# Развертывание ADFS на Windows Serverдля авторизации на внешних площадках

## Подготовительные действия

- 1.1. Добавить и настроить роль AD, завестипользователей.
- 1.2. Добавить роль IIS
- 1.3. Сгенерировать самоподписанный SSL сертификат (как сгенерировать

<u>самодписаный SSL сертификат</u>),либо использовать выпущенный для имеющегося домена

1.4. Если будет использоваться выпущенный сертификат, то необходимо выполнить его импорт

| Welcome to the Certificate Import Wizard  |
|---|
| This wizard helps you copy certificates, certificate trust lists, and certificate revocation<br>lists from your disk to a certificate store.  |
| A certificate, which is issued by a certification authority, is a confirmation of your identity<br>and contains information used to protect data or to establish secure network<br>connections. A certificate store is the system area where certificates are kept. |
| Store Location  |
| O Current User  |
| Local Machine   |
|   |

To continue, click Next.

🔶 🌛 Certificate Import Wizard

| Next | Cancel |
|------|--------|
|      |        |

🗧 🐓 Certificate Import Wizard

#### File to Import

Specify the file you want to import.

| File name:   | -      |
|--|--------|
| C: Yes the store of the store o | Browse |
| Personal Information Exchange-PKCS #12 (.PFX,.P12)   |        |

Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

|   |       |                                 |  |                                      |                                |              |              | 1        | Vext          | Cancel | ] |
|---|-------|---------------------------------|--|--------------------------------------|--------------------------------|--------------|--------------|----------|---------------|--------|---|
| ÷ | Şə c  | ertifica                        | te Import Wiz  | ard                                  |                                |              |              |          |               | ×      |   |
|   | Cer   | tificate :<br>Certific          | Store<br>ate stores are  | system area                          | as where ce                    | ertifica     | ates are kep | ot.      |               |        |   |
|   |       | Window<br>the cer               | ws can automa<br>tificate.   | tically select                       | a certificat                   | e stor       | re, or you c | an speci | ify a locatio | n for  |   |
|   |       | 0                               | Automatically s<br>Place all certific<br>Certificate stor  | elect the ce<br>ates in the f<br>re: | rtificate sto<br>following sto | re ba<br>ore | sed on the t | type of  | certificate   | _      |   |
|   | Selec | t Certif                        | Personal   |                                      |                                | ×            |              |          | Browse        | e      |   |
|   | Selec | ct the ce                       | ertificate store   | you want to                          | use.                           |              |              |          |               |        |   |
|   |       | Per<br>Tru<br>Ent<br>Int<br>Tru | sonal<br>sted Root Cert<br>erprise Trust<br>ermediate Cert<br>isted Publishers<br>trusted Certific | ification Aut<br>ification Aut<br>s  | horities<br>horities           | *            |              |          |               |        |   |
|   | S     | how phy                         | /sical stores  |                                      |                                |              |              | Ν        | lext          | Cancel |   |
|   |       |                                 | (  | OK                                   | Cancel                         |              |              |          |               |        |   |

Нажать «Next», а на следующем экране «Finish».

1.5. Открыть оснастку управления IIS и для «Default Web Site» в секции SSL Settings выбрать пункт «Bindings...», добавить порт 443 и выбрать импортированный ранее сертификат.

