
Projektdokumentation

Abschlussprüfung Winter 2023/24

Fachinformatiker für Systemintegration

# Sicherheitskonfiguration

## Zweifaktor-Authentifizierung für den internen Zugriff

**Prüfungsteilnehmer**

Nils Wilken

06.09.1995

Birkenweg 5

49699 Lindern

**Ausbildungsbetrieb**

Amoutec IT Solutions GmbH

Ecopark-Allee 7

49685 Emstek

# Inhaltsverzeichnis

# Tabellenverzeichnis



# Anhangsverzeichnis

# 1 Einleitung

Die folgende Projektdokumentation beschreibt den Entwicklungsprozess des IHK-Abschlussprojekts, welches ich im Rahmen meiner Ausbildung zum Fachinformatiker, Fachrichtung Systemintegration, durchgeführt habe.

Der zuständige Ausbildungsbetrieb war die Amoutec IT Solutions GmbH

## 1.1 Projektbeschreibung

In jedem Unternehmen ist IT-Sicherheit ein wichtiges Thema. Das gilt auch für Firmen in der Lebensmittelindustrie, wie [redacted]. Hier geht es um sensible Daten, die mit der Herstellung von Produkten, der Abstimmung von Zutaten oder der Behandlung von Rohstoffen zu tun haben. Wenn solche Daten öffentlich werden, könnte das großen wirtschaftlichen Schaden anrichten. Deshalb ist es für die [redacted] wichtig, ihre Daten gut zu schützen, besonders vor Verschlüsselungssoftware, die sie unbrauchbar machen könnte.

Bei der [redacted] werden viele Daten unverschlüsselt auf einem Server gespeichert, auf den fast alle Domänen-User Zugriff haben. Auch der Zugang zur Citrix-Umgebung von außen ist nur mit Username und Passwort gesichert. Eine Zwei-Faktor-Authentifizierung würde den Zugriff auf diese Daten sicherer machen. So wären die Daten besser geschützt, selbst wenn jemand Username und Passwort eines Users herausfindet. Durch die Einführung dieser zusätzlichen Sicherheitsmaßnahme könnte das Risiko von Ransomware-Angriffen deutlich reduziert werden.

## 1.2 Projektziel

Unser Projekt hat das Ziel, eine 2FA in unserem Unternehmen einzuführen. Diese zusätzliche Sicherheitsmaßnahme soll für jeden externen Zugriff auf die Citrix-Umgebung und jede VPN-Verbindung gelten. Außerdem planen wir, die 2FA auch für die Windows-Anmeldung an den Computern zu implementieren. So wird ein höheres Sicherheitsniveau erreicht, das auch außerhalb des Firmennetzwerks wirksam ist, ohne dabei die tägliche Arbeit zu beeinträchtigen.

Ein wichtiger Aspekt unseres Projekts ist die Flexibilität für die User. Jeder soll die Möglichkeit haben, zwischen verschiedenen Methoden der Zwei-Faktor-Authentifizierung zu wählen. So kann jeder User die für ihn bequemste und passendste Methode auswählen. Dieser Ansatz soll sicherstellen, dass die Sicherheitsmaßnahmen effektiv sind, ohne die Benutzerfreundlichkeit zu vernachlässigen.

## 1.3 Projektumfeld

Das Projekt wird [redacted].

[redacted] verfügt über eine eigene Serverlandschaft am Hauptsitz in [redacted]. Die Produktionsstandorte sind über ein MPLS-Netzwerk der EWE mit dem Hauptsitz verbunden. Zusätzlich gibt es einzelne Lager, die über VPN-Verbindungen mit [redacted] kommunizieren. In Emstek selbst befindet sich eine umfangreiche Serverlandschaft mit sechs ESX-Hosts, die redundant ausgelegt sind und etwa 80 virtuelle Maschinen betreiben. Eine wichtige Komponente ist die Citrix-Farm, über die die meisten Produktions- und

Verwaltungsstandorte arbeiten. [redacted] fungiert somit als zentrales Nervensystem für die anderen Standorte.

Aktuell ist eine 2FA über einen separaten Radius-Server eingerichtet, um den Zugang zur Citrix-Umgebung von außerhalb des Firmennetzwerks abzusichern.

