

**Buypass AS**

Nydalsveien 30A, PO Box 4364 Nydalen

Tel.: +47 23 14 59 00

E

-

mail: kundeservice@buypass.no

N

-

Oslo, Norway

0402

Fax: +47 23 14 59 01

VAT: NO 983 163 327

**INTEGRATION GUIDE**

**–**

**BP CODE**

Windows 2012 r2 Direct Access

**OPEN**

Version

:

1.0

Document date:

21.02.2017

**INTEGRATIONGUIDE**

**History of change**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Version** | **Date** | **Status** | **Description/Change** |
| 1.0 | 21.02.2017 | Final | Final |

**Contributors**

|  |  |
| --- | --- |
|  |  |
| **Company name** | **Name** |
| Buypass | Asmer Helez |

**Table of content**

[1.1 Technical requirements: 3](#_Toc475514625)

[1.2 Configure BP Code Manager 3](#_Toc475514626)

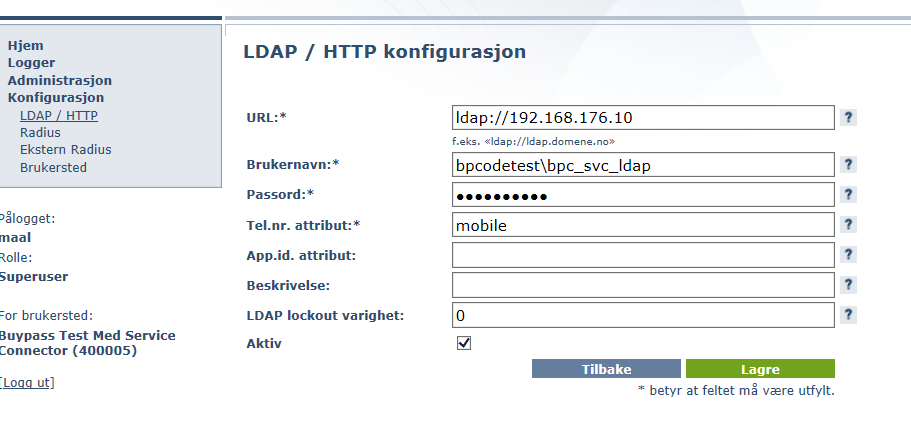
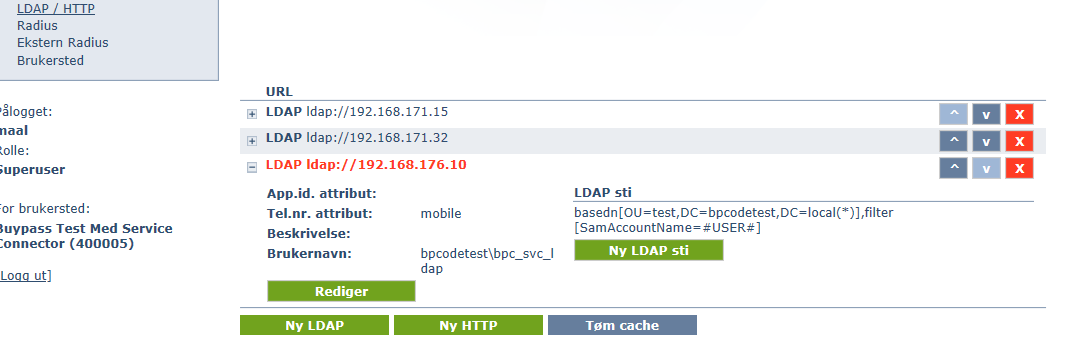
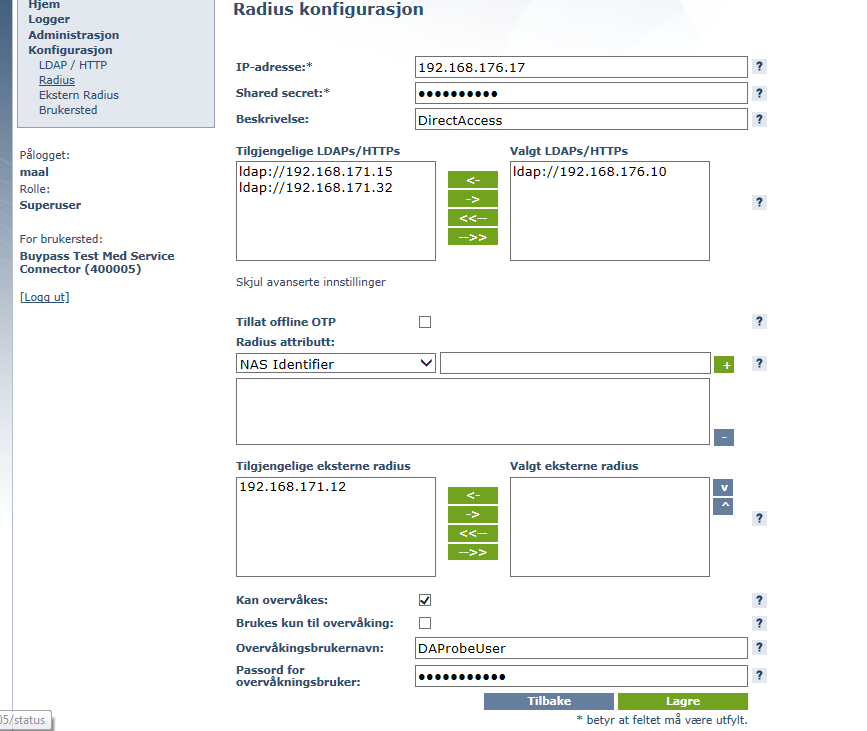
[1.3 Configure certificate templates 4](#_Toc475514627)

[1.4 Test from the client 12](#_Toc475514628)

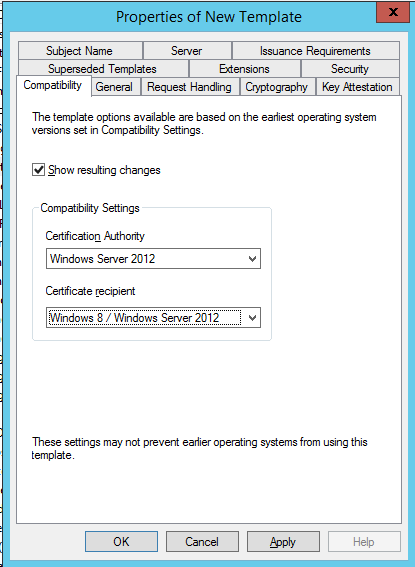
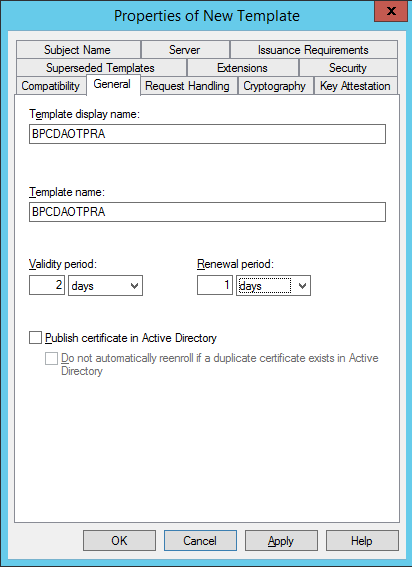
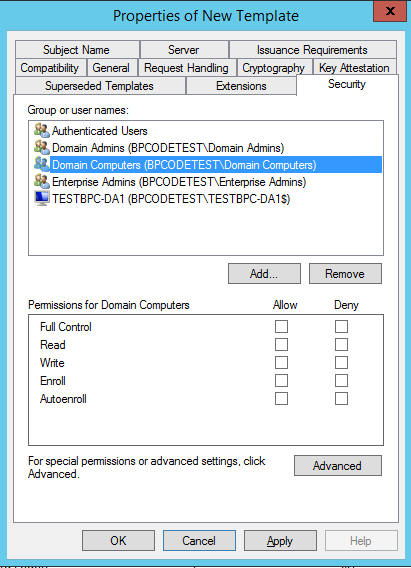
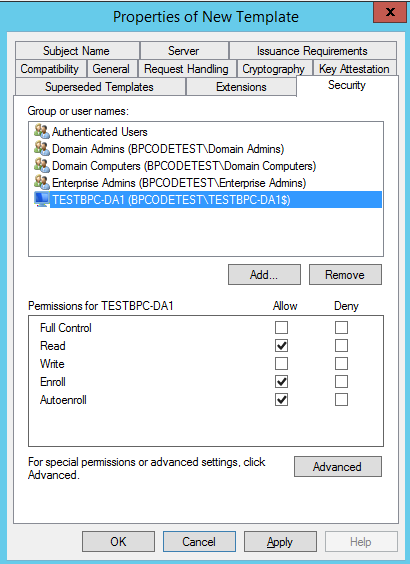
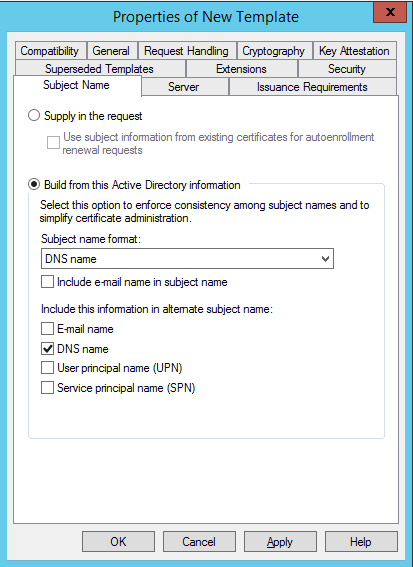
