OpenSSL.SSL.Error: [('SSL routines', 'SSL_CTX_use_certificate', 'ca md too weak')]

- Parallels Secure Workspace 5.4.0
- Parallels Secure Workspace 5.6.0
- Parallels Secure Workspace 5.5.1
- Parallels Secure Workspace 5.4.4
- Parallels Secure Workspace 5.4.2

Symptoms

- When trying to enable single sign-on in Parallels Secure Workspace, the administrator is confronted with an "Internal Server Error".
- In the log file, a similar error can be seen:

```
2023-01-04 12:06:25.899051+00:00 awingu01
awingu-api.service[/opt/awingu/awingu-core/virtualenv/bin/gunicorn:1391]:
Internal Server Error: /api/v2/domains/2/
Traceback (most recent call last):
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/django/core/ha
line 47, in inner
    response = get_response(request)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/django/core/ha
line 181, in _get_response
    response = wrapped_callback(request, *callback_args,
**callback_kwargs)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/django/views/
line 54, in wrapped_view
    return view_func(*args, **kwargs)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/rest_framework
line 125, in view
    return self.dispatch(request, *args, **kwargs)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/rest_framework
line 509, in dispatch
    response = self.handle_exception(exc)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/rest_framework
line 469, in handle_exception
    self.raise_uncaught_exception(exc)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/rest_framework
line 480, in raise_uncaught_exception
    raise exc
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/rest_framework
line 506, in dispatch
    response = handler(request, *args, **kwargs)
```

```
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/rest_framework
line 82, in partial_update
    return self.update(request, *args, **kwargs)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/rest_framework
line 67, in update
    serializer.is_valid(raise_exception=True)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/rest_framework
line 227, in is_valid
    self._validated_data = self.run_validation(self.initial_data)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/awingucore/cor
line 45, in run_validation
    return super().run_validation(data)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/rest_framework
line 429, in run_validation
    value = self.validate(value)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/awingucore/dor
line 459, in validate
    not validators.is_valid_ssl_match(sso_ca_certificate,
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/awingucore/cor
line 200, in is_valid_ssl_match
    context.use_certificate(certificate)
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/OpenSSL/SSL.py
line 971, in use_certificate
    _raise_current_error()
  File
"/opt/awingu/awingu-core/virtualenv/lib/python3.10/site-packages/OpenSSL/_util
line 57, in exception_from_error_queue
    raise exception_type(errors)
OpenSSL.SSL.Error: [('SSL routines', 'SSL_CTX_use_certificate', 'ca md
too weak')]
```

Cause

This is caused when one or more of the certificates that are being uploaded to enable single sign-on are using an insecure signature algorithm, such as sha1RSA.

Resolution

The Workspace SubCA certificate, any intermediate certificates in the certification path, and the root certificate should use a secure signature algorithm.

At the moment of writing, sha256RSA is common.
sha1RSA is insecure.
