

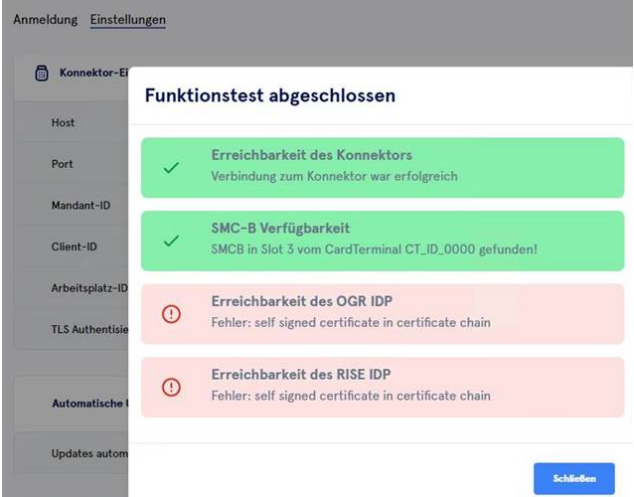

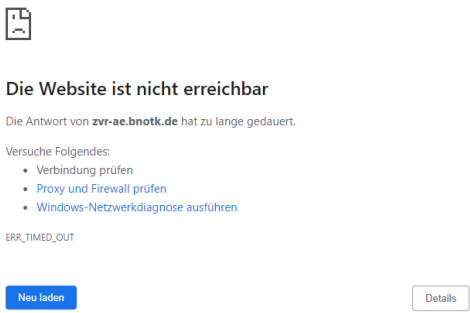


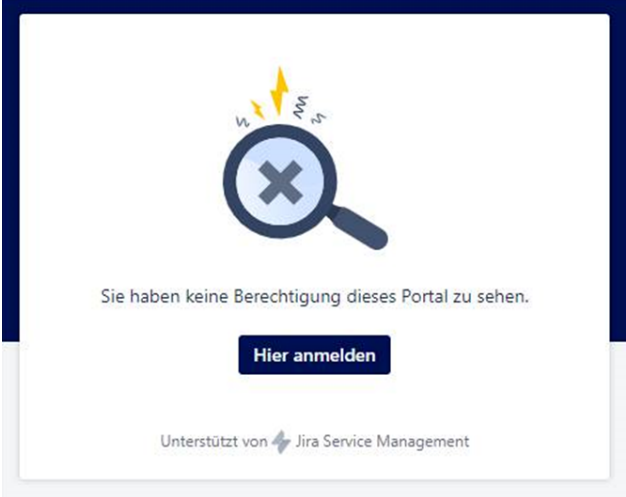

# Fragen & Antworten (FAQs)

## Für Nutzer oder Administratoren

#	Frage	Antwort
1	Was muss bei einer Installation beachtet werden?	Bitte führen Sie die Installation unter Admin so kann eine erfolgreiche Installation gart Starten Sie den Authenticator initial ebenf sodass die Software zu Beginn erfolgreich
2	Es öffnet sich plötzlich ein anderer Browser als der von mir verwendete Browser.	Stellen Sie sicher, dass der von Ihnen ver System hinterlegten default-Browser ents der Authenticator mit dem im System hint die sichere Anmeldung verwendet.
3	Was kann ich tun, wenn der Aufruf der Sharepoint-Download-URL des Authenticators sich nicht ordnungsgemäß öffnen lässt?	Versuchen Sie, die URL über den Inkogni öffnen. Wenn Sie selbst ein firmeninternes der Aufruf des gematik Sharepoint-Links c
4	Welche Karten unterstützt der Authenticator und wie wird entschieden, welche genutzt werden soll?	Der Authenticator unterstützt grundsätzlich HBA- sowie SMC-B-Karten.  Allerdings entscheidet nicht der Authentic werden soll, sondern die genutzte Fachan Die Fachanwendung gibt grundsätzlich im den Authentifizierungsprozess mittels Autl soll.  Bei Fragen hierzu wenden Sie sich bitte a Fachanwendung.
5	Der Funktionstest zeigt, dass er keine Verbindung zum Konnektor herstellen kann: <div><b>Erreichbarkeit des Konnektors</b> Fehler: Cannot read properties of undefined (reading 'body')</div> <div><b>Erreichbarkeit des Konnektors</b> Fehler:</div>	<ol style="list-style-type: none"><li>1. Stellen Sie bitte sicher, dass Sie die Adresse konfiguriert haben<ol style="list-style-type: none"><li>a. Der Port ist standardmäßig 4</li></ol></li><li>2. Prüfen Sie unter "TLS-Authentisieru"<ol style="list-style-type: none"><li>a. Bei Auswahl von "Zertifikat": l in PEM-Format<ol style="list-style-type: none"><li>i. Sind die PEM-Dateien i</li></ol></li><li>b. Bei Auswahl von "Benutzerna bitte, ob die eingegebenen Di</li></ol></li></ol>
6	Welche Dienste muss der Authenticator erreichen?	Der Authenticator kommuniziert mit dem I ng über die TI und über das Internet:  IDP-Dienst TI-Endpunkt: <a href="https://idp.zentra">https://idp.zentra</a>  IDP-Dienst Internet-Endpunkt: <a href="https://idp.z">https://idp.z</a>  Die Entscheidung, welcher Endpunkt gent Fachanwendung und <b>nicht</b> dem <b>Authenti</b>  Für eine manuelle Erreichbarkeitsprüfung Document heruntergeladen werden: <a href="https://www.gematik.de/known/openid-configuration">https://www.gematik.de/known/openid-configuration</a>  <pre>curl -v https://idp.app. well-known/openid-confi</pre>

7	<p>Der Funktionstest zeigt den IDP-Fehler <i>"Fehler: self signed certificate in certificate chain"</i></p> 	<p>Es könnte ein HTTPS-Proxy/Firewall auf c IDP vorhanden sein.</p> <p>Damit der Authenticator Ihrem HTTPS-Pr es Ihr Browser macht, muss das Public-St dieses Verzeichnis abgelegt werden: <b>C:\P Authenticator\resources\certs-idp</b></p> <p>Stichwort: SELF_SIGNED_CERT_IN_CH.</p> <p>Wir empfehlen auch immer die neueste V installiert zu haben, sodass alle aktuellste</p>
8	<p>Der Funktionstest zeigt den IDP-Fehler "Bad response: 407 mit der URL ..."</p> 	<p>Der Fehlerstatus-Code gibt an, dass der F abgesetzt werden konnte.</p> <p>Grund hierfür könnte sein, dass gültige A eine Proxy-Authentifizierung zwischen Br</p> <p>Bitte vergewissern Sie sich, dass Sie ents Autorisierungsdaten oder eine entspreche Kommunikation mit entsprechendem Endp</p> <p>Mit folgendem Curl können Sie überprüfen Endpunkte erreichen:</p> <p>IDP Internet-Endpunkt:</p> <pre>curl -v https://idp.app.well-known/openid-configuration</pre> <p>IDP PU TI Endpunkt:</p> <pre>curl -v https://idp.zentralidp.splitdns.ti-dienste.de/.well-known/openid-configuration</pre>
9	<p>Welche Anwendungen können bereits mit dem Authenticator genutzt werden?</p>	<p>das ZVR (zentrale Vorsorge-Register): <a href="#">ht</a></p>