### 1.4 Projektbegründung

Mehrere Faktoren haben zur Initiierung dieses Projekts beigetragen. Ein Hauptanliegen ist die Absicherung der Zugänge – nicht nur zur Citrix-Umgebung, sondern auch zu den VPN-Verbindungen und der Windows-Anmeldung. Unser Ziel ist es, einen zentralen Weg zu finden, um alle Zugänge zu unserem System zu regulieren und abzusichern. Denn nur mit einem durchdachten Plan können wir die maximale Sicherheit unserer Daten und Ressourcen gewährleisten.

Die Bedeutung der IT-Sicherheit hat in der heutigen Zeit stark zugenommen. Angriffe auf Systeme, um Daten zu verschlüsseln und Lösegeldforderungen zu stellen, sind häufig. Die wirtschaftlichen Verluste, die durch solche Angriffe entstehen, zeigen deutlich, wie abhängig Unternehmen von ihren IT-Systemen sind. Ein Stillstand durch verschlüsselte Daten kann für ein Unternehmen wie [redacted], das täglich Umsätze in Millionenhöhe generiert, verheerend sein. Daher ist es unser dringendes Anliegen, das System bestmöglich abzusichern und jede Sicherheitslücke zu schließen.

Ein weiterer Grund für die Entscheidung zu diesem Projekt ist das Sicherheitsgefühl, das durch abgesicherte Zugänge entsteht. Als Fachinformatiker tragen wir die Verantwortung, die Daten unserer Kunden zu schützen und das System vor Angriffen zu sichern. Diese Verantwortung begleitet uns täglich und ist eine ständige Quelle der Sorge. Sicherheitsmaßnahmen bringen uns jedoch mehr Ruhe und Sicherheit im Arbeitsalltag. Jede geschlossene Sicherheitslücke bedeutet eine Sorge weniger, die uns nachts wachhält.

### 1.5 Projektabgrenzung

Da der Projektumfang begrenzt ist, ist der komplette Rollout für alle Standort kein Bestandteil dieses Projektes. Wir beschränken uns auf dem Rollout an dem Verwaltungsstandort [redacted].

## 2 Projektplanung

### 2.1 Projektphasen

Für die Durchführung unseres Projekts hatten wir insgesamt 40 Stunden Zeit, entsprechend den Vorgaben der IHK Oldenburg. Bevor wir mit dem Projekt starteten, haben wir die verschiedenen Projektphasen genau definiert und festgelegt, wie viel Zeit wir für jede Phase einplanen. Dazu gehörte die Analyse der aktuellen Situation, die Zeit für die Erstellung des Entwurfs, die Implementierung der Lösung und schließlich die Dokumentation des gesamten Prozesses. Im Folgenden finden Sie eine tabellarische Übersicht, die zeigt, wie die 40 Stunden auf die einzelnen Phasen aufgeteilt wurden.

| | |
|---|---|
| Analyse | 6h |
| Durchführung der Ist-Analyse | 1h |
| Ermittlung der Möglichkeiten für die technische Umsetzung der Authentifizierungsmöglichkeiten | 3h |
| Durchführung einer Nutzwertanalyse | 2h |
| Planung | 7h |

| | |
|---|---|
| Analyse, welche Umsetzung technisch und wirtschaftlich am besten geeignet ist | 2h |
| Abwägung der Authentifizierungsmöglichkeiten nach Nutzen und Sinnhaftigkeit | 2h |
| Analyse der Anzahl der User und Festlegung, für welche User welche Authentifizierung sinnvoll ist | 2h |
| Bestellung der passenden Soft- und Hardware basierend auf der vorherigen Analyse | 1h |
| Implementierung | 23h |
| Ersetzen oder Erweitern des RADIUS-Servers(abhängig von der Entscheidung) | 6h |
| Ausrollen der Software zur Umstellung der Windows-Anmeldung auf 2FA | 4h |
| Konfiguration und Test der Authentifizierungsmöglichkeiten | 4h |
| Zuweisung der User zu den Authentifizierungsmöglichkeiten mittels Gruppeneinteilung | 2h |
| Umstellung der internen Citrix-Anmeldung auf Zwei-Faktor-Authentifizierung | 2h |
| Durchführung des Rollouts, zuerst für einzelne User, dann abteilungsweise und schließlich für die restliche Standorte | 5h |
| Abschluss | 4h |
| Schulung der IT-Mitarbeiter zur Administration der Zwei-Faktor-Authentifizierung | 2h |
| Erstellen einer Anleitung für die User über die verschiedenen Authentifizierungsmöglichkeiten | 2h |