| File View Help  |   |   |   |                      |                              |              |           |                                      |
|---|---|---|---|----------------------|------------------------------|--------------|-----------|--------------------------------------|
| Connections   |   | <u> </u>  | c   |                      |                              |              |           |                                      |
| 🔍 - 🗔   🖄   😪   |   | D D   | efault We   | eb Site Hon          | ne                           |              |           |                                      |
| Start Page  |   | Filter:   |   | - 🌱 Go - 🗔           | Show All                     | Group by: Ar | ea        | -                                    |
| DEV-DREAMTEAN     Application Po  | ols   | IIS   |   |                      |                              |              |           |                                      |
| V 🧃 Sites   |   | ~?  | A   | 2                    |                              |              |           |                                      |
|   | b Site  | (i)<br>Authentic  | Compressio  | CO Default           | Directory                    | 404          | Handler   |                                      |
|   |   | Authentic   | Compressio  | Document             | Browsing                     | Enor Pages   | Mappings  |                                      |
|   |   |   |   | 215                  |                              |              | 2         |                                      |
|   |   | НТТР  | Logging   |                      | Modules                      | Output       | Request   |                                      |
|   |   | Respon  | Logging   | initial types        | modules                      | Caching      | Filtering |                                      |
|   |   | A   |   |                      |                              |              |           |                                      |
|   |   | SSL   | Open Feature  |                      |                              |              |           |                                      |
|   |   |   | Evolore   |                      |                              |              |           |                                      |
|   |   | M   | Edit Permission   | ns                   |                              |              |           |                                      |
|   |   |   | Bindinas  |                      |                              |              |           |                                      |
|   |   | Con   | Basic Settings  |                      |                              |              |           |                                      |
|   |   | 1   | View Applicatio   | ons                  |                              |              |           |                                      |
|   |   |   | View Virtual Di   | rectories            |                              |              |           |                                      |
|   |   | 1   | Manage Websi  | ite 🕨                |                              |              |           |                                      |
|   |   |   |   |                      |                              |              |           |                                      |
|   |   |   | Help  |                      |                              |              |           |                                      |
|   | Site Bindings   | <b>@</b>  | Help  |                      |                              |              |           | 7                                    |
| <u> </u>  | Site Bindings   | ee Host Name  | Help  | IP Address           | Binding                      | oforma       | r         | ?<br>Add                             |
| entic Compression D   | Site Bindings   | lost Name   | Help<br>Port<br>80  | IP Address           | Binding Ir                   | nforma       |           | ?<br>Add                             |
| entic Compression D<br>Do   | Site Bindings Type H http https   | lost Name   | Help<br>Port<br>80<br>443                                       | IP Address<br>*      | Binding Ir                   | nforma       |           | ?<br>Add<br>Edit                     |
| entic Compression D<br>Do   | Site Bindings<br>Type H<br>http<br>https<br>Edit Site Bindin  | Host Name   | Help<br>Port<br>80<br>443                                       | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove           |
| entic Compression D<br>Do<br>TTP Logging M<br>pon   | Site Bindings<br>Type H<br>http<br>https<br>Edit Site Bindin  | Host Name   | Help<br>Port<br>80<br>443                                       | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove<br>Browse |
| entic Compression D<br>Do<br>TTP Logging M<br>pon   | Site Bindings<br>Type H<br>http<br>https<br>Edit Site Bindin<br>Type:   | Host Name   | Help<br>Port<br>80<br>443                                       | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove<br>Browse |
| entic Compression D<br>Do<br>TTP Logging M<br>pon   | Site Bindings<br>Type H<br>http<br>https<br>Edit Site Bindin<br>Type:<br>https  | Host Name   | Help<br>Port<br>80<br>443<br>iddress:<br>Unassigned             | IP Address<br>*<br>* | Binding Ir<br>Port-<br>V 443 | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove<br>Browse |
| entic Compression D<br>Do<br>Do<br>TTP Logging M<br>spon                                    | Site Bindings<br>Type H<br>http<br>https<br>Edit Site Bindin<br>Type:<br>https<br>Host name:                                | Host Name   | Help<br>Port<br>80<br>443<br>iddress:<br>Unassigned             | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove<br>Browse |
| entic Compression D<br>Do<br>TTP Logging M<br>Settings                                      | Site Bindings<br>Type H<br>http<br>https<br>Edit Site Bindin<br>Type:<br>https<br>Host name:                                | Host Name   | Help<br>Port<br>80<br>443<br>uddress:<br>Unassigned             | IP Address<br>*<br>* | Binding Ir<br>V 443          | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove<br>Browse |
| Anentic Compression D<br>Do<br>Do<br>TTP Logging M<br>spon<br>Settings                      | Site Bindings Type H https Edit Site Bindin Type: https Host name: Require Se   | Host Name   | Help<br>Port<br>80<br>443<br>ddress:<br>Unassigned              | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove<br>Browse |
| Anentic Compression D<br>Do<br>Do<br>TTP Logging M<br>spon<br>Settings                      | Site Bindings Type H http https Edit Site Bindin Type: https Host name: C Require Se  | Host Name   | Help<br>Port<br>80<br>443<br>uddress:<br>Unassigned<br>dication | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove<br>Browse |
| ientic Compression D<br>Do<br>Do<br>TTP Logging M<br>ipon                                   | Site Bindings Type H http https Edit Site Bindin Type: https Host name: Require Se  | Host Name   | Help Port 80 443 ddress: Unassigned dication                    | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove<br>Browse |
| entic Compression D<br>Do<br>TTP Logging M<br>pon<br>igurat<br>jigurat                      | Site Bindings Type H http https Edit Site Bindin Type: https Host name: Bindin Require Se Disable HT                        | Host Name   | Help Port 80 443 ddress: Unassigned dication                    | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove<br>Browse |
| entic Compression D<br>Do<br>TTP Logging M<br>pon<br>ettings<br>nagement<br>igurat<br>jitor | Site Bindings Type H https Edit Site Bindin Type: https Host name: C C C C C C C C C C C C C C C C C C C                    | Host Name<br>Ing<br>IP a<br>All<br>erver Name In<br>TTP/2<br>CSP Stapling             | Help Port 80 443 ddress: Unassigned dication                    | IP Address<br>*<br>* | Binding Ir<br>V 443          | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Browse<br>Browse |
| entic Compression D<br>Do<br>TTP Logging M<br>pon<br>ettings                                | Site Bindings Type H http https Edit Site Bindin Type: https Host name: Require See Disable HT Disable OC                   | Host Name<br>Ing<br>IP a<br>erver Name In<br>TTP/2<br>CSP Stapling                    | Help Port 80 443 ddress: Unassigned dication                    | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Browse<br>Browse |
| entic Compression D<br>Do<br>TTP Logging M<br>pon<br>ettings<br>nagement<br>gurat<br>itor   | Site Bindings Type H http https Edit Site Bindin Type: https Host name: Binding Require Second                              | Host Name<br>Ing<br>IP a<br>erver Name In<br>TTP/2<br>CSP Stapling                    | Help Port 80 443 ddress: Unassigned dication                    | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | X         | ?<br>Add<br>Edit<br>Browse<br>Close  |
| entic Compression D<br>Do<br>TTP Logging M<br>pon<br>ettings<br>nagement<br>gurat<br>litor  | Site Bindings Type H http https Edit Site Bindin Type: https Host name: Disable H1 Disable OC                               | Host Name<br>Host Name<br>IP a<br>All<br>erver Name In<br>TTP/2<br>CSP Stapling<br>e: | Help Port 80 443 ddress: Unassigned dication                    | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove<br>Browse |
| entic Compression D<br>Do<br>TTP Logging M<br>pon<br>ettings<br>agement<br>gurat<br>itor    | Site Bindings Type H http https Edit Site Bindin Type: https Host name: Disable HI Disable OC SSL certificate *.testfact.ru | Host Name<br>Ing<br>IP a<br>All<br>erver Name In<br>TTP/2<br>CSP Stapling<br>e:       | Help Port 80 443 ddress: Unassigned dication                    | IP Address<br>*<br>* | Binding Ir                   | nforma<br>?  | ×         | ?<br>Add<br>Edit<br>Remove<br>Browse |

1.6. Создать пользователя в AD (например ADFS\_SVC). Это специальный сервисный аккаунт для подключения к AD.

