E-CONNECT 2.0 CLIENTZERTIFIKAT ERNEUERN

Version: 1.0

Pionier der Zahnarzt-Software.
Seit 1986.

DAMPSOFT
Die Zahnarzt-Software

Inhaltsverzeichnis

1. Allgemeine Informationen

1.1. Allgemeine Informationen

Das Clientzertifikat dient der eindeutigen Identifizierung eines Clientsystems sowie der Bestätigung seiner Authentizität gegenüber dem Konnektor. Es funktioniert wie ein digitaler Ausweis: Der Client beweist damit, dass er berechtigt ist, eine gesicherte Verbindung zum Konnektor aufzubauen. Das Zertifikat wird außerdem verwendet, um die Kommunikation verschlüsselt und manipulationssicher zu machen, sodass nur authentifizierte Systeme Daten mit dem Konnektor austauschen können.

Da das Clientzertifikat nur für einen begrenzten Zeitraum gültig ist, muss es vor Ablauf erneuert bzw. ausgetauscht werden, damit die Verbindung weiterhin störungsfrei und sicher genutzt werden kann.

Hinweis!

Wenn Sie ein bestehendes, gültiges Clientzertifikat im vKonnektor löschen (z. B. das Passwort zum Clientzertifikat nicht mehr bekannt ist) und weitere Programme nutzen, die dieses Zertifikat verwenden, müssen Sie das Zertifikat auch in diesen Anwendungen ersetzen (z. B. SecAuthenticator).

Wenden Sie sich bei Bedarf an den jeweiligen Herstellersupport der betroffenen Programme.

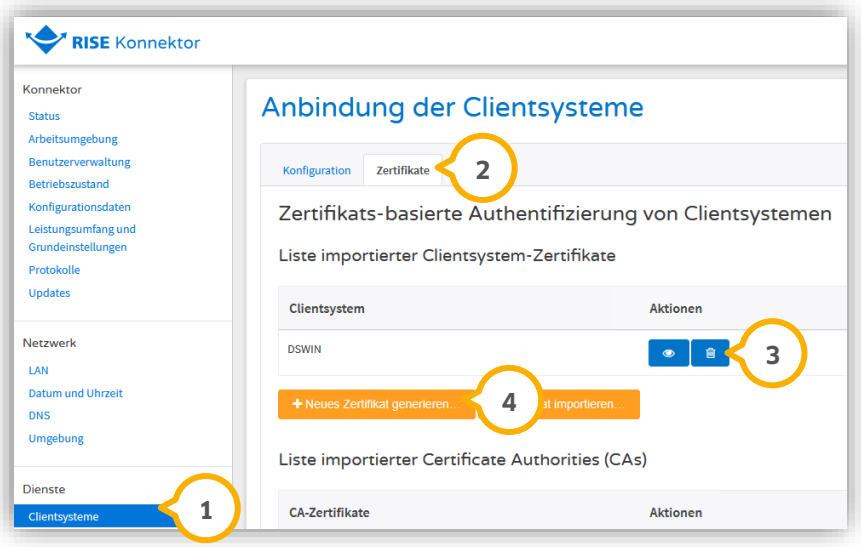
1.2. Hinweis zu DS4 in der Cloud

Hinweis!

Wenn Sie das DS4 in der Cloud nutzen, können die beschriebenen Schritte ausschließlich gemeinsam mit unserem Technischen Support durchgeführt werden. Bitte wenden Sie sich für die Umsetzung direkt an den DS4-Support.

2.1. Neues Zertifikat erstellen

Melden Sie sich am Konnektor an, wie es in der verlinkten Anleitung (https://www.dampsoft.de/wp-content/uploads/DS_Anleitung_e-connect-2.0-Konnektor-Neustart.pdf) beschrieben wird.

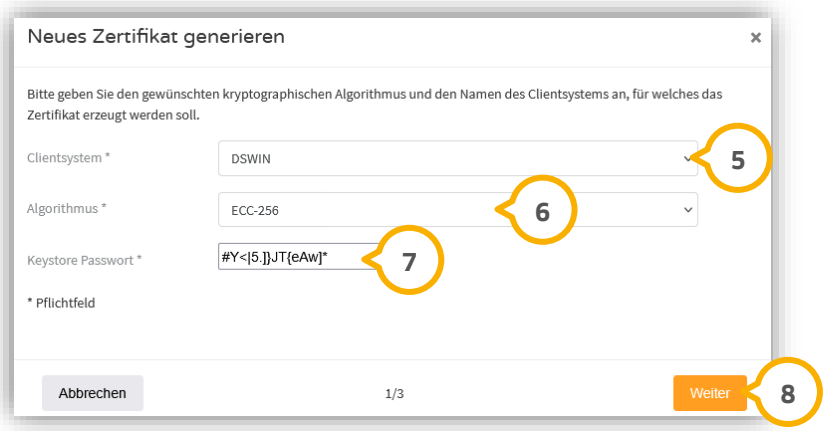


Öffnen Sie den Bereich „Clientsysteme“ ①.

Wechseln Sie in den Reiter „Zertifikate“ ②.

Löschen Sie das alte Zertifkat mit einem Klick auf den Papierkorb ③.
Sie erhalten eine Sicherheitsabfrage. Bestätigen Sie diese.

Klicken Sie auf >>Neues Zertifikat generieren…<< ④.