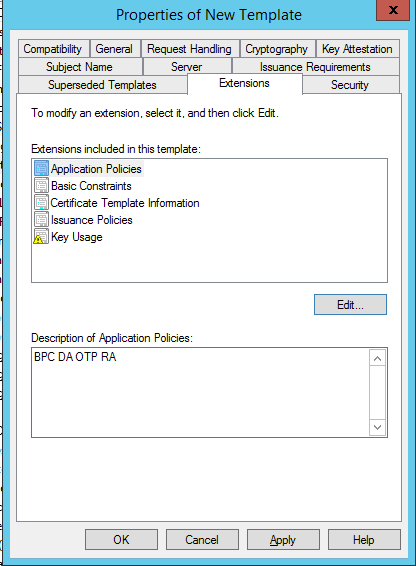
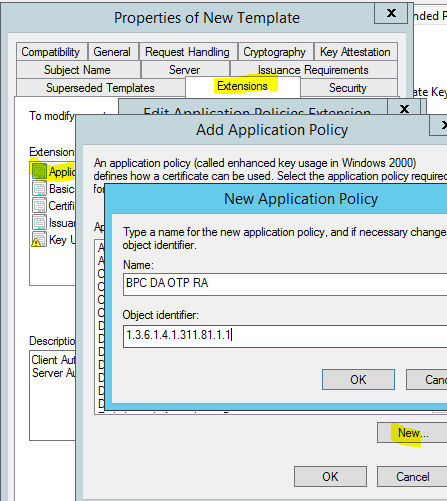
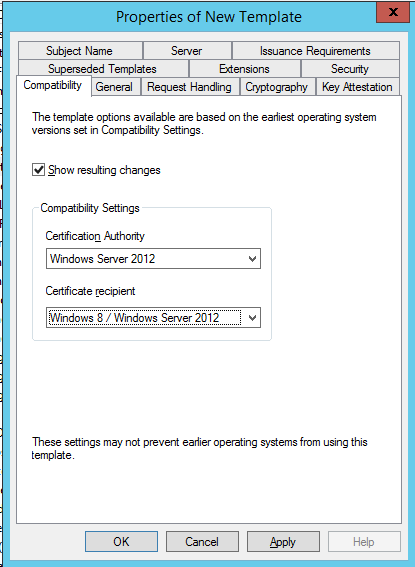
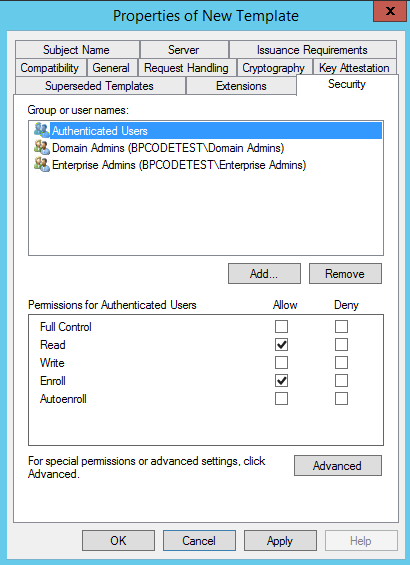
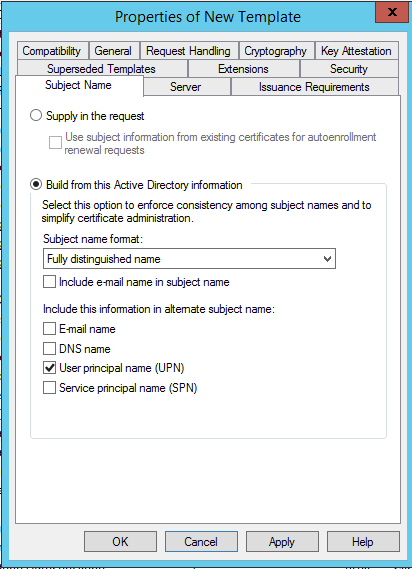
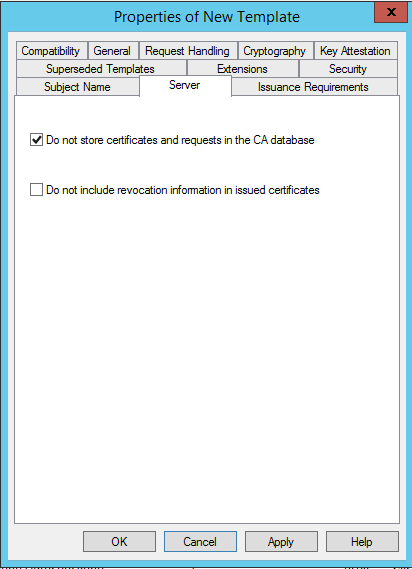
