cloud Directory Sync
 - ▷ Synchronize AD with G Suite
 - ▷ New users created
 - ▷ Disabled users suspended
 - ▷ Name changes synchronized
- ▶ G Suite Password Sync
 - ▷ Needs to be installed on EVERY AD server
 - ▷ Syncs on password change, not reset from ADUC
 - ▷ Change and Reset pages start GSPS

Key points - ADFS

- ▶ Available on any modern Windows Server
- ▶ Easy initial install
- ▶ Low overhead
- ▶ PowerShell Controls EVERYTHING
- ▶ Requires IIS redirect for short URL
 - ▷ By default - `domain.com/adfs/portal/updatepassword/`

Key points - IIS

- ▶ Available on any modern Windows Server
- ▶ Easy install
- ▶ Tons of resources available
- ▶ Needs .net installed for aspx pages
- ▶ Server needs to be domain member for domain auth

Active Directory

- ▶ 2016 Native Mode
- ▶ Using custom fields for IDM system
 - ▷ Hidden from AD Users and Computers
 - ▷ Difficult to guess from outside
 - ▷ Able to lock down access to custom fields
 - ▷ Scripts sanitized using built-in fields
- ▶ Add Custom AD Fields - <https://goo.gl/8tfUL1>
- ▶ AD Field Permissions - <https://goo.gl/PTKWE1>

The Code



Dilbert.com DilbertCartoonist@gmail.com



8-12-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick



GAM using PowerShell

```
10 ##### Universal Variables #####
11 [xml]$univar = Get-Content C:\PowerShell\UniVar\UniVar.xml
12 $resultFile = $univar.var.stulog + "RESULT_GAM_SetPasswords.txt"
13 $logfile = $univar.var.stulog + "LOG_GAM_SetPasswords.txt"
14 $detailFile = $univar.var.stulog + "DETAIL_GAM_SetPasswords.txt"
15 $gamPath = $univar.var.gam
16 $studentou = $univar.var.stuou
17 $emaildomain = $univar.var.domain
18 $defaultpw = $univar.var.defaultpw
19 ##### Consult README before modifying Universal Variables #####
20
21 # Change the properties variables to match the fields you need to use in the script.
22 # Do not remove whenCreated variable as that's needed later on.
23 $students = Get-ADUser -filter "mail -like '*$emaildomain'" -Searchbase $studentou -ResultSetSize $null -Properties whenCreated,mail,division
24
25 # Logging and housekeeping
26 Add-Content -Path $logfile -value "Process started $(Get-Date)" -PassThru
27
28 foreach ($user in $students)
29 {
30     $email = $user.mail
31     $pass = $user.Division
32
33     #Checks to see if the user was created within the last day
34     If ($user.whenCreated -ge ((Get-Date).AddDays(-1)).Date)
35     {
36
37         If ($pass -eq "Lookup_Not_Available") {
38
39             & $gamPath update user $email password $defaultpw
40
41             Add-Content -Path $detailFile -value "$(Get-Date) - Default password set for $email" -PassThru
42
43         } Else {
44
45             & $gamPath update user $email password $pass
46
47             Add-Content -Path $detailFile -value "$(Get-Date) - static password set for $email" -PassThru
48
49         }
50     }
51     }
52 else
53 {
54 }
55 }
```

```

34 #Set Current School year
35 #Sets the current year after July 1 = current year + 1 so grad year calculates correctly
36 [int]$currentmonth = Get-Date -UFormat %m
37 [int]$currentyear = Get-Date -UFormat %Y
38 $yearchange = if ($currentmonth -le 7) { 0 } else { 1 }
39 $currentschoolyear = ($currentYear + $yearchange)
40 #endregion
41
42 Function Get-GradeYear ([string]$grade)
43 {
44     If ($grade -eq "K") #If the student is in "K" grade, set the year 0
45     {
46         $grade = 0
47     }
48     If ($grade -eq "DK") #If the student is in "DK" (early childhood), set the year -1
49     {
50         $grade = -1
51     }
52     [int]$grade = [convert]::ToInt32($grade, 10)
53     [int]($currentschoolyear) - ([int]$grade - 12)
54 }
55
56
57
58
59
60
61 [string]$gradelevel = $row.grade_level
62 $gradyear = Get-GradeYear $gradelevel
63
64 ##### description
65 $out += $gradyear
66 #####
67

```

Get Graduation Year

LET'S DO MATH



A kindergarten student entered in school the 2000-2001 school year will have grad year of 2013.

If student gets entered in August and you use simple math to calculate the grad year = current_year - (grade - 12), the grad year will be off by 1 year. $2000 - (0 - 12) = 2012$ If they were enrolled after January 1, the math would be correct. $2001 - (0 - 12) = 2013$

The formula that I use determines the month first, if it's after July, we add 1 to the current_year variable. So then it looks like this $(2000 + 1) - (0 - 12) = 2013$.

My formula says "if month is less than 7, \$yearchange is 0, otherwise it's 1". After that, I get \$currentschoolyear by doing \$currentyear + \$yearchange. In the example above August of 2000 would mean $2000 + 1$.

Further down on line 44, I do \$currentschoolyear - (\$grade - 12) to determine their real graduation year.

Move inactive students

```
8
9 Import-Module ActiveDirectory
10
11 # Variables - Modify as necessary
12
13 # This is the OU that we're going to move the exited students TO
14 $TargetOU = "OU=Exited,OU=StudentOU,DC=Domain,DC=local"
15 # This is the OU that we're searching for students who are disabled
16 $SearchOU = "OU=StudentOU,DC=Domain,DC=local"
17 # Changing the graduation year so they don't show up on grad-year searches
18 $gradyear = "Exited"
19 # Removing the address from the print group
20 $prtgroup = "@"
21 # Updating the Google OU so GAM moves them to the exited OU
22 $googleou = "/Students/Exited"
23
24 # End Variable section
25
26 $DisabledAccounts = get-aduser -SearchBase $SearchOU -filter { enabled -eq $false }
27
28 ForEach ($account in $DisabledAccounts) {
29     Set-ADUser -Identity $account.SamAccountName -Description $gradyear -Department $googleou -Remove @{'ipPhone'=$prtgroup}
30     Move-ADObject -Identity $account.DistinguishedName -TargetPath $TargetOU
31 }
```

- AD FS
 - Service
 - Attribute Stores
 - Authentication Methods
 - Certificates
 - Claim Descriptions
 - Device Registration
 - Endpoints
 - Scope Descriptions
 - Web Application Proxy
 - Access Control Policies
 - Relying Party Trusts
 - Claims Provider Trusts
 - Application Groups

Endpoints					
Enabled	Proxy Enabled	URL Path	Type	Authentication Type	Security Mode
Yes	No	/adfs/services/trust/13/kerberosmixed	WS-Trust 1.3	Kerberos	Mixed
No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3	Certificate	Message
Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3	Certificate	Mixed
No	No	/adfs/services/trust/13/certificatetransport	WS-Trust 1.3	Certificate	Transport
No	No	/adfs/services/trust/13/username	WS-Trust 1.3	Password	Message
No	No	/adfs/services/trust/13/usernamebasictransport	WS-Trust 1.3	Password	Transport
Yes	Yes	/adfs/services/trust/13/usernamemixed	WS-Trust 1.3	Password	Mixed
No	No	/adfs/services/trust/13/issuetokenasymmetricbasic256	WS-Trust 1.3	SAML Token (Asym...	Message
No	No	/adfs/services/trust/13/issuetokenasymmetricbasic256h...	WS-Trust 1.3	SAML Token (Asym...	Message
Yes	Yes	/adfs/services/trust/13/issuetokenmixedasymmetricbasic...	WS-Trust 1.3	SAML Token (Asym...	Mixed
No	No	/adfs/services/trust/13/issuetokenmixedasymmetricbasic...	WS-Trust 1.3	SAML Token (Asym...	Mixed
Yes	Yes	/adfs/services/trust/13/issuetokenmixedsymmetricbasic2...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuetokenmixedsymmetricbasic2...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuetokensymmetricbasic256	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuetokensymmetricbasic256ha...	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuetokensymmetrictriplede...	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuetokensymmetrictriplede...	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuetokenmixedsymmetrictriple...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuetokenmixedsymmetrictriple...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/windows	WS-Trust 1.3	Windows	Message
No	No	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3	Windows	Mixed
No	No	/adfs/services/trust/13/windowstransport	WS-Trust 1.3	Windows	Transport
Yes	No	/adfs/services/trusttcp/windows	WS-Trust 2005	Local Windows	Message
No	No	/adfs/services/trust/artifactresolution	SAML-ArtifactResolution	Anonymous	Transport
Yes	Yes	/adfs/oauth2/	OAuth	Anonymous	Transport
Metadata					
Yes	Yes	/adfs/services/trust/mex	WS-MEX	Anonymous	Transport
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata	Anonymous	Transport
Yes	No	/adfs/fs.federationserver/service.asmx	ADFS 1.0 Metadata	Anonymous	Transport
OpenID Connect					
Yes	Yes	/adfs/.well-known/openid-configuration	OpenID Connect Discovery	Anonymous	Transport
Yes	Yes	/adfs/.discovery/keys	OpenID Connect JWKS	Anonymous	Transport
Yes	Yes	/adfs/.userinfo	OpenID Connect UserInfo	Anonymous	Transport
Proxy					
Yes	No	/adfs/proxy/	Web Application Proxy	Proxy Trust Certificate	Transport
Yes	No	/adfs/proxy/EstablishTrust/	Web Application Proxy	Password	Transport
Device Registration					
Yes	Yes	/EnrollmentServer/	Device Registration	Anonymous	Transport
WebFinger					
Yes	Yes	/.well-known/webfinger	WebFinger	Anonymous	Transport
Other					
Yes	Yes	/adfs/portal/updatepassword/	HTTP	Anonymous	Transport
No	No	/adfs/CertificateAuthority/crl	Certificate Authority CRL	Anonymous	Transport

- Actions
- Endpoints
 - View
 - New Window from Here
 - Refresh
 - Help
 - /adfs/services/trust/mex
 - Enable on Proxy
 - Disable
 - Help

URL Rewrite for ADFS password change portal



URL Rewrite

Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern	Action Type	Action URL	Stop Proce...	Entry Type	
  http to https	URL path after '/'	Matches	(.*)	Redirect	https://{HTTP...	True	Local	



Edit Inbound Rule

Name:

http to https

Match URL

Requested URL:

Matches the Pattern

Using:

Regular Expressions

Pattern:

(.*)

Test pattern...

☒ Ignore case

Conditions

Logical grouping:

Match All

Input	Type	Pattern	
{HTTPS}	Matches the Pattern	^OFFS	

Add...

Edit...

Remove

Move Up

Move Down

☐ Track capture groups across conditions

Server Variables

Action

Action type:

Redirect

Action Properties

Redirect URL:

`https://{HTTP_HOST}/adfs/portal/updatepassword/{R:1}`

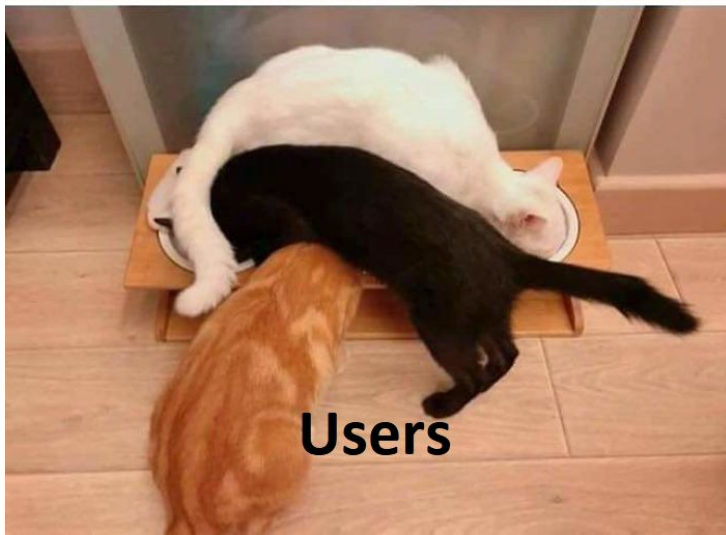
☒ Append query string

Redirect type:

See Other (303)



Developer: Makes a simple, intuitive UI



Users



4,6k ↓

27

Share

BEST COMMENTS ▼

durafuto • 2h

toastednutella • 1h

Why you shouldn't hardcode things

QUESTIONS?



QUESTIONS?



HELPFUL LINKS

Links / Instructions - PowerShell

PowerShell Scripting Tutorial for Beginners

<https://blog.netwrix.com/2018/02/21/windows-powershell-scripting-tutorial-for-beginners/>

Microsoft Virtual Academy: PowerShell Beginners

<https://mva.microsoft.com/learning-path/powershell-beginner-12>

PowerShell Basics

<https://www.darkoperator.com/powershellbasics/>

TechNet Script Gallery

<https://gallery.technet.microsoft.com/>

Links / Instructions - GAM

GAM Cheat Sheet (Original & Advanced)

<http://www.gamcheatsheet.com>

Original GAM

<https://github.com/jay0lee/GAM/releases>

Advanced GAM

<https://github.com/taers232c/GAMADV-X/releases>

Nice PowerShell/GAM breakdown

<https://sysadminedu.wordpress.com/2017/01/19/managing-gafe-with-powershell/>

Official GAM wiki

<https://github.com/jay0lee/GAM/wiki>

Links / Instructions - GCDS & GSPS

GCDS Download

<https://support.google.com/a/answer/6120989?hl=en>

GCDS Setup Instructions

<https://support.google.com/a/answer/6162412?hl=en>

GSPS Download

<https://support.google.com/a/answer/2611842?hl=en>

Links / Instructions - IIS & Custom Scripts

Step-by-step IIS Installation Guide

<https://www.rootusers.com/how-to-install-iis-in-windows-server-2016/>

URL Rewrite

<https://www.iis.net/downloads/microsoft/url-rewrite>

IIS Site Bindings (2 sites, one server)

<https://www.sherweb.com/blog/how-to-set-up-site-bindings-in-internet-information-services-iis/>

Links / Instructions - ADFS

Setup

<https://www.semperis.com/using-ad-fs-to-change-your-ad-password-anywhere-anytime/>

Make it so the user just enters “username” instead of “username@domain.local” for password reset

<https://blogs.technet.microsoft.com/pie/2015/09/02/accept-sam-account-name-as-a-login-format-on-the-adfs-form-based-password-update-page/>

Customize the ADFS page

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/ad-fs-user-sign-in-customization>

Advanced customization options

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/ad-fs-customization-in-windows-server>

IIS Redirect

<https://docs.microsoft.com/en-us/iis/configuration/system.webserver/httpredirect/>