Wählen Sie das Clientsystem ⑤ aus.

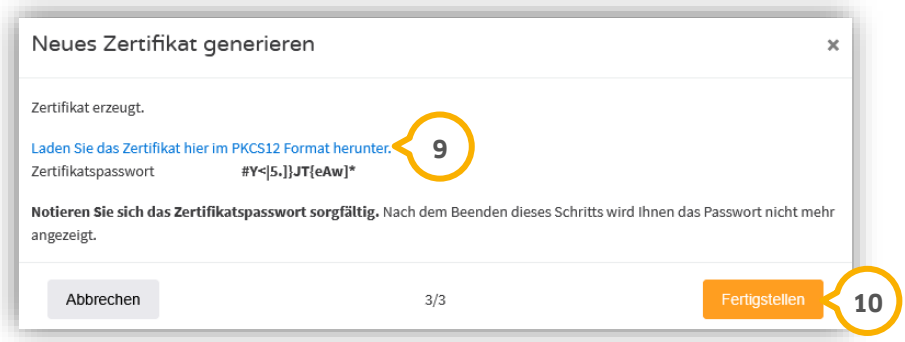
Wählen Sie bei Algorithmus ⑥ „ECC-256“.

Tipp: Sie können als „Keystore Passwort“ ⑦ das vordefinierte oder ein eigenes Passwort verwenden.

Klicken Sie auf >>Weiter<< (8).

Achtung!

Im nächsten Schritt können Sie das Zertifikat herunterladen und das zugehörige Passwort einmalig anzeigen lassen. Nach Abschluss dieses Schritts sind diese Informationen nicht erneut abrufbar. Speichern Sie Zertifikat und Passwort daher sicher ab. Sollten die Daten verloren gehen, muss ein neues Zertifikat erstellt werden.



Um die Zertifikatsdatei auf dem PC zu speichern, klicken Sie auf den blauen Schriftzug „Laden Sie das Zertifikat hier im PKCS12 Format herunter“ (9).

Tipp: Wir empfehlen, die Datei im Verzeichnis „C:\e-connect 2.0“ und zusätzlich auf dem Server „Lw:\TDAMP\DS\e-connect 2.0“ zu speichern.

Im selben Verzeichnis befindet sich eine Textdatei mit allen erforderlichen Daten für e-connect 2.0.

Tragen Sie dort das neue Passwort für das Clientzertifikat unter „Client-Zertifikat Passwort“ ein.
Notieren Sie sich das dazugehörige Zertifikatspasswort.

Um den Vorgang abzuschließen, klicken Sie auf >>Fertigstellen<< (10).

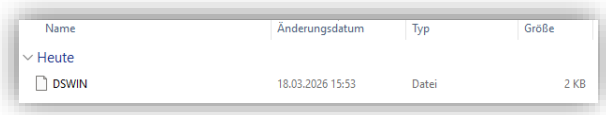
Die Vorbereitung ist abgeschlossen und Sie können sich vom vKonnektor abmelden.

Hinweis!

Falls die Datei beim Erstellen des Zertifikats keine Dateiendung aufweist, führen Sie unbedingt den folgenden Vorgang durch.

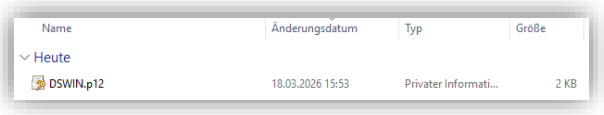
Öffnen Sie den Dateimanager (z. B. Windows Explorer).

Öffnen Sie das Verzeichnis mit der Zertifikatsdatei.



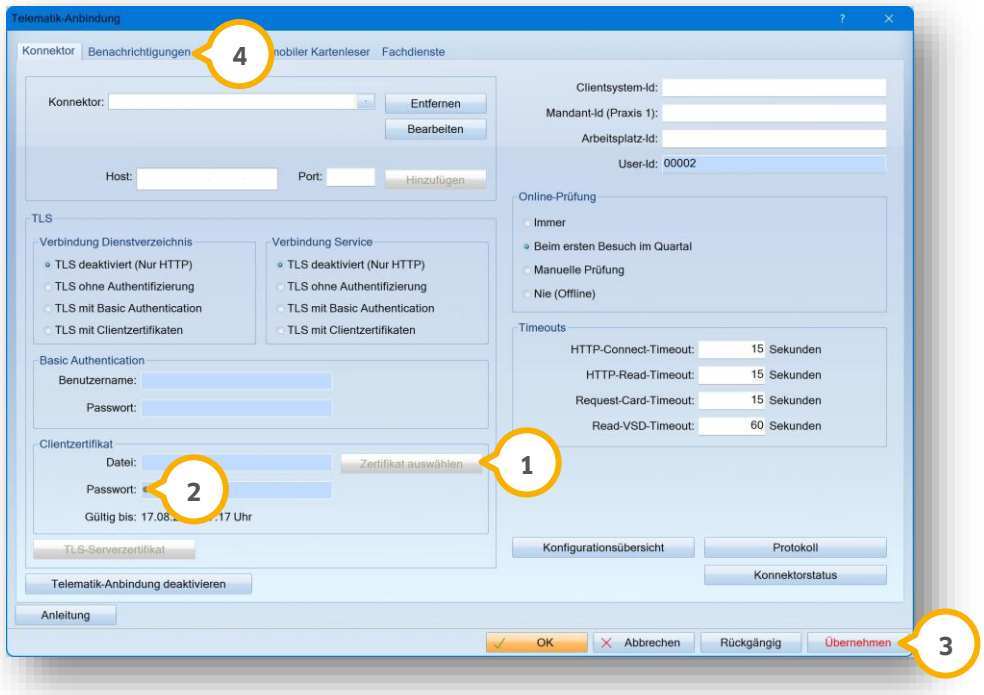
Klicken Sie mit der rechten Maustaste auf die Datei.
Wählen Sie „Umbenennen“ aus.

Ergänzen Sie am Ende des Dateinamens die Endung „.p12“.
Bestätigen Sie die Änderung mit der Enter-Taste.



2.1.1. DS-Win: Neues Zertifikat einfügen

Folgen Sie im DS-Win dem Pfad „Einstellungen/Kartenleser/Telematik“.

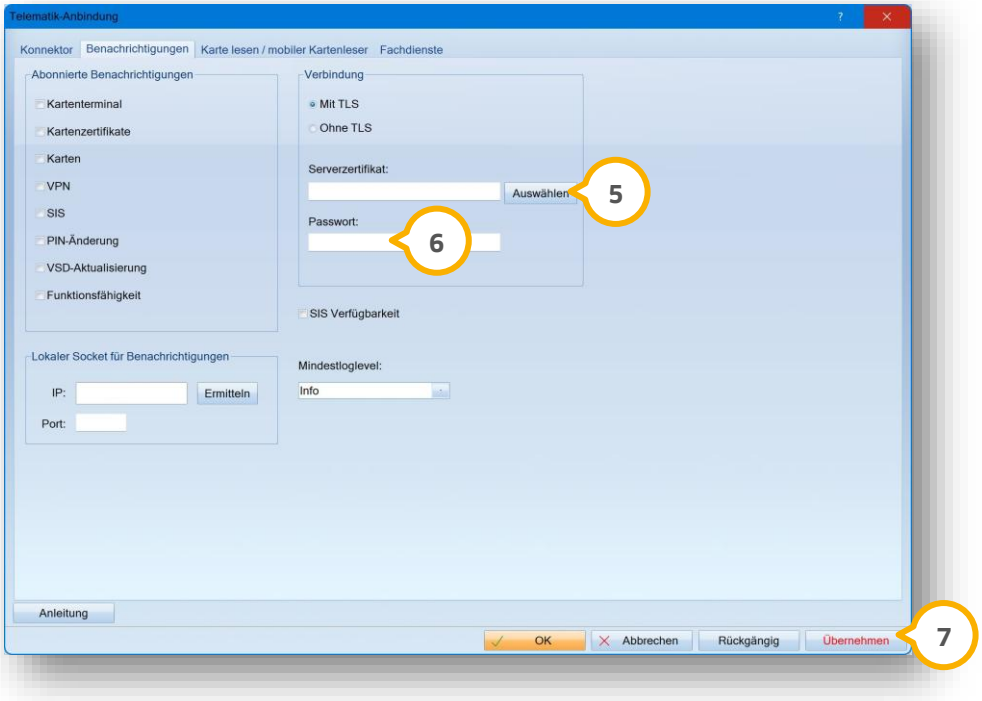


Klicken Sie auf >>Zertifikat auswählen<< ① und wählen Sie das neue Clientzertifikat aus.

Geben Sie bei ② das Passwort ein.

Speichern Sie die Änderungen mit >>Übernehmen<< ③.

Wechseln Sie in den Reiter „Benachrichtigungen“ ④.



Klicken Sie auf >>Auswählen<< ⑤ und wählen Sie das neue Clientzertifikat aus.

Geben Sie bei ⑥ das Passwort ein.

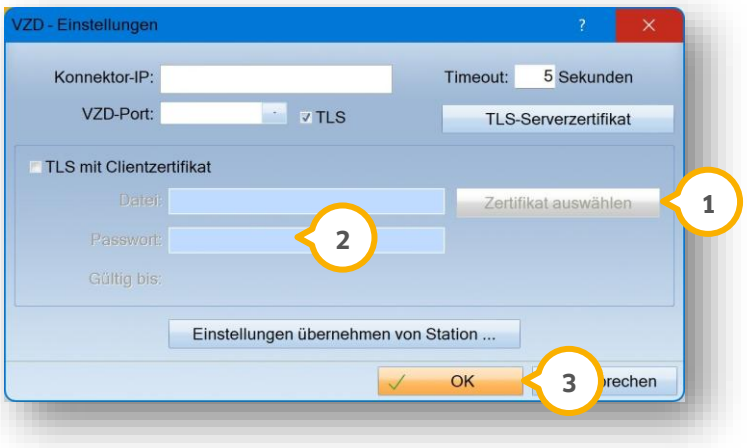
Speichern Sie die Änderungen mit >>Übernehmen<< ⑦.

VZD-Einstellungen anpassen

Hinweis!

Wenn Sie im DS-Win mehrere Stationen mit aktiver TI betreiben, muss der folgende Schritt an jeder einzelnen Station durchgeführt werden.

Folgen Sie im DS-Win dem Pfad „Einstellungen/e-health/VZD“.



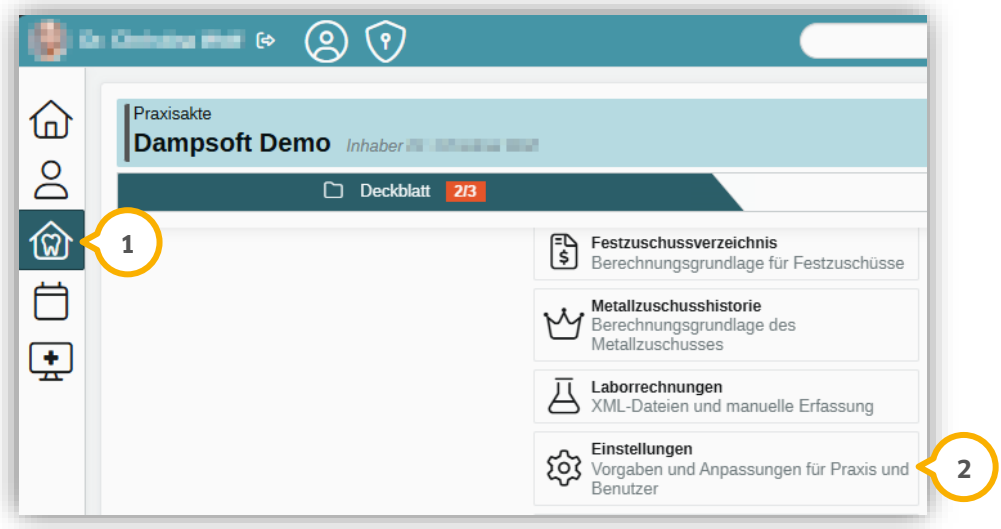
Klicken Sie auf >>Zertifikat auswählen<< ① und wählen Sie das neue Clientzertifikat aus.

Geben Sie bei ② das Passwort ein.

Speichern Sie die Änderungen mit >>OK << ③.

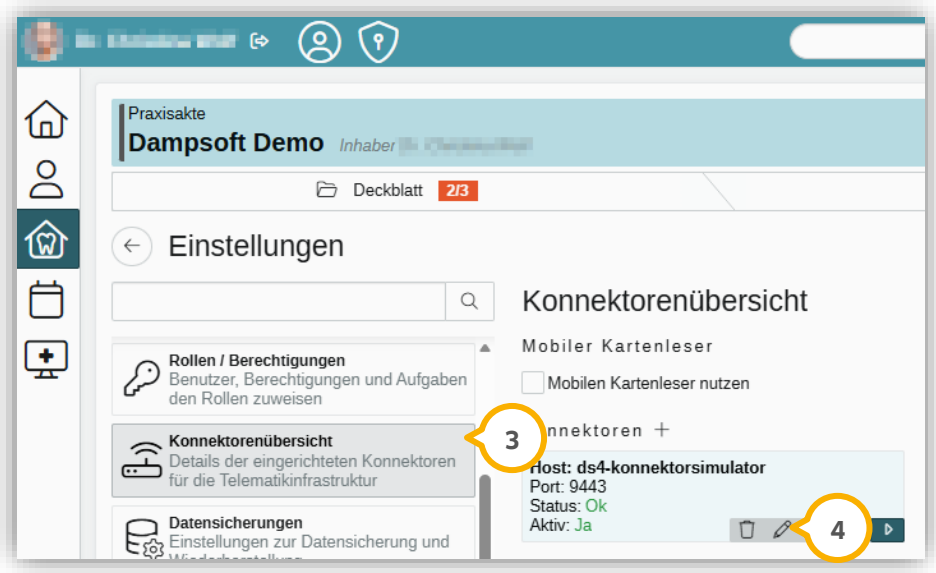
2.1.2. DS4: Neues Zertifikat einfügen

Öffnen Sie im DS4 die „Praxisakte“ ①.

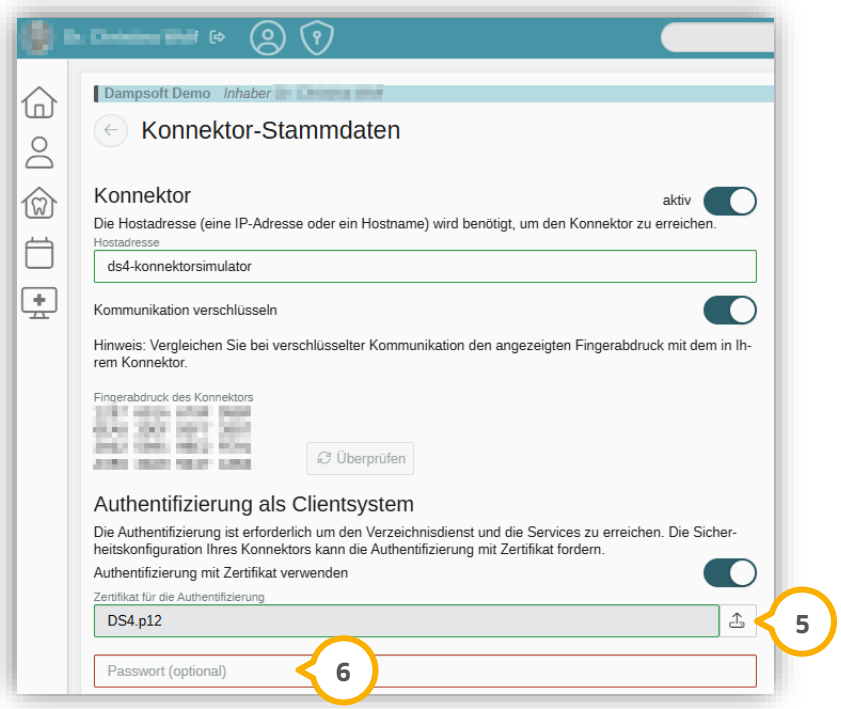


Wechseln Sie in die „Einstellungen“ ②.

2. Zertifikat im RISE-Konnektor erstellen und einfügen



Wechseln Sie in den Bereich „Konnektorenübersicht“ (3).
Klicken Sie auf das Stift-Symbol (4).



Fügen Sie bei „Authentifizierung als Clientsystem“ (5) das neue Zertifikat hinzu.

Geben Sie bei (6) das Passwort ein.

Klicken Sie unten auf der Seite auf >>Speichern<<.

Das Clientzertifikat wird im Hintergrund automatisch an die Easy-TI übertragen.

3.1. Allgemeine Informationen

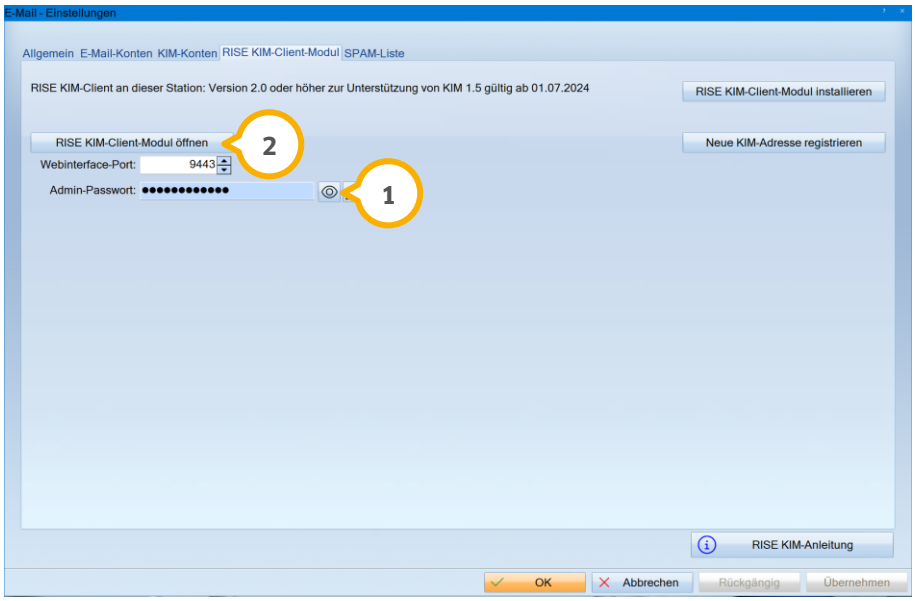
Sollten Sie keine „@dampsoft.kim.telematik“-Adresse verwenden, wenden Sie sich für den Austausch des Clientzertifikats bitte an den Support Ihres KIM-Anbieters.

3.2. DS-Win: Zertifikat im KIM-Client-Modul einfügen

Hinweis!

Für den folgenden Vorgang wird das Administratorpasswort des RISE KIM-Client-Moduls benötigt. Dieses Passwort wurde während der Installation des Moduls vergeben und muss vor Beginn der Durchführung bereitliegen.

Folgen Sie im DS-Win dem Pfad „Einstellungen/e-health/KIM“.



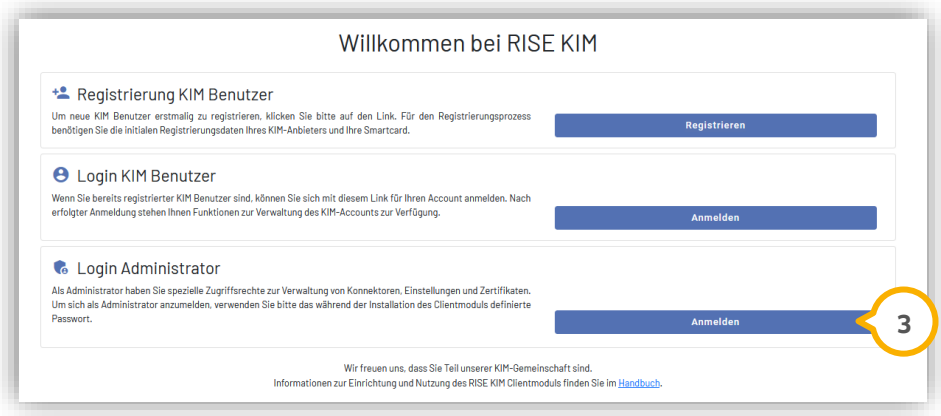
Wechseln Sie in den Reiter „RISE KIM-Client-Modul“.

Klicken Sie auf das Auge ① und kopieren Sie das Passwort.

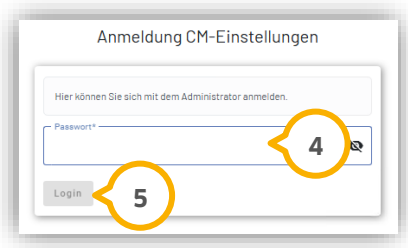
Klicken Sie auf „RISE KIM-Client-Modul öffnen“ ②.