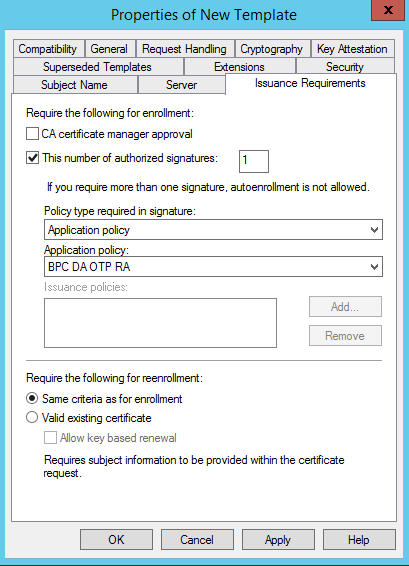
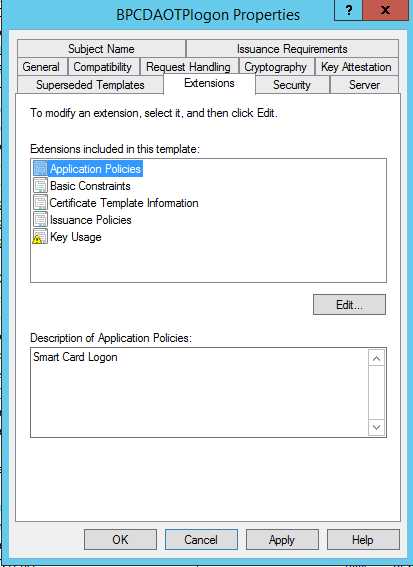
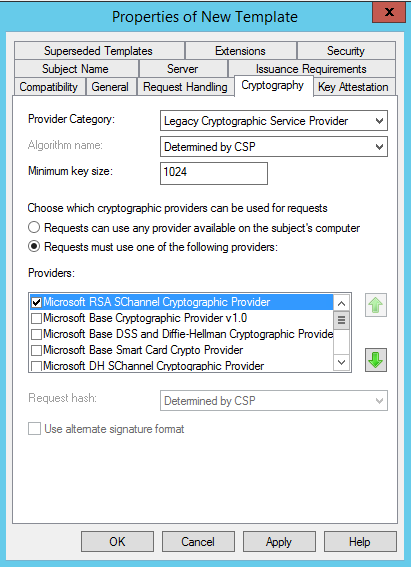
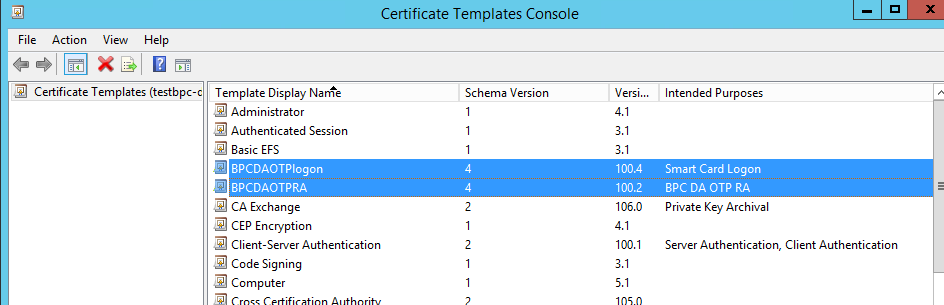
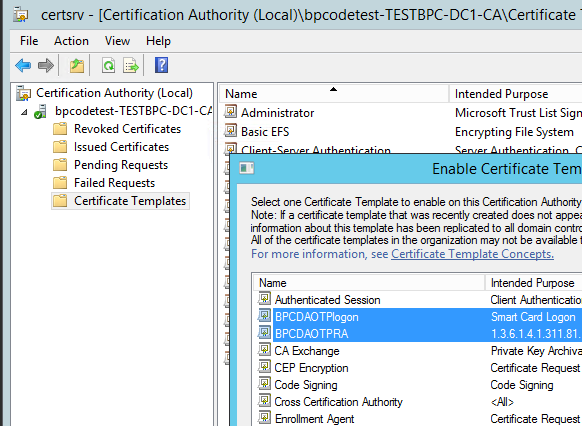
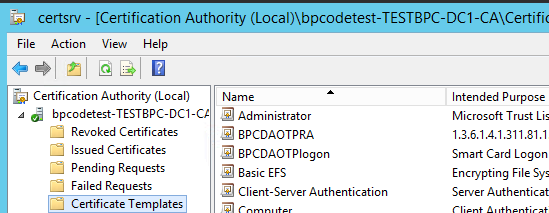
