Microsoft Windows Server: Verify retrieval of Certificate Revocation List (CRL)

- Parallels Secure Workspace

Symptoms

Single sign-on authentication issues.

Cause

If a Microsoft Windows Domain Controller can not reach the Certificate Revocation List (CRL) of the Parallels Secure Workspace appliance, single sign-on authentication will fail.

Resolution

On each of the Microsoft Windows servers taking care of Kerberos authentication (for instance on the domain controllers):

1. Open a **Windows PowerShell** console.
2. Execute this command:
   `certutil -URL "http://<workspace_internal_ip>/crl/<WORKSPACEDOMAINNAME>.crl"`
   "http": leave this, the CRL is indeed fetched through HTTP (HTTPS not required).
   <workspace_internal_ip> : replace this with the IP of the Parallels Secure Workspace appliance.
   <WORKSPACEDOMAINNAME> : should match the Workspace domain name - always in capitals (visible under **System Settings > Global > Domains**).
3. In the window that appears, click **[Retrieve].**

If there is a problem obtaining the CRL, the reason can be found in the **Windows Event Viewer** under **Custom > Administrative Events**.

Microsoft Windows Servers should be able to access port 80 on the Parallels Secure Workspace appliance. In customer cases, often a firewall is blocking this access.

It's worth noting that Microsoft Windows Server caches CRLs. To clear this cache:

Execute these commands on the Kerberos Domain Controllers:

```
certutil -urlcache * delete
certutil -setreg chain\ChainCacheResyncFiletime @now
net stop certsvc && net start certsvc
```