# Добавление и настройка ADFS

# 2.1. Добавить роль ADFS



### 2.2. После установки необходимо вызвать мастер конфигурирования ADFS

## 2.3. Шаги мастера настройки следующие:



Указываем УЗ с правами администратора домена, от имени которой будем выполнять конфигурирование

| ctive Directory Federation Serv  | ices Configuration Wizard   | -                       |        | ×   |
|--|---|-------------------------|--------|-----|
| onnect to Active   | Directory Domain Services   | TARG                    | ET SER | VER |
| Welcome<br>Connect to AD DS  | Specify an account with Active Directory domain administrator pe<br>federation service configuration. | rmissions to perform th | ne     |     |
| Specify Service Properties<br>Specify Service Account<br>Specify Database<br>Review Options<br>Pre-requisite Checks<br>Installation<br>Results | Administrator (Current user)  | hange                   |        |     |

Выбираем сертификат, который мы импортировали на шаге 1.4, имя (например adfs.yourdomain.ru) и выводимое имя (оно будет отображаться на странице авторизации).

| 🚵 Active Directory Federation Serv   | ices Configuration Wizard                                    |   | -           |           | ×           |
|--|--|---|-------------|-----------|-------------|
| Specify Service Pr   | operties   | -   | T/          | ARGET SEF | VER         |
| Welcome<br>Connect to AD DS  | SSL Certificate:   | <br>View  | ]           | Import    |             |
| Specify Service Properties<br>Specify Service Account<br>Specify Database<br>Review Options<br>Pre-requisite Checks<br>Installation<br>Results | Federation Service Name:<br>Federation Service Display Name: | Example: fs.contoso.com<br>Users will see the display name at sig<br>Example: Contoso Corporation | ]<br>]n in. |           |             |
|  |  | < Previous Next > Config<br>https://blogs.technet/  | gure        | Cance     | 4<br>nttrie |

Далее выбираем тип БД, создаем ее и завершаем настройку, пройдя по оставшимся шагам мастера (на этих шагах уже никаких парамеров менять/выбирать не нужно).

# Настройка ADFS

3.1. Запускаем оснастку управления



3.2. Убедимся, что используется протокол HTTPS. Если HTTP, то меняем на HTTPS (иначе при отправке запросов на авторизацию будем получать ошибку)

|          | 🏟 AD FS   |  |             |
|----------|---|--|-------------|
|          | 🇌 File 🛛 Action   | View Window Help   |             |
|          | 🗢 🄿 🔁 🗖   | ? 🗊  |             |
|          | AD FS<br>Service<br>Attr<br>Aut<br>Cer<br>Cla<br>Dev                        | Edit Federation Service Properties<br>Revoke All Proxies<br>View | )<br>3<br>> |
| Feder    | Enc<br>Sco<br>We<br>Access  | New Window from Here Refresh Help                                | fc          |
| Gene     | ral Organization Event  | s  |             |
| Fe       | deration Service display n  | ame:   |             |
| Fa       | et CIT  |  |             |
| Ex<br>Fe | ample: Fabrikam Federation<br>deration Service name:<br>eamteam.testfact.ru | on Service   |             |
| Ex       | ample: fs.fabrikam.com  |  |             |
| E        | deration Service identifier:  |  |             |
| htt      | tps://dreamteam.testfact.n  | u/adfs/services/trust  |             |
| Ex       | ample: http://fs.fabrik.am.o  | com/adfs/services/trust  |             |
| W        | eb SSO lifetime (minutes):  | 480 🜲  |             |

3.3 Выполнить вход в <u>https://dev1.dreamteam.fact.digital</u> под своей учетной записью

3.4. Перейти в меню «Настройки» - «Аутентификация», активировать «Аутентификация SAML», внести информацию в следующие поля и нажать «Сохранить».

URL IDP SSO <u>https://adfs.yourdomain.ru/adfs/ls/</u> IDP Entity ID <u>https://adfs.yourdomain.ru/adfs/services/trust</u>

| 👽 Мое развитие   |  |
|------------------|--|
| ど База знаний    | Поставщик единого входа (SSO)                    |
| 🍯 Есть идея      | Нет Аутентификация SAML<br>URL IDP SSO *         |
| 🗴 Новости        | https:// anteam.test/mutp/adfs/ls/               |
| 😽 Пульс компании | IDP Entity ID *                                  |
| комплыия         | https://topontcam.testfactor/adfs/services/trust |

3.5. После нажатия на кнопку «Сохранить» в полях **ACS URL** и **Entity ID** появятся ссылки, которые нам потребуются позже

| ACS URL:<br>https://dev1.dreamteam.   | fact.digital/api/saml/to_01119-1 | d8f-465f-b08a-8701c19d8 | 7/acs    |
|---------------------------------------|----------------------------------|-------------------------|----------|
| Entity ID:<br>https://dev1.dreamteam. | fact.digital/api/saml/           | d8f-4e5f-b08a-8701c19dd | metadata |
| Сохранить                             |                                  |                         |          |

3.6. Возвращаемся в консоль управления ADFS и создаем новый Relying Party Trust

| 📔 AD FS  |                | Relying Party Trus  |
|--|----------------|---|
| <ul> <li>Service</li> <li>Attribute Stores</li> <li>Authentication Meth</li> <li>Certificates</li> <li>Claim Descriptions</li> <li>Device Registration</li> <li>Endpoints</li> <li>Scope Descriptions</li> <li>Web Application Pro</li> <li>Access Control Policies</li> </ul> | iods<br>xy     | Display Name<br>factnetwork.pec<br>ismyteam.testfac<br>dev1.dreamtear |
| Claims Provider Tru  | Add Relying Pa | rty Trust   |
| Application Groups   | View           | >   |
|  | New Window fi  | rom Here  |
|  | Refresh        |   |
|  | Help           |   |

# Выбираем тип «Claim aware»

훾 Add Relying Party Trust Wizard

#### Welcome

| Steps  | Welcome to the Add Relving Party Trust Wizard  |
|--|--|
| Welcome  |  |
| Select Data Source                                   | Claims-aware applications consume claims in security tokens to make authentication and<br>authorization decisions. Non-claims-aware applications are web-based and use Windows |
| Specify Display Name                                 | Integrated Authentication in the internal network and can be published through Web Application<br>Proxy for extranet access. Learn more  |
| Configure Certificate                                |  |
| Configure URL  | Claims aware   |
| Configure Identifiers                                | O Non claims aware   |
| <ul> <li>Choose Access Control<br/>Policy</li> </ul> |  |
| Ready to Add Trust                                   |  |
| Finish   |  |
|  | < Previous Start Cancel  |

Х

| 🙀 Add Relying Party Trust  | Wizard   | < |
|--|--|---|
| Select Data Source   |  |   |
| Steps<br>Welcome<br>Select Data Source<br>Specify Display Name<br>Configure Certificate<br>Configure URL<br>Configure Identifiers<br>Choose Access Control<br>Policy<br>Ready to Add Trust<br>Finish | Select an option that this wizard will use to obtain data about this relying party: <ul> <li>Import data about the relying party published online or on a local network</li> <li>Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata andines or on a local network.</li> <li>Federation metadata address (host name or URL): <ul> <li>Example: fs.contoso.com or https://www.contoso.com/app</li> </ul> </li> <li>Import data about the relying party from a file</li> <li>Use this option to import the necessary data and certificates from a relying party organization that has exported ts federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.</li> </ul> Federation metadata file location: <ul> <li>Browse</li> </ul> Provide: The relying party manually Use this option to manually input the necessary data about this relying party organization. |   |
|  | < Previous Next > Cancel   |   |

На следующем экране вводим отображаемое имя (можно использовать любое, это ни на что не влияет), нажимаем 2 раза «Next».

# Активируем протокол SAML 2.0 и вставляем ссылку вида https://dev1.dreamteam.fact.digital/api/saml/уникальный-идентификатор/acs из поля ACS URL МоейКоманды

🏟 Add Relying Party Trust Wizard

 $\times$ 

# Configure URL

| Steps  | AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If   |  |  |  |  |
|--|--|--|--|--|--|
| Welcome  | WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the<br>URLs to use. Support for the WS-Trust protocol is always enabled for a relying party. |  |  |  |  |
| Select Data Source                                   | Finally support for the WC Enderstine Provide antical location and ying party.   |  |  |  |  |
| Specify Display Name                                 |  |  |  |  |  |
| Configure Certificate                                | The WS-rederation Passive protocol URL supports Web-browser-based claims providers using the<br>WS-Federation Passive protocol.  |  |  |  |  |
| Configure URL  | Relying party WS-Federation Passive protocol URL:  |  |  |  |  |
| Configure Identifiers                                |  |  |  |  |  |
| <ul> <li>Choose Access Control<br/>Policy</li> </ul> | Example: https://fs.contoso.com/adfs/ls/   |  |  |  |  |
| Ready to Add Trust                                   | Enable support for the SAML 2.0 WebSSO protocol  |  |  |  |  |
| 🥥 Finish   | The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the<br>SAML 2.0 WebSSO protocol.   |  |  |  |  |
|  | Relying party SAML 2.0 SSO service URL:  |  |  |  |  |
|  | https://dev1.dreamteam.fact.digital/api/saml/уникальный-идентификатор/acs  |  |  |  |  |
|  | Example: https://www.contoso.com/adfs/ls/  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | < Previous Next > Cancel   |  |  |  |  |

Вставляем ссылку вида https://dev1.dreamteam.fact.digital/api/saml/уникальный-идентификатор/acs из поля **Entity ID** МоейКоманды

| 🇌 Add Relying Party Trust Wi                         | zard  | ×                |
|--|---|------------------|
| Configure Identifiers                                |   |                  |
| Steps  | Relying parties may be identified by one or more unique identifier strings. Specify the identifiers | for this relying |
| Welcome  | party trust.  |                  |
| Select Data Source                                   | Relying party trust identifier:   |                  |
| Specify Display Name                                 | https://dev1.dreamteam.fact.digital/api/saml/уникальный-идентификатоp/metadata                      | Add              |
| Configure Certificate                                | Example: https://fs.contoso.com/adfs/services/trust   |                  |
| Configure URL  | Relying party trust identifiers:  |                  |
| Configure Identifiers                                |   | Remove           |
| <ul> <li>Choose Access Control<br/>Policy</li> </ul> |   |                  |
| Ready to Add Trust                                   |   |                  |
| Finish   |   |                  |
|  |   |                  |
|  | < Previous Next >   | Cancel           |

# **Choose Access Control Policy**

| Steps                 | Choose an access control policy:  |   |     |
|-----------------------|---|---|-----|
| Welcome               | Name  | Description   | ^   |
| Select Data Source    | Permit everyone   | Grant access to everyone.                                     |     |
| Specify Display Name  | Permit everyone and require MFA   | Grant access to everyone and requir                           | ;   |
| Configure Certificate | Permit everyone and require MFA for specific group  | Grant access to everyone and requir                           |     |
| Configure LIPI        | Permit everyone and require MFA from extranet access  | Grant access to the intranet users an                         |     |
|                       | Permit everyone and require MFA from unauthenticated devices  | Grant access to everyone and requir                           |     |
| Configure Identifiers | Permit everyone and require MFA, allow automatic device registr   | Grant access to everyone and requir                           | -   |
| Choose Access Control | Permit everyone for intranet access   | Grant access to the intranet users.                           |     |
| Policy                | Permit enerific amun<br>≪   | Grant access to users of one or more                          | f I |
| Ready to Add Trust    |   |   |     |
| Finish                | Pemit everyone Pemit everyone I do not want to configure access control policies at this time. No application. <prev< th=""><th>user will be permitted access for this<br/>rious Next &gt; Cancel</th><th></th></prev<> | user will be permitted access for this<br>rious Next > Cancel |     |

翰 Add Relying Party Trust Wizard

#### Ready to Add Trust

| Steps                           | The relying p  | arty trust has  | s been config    | ured Review   | w the following settir | nos and then o | lick Next to | add the  |
|---------------------------------|--|-----------------|------------------|---------------|------------------------|----------------|--------------|----------|
| Welcome                         | relying party t  | rust to the A   | D FS configu     | ration datab  | ase.                   |                |              |          |
| Select Data Source              | Monitoring   | Identifiers     | Encryption       | Signature     | Accepted Claims        | Organization   | Endpoints    | Note + + |
| Specify Display Name            | Specify the  | monitoring s    | settings for thi | s relying par | ty trust.              |                |              |          |
| Configure Certificate           | Relying p  | arty's federa   | ation metadat    | a URL:        |                        |                |              |          |
| Configure URL                   |  |                 |                  |               |                        |                |              |          |
| Configure Identifiers           | Monit  | or relving pa   | atv              |               |                        |                |              |          |
| Choose Access Control<br>Policy |  | utomatically    | update relying   | g party       |                        |                |              |          |
| Ready to Add Trust              | This re  | lving partv's   | federation m     | etadata data  | was last checked       | on:            |              |          |
| Finish                          | < neve   | <never></never> |                  |               |                        |                |              |          |
|                                 | This relying party was last updated from federation metadata on: |                 |                  |               |                        |                |              |          |
|                                 | < neve   | er >            |                  |               |                        |                |              |          |
|                                 |  |                 |                  |               |                        |                |              |          |
|                                 |  |                 |                  |               |                        |                |              |          |
|                                 |  |                 |                  |               |                        |                |              |          |
|                                 |  |                 |                  |               |                        |                |              |          |
|                                 |  |                 |                  |               |                        |                |              |          |
|                                 |  |                 |                  |               |                        |                |              |          |
|                                 |  |                 |                  |               |                        |                |              |          |
|                                 |  |                 |                  |               |                        |                |              |          |
|                                 |  |                 |                  |               | < Previo               | ous Nex        | d >          | Cancel   |

