Setting Up Remote Application Server to work with ADFS as Identity Provider over SAML

- Parallels Remote Application Server

This article is a step by step guide to configure **SSO Authentication** using the **Security Assertion Markup Language (SAML)** authentication mechanism. SAML is an XML-based authentication mechanism that provides single sign-on (SSO) capability between different organizations by allowing the user authentication without sharing the local identity database. As part of the SAML SSO process, the new **Parallels RAS Enrollment Server** communicates with Microsoft Certificate Authority (CA) to request, enroll and manage digital certificates on behalf of the user to complete authentication without requiring the users to put in their Active Directory credentials.

Service providers and Enterprises with multiple subsidiaries (acquisitions) don't have to maintain your own internal Identity Management solutions or complex domains or forest trusts. Integrating with 3rd party Identity Providers allow customers' and partners' end users a true SSO experience.

As an example, we will review the process of configuring **Active Directory Federation Servicies (ADFS)** as Identity Provider.

Prerequisites:

1. Local Active Directory:
    - ♦ A local AD user account for use as enrollment agent (CA terminology).
    - ♦ A local AD limited user account for NLA authentication.
2. Microsoft Certification Authority (CA) in Enterprise mode (example in more details at Microsoft TechNet look after standalone root CA):
    - ♦ Enrollment Agent Certificate Template
    - ♦ Smartcard Logon Certificate Template
3. Third-party Identity Provider (Azure, Safenet, Gemalto, Okta etc):
    - ♦ This is where the user accounts should reside and synchronized into the third-party SAML identity provider.
    - ♦ The local AD is typically synchronized to the third-party provider using an Active Directory Connector. Please consult with the provider on how to properly synchronize users.
4. Domain Controllers must have Domain Controller certificates. The certificates on the Domain Controllers must support smart card authentication. Certificates created using the Microsoft CA certificate template named Domain Controller Authentication supports smart cards. Manually created Domain Controller certificates might not work.
5. Since SAML is a web-based authentication, it requires a browser (used to log in to HTML5 portal and get application listing). Native Parallels Client for Windows is used to launch RDP sessions.
6. For security reasons, ES must be a separate server and must not be installed on a Connection Broker server. ES should be installed on a secure, standalone server that does not have any other components and roles installed.

Setting up Windows Server side to comply RAS SAML pre-requisites

Per prerequisites above, configure Microsoft Certification Authority, Certificate templates and add required user accounts. Detailed instructions available here: https://kb.parallels.com/124813

Adding RAS Enrollment Server Agent

Install **RAS Enrollment Server Agent** either manually or from RAS Console:

- In **RAS Console** **Enrollment Servers** click "**+**" icon to add a new agent.
- In case of manual ES setup (RASInstaller.msi Custom) it is necessary to put the **ES host registration key** to folder **%installation_path%\Parallels\ApplicationServer\x64**. To export the registration key, open the **RAS Console** **Enrollment Servers** **Tasks** **Export registration key** **registration.crt** (remote pushing does this automatically).

In **RAS Console** **Enrollment Servers** **AD Integration** tab specify the CA and user accounts for **Enrollment agent** and **NLA user** you configured and apply the changes

Final checks

Make sure, **Enrollment Agent** server status is **OK**.

Switch to **AD Integration** tab and click on **Validate AD Integration settings**, make sure that all checks are passed

Adding Identity Provider to Parallels RAS

1. Open Parallels **RAS Console** **Connection** **SAML** tab click **Add**.

2. In the opened **Add Identity Provide**r wizard, give it a name (e.g. **ADFS**), choose **Manually enter the IdP information** and click **Next**.

3. On the next page enter any information to satisfy the requirements to not leave the fields blank, (we will import **ADFS** settings using metadata file later) and click **Finish**.

4. Apply the configuration by clicking the **Apply** button.

Export SP settings (metafile)

1. Open just created IdP Ping properties and switch to **SP** tab.

2. Specify external FQDN or public IP address in the **Host** field. It's the address where users will be redirected after successful authentication, so it must be accessible for them. In general, it's the public FQDN of your RAS Farm.

3. Click **Export SP entity ID metadata to file** and save the .xml file:

4. Now you are ready to proceed with configuring ADFS.

ADFS Side Configuration

1. On a **Domain Controller** go to **Administrative Tools-> AD FS Management**

2. Navigate to **Relying Party Trust**-> Add **Relying Party Trust...**

- In the opened wizard select **Claims aware** on the Welcome screen and hit **Start** button.
- Select 'Import data about the relying partly from a file' in the **Select Data Source** section and specify the exported before **SP entity ID metadata file.**
- Set a **Display name**.
- Choose an access control policy.
- Hit next on the **Ready to Add Trust** page.

3. Once Relying Party Trust is ready right click on it and go to Edit Claim Issuance Policy

- **Add Rule**-> select **Send LDAP Attributes as Claims**.
- **Configure Claim Rule**: In Attribute store select **Active Directory** and configure Attributes per screenshot:

Note, Attribute **SAM-Account-Name** -> **Name ID** is required.

Final steps in RAS configuration

1. Return to RAS Console, click **Import IdP metadata** and open the .xml file you saved on the previous step:

3. Switch to the **Attributes** tab and specify what attributes will be used for mapping users. For example, you may use email addresses or User Principal Name: