

# **НАСТРОЙКА** VPN СОЕДИНЕНИЯ

- 1. Скачайте и установите на личный компьютер следующие программы и файлы:
  - <u>eToken PKI Client;</u>
  - Cisco VPN Client:
    - для 32 разрядной операционной системы;
    - ф для 64 разрядной операционной системы;
- В службе поддержки пользователей (СПП) запросите Сертификаты. Для этого напишите письмо в произвольной форме на адрес <u>oos@qiwi.ru</u> с просьбой выслать сертификаты для подключения к VPN, а так же Пароль и Имя учетной группы. В теме письма укажите «Сертификат для VPN».
- 3. Экспортируйте сертификаты СА01 и ROOT СА в систему двойным щелчком мыши.
  - Для сертификата СА01 выберете автоматический способ выбора хранилища.
  - Сертификат ROOT CA установите вручную в Доверенные корневые центры сертификации (Рис. 1).

#### Рис. 1. Экспорт сертификатов

4. После успешной установки всех программ запустите Cisco VPN Client (Рис. 2).

## Рис. 2. Программа Cisco VPN Client

| 👌 status: Disconnected   VPN Client - Version 5.0.07.0410 | )    |           |       |
|---|------|-----------|-------|
| Connection Entries Status Certificates Log Options Help   |      |           |       |
| Connect New Import Modify Delete                          |      |           | cisco |
| Connection Entries Certificates Log                       |      |           |       |
| Connection Entry  | Host | Transport |       |
|   |      |           |       |
|   |      |           |       |
|   |      |           |       |
|   |      |           |       |
|   |      |           |       |
|   |      |           |       |
|   |      |           |       |
|   |      |           |       |
|   |      |           |       |
|   |      |           |       |
| Not connected.  |      |           |       |

- 5. Нажмите кнопку NEW и в появившемся окне заполните поля (Рис. 3):
- Рис. 3. Настройка параметров нового соединения

| VPN Client   Create New VPN Connection Entry  | ×             |
|---|---------------|
| Connection Entry:   |               |
| Description:  |               |
| Host:   | cisco         |
| Authentication Transport Backup Servers Dial-Up   |               |
| <u>G</u> roup Authentication <u>M</u> utual Group Aut   | uthentication |
| Name:   |               |
| Password:   |               |
| Confirm Password:   |               |
| <ul> <li>Certificate Authentication</li> <li>Name:</li> <li>Send CA, Certificate Chain</li> </ul> |               |
| Erase User Password   | Cancel        |

- Connection Entry и Description введите любое название, например, QIWI.
- Host укажите адрес сервера 79.142.22.2.

- Name, Password и Confirm Password укажите Имя и Пароль группы высланные вам в письме от СПП (см. <u>1 пункт</u>). запросите в Службе технической поддержки. Если вы это не делали ранее, тогда напишите в произвольной форме письмо по адресу <u>oos@qiwi.ru</u>, с просьбой выслать данные по указанным пунктам. В теме письма укажите «Сертификат для VPN».
- 6. Нажмите кнопку Save.
- 7. В открытом окне *Cisco VPN Client* выберите только что созданную настройку и нажмите кнопку **Connect** (<u>Рис.</u> <u>4</u>).

#### Рис. 4. Выбор соединения

| 👌 status: Disconnected   VPN Client    | - Version 5.0.07.0410 |             |           |                 |
|--|-----------------------|-------------|-----------|-----------------|
| Connection Entries Status Certificates | Log Options Help      |             |           |                 |
| Connect New Import                     | Modify Delete         |             |           | uluilu<br>cisco |
| Connection Entries Certificates Log    |                       |             |           |                 |
| Connection Entry                       |                       | Host        | Transport |                 |
| qi <del>w</del> i                      |                       | 79.142.22.2 | IPSec/UDP |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
|  |                       |             |           |                 |
| <u> </u>                               |                       |             |           |                 |
| Not connected.                         |                       |             |           | ///             |

8. После этого появиться окно, в котором необходимо ввести ваши учётные данные (Рис. 5):

Рис. 5. Ввод доменных авторизационных данных

| PN Client   User Authentication for "qiwi"                      |   |  |  |
|---|---|--|--|
| The server has request authentication.                          | ed the following information to complete the user |  |  |
| uluulu <u>U</u> sername:  <br><b>cisco</b><br><u>P</u> assword: | usrp\i.ivanov<br>******                           |  |  |
|   | OK Cancel   |  |  |

- Username имя пользователя, в формате usrpli.ivanov;
- Password доменный пароль.
- 9. Нажмите кнопку ОК.

