

# SSO Leiðbeiningar

CCQ | Cloud Compliance & Quality v.2019.03

Origo 03/2019

## EFNISYFIRLIT

AÐ BÚA TIL RELYING PARTY TRUST	4
AÐ BÚA TIL CLAIM REGLUR	1
EMAIL REGLA12	2
GROUP REGLA1	5
NAME REGLA	Э
CCQ STILLINGAR	2
INNSKRÁNING OG AÐGANGSSTÝRING	3
ADFS   AÐGANGSHÓPAR KERFISEININGA	7
ADFS   CCQ NOTENDAHÓPAR	Э
ADFS   SSO STILLINGAR	C
VOTTORÐ / X509 CERTIFICATE	1
GÁTLISTI / YFIRLIT	3

CCQ kerfið styður "Single sign-on" (SSO) sem er virkni sem gerir notendum kleift að auðkenna sig og skrá sig inn í kerfið í gegnum ADFS. Eftirfarandi leiðbeiningar eru ætlaðar kerfisstjórum með aðgang að AD/ADFS og CCQ og eiga þær að útlista hvernig koma skal á tengingu milli ADFS og CCQ. Sérstaklega verður skoðað hvernig á að búa til "relying party trust" og "claim reglur" í því tilliti. Að lokum verða stillingar í CCQ kerfinu sjálfu skoðaðar í þaula, farið yfir aðgangsstýringar og hvernig hópar í AD eru flokkaðir saman með aðgangshópum í CCQ. Lykilatriði er að nota **enga séríslenska stafi** í nöfnum á grúppum eða claimum.

Uppsetning ADFS liggur utan umfangs þessara leiðbeininga, en hægt er að styðja sig við ágætis grein þess efnis sem <u>má finna hér</u>. Gert er ráð fyrir að uppsetningu á ADFS netþjón sé lokið og að notendum sé búið að skipta niður í rétta aðgangshópa í AD.

# AÐ BÚA TIL RELYING PARTY TRUST

Fyrsta skref er að búa til "relying party trust" fyrir CCQ.

Opnið ADFS Management viðmótið.

Undir ADFS > Trust Relationships, hægri-smellið á Relying Party Trusts og veljið Add Relying Party Trust...



Smellið á Start til að opna RPT wizardinn sem fer með okkur í gegnum ferlið skref fyrir skref.

## 1. Select Data Source

Fyrsta skrefið er að velja "data source."

Hér veljum við neðsta radio takkann - Enter data about the relying party manually - og smellum á Next.

Steps	Select an option that this wizard will use to obtain data about this relying party:
Welcome	Impart data shout the relation party outlished online or on a local perturbative
Select Data Source	Use this option to import the necessary data and certificates from a rehing party organization that publishe
Specify Display Name	its federation metadata online or on a local network.
Choose Profile	Federation metadata address (host name or URL):
Configure Certificate	
Configure URL	Example: fs.contoso.com or https://www.contoso.com/app
Configure Identifiers	Import data about the relying party from a file
Configure Multi-factor Authentication Now?	Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not
Choose Issuance Authorization Rules	validate the source of the file. Federation metadata file location:
Ready to Add Trust	Browse
Finish	Enter data about the relying party manually
	Use this option to manually input the necessary data about this relying party organization

#### 2. Specify Display Name

Veljið eitthvað viðeigandi **Display Name** - til dæmis "CCQ" - og skrifið stutta lýsingu í **Notes** - t.d. "Configures relying party trust for SSO via SAML to CCQ." Smellið á **Next**.

#### 3. Choose Profile

Hér er best að halda sig við sjálfvirka valið: ADFS profile.



#### 4. Configure Certificate

Smellið á Next til að hoppa yfir næsta skref þar sem hægt er að velja "token signing certificate."

## 5. Configure URL

Hakið við gátreitinn **Enable support for the SAML 2.0WebSSO protocol**. Hér þarf að slá inn rétt CCQ endpoint URL í **Relying party SAML 2.0 SSO service URL** og smella á **Next**. CCQ endpoint URL: https://quality.ccq.cloud/\_saml/validate/adfs/<OrganizationID> þar sem <OrganizationID> er auðkenni fyrirtækisins í CCQ.