10	<p>Was muss getan werden, wenn ich auf eine Fachanwendung nicht zugreifen kann? Bspw. ZVR: <a href="https://zvr-ae.bnotk.de/">https://zvr-ae.bnotk.de/</a></p> <div></div>	<p>Der gematik Authenticator wird im Zusammenspiel mit den Anwendungen der TI (WANDA) eingesetzt. Bei der Nutzerinteraktion mit einer Web-Anwendung (Web-Browser oder Web-Anwendung). Je nach Anwendung und Netzwerkumgebung kann es erforderlich sein, ein IP Routing zu konfigurieren, damit die Anwendung über das zentrale Gateway konfiguriert werden kann.</p> <p>Achten Sie daher darauf, dass ein entsprechendes Routing für die jeweilige Fachanwendung eingerichtet wird.</p> <p>Dies können Sie mittels folgendem Befehl in der Kommandozeile (Kommandozeile CMD) realisieren:</p> <pre>route add &lt;Netzwerk&gt; MASK &lt;Mask&gt; &lt;Gateway&gt;</pre> <p>Nach Einrichtung des Routings können Sie innerhalb der Kommandozeile testen, ob die Verbindung hergestellt werden kann:</p> <ul style="list-style-type: none"><li>• <b>tracert &lt;Netzwerk&gt;</b></li><li>• <b>ping &lt;DNS Fachanwendung&gt;</b><ul style="list-style-type: none"><li>◦ Bsp. ZVR: ping zvr-ae.bnotk.de</li></ul></li></ul> <p>Weitere Informationen hierzu finden Sie in den Installationshandbüchern unter dem Punkt "Netzwerkumgebung".</p> <p>Des Weiteren sollte auch geprüft werden, ob die Kommunikation mit der Fachanwendung über das zentrale Gateway daher bitte auch die entsprechenden Firewall-Einstellungen.</p>																					
11	<p>Welche Firewall-Freischaltungen sind für die Nutzung des Authenticators notwendig?</p>	<table><thead><tr><th>Description</th><th>Source</th><th>Destination</th></tr></thead><tbody><tr><td>Verbindung zum IDP via Internet</td><td>Lokaler Client / Workstation (localhost)</td><td><a href="https://idp.app.ti-dienste.de">idp.app.ti-dienste.de</a></td></tr><tr><td>Verbindung zum IDP via TI Endpunkt</td><td>Lokaler Client / Workstation (localhost)</td><td><a href="https://idp.zentral.ti-dienste.de">idp.zentral.ti-dienste.de</a></td></tr><tr><td>Verbindung zu WANDA Applikationen Bsp.: Zentrales Vorsorgeraster</td><td>Lokaler Client / Workstation (localhost) Bsp.: Lokaler Client / Workstation (localhost)</td><td>100.102.0.0 Bsp.: <a href="https://zvr-ae.bnotk.de">https://zvr-ae.bnotk.de</a></td></tr><tr><td>Auto-Updatefunktion</td><td>Lokaler Client / Workstation (localhost)</td><td><a href="https://github.com/gematik/app-authenticator">https://github.com/gematik/app-authenticator</a></td></tr><tr><td>Konnektor</td><td>Lokaler Client / Workstation (localhost)</td><td>internes Netzwerk</td></tr><tr><td>Kartenterminal</td><td>Lokaler Client / Workstation (localhost)</td><td>internes Netzwerk</td></tr></tbody></table>	Description	Source	Destination	Verbindung zum IDP via Internet	Lokaler Client / Workstation (localhost)	<a href="https://idp.app.ti-dienste.de">idp.app.ti-dienste.de</a>	Verbindung zum IDP via TI Endpunkt	Lokaler Client / Workstation (localhost)	<a href="https://idp.zentral.ti-dienste.de">idp.zentral.ti-dienste.de</a>	Verbindung zu WANDA Applikationen Bsp.: Zentrales Vorsorgeraster	Lokaler Client / Workstation (localhost) Bsp.: Lokaler Client / Workstation (localhost)	100.102.0.0 Bsp.: <a href="https://zvr-ae.bnotk.de">https://zvr-ae.bnotk.de</a>	Auto-Updatefunktion	Lokaler Client / Workstation (localhost)	<a href="https://github.com/gematik/app-authenticator">https://github.com/gematik/app-authenticator</a>	Konnektor	Lokaler Client / Workstation (localhost)	internes Netzwerk	Kartenterminal	Lokaler Client / Workstation (localhost)	internes Netzwerk
Description	Source	Destination																					
Verbindung zum IDP via Internet	Lokaler Client / Workstation (localhost)	<a href="https://idp.app.ti-dienste.de">idp.app.ti-dienste.de</a>																					
Verbindung zum IDP via TI Endpunkt	Lokaler Client / Workstation (localhost)	<a href="https://idp.zentral.ti-dienste.de">idp.zentral.ti-dienste.de</a>																					
Verbindung zu WANDA Applikationen Bsp.: Zentrales Vorsorgeraster	Lokaler Client / Workstation (localhost) Bsp.: Lokaler Client / Workstation (localhost)	100.102.0.0 Bsp.: <a href="https://zvr-ae.bnotk.de">https://zvr-ae.bnotk.de</a>																					
Auto-Updatefunktion	Lokaler Client / Workstation (localhost)	<a href="https://github.com/gematik/app-authenticator">https://github.com/gematik/app-authenticator</a>																					
Konnektor	Lokaler Client / Workstation (localhost)	internes Netzwerk																					
Kartenterminal	Lokaler Client / Workstation (localhost)	internes Netzwerk																					
12	<p>Wie sieht die aktuelle Ablaufkette für die Authentisierung mittels Authenticator aus?</p>	<ol style="list-style-type: none"><li>1. Über einen Anmeldeprozess innerhalb der Fachanwendung wird der Authenticator gestartet, um den Anmeldeprozess durchzuführen.</li><li>2. Die Anfrage in der Fachanwendung wird an den Authentifizierungsprozess weitergegeben.</li><li>3. Je nachdem, ob die Anmeldung über einen Konnektor oder ein entsprechendes Terminal erfolgt, wird die Karte zur Prüfung vorgelegt.</li><li>4. Prüfung, ob die entsprechende Karte für den Nutzer zugeordnet ist.</li><li>5. Der Nutzer muss eine PIN eingeben, die der Karte zugeordnet ist.</li><li>6. Daraufhin erfolgt eine Überprüfung der Identität durch den Authentifizierungsdienst.</li><li>7. Ist die Überprüfung erfolgreich, kehrt der Nutzer zur Fachanwendung zurück und kann die Anmeldung abschließen.</li></ol>																					

13	<p>Was muss getan werden, wenn der Zugriff auf das Anfrageportal der gematik nicht funktioniert?</p> 	<p>Es kann vorkommen, dass die Useranlage Anfrageportals des Authenticators für den nicht direkt reibungslos funktioniert. In diesem Fall sollte folgender Workaroun sodass das Kundenkonto erfolgreich eing</p> <ul style="list-style-type: none"> <li>• Bitte folgen Sie diesem Link <a href="https://serviceesk/customer/user/forgotp">https://serviceesk/customer/user/forgotp</a> Passwort zurück.</li> <li>• Benutzen Sie hierbei Ihre E-Mail-Adresse Info: Diese E-Mail muss ident Adresse Ihrer Support- oder S</li> </ul>
14	<p>Anmeldung mittels Smartcard nicht erfolgreich</p> <p>Was muss getan werden, wenn zwar alle Funktionstests grün sind, der Login im Browser jedoch mit folgender Fehlermeldung fehlschlägt?</p> <p><b>Das AUT Zertifikat ist ungültig</b></p>	<p>Überprüfen Sie, ob die eingesetzte Karte i aktiviert wurde.</p> <p>Zur Nutzung einer Karte bedarf es einer v Diese besteht zum einen in der Änderung einer Aktivierung in Richtung OCSP. In de bei Aushändigung wird das explizit erwähi</p> <p>Der Fehler deutet auf einen Fehler mit der hin, welcher durch vollständige Aktivierung</p>
15	<p>Wenn ich den Funktionstest ausführe, erhalte ich die Meldung</p> <p>"Fehler: Hostname/IP does not match certificate's alnames: IP: XXX.XX.X.XX is not in the cert's list."</p> <p><b>Funktionstest abgeschlossen</b></p> 	<p>Hier ist das Problem, dass der FQDN nicht enthalten ist. In einer TLS-Verbindung wird Domain Name) der URL gegen den Subjekt des Serverzertifikats geprüft. Während der Client, ob der FQDN mit dem Common Name Serverzertifikats übereinstimmt.</p> <p>Der Fehler kann daher auftreten, wenn im Überprüfung auf "aktiviert" gesetzt wird.</p> <p><b>Lösung:</b> Im Authenticator die TLS-Überprüfung setzen</p>

## Für Anwendungen bei der Integration

Frage	Antwort
Welche Fehlercodes gibt es?	Alle aktuellen Fehlercodes können Sie auf folgender Seite einsehen: <a href="#">Authenticator Fehlercodes</a>
Woher bekomme ich den Quelltext des Authenticators?	<a href="https://github.com/gematik/app-Authenticator">https://github.com/gematik/app-Authenticator</a>
Gibt es eine Beispielkonfiguration für nginx oder apache für die OpenID-Authentifizierung mit dem Authenticator und dem IDP der Gematik, insbesondere wegen der zusätzlichen Verschlüsselung?	Es ist kein nginx oder apache im Einsatz - daher gibt es auch keine entsprechende Beispielkonfiguration.
Besteht die Möglichkeit, den Authenticator auch lokal ohne jegliche Freischaltungen zu testen?	Ja - hierzu kann der Authenticator ab Version 2.1.0 genutzt werden. Diese Version beinhaltet einen Mockmodus, der zum Testen genutzt werden kann.

Woher weiß der Fachdienst, welcher challenge_path im deeplink genutzt werden muss?	Der Dienst bekommt das über den "authorization_endpoint " mit. Zu finden innerhalb des Discovery Document des IDPs (/well-known/openid-configuration)												
Was muss der Fachdienst noch machen, wenn er vom Authenticator den Authorization_Code weitergeleitet bekommt?	<div>1. Der Authorization_Code muss per Token Request beim Token-Endpoint des IDP-Dienstes eingereicht werden.</div> <div>2. Im Token Request wird der Authorization_Code über den Parameter "code" übergeben.</div> <div>3. Zusätzlich muss zum "code" noch der Parameter "key_verifier" mitgegeben werden.</div> <div>4. Der "key_verifier" enthält einen verschüsselten JWT (also einen JWE) mit dem code_verifier und einem token_key (= AES-Schlüssel) im Body</div> <div>5. In dem HTTP-Request MUSS der HTTP-Header user-agent gemäß [RFC7231] mit &lt;Produktname&gt;/&lt;Produktversion&gt; &lt;Herstellernamen&gt;/&lt;client_id&gt; mit: &lt;Produktname&gt; gemäß eigener Definition, Länge 1-20 Zeichen, Zeichenvorrat [0-9a-zA-Z\-\.] &lt;Produktversion&gt; gemäß Produktidentifikation &lt;Herstellernamen&gt; gemäß eigener Definition, Länge 1-20 Zeichen, Zeichenvorrat [0-9a-zA-Z\-\.] &lt;client_id&gt; gemäß Registrierung bei der gematik mitgesendet werden. Siehe "A_20015-01 - PS" der Spezifikation im <a href="#">Fachportal</a>.</div> <div>6. Der Token Response enthält "id_token" und "access_token". Beide sind JWEs, die mit dem token_key=AES-Schlüssel entschlüsselt werden können.</div> <div>7. Abschluss. Der Dienst hat jetzt den entschlüsselten ID/ACCESS Token</div>												
Woher weiß der Fachdienst, wohin der Token-Request gesendet werden muss?	Der Dienst bekommt das über den "token_endpoint" mit. Zu finden innerhalb des Discovery Document des IDPs (/well-known/openid-configuration)												
Wie muss der Fachdienst den "key_verifier" erstellen?	<div>1. AES-Schlüssel würfeln und merken</div> <div>2. code_verifier aus dem Speicher nehmen</div> <div>3. Beides als body_claims in einen JWT schreiben</div> <div>4. JWT mit dem ENC-Schlüssel des IDPs verschlüsseln</div> <div>5. Der resultierende JWE ist der key_verifier</div>												
Was muss ich tun, um mich erfolgreich für die Nutzung des zentralen IDP's zu registrieren?	Sie müssen sich bezüglich der Anbindung an folgende Adresse wenden: <a href="#">IDP-Registrierung@gematik.de</a> und werden dann alle weiteren Informationen von den zuständigen Transitionmanagern erhalten.												
Muss ich auch im Voraus Zertifikate beantragen oder registrieren?	Eine Registrierung von Zertifikaten ist nicht notwendig. Der zentrale IDP-Dienst ist mit einem TLS-Server-Zertifikat ausgestattet, welches gegen den Truststore des Authenticators geprüft wird. Eine beidseitige Authentisierung mittels TLS-Client-Zertifikat ist nicht vorgesehen. Die Zertifikate aus den Smartcards (HBA/SMC-B) müssen dem zentralen IDP-Dienst vorab nicht bekannt sein und müssen nicht registriert werden.												
Bei welchem Endpunkt tausche ich als WANDA den Authorization Code gegen den Access Token ein?	<div>Für das Einlösung des Authorization Code beim Token Endpoint muss der Endpunkt genommen werden, welcher laut Wanda Basic/Smart erreichbar ist:</div> <table><tr><th>Welcher IDP-Dienst Endpunkt muss verwendet werden?</th><th>WANDA Basic</th><th>WANDA Smart</th></tr><tr><td>Deeplink (Authenticator IDP-Dienst)</td><td>Internet-IDP</td><td>TI-Endpoint</td></tr><tr><td>Token Request (Fachanwendung IDP-Dienst)</td><td>Internet-IDP</td><td>TI-Endpoint</td></tr></table>	Welcher IDP-Dienst Endpunkt muss verwendet werden?	WANDA Basic	WANDA Smart	Deeplink (Authenticator IDP-Dienst)	Internet-IDP	TI-Endpoint	Token Request (Fachanwendung IDP-Dienst)	Internet-IDP	TI-Endpoint			
Welcher IDP-Dienst Endpunkt muss verwendet werden?	WANDA Basic	WANDA Smart											
Deeplink (Authenticator IDP-Dienst)	Internet-IDP	TI-Endpoint											
Token Request (Fachanwendung IDP-Dienst)	Internet-IDP	TI-Endpoint											
Wie heißen die IDP Endpunkte?	<table><tr><td>Identity Provider</td><td>RU Internet</td><td><a href="#">idp-ref.app.ti-dienste.de</a></td></tr><tr><td></td><td>RU TI-Endpoint</td><td><a href="#">idp-ref.zentral.idp.splitdns.ti-dienste.de</a></td></tr><tr><td></td><td>PU Internet</td><td><a href="#">idp.app.ti-dienste.de</a></td></tr><tr><td></td><td>PU TI-Endpoint</td><td><a href="#">idp.zentral.idp.splitdns.ti-dienste.de</a></td></tr></table>	Identity Provider	RU Internet	<a href="#">idp-ref.app.ti-dienste.de</a>		RU TI-Endpoint	<a href="#">idp-ref.zentral.idp.splitdns.ti-dienste.de</a>		PU Internet	<a href="#">idp.app.ti-dienste.de</a>		PU TI-Endpoint	<a href="#">idp.zentral.idp.splitdns.ti-dienste.de</a>
Identity Provider	RU Internet	<a href="#">idp-ref.app.ti-dienste.de</a>											
	RU TI-Endpoint	<a href="#">idp-ref.zentral.idp.splitdns.ti-dienste.de</a>											
	PU Internet	<a href="#">idp.app.ti-dienste.de</a>											
	PU TI-Endpoint	<a href="#">idp.zentral.idp.splitdns.ti-dienste.de</a>											
Wo kann ich meine Konnektor-Zertifikate hinterlegen?	<div>Die notwendigen Zertifikate müssen im Verzeichnis:</div> <div><b>C:\Program Files\gematik Authenticator\resources\certs-konnektor</b></div> <div>hinterlegt werden.</div>												
Wo kann ich fachanwendungsspezifische Zertifikate hinterlegen?	<div>Die notwendigen Zertifikate müssen im Verzeichnis:</div> <div><b>C:\Program Files\gematik Authenticator\resources\certs-idp</b></div> <div>hinterlegt werden.</div>												