После успешного ввода данных окно закроется и в области уведомлений появиться значок закрытого желтого замка (Рис. 6).

Рис. 6. Область уведомлений Windows



Теперь у вас есть доступ к внутреннему сайту для получения сертификата.

10. В браузере *Internet Explorer* откройте следующую страницу <u>http://v-rt-ca01.rt.local/certsrv/.</u> Система попросит вас ввести учётные данные от домена USRP (<u>Puc. 7</u>).

Рис. 7. Подключение к v-rt-ca01.rt.local

| Подключение к v-  | rt-ca01.rt.local             |
|-------------------|------------------------------|
| <b>R</b>          | GE                           |
| Выполняется подкл | ючение к v-rt-ca01.rt.local. |
| Подьзователь:     | 🖸 usrp\j.ivanov 💽 🗾          |
| Пароль:           | •••••                        |
|                   | Сохранить пароль             |
|                   | ОК Отнена                    |

- Пользователь имя пользователя, в формате usrpli.ivanov,
- Пароль доменный пароль.
- 11. После успешного ввода данных откроется следующая страничка:

#### Рис. 8. Главная страница службы сертификации Active Directory

| 🦉 Службы сертификации Active Directory (Microsoft) - Windows Internet Explorer  |
|---|
| Файл Правка Вид Избранное Сервис Справка  |
| S ≥  ktp://v-rt-ca01.rt.local/certsrv/  |
| 🖕 Избранное 🖉 Службы сертификации Active Directory (Microsoft)  |
| Службы сертификации Active Directory ( <b>Microsoft</b> ) САD1  |
| Добро пожаловать  |
| Этот веб-сайт позволяет запросить сертификат для вашего обозревателя веба, клиента электронной почты, других программ. С помощ<br>зависимости от типа запрошенного сертификата, выполнять другие действия, связанные с обеспечением безопасности в Интернете. |
| Этот веб-сайт позволяет также загрузить сертификат Центра Сертификации (ЦС), цепочку сертификатов или список отзыва сертификат  |
| Дополнительные сведения о службе сертификатов Active Directory см. в документации служб сертификации Active Directory.  |
| Выберите нужное действие:   |
|   |
| просмотр состояния ожидаемого запроса сертификата<br>Загрузка сертификата IIC, целочки сертификатов или CRI   |
|   |
|   |

- 12. Последовательно нажмите ссылки: Запросить сертификат **> Создать и выдать запрос к этому ЦС**.
- 13. На новой странице в поле Шаблон сертификата выберите Пользователь с eToken, в поле Размер ключа выберите размер 1024 (<u>Рис. 9</u>).

Рис. 9. Настройка параметров сертификата в службе сертификации Active Directory

| 🥭 Службы сертификации Active Directory (Microsoft) - Windows Internet Explorer   |
|--|
| Файл Правка Вид Избранное Сервис Справка   |
| Solution of the second sec |
| 🖕 Избранное 🛛 🏉 Службы сертификации Active Directory (Microsoft)   |
| Commentation Discology / ##  |
| Cлужов сертификации Active Directory ( <b>илстозон</b> ) CADT  |
| Расширенный запрос сертификата   |
| Шаблон сертификата:  |
| Пользователь с eToken 💌  |
|  |
| паражетра клюта.<br>© Создать новый набол ключей — О Использовать существующий набол ключей  |
| CSP: eToken Base Cryptographic Provider  |
| Использование ключей: @ Exchange   |
| Размер ключа: 1024 Минимальный:1024 (отандартные размеры ключей: <u>1024 2048</u> .)   |
| • Автоматическое имя контейнера ключа • Заданное пользователем имя контейнера ключа  |
| 🗖 Пометить ключ как экспортируемый   |
| 🜌 Включить усиленную защиту закрытого ключа  |
| Дополнительные параметры:  |
| Формат запроса: 💿 СМС 🔷 С РКСS10   |
| Алгоритм хеширования: SHA-1 💌  |
| Используется только для подписания запроса.  |
| 🗆 Сохранить запрос   |
|  |
|  |
| Понятное имя:  |
|  |
| Выдать >   |
|  |
|  |

14. Нажмите кнопку Выдать, и введите пароль от eToken (Рис. 10).