Es wird automatisch Ihr Standard-Browser geöffnet.

3. Zertifikat im RISE KIM-Client-Modul für Dampsoft-KIM-Adressen einfügen

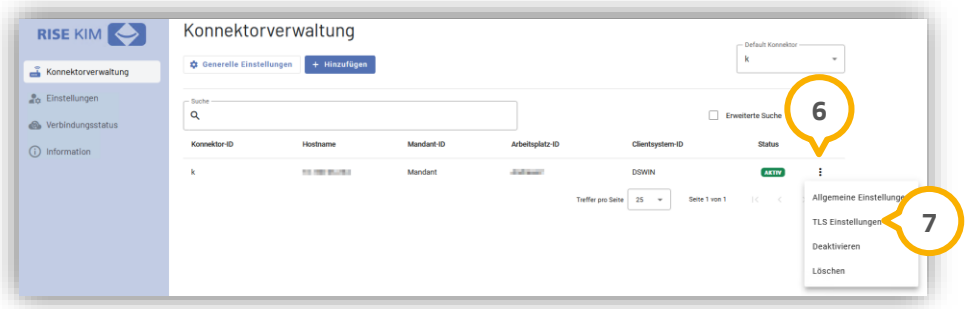


Klicken Sie bei „Login Administrator“ auf >>Anmelden<< (3).



Fügen Sie das zuvor kopierte Passwort bei „Passwort“ (4) ein.

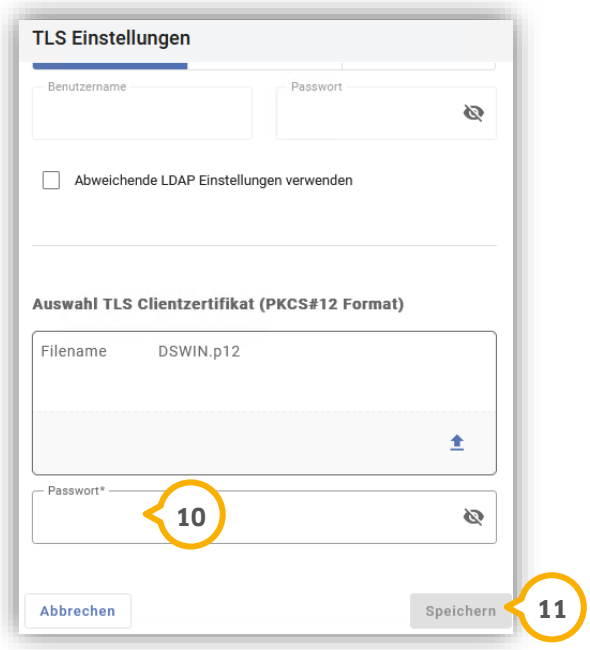
Klicken Sie auf >>Login<< (5).



Klicken Sie auf die 3 Punkte (6) und wählen Sie „TLS Einstellungen“ (7) aus.

Klicken Sie auf den Pfeil (8) und wählen Sie das neue Zertifikat aus.

Speichern Sie die Änderungen mit >>Speichern<< (9).



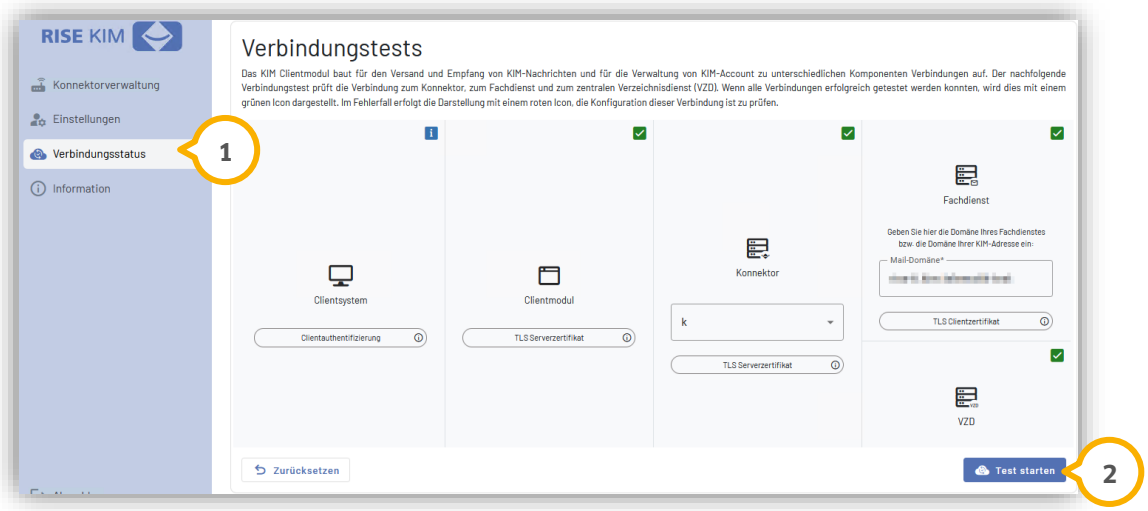
Geben Sie das Passwort (10) vom Zertifikat ein.

Klicken Sie auf >>Speichern<< (11).