<b>\$</b>	Add Relying Party Trust Wizard
Configure URL	
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers	AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.  Enable support for the WS-Federation Passive protocol The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol URL: Example: https://fs.contoso.com/adfs/ls/
<ul> <li>Configure Multi-factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	<ul> <li>Enable support for the SAML 2.0 WebSSO protocol</li> <li>The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.</li> <li>Relying party SAML 2.0 SSO service URL:</li> <li>https://quality.ccq.cloud/_saml/validate/adfs/<organizationid></organizationid></li> <li>Example: https://www.contoso.com/adfs/ls/</li> </ul>

OrganizationID fyrirtækisins þarf að finna í CCQ kerfinu, en það er 17 stafa strengur með bæði há- og lágstöfum og tölustöfum. Þetta auðkenni geta notendur CCQ fundið með því að smella á tannhjólið og velja **Organization**.



Nafn fyrirtækisins birtist þá í lista ásamt öðrum upplýsingum, og ef smellt er á nafnið þá ætti auðkenni fyrirtækisins að leynast aftast í URLinu: https://quality.ccq.cloud/organizations/<OrganizationID>

Þessu OrganizationID er svo bætt aftast í CCQ endpoint URLið í RPT wizardnum, eins og lýst er hér að ofan.



## 6. Configure Identifiers

Í **Relying party trust identifier** textareitinn þarf að slá inn rétt CCQ identifier URL og smella svo á **Add**. CCQ identifier URL: https://quality.ccq.cloud

<b>\$</b>	Add Relying Party Trust Wizard	٢.
Configure Identifiers		
Configure Identifiers Steps  Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Identifiers Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.         Relying party trust identifier:         https://quality.ccq.cloud         Example: https://fs.contoso.com/adfs/services/trust         Relying party trust identifiers:         Relying party trust identifiers:	]
	< Previous Next > Cancel	

#### 7. Configure Multi-factor Authentication Now?

Smellið á Next til að stilla "multi-factor authentication" uppsetninguna, ef þörf krefur.

#### 8. Choose Issuance Authorization Rules

Smellið á Next til að samþykkja sjálfgefnu "issuance authorization" reglurnar.

### 9. Ready to Add Trust

Farið yfir stillingarnar ykkar og smellið á **Next** til að bæta við CCQ relying party trustinu.

### 10. Finish

Skiljið eftir hakað við gátreitinn **Open the Edit Claim Rules dialog** og smellið á **Close** til að loka þessum wizard og opna **Edit Claim Rules** gluggann fyrir þetta relying party trust.



# AÐ BÚA TIL CLAIM REGLUR

Hér fyrir neðan eru nokkur skjáskot sem vonandi gefa hugmynd um hvernig búa skal til **Claim Rules** fyrir CCQ. Um þrjár mismunandi tegundir claim reglna er að ræða.

- 1. Email
- 2. Group
- 3. Name

Mikilvægt er að öll fyrirtæki setji upp claim reglur fyrir Email og Name, en það er að sjálfsögðu mismunandi eftir fyrirtækjum hvaða AD grúppur er verið að nota og hvað þær heita.

Þegar búið er setja upp relying party trust Í ADFS þá er hægt að búa til claim reglur fyrir viðkomandi RPT. **Edit Claim Rules** glugginn er opnaður og smellt á **Add Rule...** til að opna **Add Transform Claim Rule** wizardinn sem tekur okkur í gegnum ferlið skref fyrir skref.

ę,			Edit Claim Rul	es		_		x
ŀ	ssuance 1	Transform Rules	Issuance Authorization Rul	es Delegat	tion Authoriza	tion R	ules	
	The follo	owing transform n	ules specify the claims that w	ill be sent to	the relying pa	arty.		
	Order	Rule Name		Issued Cla	iims			
								-
							-	<u></u>
Г	Add F	Rule Edit F	Rule Remove Rule	7				
L	,		nonovo hulo					
				ОК	Cancel		Арр	ly

## EMAIL REGLA

## 1. Choose Rule Type

Fyrsta skrefið er að velja rétta týpu af claim reglu.

Fyrir "email reglu" skal velja Send LDAP Attributes as Claims undir Claim rule template – og smella á Next.

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template. Claim rule template: Send LDAP Attributes as Claims v
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template. Claim rule template: Send LDAP Attributes as Claims
Claim rule template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group
emberships, use the Send Group Membership as a Claim rule template.

2. Configure Claim Rule

Næsta skref er að gefa reglunni eitthvað lýsandi nafn og velja "Active Directory" sem Attribute store.

Þá þarf að velja "*E-Mail-Addresses*" sem **LDAP Attribute** og mappa saman við "*E-Mail-Address*" undir **Outgoing Claim Type**. Smellið á **Finish** til að vista regluna.

<b>\$</b>		Add Transform Claim Rule	Wizard
Configure Rule			
Steps • Choose Rule Type • Configure Claim Rule	You ca which t issued Claim n Email Rule te Attribut Active Mappir	an configure this rule to send the values of L to extract LDAP attributes. Specify how the from the rule. ule name: emplate: Send LDAP Attributes as Claims te store: Directory ng of LDAP attributes to outgoing claim type LDAP Attribute (Select or type to add more) E-Mail-Addresses ✓	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be s: Outgoing Claim Type (Select or type to add more) E-Mail-Address v
			< Previous Finish Cancel

Auðvelt er að breyta reglum eftir á, ef þörf krefur, með því að smella á **Edit Rule…** Mikilvægt er að email-svæði séu rétt útfyllt í AD, því netföng eru notuð til auðkenningar á notendum í CCQ.

<b>\$</b>					AD FS	
翰 File Action View	Window Help					
🗢 🄿 🙍 🖬 🛛	Ī					
AD FS		Relying Party Trusts		_		
⊿ ☐ Trust Relationships		Display Name Microsoft Office 365 Identity Platform	Enabled Yes	Type WS-	e Identifier -T https://login.microsoftonline.com/ext	
Claims Provider	r I rusts	CCQ - Gaedahandbok	Yes	WS-	T https://quality.ccq.cloud	
Attribute 9	Edit (	Claim Rules for CCQ – Gaedahandb	ok 🗕 🗆 🗙		Edit	Rule - Email X
▷ Authenticatio Is	ssuance Transform Rules	Issuance Authorization Rules Delegation Auth	norization Rules		You can configure this rule to send the values of I which to extract LDAP attributes. Specify how the	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be
	The following transform n	rules specify the claims that will be sent to the relyi	ng party.		issued from the rule.	
	Order Rule Name	Issued Claims			Claim rule name:	
	1 Email 2 CCO Access	E-Mail Address Group			Pula templata: Sand LDAP Attributes as Claims	
	3 CCQ Admin	Group			Nulle template. Send EDAn Attibutes as Claims	
	4 CCQ Published	d Group			Attribute store:	
	6 CCQ Quality	k Group			Active Directory	<u> </u>
	7	Group			Mapping of LDAP attributes to outgoing claim type	s:
	8 9 Passthrough -	Group Name Name			LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
			4		► E-Mail-Addresses ✓	E-Mail Address 🗸 🗸
					*	~
	Add Rule Edit F	Rule Remove Rule				
		OK Canc	el Apply			
					View Rule Language	OK Cancel

## GROUP REGLA

#### 1. Choose Rule Type

Misjafnt er eftir CCQ áskrift fyrirtækja hversu mörgum kerfiseiningum þau hafa aðgang að, en fyrir hvern aðgangshóp í AD þarf að búa til "group" claim reglu. Ferlið er það sama fyrir flestar tegundir claim reglna og sniðmátin ósköp svipuð, en í þessu tilfelli þarf að velja **Send Group Membership as a Claim** undir **Claim rule template** – og smella á **Next**.

<b>S</b>	Add Transform Claim Rule Wizard
Select Rule Template	
Steps Ghoose Rule Type	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Configure Claim Rule	Claim rule template:
	Send Group Membership as a Claim $\checkmark$
	Claim rule template description:
	Using the Send Group Membership as a Claim rule template you can select an Active Directory security group to send as a claim. Only a single claim will be emitted from this rule, based on the group selected. For example, you can use this rule template to create a rule that will send a group claim with a value of "Admin" if the user is a member of the "Domain Admins" security group. This rule template should only be used for users of the local Active Directory Domain.
	< Previous Next > Cancel

### 2. Configure Claim Rule

Nafn reglunnar þarf helst að vera nokkuð lýsandi, og hér þarf að passa vel upp á að velja réttan AD aðgangshóp undir **User's group**. Þá þarf að velja "*Group*" sem **Outgoing claim type** og eitthvað gildi á **Outgoing claim value**. Ágætis venja er að nota sama nafn og er á claim reglunni sjálfri í **claim value** reitnum, til að draga úr líkum á ruglingi og stafsetningarvillum. Smellið á **Finish** til að vista regluna.