#### 훾 Add Relying Party Trust Wizard

#### Finish

| S | teps                            |
|---|---------------------------------|
| 0 | Welcome                         |
| 6 | Select Data Source              |
| 6 | Specify Display Name            |
| 6 | Configure Certificate           |
| • | Configure URL                   |
| 6 | Configure Identifiers           |
| 6 | Choose Access Control<br>Policy |
| 6 | Ready to Add Trust              |
| • | Finish                          |
|   |                                 |
|   |                                 |
|   |                                 |
|   |                                 |
|   |                                 |
|   |                                 |
|   |                                 |
|   |                                 |
|   |                                 |
|   |                                 |
|   |                                 |

3.7. Создание правил трансформации отпечатка авторизации



Нажимаем «Add» и выбираем шаблон

 $\times$ 

| s  | Salast the template for the el   | simple that you want to enable from the following list. The description provide   |
|--|--|---|
| noose Rule Type  | details about each claim rule  | template.   |
| onfigure Claim Rule  | Claim rule template:   |   |
|  | Send LDAP Attributes as Cla  | ims 🗸   |
|  | Claim rule template descriptio   | n:  |
|  | Using the Send LDAP Attrib<br>store such as Active Direct<br>multiple claims from a single<br>a rule that will extract attribu<br>Active Directory attributes a<br>be used to send all of the u<br>memberships, use the Send | ute as Claims rule template you can select attributes from an LDAP attribute<br>by to send as claims to the relying party. Multiple attributes may be sent as<br>rule using this rule type. For example, you can use this rule template to create<br>te values for authenticated users from the displayName and telephoneNumbe<br>nd then send those values as two different outgoing claims. This rule may als<br>ser's group memberships. If you want to only send individual group<br>Group Membership as a Claim rule template. |
|  |  |   |
|  |  | < Previous Next > Cancel  |
| im rule name:  |  |   |
|  |  |   |
| and LDAP Attributes  |  |   |
| end LDAP Attributes<br>le template: Send LD/   | AP Attributes as Claims  |   |
| end LDAP Attributes  | AP Attributes as Claims  |   |
| end LDAP Attributes<br>le template: Send LD/<br>ibute store:   | AP Attributes as Claims  |   |
| end LDAP Attributes<br>le template: Send LD/<br>ibute store:<br>tive Directory   | AP Attributes as Claims  | ~   |
| end LDAP Attributes<br>le template: Send LD,<br>ibute store:<br>tive Directory<br>pping of LDAP attribu  | AP Attributes as Claims<br>tes to outgoing claim type:   | →<br>3:   |
| Ind LDAP Attributes<br>le template: Send LD,<br>ibute store:<br>tive Directory<br>pping of LDAP attribute<br>LDAP Attribute  | AP Attributes as Claims<br>tes to outgoing claim type:<br>e (Select or type to   | s:<br>Outgoing Claim Type (Select or type to add more)  |
| Ind LDAP Attributes Ie template: Send LDAP ibute store: tive Directory pping of LDAP attribute LDAP Attribute add more)  | AP Attributes as Claims<br>tes to outgoing claim type:<br>e (Select or type to   | S:<br>Outgoing Claim Type (Select or type to add more)  |
| Ind LDAP Attributes Ie template: Send LD/ ibute store: tive Directory pping of LDAP attribute     LDAP Attribute     add more)     E-Mail-Address                        | AP Attributes as Claims<br>tes to outgoing claim types<br>e (Select or type to<br>es ~   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |
| Ind LDAP Attributes Ie template: Send LDA ibute store: tive Directory pping of LDAP attribute LDAP Attribute add more) E-Mail-Address User-Principal-I                   | AP Attributes as Claims<br>tes to outgoing claim type:<br>e (Select or type to<br>es ~<br>Name ~   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |
| Ind LDAP Attributes Ie template: Send LD, ibute store: tive Directory pping of LDAP attribute     LDAP Attribute     add more)     E-Mail-Address     User-Principal-I   | AP Attributes as Claims<br>tes to outgoing claim types<br>e (Select or type to<br>es ~<br>Name ~   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |
| Ind LDAP Attributes Ie template: Send LDAP ribute store: tive Directory pping of LDAP attribute     LDAP Attribute     add more)     E-Mail-Address     User-Principal-I | AP Attributes as Claims<br>tes to outgoing claim types<br>e (Select or type to<br>es   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |
| Ind LDAP Attributes Ie template: Send LDA ibute store: tive Directory pping of LDAP attribute     LDAP Attribute     dd more)     E-Mail-Address     User-Principal-1    | AP Attributes as Claims<br>tes to outgoing claim types<br>e (Select or type to<br>es ~<br>Name ~   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |
| Ind LDAP Attributes Ie template: Send LDAP ribute store: tive Directory pping of LDAP attribute     LDAP Attribute     dd more)     E-Mail-Address     User-Principal-I  | AP Attributes as Claims<br>tes to outgoing claim types<br>e (Select or type to<br>es ~<br>Name ~   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |
| Ind LDAP Attributes Ie template: Send LD/ ribute store: tive Directory pping of LDAP attribute add more) E-Mail-Address User-Principal-1                                 | AP Attributes as Claims<br>tes to outgoing claim types<br>e (Select or type to<br>es ~<br>Name ~   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |
| Ind LDAP Attributes Ie template: Send LDA ibute store: tive Directory pping of LDAP attribute  | AP Attributes as Claims<br>tes to outgoing claim types<br>e (Select or type to<br>es ~<br>Name ~   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |
| Ind LDAP Attributes Ie template: Send LDAP ribute store: ctive Directory pping of LDAP attribute add more) E-Mail-Address User-Principal-1                               | AP Attributes as Claims<br>tes to outgoing claim types<br>e (Select or type to<br>es ~<br>Name ~   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |
| Ind LDAP Attributes Ie template: Send LDAP ribute store:  tive Directory pping of LDAP attribute add more) E-Mail-Address User-Principal-I                               | AP Attributes as Claims<br>tes to outgoing claim types<br>e (Select or type to<br>es ~<br>Name ~   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |
| Ind LDAP Attributes Ie template: Send LDA ibute store: ctive Directory pping of LDAP attribute add more) E-Mail-Address User-Principal-1                                 | AP Attributes as Claims<br>tes to outgoing claim types<br>e (Select or type to<br>es ~<br>Name ~   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |
| Ind LDAP Attributes Ie template: Send LDA ibute store:  tive Directory pping of LDAP attribute add more) E-Mail-Address User-Principal-I                                 | AP Attributes as Claims<br>tes to outgoing claim types<br>e (Select or type to<br>es ~<br>Name ~   | s:<br>Outgoing Claim Type (Select or type to add more)<br>E-Mail Address  |