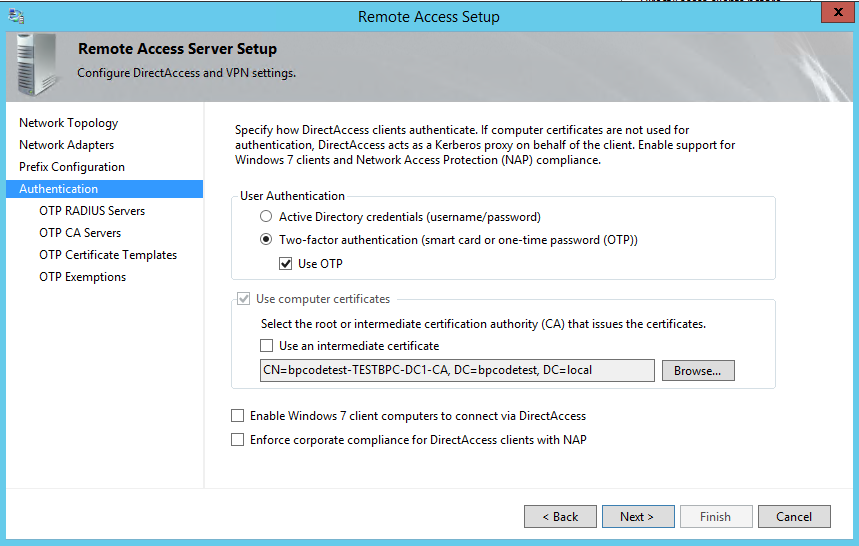
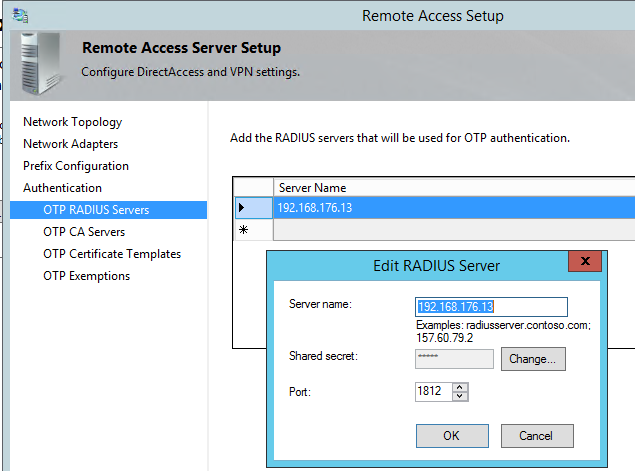
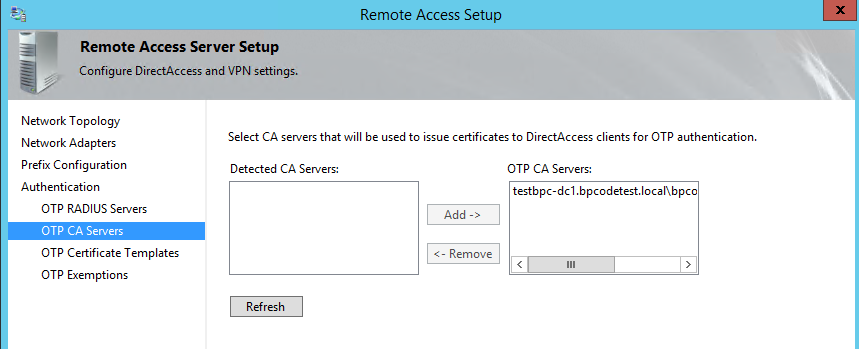
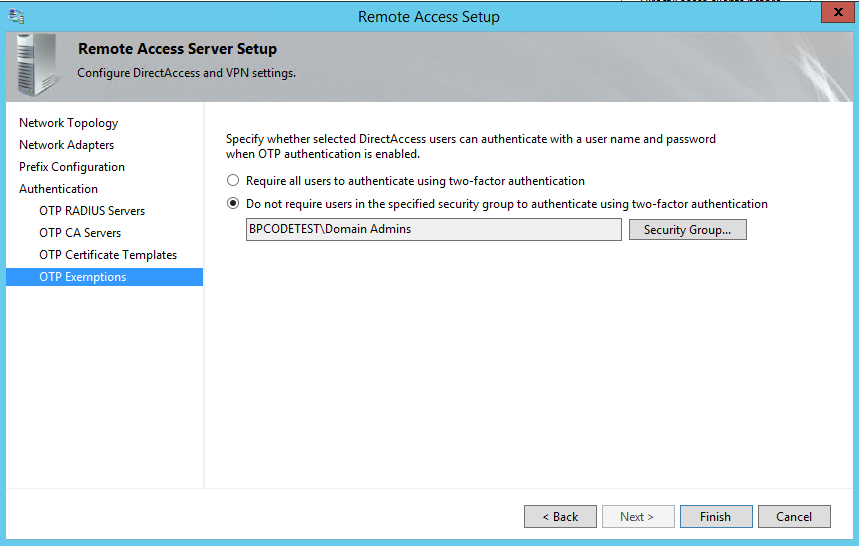
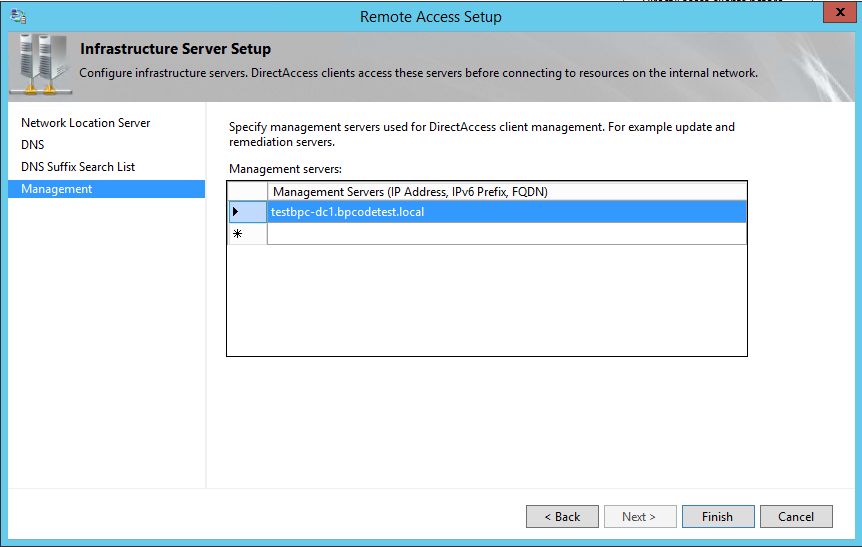
## Technical requirements:

* Direct access must be configured and working
* Buypass Code service connector (BPSC) must be installed according installation guide for BPSC)
* Access to Buypass Code manager verified
* Service account in Active Directory for LDAP query
* Access to internal Certificate authority to configure necessary templates
* Radius port UDP 1812 open between Direct Access server and BPCSC
* LDAP port TCP 389 open between BPCSC and LDAP catalog severs
* HTTPS port TCP 443 open from BPCS to internet

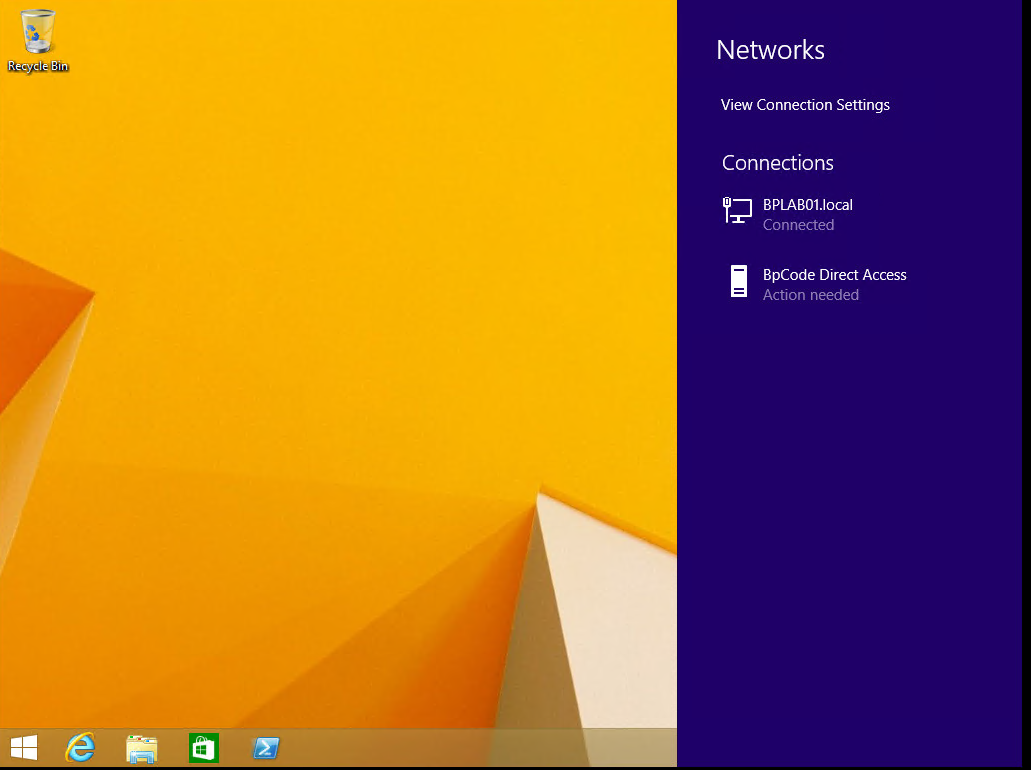
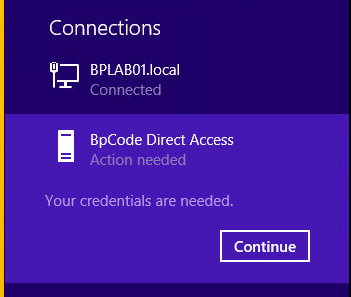
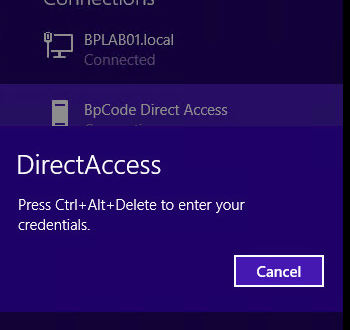
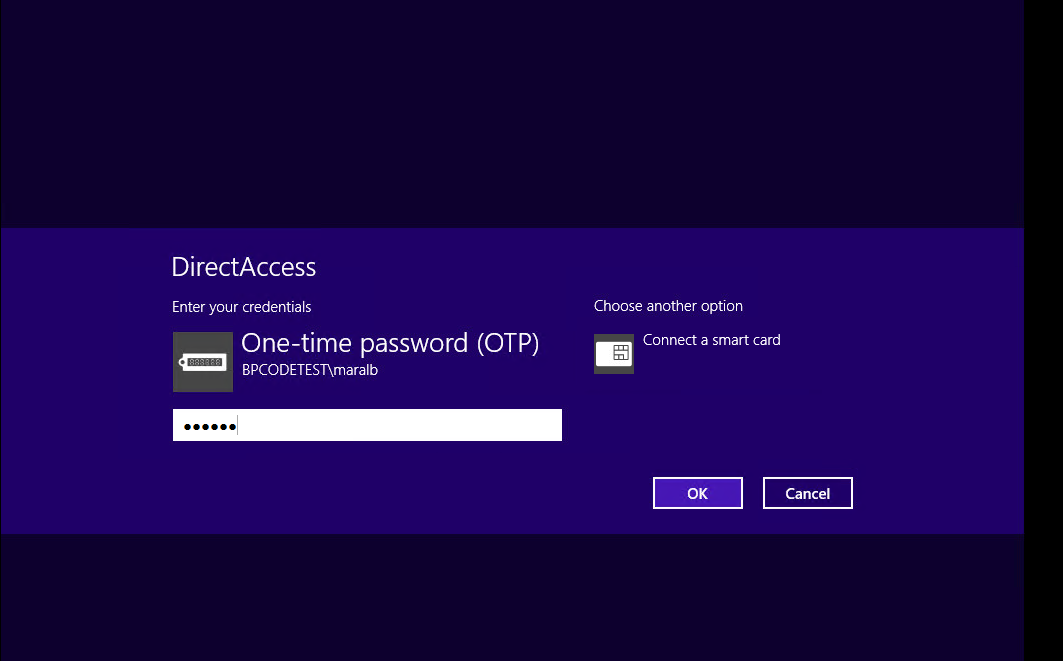
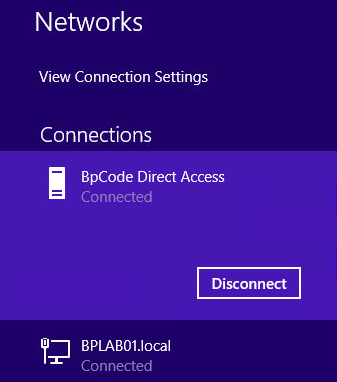
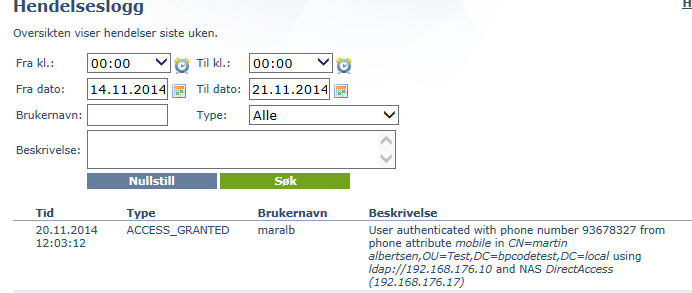
## Configure BP Code Manager