<b>\$</b>	Add Transform Claim Rule Wizard
Configure Rule	
Configure Rule Steps • Choose Rule Type • Configure Claim Rule	You can configure this rule to send a claim based on a user's Active Directory group membership. Specify the group that the user is a member of, and specify the outgoing claim type and value to issue. Claim rule name: CCQ Access Rule template: Send Group Membership as a Claim User's group: USER \CCQ Access Browse Outgoing claim type: Group Outgoing name ID format: Unspecified Outgoing claim value: CCQ_Access
	< Previous Finish Cancel

Mikilvægt er að gildið sem slegið er inn í **Outgoing claim value**, sé það sama og það sem er notað í SSO stillingunum í CCQ.

<b>\$</b>			AD FS
🙀 File Action View Window Help			
🔶 🧼 🖄 📰 🛛 🖬			
AD FS Relyin	g Party Trusts		
A Trust Relationships	splay Name	Enabled	Type Identifier
Claims Provider Trusts	crosoft Office 365 Identity Platform	Yes	WS-T https://ogin.microsoftonline.com/ext
Relying Patternet	.u - Gaedanandbok		WS-T https://quality.ccq.cloud
Attribute Edit Claim	Rules for CCQ – Gaedahandbok 💶	×	Edit Rule - CCQ Access
Ssuance Transform Rules Issuar	ce Authorization Rules   Delegation Authorization Rul	les	You can configure this rule to send a claim based on a user's Active Directory group membership. Specify the group that the user is a member of, and specify the outgoing claim type and value to issue.
The following transform rules spe	cify the claims that will be sent to the relying party.		Claim rule name:
Order Rule Name	Issued Claims		CCQ Access
1 Email	E-Mail Address		Rule template: Send Group Membership as a Claim
2 CCQ Access	Group		
4 CCQ Published	Group		Users group:
5 CCQ Quality	Group		USER VCCQ Access Browse
6 CCQ Workbook	Group		Outgoing claim type:
7	Group		Group
9 Passtbrough - Name	Name	T	
			Outgoing name ID format:
			Unspecified
			Outgoing claim value:
			CCQ_Access
Add Rule Edit Rule	Remove Rule		
-			
	OK Cancel	Apply	
			View Rule Language OK Cancel

Nánar verður farið í það hvernig grúppur eru mappaðar saman í kaflanum **ADFS | Aðgangshópar kerfiseininga** hér fyrir neðan, en samsvarandi grúppur og sjást á myndinni hér að ofan þyrftu að líta einhvern veginn svona út CCQ megin:



## NAME REGLA

## 1. Choose Rule Type

Að lokum þarf að bæta við claim reglu af tegundinni "name."

Undir Claim rule template skal velja Pass Through or Filter an Incoming Claim og smella á Next.

<b>\$</b>	Add Transform Claim Rule Wizard
Select Rule Template	
Steps Choose Rule Type Configure Claim Rule	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template. Claim rule template: Claim rule template description: Using the Pass Through or Filter an Incoming Claim rule template you can pass through all incoming claims with a selected claim type. You can also filter the values of incoming claims with a selected claim type. You can use this rule template to create a rule that will send all incoming group claims. You can also use this rule to send only UPN claims that end with "@fabrikam". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.
	< Previous Next > Cancel

2. Configure Claim Rule

Gefa skal reglunni nafn eins og áður, og í **Incoming claim type** þarf að velja "*Name*." Nauðsynlegt er að haka í "*Pass through all claim values*" radio takkann og smella á **Finish** til að vista regluna.

<b>S</b>	Add Transform Claim Rule Wizard
Configure Rule	
Steps Choose Rule Type	You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim subure changed area through
<ul> <li>Configure Claim Rule</li> </ul>	Claim rule name:
	Passthrough - Name
	Rule template: Pass Through or Filter an Incoming Claim
	Incoming claim type: Name
	Incoming name ID format:
	Pass through all claim values
	O Pass through only a specific claim value
	Incoming claim value:
	Pass through only claim values that match a specific email suffix value:
	Email suffix value:
	Example: fabrikam.com
	Pass through only claim values that start with a specific value:
	Starts with:
	Example: FABRIKAM\
	< Previous Finish Cancel

<b>\$</b>			AD FS
🗌 File Action View Window Help			
🗢 🔿 📶 🚺 🖬			
AD FS Service Claims Provider Trusts Claims Provider Trusts Claims Provider Trusts Claims Provider Trusts Claims Provider Trusts Attribute S Authenticatio Order Rule Name 1 Email 2 CCQ Acce 3 CCQ Admir 4 CCQ Publis 5 CCQ Qualit 6 CCQ Work 7 8 9 Passthroug	Relying Party Trusts         Display Name       Microsoft Office 365 Identity Platform         CCQ - Gaedahandbok       CQ - Gaedahandbok         Litt Claim Rules for CCQ - Gaedahandbok       It         Ides       Issuance Authorization Rules       Delegation Authorization F         imm rules specify the claims that will be sent to the relying party.       Issued Claims         E-Mail Address       Essa         ss       Group         shed       Group         group       Group         group	Enabled Yes Yes Rules	Type       Identifier         WS-T       https://quality.ccq.cloud         X         Vou can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.         Claim rule name:         Passthrough       Name         Rule template:       Pass through or Filter an Incoming Claim         Incoming claim type:       Name         Incoming claim values       Image:         Pass through all claim values       Pass through only a specific claim value         Incoming claim value:       Image: Eabricam.com         Pass through only claim values that match a specific email suffix value:       Image: Eabrikam.com         Pass through only claim values that start with a specific value:       Starts with:         Example:       FABRIKAM\
			View Rule Language OK Cancel

## CCQ STILLINGAR

Til að ná SSO tengingu við CCQ þarf að huga að ýmsum stillingum í CCQ kerfinu sjálfu. Það þarf að byrja á að fara í tannhjólið uppi hægra megin og velja **Organization**. Þar er farið í flipann **CCQ access** og hakað við "ADFS login is enabled."



Ef hakað er við fyrsta gátreitinn, "ADFS login is enabled" – þá geta notendur skráð sig inn í kerfið með notandanafni og lykilorði eins og áður, en þeir hafa sömuleiðis þann valkost að nota SSO. Aðgangi að kerfiseiningum er hins vegar ennþá hægt að stýra í CCQ kerfinu. Tilgangurinn með þessum gátreit er að halda möguleikanum opnum fyrir notendur að skrá sig inn í kerfið með notandanafni og lykilorði, meðan verið er að koma á ADFS tengingu og prófa SSO virknina.

## INNSKRÁNING OG AÐGANGSSTÝRING

Ofangreindir gátreitir stýra því hvernig aðgangi og innskráningu er háttað í CCQ kerfinu.

Ákveðið samspil er á milli þessara reita og misjöfn virkni eftir því við hvað er hakað. Í öllum tilfellum þarf að vera hakað við "ADFS login is enabled". Um leið og hakað er við þennan gátreit, þá birtist valkosturinn *""User can only use ADFS to log in"* með undirvalkostum, auk fellilistanna – *"SSO information"*, "Access to Applications" og *"CCQ Groups*":

- 1. User can only use ADFS to log in
- 2. Access in CCQ is controlled by ADFS
- 3. Access is controlled by CCQ

~	ADFS login is enabled
	User can only use ADFS to log in
	Access in CCQ is controlled by ADFS
	O Access is controlled by CCQ
	Turn off automatic user deactivation
>	SSO information
>	Access to Applications
``	
	CCQ Groups

#### 1. User can only use ADFS to log in

Ef hakað er við fyrsta gátreitinn, "*ADFS login is enabled* " – þá geta notendur skráð sig inn í kerfið með notandanafni og lykilorði eins og áður, en þeir hafa sömuleiðis þann valkost að nota SSO. En þegar einnig er hakað við *"User can only use ADFS to log in*" er einungis hægt að skrá sig inn með SSO, nema með svokallaðri *Login Exception* sem verður minnst á hér á eftir. Nú þarf einnig að taka ákvörðun um hvort aðgangi að kerfiseiningum er stýrt í gegnum ADFS eða CCQ:



## 2. Access in CCQ is controlled by ADFS

Þegar búið er að setja upp og tengja ADFS og SSO virknin komin í gang er hakað við gátreitinn "*Access is controlled by ADFS*." Notendur kerfisins geta þá eins og áður sagði eingöngu notað ADFS til innskráningar í CCQ – þ.e. möguleikinn á að skrá sig inn með notandanafni og lykilorði dettur út. Þess skal samt geta að nauðsynlegt er að enn sé hakað við "*Company uses AD for login*."