Abschließend können Sie im RISE KIM-Client-Modul einen Verbindungstest durchführen.

Verbindungstest RISE KIM-Client-Modul durchführen:

Melden Sie sich am Konnektor an, wie es in der verlinkten Anleitung (https://www.dampsoft.de/wp-content/uploads/DS_Anleitung_e-connect-2.0-Konnektor-Neustart.pdf) beschrieben wird.



Wechseln Sie in den Bereich „Verbindungsstatus“ ①.

Klicken Sie auf >>Test starten<< ②.

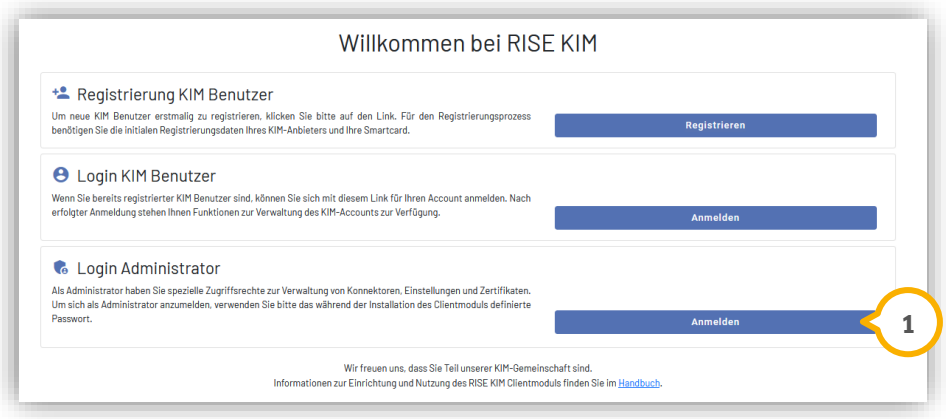
Wenn der Test erfolgreich ist, werden in der gesamten Übersicht grüne Häkchen angezeigt.

3.3. DS4: Zertifikat im KIM-Client-Modul einfügen

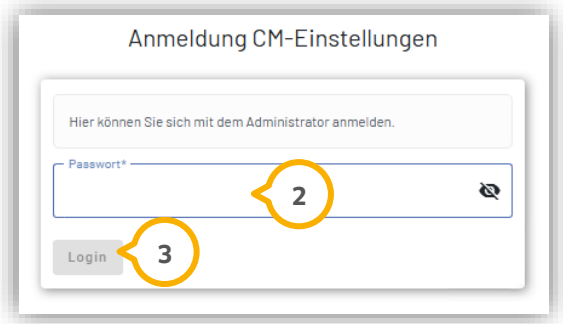
Hinweis!

Für den folgenden Vorgang wird das Administratorpasswort des RISE KIM-Client-Moduls benötigt. Dieses Passwort wurde während der Installation des Moduls vergeben und muss vor Beginn der Durchführung bereitliegen.

Öffnen Sie einen Browser und geben Sie in der Adresszeile Folgendes ein: „https://localhost:9443“.



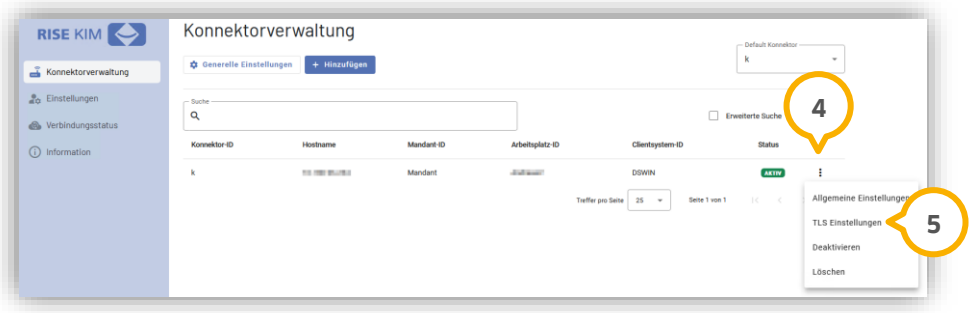
Klicken Sie bei „Login Administrator“ auf >>Anmelden<< ①.



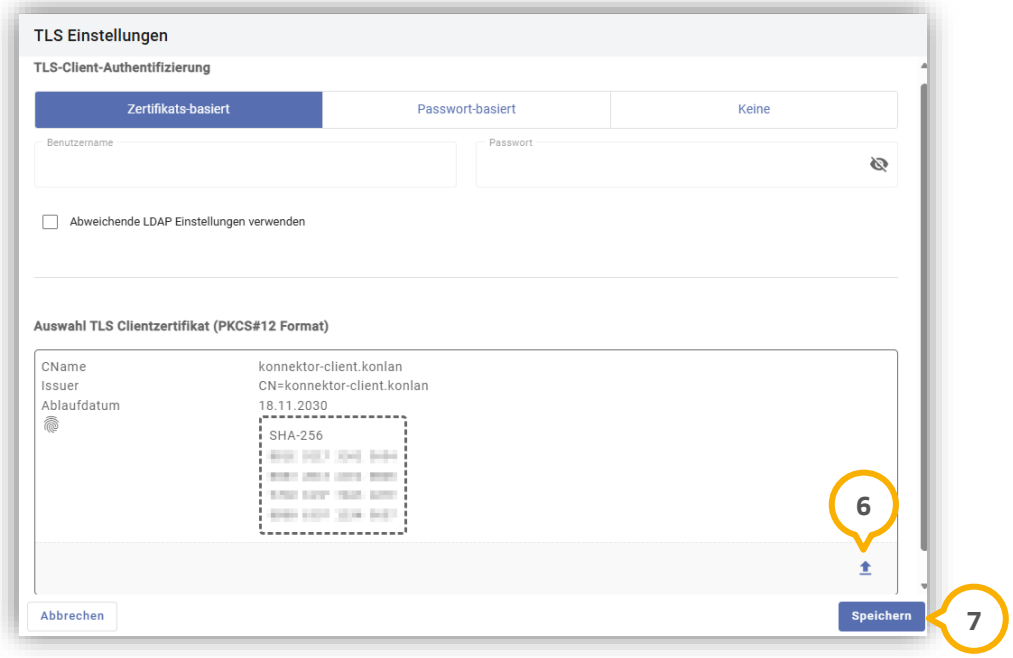
Fügen Sie das zuvor kopierte Passwort bei „Passwort“ ② ein.

