Server 2012 RDS has been a huge game changer for shared hosted desktops as well as for hosted VDI deployments. The capabilities you get out of the box fit the requirements of a lot companies I’d say, and when I say a lot I don’t mean all. There are still uses cases where Citrix has to be in place and I feel that being still a good point because it keeps the innovation cycle up and running.

However in this post I’m going to cover a topic that arises in almost every RDS project.

* Does RDS / Connection Broker / RDS Web / RDS Gateway support Single Sign On authentication?
* What with Remote Apps and different collections?
* What about Smart Card?

**The definition of the term “SSO”**Single Sign On can be implemented in several ways, but what I’m talking about here is the fact, the user has to enter his credentials only once at the primary contact device (endpoint). Subsequent logons will then be authenticated via the original credential set, which can be user name and password or PIN if using Smart Card. The credential forwarding occurs on Kerberos / CredSSP level, so no freaky agent behind the scenes filling in some user credentials.

**Out of the box behaviour**

Depending on how you design the solution the entry point for the user might be different. But however, I’m going to cover all possible pitfalls.
By default the procedure to start a remote app or desktop is as follows:

* User logs on to client computer providing his domain credentials / PIN
* User launches the RDWeb website
* User enters domain credentials / PIN (with cert based auth)
* User launches app / desktop
* User confirms untrusted rdp file signing message
* If Smart Cards are used, another PIN prompt to complete

There are way too much authentication points and click steps until the user reaches the app / desktop. And you might be annoyed by pop-up boxes like these….




**Components (tiers) involved**



While the RDWeb site is using Kerberos for SSO, subsequent authentication processes use CredSSP by providing default or fresh credentials depending on the authentication mechanism at the web tier.

**How to configure it correctly**

There are basically four steps to complete

* Issue and assign a valid SSL certificate to RDS Gateways, RD Web Servers and RD Connection Brokers
* Provide the certificate’s thumbprint within GPO to enable trusted rdp file signing
* Enable Web SSO on the RD Web Servers
* Create GPO for Credential Delegation Settings
* Add the RDWeb URL to IE’s “Local Intranet” Zone

…how to get there?

**1. Issue a valid SSL certificate and assign it to the server components**I’m not covering how to request and issue a SSL certificate here, you might know that already, I’m sure. But keep in mind the Key Usage must contain “Server Authentication”.

Assign the certificate for connection broking, rdp file-signing and web access


**2. Enable SSO on Web tier**
This step requires a bit more work including web config file editing. Be sure to create a backup of the files before screwing them up 



Edit: **%SYSTEMROOT%\Web\RDWeb\pages\web.config**

**Find the Authentication key and change it from:**

**<!– <authentication mode=”Windows”/> –>**

<authentication mode=”Forms”>

<forms loginUrl=”default.aspx” name=”TSWAAuthHttpOnlyCookie” protection=”All” requireSSL=”true” />

</authentication>

To:

**<authentication mode=”Windows”/>**

**<!–**<authentication mode=”Forms”>

<forms loginUrl=”default.aspx” name=”TSWAAuthHttpOnlyCookie” protection=”All” requireSSL=”true” />

</authentication> **–>**

**Comment out the module and security sections:**

<system.webServer>

**<!–**<modules runAllManagedModulesForAllRequests=”true”>

<remove name=”FormsAuthentication” />

<add name=”RDWAFormsAuthenticationModule” type=”Microsoft.TerminalServices.Publishing.Portal.FormAuthentication.TSFormsAuthentication” />

</modules> **–>**

**<!–** <security>

<authentication>

<windowsAuthentication enabled=”true” />

<anonymousAuthentication enabled=”false” />

</authentication>

</security> **–>**

<httpRedirect enabled=”true” />

</system.webServer>

Edit: **%SYSTEMROOT%\Web\RDWeb\Pages\en-us\Default.aspx**

Change the following line to specify the private mode by default:

//
// Page Variables
//
public string sHelpSourceServer, sLocalHelp, sRDCInstallUrl, strWorkspaceName;
public Uri baseUrl, stylesheetUrl, renderFailCssUrl;
**public bool bShowPublicCheckBox = false, bPrivateMode = true, bRTL = false;**

**3. Enable trusted rdp file signing for clients**

Get the certificate thumbprint on your Connection Broker via Powershell



|  |  |
| --- | --- |
| 1 | <span style="font-family: Consolas; font-size: 10pt;">Get-Childitem CERT:\LocalMachine\My </span> |



Copy the thumbprint of the corresponding certificate to clipboard

Edit your clients GPO to include the thumbprint and to trust signed rdp files with this certificate