.....

# Нажимаем «Add» и выбираем шаблон

翰 Add Transform Claim Rule Wizard

## Select Rule Template

| Steps                                    | Select the template for the claim rule that you want to create from the following list. The description provides  |
|--|---|
| Choose Rule Type                         | details about each claim rule template.   |
| <ul> <li>Configure Claim Rule</li> </ul> | Cain rule template:   Image: |
|  | < Previous Next > Cancel  |

| Edit Rule - Transform Nar   | ne to Name_ID  |  |   | ×                        |
|---|--|--|---|--------------------------|
| You can configure this rule<br>also map an incoming claim<br>outgoing claim type and wh | to map an incomir<br>value to an outgo<br>ether the claim va | ig claim type to an outgoing claim<br>ing claim value. Specify the incon<br>lue should be mapped to a new cl | type. As an option<br>ning claim type to<br>laim value. | n, you can<br>map to the |
| Claim rule name:  |  |  |   |                          |
| Transform Name to Name  | ID   |  |   |                          |
| Rule template: Transform a  | n Incoming Claim   |  |   |                          |
| Incoming claim type:  | E-Mail Address   |  |   | ~                        |
| Incoming name ID format:  | Unspecified  |  |   | ~                        |
| Outgoing claim type:  | Name ID  |  |   | ~                        |
| Outgoing name ID format:  | Email  |  |   | ~                        |
| Replace an incoming claim value:  | aim value with a d   | fferent outgoing claim value   |   |                          |
| Outgoing claim value:   |  |  |   | Browse                   |
| O Replace incoming e-mai  | il suffix claims with  | a new e-mail suffix  |   |                          |
| New e-mail suffix:  |  |  |   |                          |
|   | Example: fabrika   | n.com  |   |                          |
|   |  |  |   |                          |
|   |  |  |   |                          |
|   |  |  |   |                          |
|   |  |  |   |                          |
| View Rule Language  |  |  | ОК  | Cancel                   |

# 3.8. Создание группы приложений

| <ul> <li>Kelying Party Trusts</li> <li>Claims Provider Trusts</li> <li>Application Groups</li> </ul> |                       |   |
|--|-----------------------|---|
| - Application croup.   | Add Application Group |   |
|  | View                  | > |
|  | New Window from Here  |   |
|  | Refresh               |   |
|  | Help                  |   |
|  |                       |   |

🏟 Add Application Group Wizard

#### Welcome

| Steps   | Name:  |
|---|--|
| Welcome   | dev1.dreamteam.fact.digital  |
| Server application  | Description:   |
| <ul> <li>Configure Application<br/>Credentials</li> </ul> |  |
| Summary   |  |
| Complete  | Template:         Client-Server applications <ul> <li>Native application accessing a web API</li> <li>Server application accessing a web application</li> <li>Standalone applications</li> <li>Native application</li> </ul> <ul> <li>Native application</li> <li>Server application</li> <li>Web browser accessing a web application</li> </ul> <ul> <li>Web browser accessing a web application</li> <li>Standalone applications</li> <li>Native application</li> <li>Web API</li> </ul> |
|   | More information < Previous Next > Cancel  |

Х

훾 Add Application Group Wizard

#### Server application

| Steps   | Name:   |        |
|---|---|--------|
| Welcome   | dev1.dreamteam.fact.digital - Server application 1                        |        |
| Server application  |   |        |
| <ul> <li>Configure Application<br/>Credentials</li> </ul> | 410d486b-e8f1-4f30-a16d-c2b6d05b835e                                      |        |
| Summary   | Redirect URI:   |        |
| Complete  | https://dev1.dreamteam.fact.digital/api/saml/уникальный-идентификатор/acs | Add    |
|   | Description:  | Remove |
|   | < Previous Next >   | Cancel |

Нужно отметить поле «Generate a shared secret». Сам этот секрет нигде прописывать не нужно, но без него нельзя завершить настройку.

| Add Application Group W   | izard<br>Gradaatiala  | ×       |
|---|---|---------|
| configure Application   |   |         |
| Steps<br>• Welcome<br>• Server application<br>• Configure Application<br>Credentials<br>• Summary<br>• Complete | Select credentials used by the application to authenticate itself with AD FS when requesting access tokens         □ Register a key used to sign JSON Web Tokens for authentication         □ Configure         □ Windows Integrated Authentication         Select the AD Account:         Example: CONTOSO vexpensevc         Senerate a shared secret         Secret:         QTtXGDGXbiU2Z3BoLw_cXKsz_ZtLfTsdFgeJXZL0       Copy to clipboar         Image: Copy and save the secret. You will not be able to view the secret after the application group i created. You can reset the secret later if required. | rd<br>s |
|   | < Previous Next > Cancel  |         |

На следующем экране нажимаем «Next», а затем «Close».

