
HANDS-ON: SETTING UP MICROSOFT CERTIFICATE LOGON

PREREQUISITES:

Windows 2008 R2 Enterprise domain server with IIS

Client machine with local administrator rights, connected to the servers domain.

Test users

Course topics: SAC 8.0, token supporting MS PKI Solutions

DURATION:

60 minutes

THE AIM OF THIS HANDS-ON SESSION:

At the end of this hands-on session you will know how to:

1. Configure Microsoft certificate services for smartcard logon (certificate templates and enrollment rights)
2. Create and configure a duplicate certificate template
3. Enroll an Enrollment Agent certificate for the admin and smartcard user certificate on behalf of the users
4. Use a hardware token for smartcard logon to the domain
5. Enforce the user to logon using a token and define smartcard removal behavior

STEP BY STEP SERVER SETUP FOR SMARTCARD LOGON

Prerequisite: Install Microsoft certificate services:

Refer to the Hands-on Appendix document: *SETTING UP MICROSOFT SERVER*, for instructions on setting up a Microsoft Enterprise CA and Certification Authority Web Enrollment.

Step 1 - Configure the CA to support the required certificate templates:

1. From Windows *Start* menu, select **Programs > Administrative Tools > Certification Authority**.
2. Expand the local CA tree to view items.
3. Stand on certificate templates. Right click *Certificate Templates* and select **New > Certificate Template to Issue**. A window with the available certificate templates opens.
4. Use the CTRL button to select multiple certificate templates:
 - Smartcard User
 - Smartcard Logon
 - Enrollment Agent
5. Click **OK**

The selected templates are now added to the certificate templates list.

Caution – when deleting a template from this view, the template is deleted from the CA and will no longer be issued from this CA.

Step 2 - Add user permission to enroll the certificates:

1. Select the *Certificate Templates* tree item.
2. Right click the *Certificate Templates* and select **Manage**. The *certificate template* console window appears.
3. Right click the **Smartcard User** certificate template and select **Properties**.
4. Select the **Security** tab and mark the **Read** and the **Enroll** rights for all *Authenticated users*.
5. Click **OK** to save settings.
6. Grant the same permissions to the **Smartcard Logon** template.
7. Click **OK** to save settings.

Step 3 - Install the Root CA certificate on the server and on the workstations:

1. Launch the *Certsrv* enrollment web pages (<http://localhost/certsrv>) and click the link "**Download a CA certificate, Certificate chain, or CRL**".
2. (Click **Yes** if a messages appears prompting you to approve running ActiveX on the page)
3. Click "**Download CA Certificate**".
4. On the *File Download* window, click **Open** to automatically add the Root certificate to the trusted root CAs on the server.
 - a. Alternatively, click **Save** to install the Root certificate on the workstation. After saving the Root certificate you will need to right click and install it.

Step 4 - Enroll an Enrollment Agent certificate for the administrator who enrolls on behalf

1. Log on as administrator or a user with administrative rights. This user will issue the Smartcard logon certificates on behalf of the domain users.
2. From *Run* start MMC.
3. From the console's **File** menu, click **Add/Remove Snap-in**.
4. Select the *Certificates* snap-in and click the **Add** button.
5. Select the snap-in for "My user account" click **Finish** and then click **OK**.
6. In the console tree, under *Certificates*, right click **Personal**.
7. Launch *All Tasks* and select **Request New Certificate**.
8. The *certificate request wizard* opens. Click **Next**.
9. Click **Next** again
10. From the certificate types select **Enrollment Agent**.
11. Install the certificate: click the **Enrol** button.
12. Click **Finish** to close the wizard

Alternatively, you can use the CA web services to issue the Enrollment Agent certificate

Step 5 - Enroll Smartcard logon certificate on the token for user authentication

You will now issue the Smartcard logon certificates on behalf of the domain users.