Frage	Antwort
<b>Was ist der Credential Manager im Kontext des Authenticators?</b>	Der Credential Manager ist ein Sicherheitsfeature, das ab Version 4.8.0 im Authenticator integriert ist. Er dient dazu, sensible Informationen wie Passwörter sicher zu speichern und zu verwalten, anstatt sie im Klartext in der Konfigurationsdatei zu hinterlegen.
<b>Welche Informationen werden im Credential Manager gespeichert?</b>	Im Credential Manager werden folgende Daten gespeichert: <ul style="list-style-type: none"> <li>• Konnektor Basic Auth Benutzername</li> <li>• Konnektor Basic Auth Passwort</li> <li>• Proxy Basic Auth Benutzername</li> <li>• Proxy Basic Auth Passwort</li> <li>• P12-Zertifikat Passwort</li> </ul>
<b>Wie wird der Benutzername für das P12-Zertifikat im Credential Manager gespeichert?</b>	Da im P12-Zertifikat keine Benutzerinformationen enthalten sind, wird der Benutzername standardmäßig als "p12Password" im Credential Manager gespeichert.
<b>Wie funktioniert der Credential Manager in der Standalone-Version des Authenticators?</b>	In der Standalone-Version des Authenticators werden die Einstellungen automatisch gespeichert. Dabei werden sensible Daten im Credential Manager und nicht sensible Daten in der Konfigurationsdatei config.json gespeichert.
<b>Was passiert, wenn keine Eintragung im Credential Manager möglich ist?</b>	In der Version 4.8.0 des Authenticators ist der Zugriff auf den Credential Manager in vielen Fällen zwingend erforderlich. Sollte ein Fehler beim Zugriff oder bei der Speicherung der Daten im Credential Manager auftreten, wird ein Fehler mit dem Code AUTHCL0010 angezeigt.
<b>Muss ich bei einer zentralen Konfiguration alle Clients einzeln aktualisieren?</b>	Derzeit arbeiten wir an einem Skript, das die Passwörter in einer Massenaktion für alle Clients in den Credential Manager überträgt. Sie können die Möglichkeiten, die Ihre Systeme bieten, nutzen, um Einstellungen für alle Clients gleichzeitig vorzunehmen. Mit anderen Worten, ist es möglich, die Aktualisierung der Clients zentralisiert zu handhaben, indem Sie die Werkzeuge und Funktionen Ihres Systems verwenden, um die notwendigen Änderungen für alle Clients gleichzeitig durchzuführen. Dies erleichtert den Prozess und spart Zeit, im Vergleich zur individuellen Aktualisierung jedes einzelnen Clients.