Правый щелчок мыши на вновь созданном Application Group и выбираем «Properties»

| AD FS   | Application Groups   |                              |
|---|--|------------------------------|
| <ul> <li>Service</li> <li>Attribute Stores</li> <li>Authentication Methods</li> <li>Certificates</li> <li>Claim Descriptions</li> <li>Device Registration</li> <li>Endpoints</li> <li>Scope Descriptions</li> <li>Web Application Proxy</li> <li>Access Control Policies</li> <li>Relying Party Trusts</li> <li>Claims Provider Trusts</li> <li>Application Groups</li> </ul> | Name<br>factnetwork.peopleforce<br>dev1.dreamteam<br>dev1.dreamteam.fact.digital<br>ismyteam.testfact.ru | Properties<br>Delete<br>Help |

| dev1.dreamteam Properties                                 | × |
|---|---|
| General   |   |
| Name:   |   |
| dev1.dreamteam  |   |
| Description:  |   |
|   |   |
|   |   |
|   |   |
| Applications:   |   |
| Name Description  |   |
| Server application<br>dev1.dreamteam - Server application |   |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |
| Add application Edit Remove                               |   |
| OK Cancel Apply   |   |

🏟 Add a new application to dev1.dreamteam

#### Welcome

| Steps   | Name:  |
|---|--|
| Welcome   | dev1.dreamteam   |
| Configure Web API   | Description  |
| Apply Access Control Policy                               |  |
| <ul> <li>Configure Application<br/>Permissions</li> </ul> |  |
| Summary   | Template:  |
| Complete  | Standalone application         Image: Server application         Image: Web API         More information |
|   | < Previous Next > Cancel   |

翰 Add a new application to dev1.dreamteam

# Configure Web API

| Steps   | Name:   |        |
|---|---|--------|
| Welcome   | dev1.dreamteam - Web API  |        |
| Configure Web API   |   |        |
| Apply Access Control Policy                               | https://dev1.dreamteam.fact.digital/api/saml/уникальный-илентификатор/acs | Add    |
| <ul> <li>Configure Application<br/>Permissions</li> </ul> |   | Remove |
| Summary   |   |        |
| Complete  |   |        |
|   | Description:  | Cancel |

× [



# Choose Access Control Policy

| Steps   | Choose an access control policy:   |  |
|---|--|--|
| Welcome   | Name   | Description  |
| Configure Web API   | Permit everyone  | Grant access to everyone.  |
| <ul> <li>Apply Access Control Policy</li> <li>Configure Application<br/>Permissions</li> <li>Summary</li> <li>Complete</li> </ul> | Permit everyone and require MFA<br>Permit everyone and require MFA for specific group<br>Permit everyone and require MFA from extranet access<br>Permit everyone and require MFA from unauthenticated<br>Permit everyone and require MFA, allow automatic devi<br>Permit everyone for intranet access<br>Permit specific group | Grant access to everyone and require MFAf<br>Grant access to everyone and require MFAf<br>Grant access to the intranet users and requir<br>Grant access to everyone and require MFAf<br>Grant access to everyone and require MFAf<br>Grant access to the intranet users.<br>Grant access to users of one or more specifi |
|   | Permit everyone Permit everyone I do not want to configure the access control policy at the application.   | is time. No users will be permitted access for this  |

#### **Configure Application Permissions**

| Steps   | Configure permissions                             | s to enable client applications to access this Web API.  |                       |           |
|---|---|--|-----------------------|-----------|
| Welcome   | Client application (cal                           | ller):   |                       |           |
| Configure Web API   | Name  | Description  |                       |           |
| Apply Access Control Policy                               | dev1.dreamteam - S                                | Server application   |                       |           |
| <ul> <li>Configure Application<br/>Permissions</li> </ul> |   |  |                       | '         |
| Summary   |   |  |                       |           |
| Complete  |   |  |                       |           |
|   |   |  | Add                   | Remove    |
|   | Permitted scopes:                                 |  |                       |           |
|   | Scope Name  | Description  |                       | ^         |
|   | ☐ allatclaims<br>☐ aza<br>☐ email<br>☐ logon_cert | Requests the access token claims in the identity toker<br>Scope allows broker client to request primary refresh to<br>Request the email claim for the signed in user.<br>The logon_cert scope allows an application to request | ı.<br>oken.<br>t logo |           |
|   | 🗹 openid  | Request use of the OpenID Connect authorization pro  | tocol.                |           |
|   | profile   | Request profile related claims for the signed in user.   |                       |           |
|   | vpn_cert  | Request permission for the application to access the re-<br>The vpn cert scope allows an application to request \  | esour<br>√PN          | ~         |
|   | - T Voir Con                                      |  |                       | New scope |
|   |   | < Previous   | Next >                | Cancel    |

Еще раз нажимаем «Next» и «Close».

**3.9.** В процессе настройки, мастером, возможно, будет предложено выпустить сертификаты, которые используется для подписи и шифрования. Если этого не произойдет, то нужно будет создать их самостоятельно. и указать его в личном кабинете «МояКоманды».

| AD FS \Service\Certificates   |   |   |  |
|---|---|---|--|
| 📔 AD FS   | Certificates  |   | Actions  |
| <ul> <li>Service</li> <li>Attribute Stores</li> <li>Authentication Methods</li> <li>Certificates</li> <li>Claim Descriptions</li> <li>Device Registration</li> <li>Endpoints</li> <li>Scope Descriptions roxy</li> <li>Access Control Policies</li> <li>Relying Party Trusts</li> <li>Claims Provider Trusts</li> <li>Application Groups</li> </ul> | Subject<br>Service communications<br>CN=* testfact.ru<br>Token-decrypting<br>CN=ADFS Encryption - testfact.ru<br>Token-signing<br>CN=ADFS Signing - testfact.ru | Issuer<br>CN=R3, O=Let's<br>CN=ADFS Enon<br>CN=ADFS Signi | Certificates<br>Add Token-Signing Certificate<br>Add Token-Decrypting Certificate<br>Set Service Communications Certificate<br>View<br>New Window from Here<br>Refresh<br>Help |

 $\times$ 

Сертификат для подписи необходимо сохранить в файл, конвертировать в формат рет и в текстовом виде вставить в поле «Сертификат» (только сам сертификат без секций «BEGIN CERTIFICATE» и «END CERTIFICATE») в личном кабинете «МояКоманды».