Með þessari stillingu er aðgangi að kerfiseiningum alfarið stýrt í AD sem þýðir að notendur kerfisins verða að vera í réttum grúppum í AD, eigi þeir að fá aðgang að CCQ. Þetta hefur einnig í för með sér að aðgangsstýringin CCQ megin verður óvirk.

Lítið mál er að bæta við nýjum notendum í CCQ eftir að ADFS tengingu er komið á. Nýr notandi er sjálfkrafa stofnaður í kerfinu þegar hann loggar sig inn í fyrsta skipti í gegnum ADFS, að því gefnu að viðkomandi notandi er til staðar í viðeigandi grúppum í AD.

Því skal haldið til haga að þegar hakað er við "Access is controlled by ADFS", þá birtist fellilistinn Login exceptions þar sem hægt er að gera undantekningar á innskráningum.

Ef einstaka notendur eiga að geta skráð sig inn í kerfið með notandanafni og lykilorði – þó svo að ADFS innskráningin sé við lýði – þá er hægt að lista þá hér. Þessir notendur nota ekki ADFS til innskráningar og aðgangi þeirra í kerfið er því alfarið stýrt CCQ megin. Meiningin er að þetta sé eingöngu notað þegar undantekningar skjóta upp kollinum. Til dæmis þegar ráðgjafi, lögfræðingur eða einhver utanaðkomandi aðili þarf á sérstökum (eða tímabundnum) aðgangi að CCQ að halda, og erfitt reynist að réttlæta tilfæringar í AD.



#### 3. Access is controlled by CCQ

Ef fyrirtæki vilja af einhverjum ástæðum halda aðgangsstýringu að kerfiseiningum CCQ megin, en nota samt ADFS fyrir innskráningu – þá skal haka við "*Access is controlled by CCQ*." Eftir sem áður þarf einnig að vera hakað við "*Company uses AD for login*." Nýjum notendum er þá bætt við á sama hátt og áður í CCQ, og öllum aðgangi stýrt þaðan.

ADFS login is enabled
User can only use ADFS to log in
O Access in CCQ is controlled by ADFS
Access is controlled by CCQ

## Turn off automatic user deactivation

Að lokum er einn reitur ónefndur, "*Turn off automatic user deactivation*", eða Notendur verða ekki sjálfkrafa gerðir óvirkir. Ef hakað er í þennan reit eru notendur ekki gerðir óvirkir þó þeir hafi ekki skráð sig inn undanfarna 3 mánuði. Þetta er hugsað til að fyrirtæki séu ekki að borga fyrir óvirka notendur.

Athugið að þó þeir séu gerðir óvirkir eru þeir einfaldlega virkjaðir aftur næst þegar þeir skrá sig inn í kerfið, svo lengi sem þeir eru enn í viðkomandi AD aðgangshópum.

## ADFS | AÐGANGSHÓPAR KERFISEININGA

### Access to Applications, felligluggi:

Í Access to Applications þarf að mappa saman aðgangsgrúppur ADFS og CCQ.

Eins og fram kom hér að ofan, þá er mikilvægt að **outgoing claim value** viðkomandi grúppu í ADFS sé það sama og það sem er skráð hér. Fjöldi inntaksreita fer auðvitað eftir því hversu mörgum einingum fyrirtækið er í áskrift að, en það þarf að búa til aðgangsgrúppur í AD fyrir hverja einingu. Hafa skal í huga að oftast þarf 2 grúppur fyrir hverja einingu:

- 1. eina grúppu fyrir notendur með lesaðgang,
- 2. eina grúppu fyrir þá sem eru með ritaðgang,

Og að lokum grúppur fyrir aðgang að CCQ einingunum yfirhöfuð (Can access CCQ), í henni þurfa allir að vera sem mega skrá sig inn, og svo stjórnendur (Admin).