#### Рис. 10. Ввод пароля eToken

| 🔁 Вход: i.ivanov  |                       |  |  |
|-------------------|-----------------------|--|--|
|                   | вход на етокеп eToken |  |  |
| Введите пароль еї | ĩoken                 |  |  |
| Имя eToken:       | i.ivanov              |  |  |
| Пароль:           | ******                |  |  |
| Текущий язык: EN  |                       |  |  |
|                   | ОК Отмена             |  |  |

15. Далее нажмите ссылку Установить этот сертификат (Рис. 11).

### Рис. 11. Установка сертификата

| 🔏 Службы сертификации Active Directory (Microsoft) - Windows Internet I |           |            |                          |                 |                             |
|---|-----------|------------|--------------------------|-----------------|-----------------------------|
| <u>Ф</u> айл  | Правка    | Вид        | <u>И</u> збранное        | С <u>е</u> рвис | Справка                     |
| 0   | ) - 🧧     | http:      | //v-rt-ca01. <b>rt. </b> | ocal/certsr     | rv/certfnsh.asp             |
| 🔶 Изб   | ранное    | <b>6</b> 0 | тужбы сертиф             | рикации Ас      | ctive Directory (Microsoft) |
| Слух  | кбы серти | іфика      | ции Active D             | Directory (     | ( <b>Microsoft</b> ) CA01   |
| Сер   | тифика    | ат ве      | ыдан                     |                 |                             |
| Запрошенный вами сертификат был вам выдан.                              |           |            |                          |                 |                             |
| Установить этот сертификат  |           |            |                          |                 |                             |
| Сохранить ответ   |           |            |                          |                 |                             |
|   |           |            |                          |                 |                             |

Теперь на eToken записан сертификат, который необходим для настройки полноценного VPN.

16. Снова откройте *Cisco VPN Client* и нажмите кнопку **NEW** (<u>Puc. 12</u>). Настройте параметры в соответствии с описанием:

#### Рис. 12. Ввод параметров для vpn соединения

| 👶 VPN Client 📔 Create New VPN Connection Entry  | ×                 |
|---|-------------------|
| Connection Entry: giwi vpn  |                   |
| Description: giwi vpn   | cisco             |
| Host: 79.142.22.2   |                   |
| Authentication Transport Backup Servers Dial-Up   |                   |
| C Group Authentication C Mutual Gro   | up Authentication |
| Name:   |                   |
| Password:   |                   |
| C <u>o</u> nfirm Password:  |                   |
| <ul> <li>Certificate Authentication</li> <li><u>N</u>ame: 1 - Ivanov Ivan (Microsoft)</li> <li>Send CA Certificate Chain</li> </ul> |                   |
| Erase User Password Save  | Cancel            |

- Connection Entry и Description укажите любое название, например, QIWI VPN.
- **Host** укажите адрес нашего сервера 79.142.22.2.
- Установите флаг Certificate Authentication и выберите ваш доменный сертификат.
- 17. Нажмите кнопку Save.
- 18. В открытом окне Cisco VPN Client выберите вновь созданную конфигурацию подключения и нажмите кнопку Connect.

После нажатия кнопки появиться запрос на ввод пароля от eToken (Рис. 13).

#### Рис. 13. Ввод пароля eToken

| 🚍 Вход: i.ivanov  |                       |
|-------------------|-----------------------|
|                   | вход на етокеп еТокеп |
| Введите пароль еТ | ōken                  |
| Имя eToken:       | i.ivanov              |
| Пароль:           | *******               |
|                   | Текущий язык: EN      |
|                   | ОК Отмена             |

#### 19. Введите пароль и нажмите кнопку ОК.



Пароль желательно ввести в течение 20 секунд.

В случае успеха в области уведомлений снова появиться желтый закрытый замок (Рис. 14).

Рис. 14. Область уведомлений



Теперь вы имеете доступ ко всем внутренним ресурсам компании.