*Tabelle 1: Zeitplan*

# 3 Analysephase

## 3.1 Ist-Analyse

Wie schon in der Projektbeschreibung erwähnt, verfügt die [redacted] über eine Serverlandschaft mit einer Citrix-Umgebung. Aktuell wird ein Radius-Server eingesetzt, um den externen Zugriff auf diese Citrix-Umgebung abzusichern. Bei den VPN-Verbindungen hingegen gibt es derzeit keine Zwei-Faktor-Authentifizierung; die Anmeldung erfolgt lediglich mit Username und Passwort. Gleiches gilt für die Windows-Anmeldung, die ebenfalls nur über Username und Passwort funktioniert.

Der Radius-Server generiert ein sechsstelliges OTP, dass der User bei der Anmeldung in der Citrix-Umgebung von extern eingeben muss. Die einzige Möglichkeit für den User, sich gegenüber dem Radius-Server zu authentifizieren, ist über den generierten QR-Code und das sechsstellige OTP, das von der App registriert wird.

Um einen klaren Überblick über den aktuellen Stand der Sicherheitsmaßnahmen zu haben, wurde eine Übersicht über die verschiedenen Verbindungen und deren Absicherung erstellt. Einen Ausschnitt dieser Übersicht finden Sie im Anhang. Man kann erkennen, dass nur die externe Citrix Verbindung eine abgesicherte Verbindung ist

## 3.2 Radius oder nicht

Die erste wichtige Entscheidung, die wir treffen mussten, betraf die Zukunft unseres Radius-Servers: Sollten wir ihn beibehalten und erweitern, oder sollten wir ihn durch ein anderes Produkt ersetzen? Unser Ziel, wie im Projekt beschrieben, ist es, ein System zu haben, das die Zwei-Faktor-Authentifizierung für die Citrix-Umgebung, die VPN-Verbindungen und die Windows-Anmeldung ermöglicht. Wir möchten einen zentralen Ort, an dem wir alle Authentifizierungen überwachen und steuern können.

Da unser aktueller Radius-Server auf Windows-Basis nicht in der Lage ist, all diese Anforderungen zu erfüllen, wurde uns klar, dass wir ein zusätzliches System benötigen. Dieses System sollte sowohl mit der Windows-Anmeldung als auch mit der Firewall kommunizieren können, um dort die 2FA einzurichten. Allerdings möchten wir nur ein einziges System für die gesamte Administration haben. Solange wir den Radius-Server behalten, können wir nicht alles von einem Ort aus verwalten. Daher kamen wir zu dem Schluss, dass ein anderes Produkt, das speziell für diese Zwecke entwickelt wurde, unsere Anforderungen erfüllen und gleichzeitig die Aufgaben des Radius-Servers übernehmen könnte. Dies würde es uns ermöglichen, den Radius-Server zu ersetzen.

## 3.3 Nutzwertanalyse

Nachdem wir uns entschieden hatten, nach einem Produkt zu suchen, das all unsere Anforderungen erfüllt und gleichzeitig unseren Radius-Server ersetzen kann, begannen wir mit einer sorgfältigen Analyse. Aus unserer Internetrecherche kristallisierten sich drei Marken und Produkte heraus, die uns interessant erschienen. Um die beste Wahl zu treffen, erstellten wir eine Nutzwertanalyse. Dabei legten wir Kriterien fest, die uns wichtig waren, und gewichteten diese entsprechend unseren Vorstellungen. Beispielsweise war uns die Zuverlässigkeit wichtiger als der Preis, da eine geringe Zuverlässigkeit größeren Schaden anrichten könnte als ein etwas höherer Preis. Zudem legten wir Wert auf eine zentrale Oberfläche und vielfältige Authentifizierungsmöglichkeiten, um es den Usern so angenehm wie möglich zu machen. Die vollständige Nutzwertanalyse finden Sie im Anhang.

Wie das Ergebnis der Nutzwertanalyse zeigt, haben wir uns für Fortinet entschieden. Mehrere Faktoren führten zu dieser Entscheidung. Zum einen kennen und nutzen wir Fortinet-Produkte bereits seit längerem erfolgreich. Wir setzen Fortinet-Firewalls an allen unseren Standorten ein und hatten damit noch nie Probleme. Auch die Fortinet-Accesspoints haben uns überzeugt. Ein weiterer Pluspunkt war die einfache und unkomplizierte Einrichtung der Accesspoints mit den Fortigate-Firewalls. Der Vorteil der Verwendung von Produkten desselben Herstellers ist hier groß, da die Schnittstellen immer vorhanden sind und es zu weniger Problemen kommt. Da wir mit dem neuen Produkt auch eine Schnittstelle zu den Fortinet-Firewalls benötigen, ist es ein großer Vorteil, ein Produkt von Fortinet zu wählen, bei dem die Kompatibilität bereits gegeben ist.

Ein weiterer wichtiger Aspekt ist unsere Partnerschaft mit Fortinet. Als offizieller Fortinet-Partner hatten wir die Möglichkeit, uns ausführlich über das Produkt und seine Vor- und Nachteile informieren zu lassen. Zudem erhalten wir als Partner Rabatte auf Fortinet-Produkte, was in unserem Fall ein weiterer Grund für die Entscheidung war. Durch den Premium-Support von Fortinet können wir außerdem darauf vertrauen, bei Problemen schnell Unterstützung zu erhalten.

Die Berechnung der Kosten für die 3 Marken Fortinet, WatchGuard und Protectimus finden Sie ebenfalls im Anhang.

Zusammenfassend lässt sich sagen, dass Fortinet in unserem Fall die einzig sinnvolle Wahl war. Unsere Umgebung basiert auf Fortinet-Produkten, und für die Windows-Anmeldung hat Fortinet bereits einen speziellen Agenten entwickelt, was die Kompatibilität sicherstellt. Durch unsere Partnerschaft mit Fortinet profitieren wir von Preisnachlässen und exzellentem Support, was uns zusätzliche Sicherheit und Verlässlichkeit bei eventuellen Problemen bietet.

## 3.4 Cloud oder On Premises

Ein weiterer wichtiger Aspekt, den wir in Betracht ziehen mussten, war die Entscheidung zwischen einer Cloud-Lösung und einer On-Premises-Lösung, sowie ob wir uns für eine virtuelle Maschine oder ein physisches Hardware-Gerät entscheiden sollten. Wir haben uns für die virtuelle Maschine entschieden, anstatt ein physisches Gerät zu nutzen. Der Hauptgrund dafür ist, dass wir bereits über eine umfangreiche Serveranlage verfügen, auf der wir virtuelle Maschinen erstellen können. So sparen wir Platz in unserem Serverraum, da kein zusätzliches Hardware-Gerät benötigt wird. Ein weiterer Vorteil der virtuellen Maschine ist die erhöhte Ausfallsicherheit. Da sie auf mehreren ESX-Hosts in einem Cluster läuft, kann die Maschine auch bei einem Ausfall eines Hosts weiterlaufen, was eine höhere Ausfallsicherheit bietet als bei einer Hardware-Lösung. Zudem sind Backup- und Wiederherstellungsoptionen bei virtuellen Maschinen in einem Cluster einfacher zu handhaben als bei einem einzelnen Hardwaregerät.