Á myndinni hér að neðan er sýnt hvernig grúppurnar eru mappaðar saman, en maður einfaldlega skráir inn nöfnin á tilsvarandi grúppum í ADFS (outgoing claim value). Nöfnin þurfa helst að vera lýsandi og eru notendur hvattir til að styðjast við tillögurnar sem hér er að finna á næstu mynd:

#### ✓ Access to Applications

Access in CCQ

Can access CCQ

Admin

QM published documents

QM workbook documents

RI read access

RI write access

Audit

Incidents & Complaints

Asset management

Competency management

QS published

QS workbook

#### Groups in AD

CCQ\_Access

CCQ\_Admin

CCQ\_QualityPublished

CCQ\_QualityManualWorkbook

CCQ\_Risk\_Read

CCQ\_Risk\_Write

CCQ\_Audit

CCQ\_IncidentsComplaints

CCQ\_AssetManagement

CCQ\_Competency

CCQ\_QeustionnairePublished

CCQ\_QuestionnaireWorkbook

> CCQ Groups

## ADFS | CCQ NOTENDAHÓPAR

Í CCQ kerfinu er hægt að búa til hina og þessa notendahópa, en undir tannhjólinu (uppi hægra megin) er valmöguleiki sem heitir **User groups**. Þessar grúppur stýra ekki beint aðgangi að kerfi, heldur eru þetta innankerfishópar sem hægt er að nýta til að stýra aðgangi að einstökum skjölum. Notandi þarf eftir sem áður að vera með aðgang að CCQ kerfinu fyrst.

	🔎 a -
User group	Approval process      Close     Save
	Template documents     Quality standards
Title	Laws and regulations     Laws and regulations     Creanization     Viser templates
Description	Software Report
User list	Attachments - overview
Select	C Open Monitor
✓ Mail group ✓ Access group ←	

Þeir aðgangshópar sem þú býrð til þar birtast í kjölfarið í **CCQ Groups** felliglugganum, en þá hópa geturðu einnig mappað við grúppur í AD. Taka skal fram að nauðsynlegt er að haka við "*Access group*" til að hópurinn birtist í **CCQ Groups** listanum.

CCQ Groups, felligluggi:

Grúppurnar eru mappaðar saman á sama hátt og í **Access to Applications** sem lýst er hér að ofan. Samsvarandi grúppur eru búnar til í AD, og nöfn þeirra – eða öllu heldur "outgoing claim value" – eru skráð í **Groups in AD** listann:

<ul> <li>CCQ Groups</li> <li>Groups in CCQ</li> </ul>	Groups in AD
Mannauðshópur	CCQ_Human_Assets

## ADFS | SSO STILLINGAR

Einn felliglugginn undir kallast SSO information, en þar þurfa þrjú atriði að vera til staðar til að ná tengingu á milli CCQ og ADFS.

- 1. Certificate
- 2. Entry point
- 3. List of domains

Ítarlegar leiðbeiningar um hvar og hvernig maður sækir rétt **Certificate** er að finna í næsta undirkafla.

Aftur á móti er tiltölulega einfalt að tilgreina hin tvö atriðin. Þegar búið er að setja upp ADFS fyrir fyrirtækið, þá þarf að taka fram inngangspunktinn í reitnum **Entry point**. Hér þarf að skrá inn vefslóðina á ADFS netþjóninn, og ef sjálfgefnar SAML stillingar eru notaðar við uppsetninguna á ADFS, þá ætti endirinn á URLinu að vera "/adfs/ls/". Mismunandi er eftir fyrirtækjum hvernig þessu er háttað. Hér er dæmi um hvernig þetta kann að líta út: https://adfs.vistun.is/adfs/ls/

Einnig þarf að skilgreina þau lén sem fyrirtækið er að nota, svo sem fyrir vefsíðuna sína eða innranet – og er það gert undir List of domains. Í tilviki Origo væri til dæmis "origo.is" fært inn í þennan reit, en hér er óþarfi að setja "https://www." fyrir framan.