1. Install SafeNet Authentication Client on the server or workstation on which you intend to enroll (if it is not already installed)
2. Insert the user's token to the USB port.
3. From *Run* start MMC.
4. From the console's **File** menu, click **Add/Remove Snap-in**.
5. Select the *Certificates* snap-in and click the **Add** button.
6. Select the snap-in for "My user account". Click **Finish** and then click **OK**.
7. In the content tree, under **Certificates > Personal**, right click **Certificates** and select **All Tasks > Advanced Operations... > Enroll on behalf of...**
8. Click **Next**.
9. Click next again
10. Select the *Enrollment Agent certificate*: Browse and select the **Administrator** certificate you have enrolled in the previous step and click ok. Click **Next**.
11. The Certificate Enrollment page opens, and you can select the type of certificate to enroll.
12. Select **Smartcard logon** certificate. Click the Details scroll down menu button to view further options.
13. Click the **Properties** button. In the *Private Key* tab, open the **Cryptographic Service Provider** scroll down menu.
14. Select **eToken Base Cryptographic Provider** and remove **Microsoft Strong Cryptographic Provider (Encryption)**.
15. Click **OK**. Click **Next** to proceed with enrollment.
16. Select a domain user and click **Enroll**. (You may need to re-insert the token)
17. When prompt, type in the token's password and click **OK**.
18. After enrollment succeeds, Close the enrollment window
19. View the new enrolled certificate details.
20. Close the enrollment window.
21. You can view the enrolled certificate on the token using SAC 8.0 Advanced view options.

Use the eToken for Smartcard logon to the domain as the user

1. Log off the workstation or the server to which the enrolled user will now log on.
2. Insert the user's Token and click **Smartcard logon**. (You may need to click on **Switch user** to see the option for Smartcard logon).
3. Type in the Token's password in the PIN entry field and logon. The user is logged on to the domain.
4. Pull out the Token, what happens?

Note: If logon is tested directly on the server, the user must be granted rights to logon locally to the server. This is done through **Administrative Tools > Group Policy Management**.

- a. Expand the **Forest** tree, expand the domains and your domain, expand the **Domain Controllers** and right click the **Default Domain Controllers Policy**. Click **Edit...**
- b. In the console tree, expand **Computer Configuration > Policies > Windows Settings > Security Settings > and Local Policies**, and then click **User Rights Assignment**.
- c. In the details pane (right pane), double-click Allow Logon Locally.
- d. Ensure that the **Define these policy settings** check box is selected, and then click **Add User or Group**.
- e. Add the *Administrators* group and add also the name of the test user that you want to allow to log on locally. Click OK.
- f. After you have the account name entered, click **OK** in the *Add User or Group* dialog box, and then click **OK** in the *Allow log on locally Properties* dialog box.

Step 6 – Set Smartcard Logon Policies:

In this step you will define the smartcard removal behavior:

1. Log on to the server as the domain administrator
2. From *Administrative tools*, open **Group Policy Management**.
3. Expand the **Forest** tree, **expand the Domains** , **expand YOUR DOMAIN**. Expand the **Domain Controllers** and right click the **Default Domain Controllers Policy**. Click **Edit...**
4. In the console tree, expand **Computer Configuration > Policies > Windows Settings > Security Settings > and Local Policies**, and then click **Security Options**.
5. Select **“Interactive logon: Smart card removal behavior”**. Right click Properties - check “define this policy setting” and define the policy to be **Lock workstation**.
6. Click **OK** to save.
1. To refresh the user policies: open Run... from Windows Start menu and type: **gpupdate /target:user /force**
2. Logon using the token as your test user. Remove the token and check the workstations behavior.

Enforcing the user to logon using the Token:

1. Log on as the domain administrator
2. From Administrative tools, open **Active Directory Users and Computers**.
3. Select your test user and open its properties.
4. In the **Account** tab, go to **Account options**. Scroll down the options.
5. Select **“Smart card is required for interactive logon”**. Click **OK**.
6. Log off administrator and try to logon as the user by typing Ctrl+alt+del. Were you able to log on? What message is displayed?

Step 7 – Revoke the Smartcard Logon Certificate

1. Log on as the domain administrator
2. From *Windows Administrative Tools*, open the “**Certification Authority**” snap-in.
3. Select “**Issued certificates**”
4. Revoke the user’s certificate: stand on the certificate, right click and select **All tasks** , Click on **Revoke certificate**.
5. Publish a new CRL for the change to take effect:
Right click “**Revoked certificates**”. Select **All tasks** → **Publish**.
Select to publish a **New CRL**. Click **OK**.
6. The CRL refresh might take a long time. Therefore run **GPupdate /force** on the server and on the workstation to refresh policies
7. Logon as your test user using the smartcard.
8. The user’s logon will fail once the certificate is revoked.