Dann stand noch die Entscheidung zwischen der FortiCloud-Lösung und dem FortiAuthenticator an. Die FortiCloud-Lösung wird direkt von Fortigate gehostet und ist über einen Internetzugang erreichbar, während der FortiAuthenticator eine virtuelle Maschine ist, die wir in unserem eigenen Haus betreiben. Wir entschieden uns für die virtuelle Maschinenlösung, da wir gerne die volle Kontrolle über die Administration unserer Systeme behalten möchten. Bei der FortiCloud-Lösung wären wir stärker von Fortinet abhängig. Da der FortiAuthenticator mehr Freiraum in der Konfiguration bietet als die FortiCloud, können wir das Produkt besser an unsere Bedürfnisse anpassen. Ein weiterer entscheidender Faktor für die Wahl des FortiAuthenticators war, dass der von uns benötigte Windows-Agent nur mit diesem System kompatibel ist.

## 3.5 Kalkulation des Angebots.

Nachdem wir uns entschieden hatten, den FortiAuthenticator als virtuelle Maschine in unserer bestehenden Serverinfrastruktur zu implementieren, stand die Auswahl der geeigneten Multi-Faktor-Authentifizierungsmethoden (MFA) an. Angesichts der verfügbaren Optionen – E-Mail, SMS, Handy-App und FortiToken USB-Sticks – mussten wir eine Lösung finden, die sowohl sicher als auch userfreundlich für unsere User ist.

Wir entschieden uns für E-Mail, SMS und die Handy-App als unsere primären MFA-Methoden. Diese Methoden wurden ausgewählt, da sie weit verbreitet, einfach zu nutzen und bei den Usern beliebt sind. Die Handy-App bietet zusätzlich eine erhöhte Sicherheitsebene, da Smartphones bereits ein fester Bestandteil des Alltags vieler User sind.

Darüber hinaus haben wir uns vorerst gegen den Erwerb von Fortitoken-USB-Sticks entschieden, da diese mit Kosten von 60 Euro pro Stück sehr teuer sind. Zudem besteht bei unseren Mitarbeitern an den Produktionsstandorten ein erhöhtes Risiko, dass die USB-Sticks schnell beschädigt werden können. Aus diesen Gründen haben wir uns zunächst gegen diese Variante entschieden, behalten uns jedoch die Option vor, sie zu einem späteren Zeitpunkt bei Bedarf einzuführen.

Wir haben uns schließlich für folgendes Angebot entschieden: Wir nehmen den FortiAuthenticator mit einem Lizenzpaket für 1-500 User, wobei wir uns für 300 Lizenzen entschieden haben. Zusätzlich haben wir eine FortiCare-Lizenz für die nächsten drei Jahre gebucht. Dies gewährleistet, dass wir Support und Updates erhalten, um unser System stets auf dem neuesten Stand zu halten. Bei Problemen können wir auf den Forti-Support

zurückgreifen, um effektive Hilfe zu erhalten. Dazu haben wir uns noch für 250 Lizenzen von der Fortitoken Mobile entschieden.

### 3.6 Berechnung der Projektkosten

Die Projektkosten, die während der Entwicklung des Projektes anfallen, sollen im Folgenden kalkuliert werden. Hierzu müssen wir die Personalkosten bestimmen und dafür rechnen wir mit einen Stundensatz für Auszubildende von 8,00 Euro Euro und für Mitarbeiter nehmen wir einen Stundensatz von 100,00 Euro. Weitere anfallende Kosten wie Räumlichkeiten, Strom usw. werden hier mit 10 Euro die Stunde als Nebenkosten bei dem Auszubildenden draufgerechnet. Aufgrund von mehreren Mitarbeitern und Auszubildenen die in dem Projekt mitgewirkt haben, fassen wir hier die Stunden unter „Mitarbeiter“ und „Auszubildende“ zusammen.

| Personal | Stunden | Stundensatz | Kosten |
|---|---|---|---|
| Auszubildender 1. | 40h | 18,00 Euro | 720,00 Euro |
| Mitarbeiter | 5h | 100,00 Euro | 500,00 Euro |
| Auszubildende | 5h | 8,00 Euro | 40,00 Euro |

*Tabelle 2: Personalkosten*

Somit belaufen sich die Personalkosten auf insgesamt 1.260,00 Euro

Dann kommen noch die Kosten für den Fortiauthenticator und die dazugehörigen Lizenzen.