1. Configure LDAP settings
   1. Add new LDAP configuration
      1. Add LDAP server IP or FQDN
      2. Add service account with read access to LDAP catalog/Active Directory
      3. Add name of attribute for mobile phone – AD attribute name is “mobile”  
         
   2. Add new LDAP path  
      
2. Configure Direct Access as radius client
   1. New radius configuration
      1. Add ip address of Direct Access server
      2. Add Shared secret
      3. Type Description – ex “ Direct Access SERVERNAME”
      4. Choose proper LDAP
      5. Click on Advanced, choose can be monitored and configure DAProbeUser and DAProbePass
      6. Save  
         
      7. Check settings  
         

## Configure certificate templates

1. Configure OTP signing certificate template (registration authority certificate)
   1. Start Certificate Template console – Start🡪certtempl.msc
   2. Duplicate Computer template
   3. **Compatibility** – Under Certification Authority, Choose Windows server 2012 or newer and under Certificate recipients Windows 8/Windows server 2012 or newer  
      
   4. **General** – In Template display name, type BPCDAOTPRA, set validity period to 2 days and renewal period to 1 day.   
      
   5. **Security** – configure following settings
      1. **Direct access server object**: Allow READ, ENROLL and AUTO ENROLL
      2. **Authenticated users**: allow READ
      3. **Domain admins**: Allow FULL CONTROLL
      4. **Enterpise admins**: Allow FULL CONTROLL
      5. **Domain computers**: remove ENROLL from Allow   
         
      6. **Apply**
      7. **Subject name –** Build from AD. Subject name format, choose DNS name. Check for DNS name box. Apply  
         
      8. **Extensions** – Edit Application policy, remove all from the list. Add new- Name **BPC DA OTP RA**. In Object identifier field, type **1.3.6.1.4.1.311.81.1.1**
2. Configure OTP logon certificate template (OTP authentication certificate)
   1. Duplicate Smartcard logon template
   2. **Compability** – Under Certification Authority , choose Windows Server 2012 or newer. Under Certificate recipients, choose Windows 8/Windows server 2012 or newer.  
      
   3. **General** – Type BPCDAOTPlogon in Template Display name. Set validity period to 1 hours and renewal period to 0 hours
   4. **Security** – Configure following settings:
      1. **Authenticated users**: Allow READ and ENROLL
      2. **Domain admins**: Allow FULL CONTROLL
      3. **Enterprise admins**: Allow FULL CONTROLL  
         
      4. **Apply**
      5. **Subject name** – Build from Active directory. Set Subject name format to fully distinguish name. Check box User Principal name (UPN).  
         
      6. **Server** – Choose “Do not store certificates and requests in the CA database”. Remove mark from “Do not include revocation information in issued” certificate  
         
      7. **Issuance requirements** – Set “This number of authorized signatures” to 1. Under Policy type required in the signature, choose Application policy. In Application policy, choose BPC DA OTP RA. Click Apply  
         
      8. **Extensions** – Edit Application policies and remove Client Authentication. Click Apply  
         
      9. **Cryptography** – Minimum Key size 1024, Request must use one of the following providers: Microsoft RSA SChannel Cryptographic provider  
         Click OK  
         
   5. Chack that new templates has BPC DA OTP RA and Smart Card Logon under Intended Purposes  
      
   6. Publiseh new Templates  
        
      
3. Configure Direct Access with OTP
   1. Start Remote Acces Management. Click Edit in Configuration Wizard, STEP 2
   2. Click Next to get to Authentication
   3. Choose Two-factor authentication and check OTP. “Use computer certificate” should be marked and proper issuing CA should be filled in. Choose if you want to enable windows 7 computers or not. Click Next.  
      
   4. In Add radius, double-click first line and add ip address of BPSC. Click Change and add shared secret (same as configured in BP code manager). Port 1812. Click ok and next.  
      
   5. Add CA server  
      
   6. Choose BPCDAOTPLogon for OTP authentication and BPCDAOTPRA dor enrollment request. Click Next.
   7. Choose if you want to exclude AD group from two factor authentication.  
      
   8. Under STEP 3 of Configuration wizard, add CA server I management section.  
      
   9. Use Powershell to configure Direct Access with OTP:
      1. Set-DAServer -UserAuthentication TwoFactor
      2. Enable-DAOtpAuthentication -CertificateTemplateName "BPCDAOTPLogon" -CAServer "testbpc-dc1.bpcodetest.local\bpcodetest-TESTBPC-DC1-CA" -RadiusServer 192.168.176.13 -SharedSecret Abcd123$ -SigningCertificateTemplateName "BPCDATPRA" –Verbose

## Test from the client

1. Logon Direct Access enabled PC outside of corporate network (homeoffice, LTE etc)
2. Click on Network icon, click on Direct Access (Action Needed)  
   
3. Click Continue  
   
4. Press CTRL+ALT+DEL  
   
5. Choose OTP and type code from BP code app. Click OK  
   
6. User is authenticated and can access corporate resources  
   
7. Entry logged in BP code manager  
   

Microsoft reference:  
<http://technet.microsoft.com/en-us/library/hh831379.aspx> - Deploy remote Access with OTP Authentication