|  | Еще | один | вариант, | при | котором | заработала | авторизация: |
|--|-----|------|----------|-----|---------|------------|--------------|
|--|-----|------|----------|-----|---------|------------|--------------|

| Jance T<br>The follo | ransform Rule                  | es<br>m rules specify the claims                                     | that will be sent to                         | the relving party.                                   |  |                                     |
|----------------------|--------------------------------|--|--|--|--|-------------------------------------|
| Order                | -<br>Rule Name                 |  | Issued Cla                                   | ims  |  |                                     |
| 1                    | Send LDAP                      | Attributes   | E-Mail Add                                   | Iress  |  |                                     |
| 2                    | Transform N                    | lame to Name_ID  | Name ID                                      |  |  |                                     |
|                      | Edit Ru                        | ile - Send LDAP Attribu  | tes  |  |  |                                     |
|                      | You ca<br>to extra<br>from the | n configure this rule to se<br>act LDAP attributes. Speci<br>e rule. | nd the values of LI<br>ify how the attribute | DAP attributes as claims<br>es will map to the outgo | s. Select an attribute<br>ing claim types that | e store from whic<br>will be issued |
|                      | Claim n                        | ule name:  |  |  |  |                                     |
|                      | Send I                         | LDAP Attributes  |  |  |  |                                     |
|                      | Rule te                        | mplate: Send LDAP Attrib   | utes as Claims                               |  |  |                                     |
|                      | Attribut                       | e store:   |  |  |  |                                     |
|                      | Active                         | Directory  |  |  | ~  |                                     |
|                      | neuve                          | Directory  |  |  |  |                                     |
|                      | Mappin                         | ng of LDAP attributes to ou  | utgoing claim types                          | :  |  |                                     |
|                      |                                | LDAP Attribute (Select<br>add more)                                  | t or type to                                 | Outgoing Claim Type                                  | (Select or type to a                           | dd more)                            |
| Add R                | lule 🕨                         | E-Mail-Addresses   | ~  | E-Mail Address                                       |  | `                                   |
| <u>M</u> ad III      | *                              |  | ~  |  |  | `                                   |
|                      |                                |  |  |  |  |                                     |
|                      |                                |  |  |  |  |                                     |
|                      |                                |  |  |  |  |                                     |
|                      |                                |  |  |  |  |                                     |
|                      |                                |  |  |  |  |                                     |
|                      |                                |  |  |  |  |                                     |
|                      |                                |  |  |  |  |                                     |
|                      |                                |  |  |  |  |                                     |
|                      |                                |  |  |  |  |                                     |
|                      |                                |  |  |  |  |                                     |
|                      |                                |  |  |  |  |                                     |
|                      | Mour                           | Rule Language  |  |  | OK   | Cancel                              |

| Edit | t Claim       | Issuance Policy    | for dev1.dreamteam.fact   | digital   |  | $\times$                               |   |  |
|------|---------------|--------------------|---|---|--|--|---|--|
| Iss  | Jance T       | ransform Rules     |   |   |  |  |   |  |
| ٦    | The follo     | wing transform ru  | les specify the claims that wil   | l be sent to the relyin   | g party.   |  |   |  |
|      | Order         | Rule Name          |   | Issued Claims   |  |  |   |  |
|      | 1             | Send LDAP Attri    | ibutes  | E-Mail Address  |  |  |   |  |
|      | 2             | Transform Name     | e to Name_ID  | Name ID   |  |  |   |  |
|      |               |                    | Edit Rule - Transform Na<br>You can configure this rule<br>also map an incoming clair<br>outgoing claim type and wi | me to Name_ID<br>e to map an incoming<br>n value to an outgoir<br>hether the claim valu | claim type to<br>ng claim value<br>e should be r | an outgoi<br>e. Specify t<br>mapped to | ng claim type. As an<br>the incoming claim ty<br>a new claim value. | option, you can<br>pe to map to the<br>Y |
|      |               |                    | Transform Name to Name  |   |  |  |   | Y  |
|      |               |                    | Transioni Name to Name  |   |  |  |   | I  |
|      |               |                    | Rule template: Transform a  | an Incoming Claim   |  |  |   |  |
|      |               |                    | Incoming claim type:  | E-Mail Address  |  |  |   | ~  |
|      |               |                    | Incoming name ID format:  | Unspecified   |  |  |   | ~  |
|      |               |                    | Outgoing claim type:  | Name ID   |  |  |   | ~  |
|      |               |                    | Outgoing name ID format:  | Email   |  |  |   | ~  |
|      | <u>A</u> dd R | ule <u>E</u> dit F | Pass through all claim v  | values  |  |  |   |  |
|      |               |                    | O Replace an incoming o   | laim value with a diff  | erent outgoin                                    | ig claim va                            | lue   |  |
|      |               |                    | Incoming claim value:   |   |  |  |   |  |
|      |               |                    | Outgoing claim value:   |   |  |  |   | Browse                                   |
|      |               |                    | O Replace incoming e-ma   | ail suffix claims with a  | new e-mail s                                     | uffix                                  |   |  |
|      |               |                    | New e-mail suffix:  |   |  |  |   |  |
|      |               |                    |   | Example: fabrikam   | .com   |  |   |  |
|      |               |                    |   |   |  |  |   |  |
|      |               |                    |   |   |  |  |   |  |
|      |               |                    |   |   |  |  |   |  |
|      |               |                    |   |   |  |  |   |  |
|      |               |                    | View Rule Language  |   |  |  | OK  | Cancel                                   |
|      |               |                    |   |   |  |  |   |  |

При этом, в УЗ пользователя в AD должно быть корректное значение в поле E-mail:

| First name:          | þleg                  | Initials: T | .A.    |
|----------------------|-----------------------|-------------|--------|
| Last name:           | Test                  |             |        |
| Display name:        | Test Oleg             |             |        |
| Description:         |                       |             |        |
| Office:              |                       |             |        |
| Telephone number:    | +789825635            |             | Other  |
|                      |                       |             | ourior |
| E-mail:              | @poreck@@fact.digital |             |        |
| E-mail:<br>Web page: | @fact.digital         |             | Other  |
| E-mail:<br>Web page: | @fact.digital         |             | Other  |
| E-mail:<br>Web page: | @fact.digital         |             | Other  |
| E-mail:<br>Web page: | @fact.digital         |             | Other  |