Klicken Sie auf >>Login<< ③.

3. Zertifikat im RISE KIM-Client-Modul für Dampsoft-KIM-Adressen einfügen

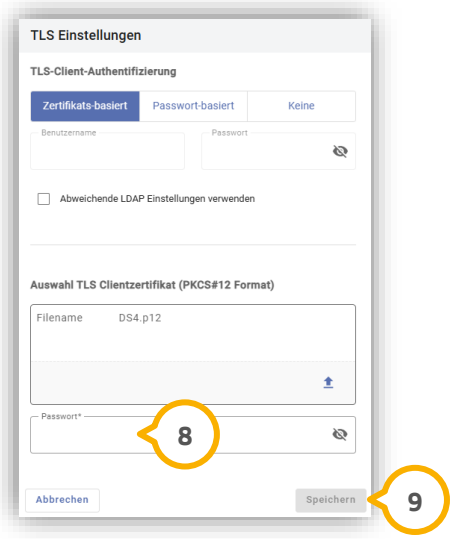


Klicken Sie auf die 3 Punkte ④ und wählen Sie „TLS Einstellungen“ ⑤ aus.



Klicken Sie auf den Pfeil ⑥ und wählen Sie das neue Zertifikat aus.

Speichern Sie die Änderungen mit >>Speichern<< ⑦.



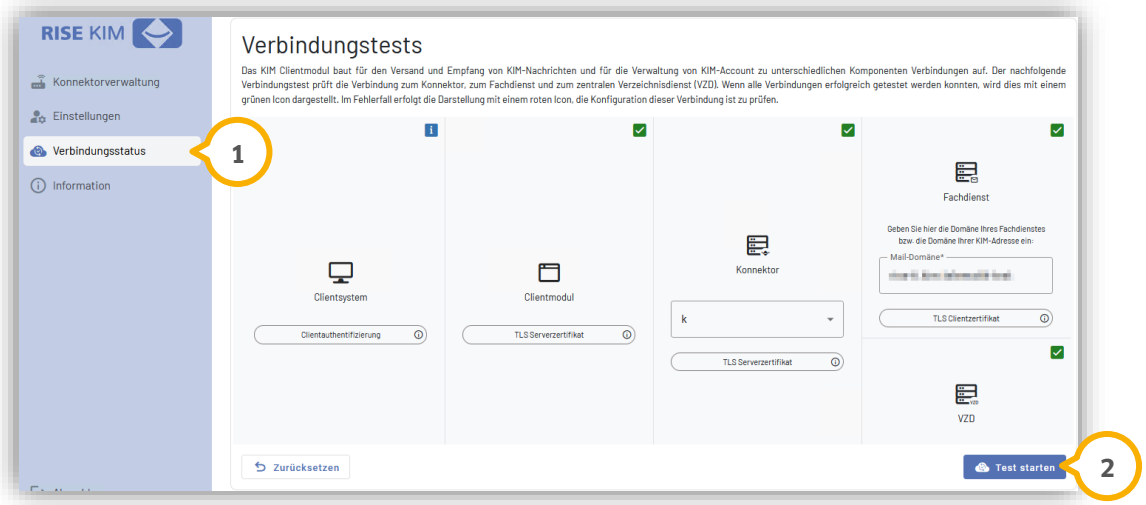
Geben Sie das Passwort (8) vom Zertifikat ein.

Klicken Sie auf >>Speichern<< (9).

Abschließend können Sie im RISE KIM-Client-Modul einen Verbindungstest durchführen.

Verbindungstest RISE KIM-Client-Modul durchführen:

Melden Sie sich am Konnektor an, wie es in der verlinkten Anleitung (https://www.dampsoft.de/wp-content/uploads/DS_Anleitung_e-connect-2.0-Konnektor-Neustart.pdf) beschrieben wird.



Wechseln Sie in den Bereich „Verbindungsstatus“ (1).

Klicken Sie auf >>Test starten<< (2).

Wenn der Test erfolgreich ist, werden in der gesamten Übersicht grüne Häkchen angezeigt.

DAMPSOFT GmbH
Vogelsang 1 / 24351 Damp

T 04352 9171-16 / F 04352 9171-90
info@dampsoft.de / www.dampsoft.de