	Information	
350		
Cert	tificate	
<ir< td=""><td>nsert X509 certificate here&gt;</td><td></td></ir<>	nsert X509 certificate here>	
Entr	y point	
htt	tps:// <server>.<domain>/adfs/ls</domain></server>	
htt	tps:// <server>.<domain>/adfs/ls</domain></server>	
htt List	tps:// <server>.<domain>/adfs/ls of domains</domain></server>	
htt List	tps:// <server>.<domain>/adfs/ls of domains nsert domains here&gt;</domain></server>	
htt List	tps:// <server>.<domain>/adfs/ls of domains nsert domains here&gt;</domain></server>	
htt List ( <ir< td=""><td>tps://<server>.<domain>/adfs/ls of domains nsert domains here&gt;</domain></server></td><td></td></ir<>	tps:// <server>.<domain>/adfs/ls of domains nsert domains here&gt;</domain></server>	
htt List	tps:// <server>.<domain>/adfs/ls of domains nsert domains here&gt;</domain></server>	
htt List ( <ir< td=""><td>tps://<server>.<domain>/adfs/ls of domains nsert domains here&gt;</domain></server></td><td></td></ir<>	tps:// <server>.<domain>/adfs/ls of domains nsert domains here&gt;</domain></server>	
List (	tps:// <server>.<domain>/adfs/ls of domains nsert domains here&gt;</domain></server>	
List of states of the states o	tps:// <server>.<domain>/adfs/ls of domains nsert domains here&gt;</domain></server>	
List -	tps:// <server>.<domain>/adfs/ls of domains nsert domains here&gt;</domain></server>	

## VOTTORÐ / X509 CERTIFICATE

Hægt er að fara ýmsar leiðir til að sækja vottorð fyrirtækisins.

Aðferðin sem lýst er hér á eftir, er fljótleg, einföld og ætti ekki að vefjast fyrir neinum – hvort sem viðkomandi hefur tæknilegan bakgrunn eða ekki.

Þegar búið er að setja upp ADFS og búa til "relying party trust" fyrir CCQ eins og lýst er að ofan, þá er næsta skref að sækja ákveðið skjal sem kallast **Federation metadata**. Um er að ræða .xml-skrá sem inniheldur ýmsar upplýsingar, en það sem við höfum áhuga á er svokallað X509 vottorð sem okkur vantar til að koma á tengingunni við CCQ. Til að sækja þessa skrá þarf að slá inn eftirfarandi URL í netvafrann:

https://server/FederationMetadata/2007-06/FederationMetadata.xml

Hér þarf augljóslega að skipta "server" út fyrir slóðina á ADFS netþjóninn. Federation metadata .xml-skránni er sjálfkrafa halað niður og hentugt er að opna hana í vafra.

	Open
	Always open files of this type
	Show in folder
	Cancel
FederationMetadaxml	~

Best er að nota fyrsta X509 vottorðið sem er að finna í .xml skránni.

Vottorðin eru yfirleitt nokkur, eitt sem er notað fyrir "encryption," annað fyrir "signing," o.s.frv. Fyrsta vottorðið í skránni ætti að vera það sama og er notað undir <KeyDescriptor use="signing"> á fleiri stöðum í skránni. Vottorðið virkar eins og rafræn undirskrift, sem CCQ síðan notar til að tékka hvort svörin sem ADFS netþjónninn sendir frá sér séu ósvikin.

Vottorðið sem þarf að afrita í **Certificate** reitinn í CCQ, er innan <X509Certificate> tagsins í .xml skránni. Búið er að má vottorðið á myndinni hér fyrir neðan og gera illsýnilegt. Taka skal fram að nauðsynlegt er að hafa lokið uppsetningu á ADFS og RPT fyrir CCQ, áður en þetta er reynt.

# GÁTLISTI / YFIRLIT

Ef framangreindum leiðbeiningum hefur verið fylgt samviskusamlega, þá ættirðu þegar hér er komið við sögu að hafa:

- 1. Búið til aðgangshópa í AD
- 2. Sett upp ADFS
- 3. Komið á *relying party trust* fyrir CCQ
- 4. Búið til claim reglur
  - i. eina reglu fyrir email
  - ii. group reglur fyrir aðgang að kerfiseiningum
  - iii. eina reglu fyrir *name*
- 5. Gengið frá SSO stillingum í CCQ
  - i. mappað saman aðgangsgrúppur AD og CCQ og passað upp á samræmi við outgoing claim value
  - ii. skilgreint entry point ADFS
  - iii. listað þau lén sem eru í notkun hjá fyrirtækinu
  - iv. fundið rétt X509 certificate í "federation metadata"
  - v. og síðast en ekki síst, ákveðið hvernig haga skal aðgangsstýringu og innskráningu í CCQ

Tengingin á milli AD <-> ADFS <-> CCQ ætti þá að vera farin að virka og notendur komnir með möguleikann á að skrá sig inn í kerfið með SSO.