| Artikel | Menge | Einzelpreis | Betrag in EUR |
|---|---|---|---|
| Fortiauthenticator VM Lizenz (100 User) | 1 | 800,78 | 800,78 |
| Fortiauthenticator VM Lizenz 100 User Upgrade | 2 | 479,40 | 958,79 |
| Fortiauthenticator 3 Jahre Forticare Support | 1 | 552,03 | 552,03 |
| | | | |
| FortitokenMobile (200 Lizenzen) | 1 | 4586,90 | 4.586,90 |
| FortitokenMobile (50 Lizenzen) | 1 | 1389,86 | 1.389,86 |
| Gesamt (Netto) | | | 8.288,36 |
| Gesamt (Brutto) | | | 9.863,14 |

*Tabelle 3: Angebot Fortinet*

Somit belaufen sich die Kosten für die Fortiauthenticator Lizenzen auf 9863,14 Euro

Jetzt berechnen wir die Gesamtkosten für das Projekt. Also die Kosten für die Fortiauthenticator Lizenzen plus die Personalkosten. Also haben kommen wir auf einen Gesamtwert von: 1.260,0 Euro + 9.683,13 Euro = 10943,13 Euro.

Also belaufen sich die Gesamtkosten für das Projekt auf 10.943,13 Euro

## 4. Implementierung

Wir starteten mit der Implementierung des FortiAuthenticators, einem wesentlichen Schritt, um unsere Netzwerksicherheit durch Multi-Faktor-Authentifizierung zu stärken. Dieser Prozess beinhaltete mehrere wichtige Schritte, angefangen bei der Einrichtung der virtuellen Maschine bis hin zur Konfiguration der Authentifizierungsdienste.

Bei Fortinet folgt die Nutzung virtueller Maschinen einem Lizenzmodell. Das bedeutet, dass man die Vorlagen oder Installationsdateien kostenlos aus seinem Fortinet-Account

herunterladen und in der eigenen Umgebung einrichten und konfigurieren kann. Allerdings ist für die vollständige Nutzung aller Funktionen des Produkts eine Lizenz erforderlich. Beim FortiAuthenticator beispielsweise gibt es eine Beschränkung auf maximal fünf User, die man nutzen kann, um sich mit dem Produkt vertraut zu machen und es in einer Testphase zu erproben.

## 4.1 Aufsetzen der virtuellen Maschine

Nachdem wir die Installationsdateien aus dem FortiPortal heruntergeladen hatten, begannen wir mit dem Aufbau der virtuellen Maschine. Fortinet stellt detaillierte Schritt-für-Schritt-Anleitungen zur Verfügung, die jeden Schritt genau erläutern. Da wir in unserer Umgebung VMware verwenden, benötigten wir die Installationsdatei im OVF-Format (Open Virtualization Format), um die virtuelle Maschine einzurichten. Die Installationsmedien umfassten eine FortiAuthenticator OVF-Datei und zwei VMDK-Dateien. Die OVF-Datei ist eine Konfigurationsdatei, die den Aufbau der virtuellen Maschine in einem standardisierten Format beschreibt, einschließlich Informationen über die Hardware-Anforderungen wie CPU, Speicher, Netzwerkeinstellungen und weitere Konfigurationsdetails. Die VMDK-Dateien (Virtual Machine Disk) sind ein von VMware verwendetes Format für virtuelle Festplatten. Diese Dateien enthalten die virtuelle Festplatte sowie die Betriebssystem- und Anwendungsdaten für den FortiAuthenticator. Über das vCenter haben wir aus diesen drei Dateien eine neue virtuelle Maschine in unserem Cluster erstellt. Angaben zu Speichergröße und Leistung waren nicht erforderlich, da diese bereits in den Installationsdateien enthalten waren. Nach der Installation und dem Start der virtuellen Maschine nahmen wir einige Konfigurationseinstellungen vor, um den FortiAuthenticator zugänglich zu machen. Zunächst legten wir über die Kommandozeile einen User an, um die Konfigurationen durchführen zu können. Anschließend führten wir einige Befehle aus, um die Konfiguration des FortiAuthenticators abzuschließen, darunter das Festlegen einer IP-Adresse inklusive Subnetzmaske, das Bestimmen des Standardgateways und das Aktivieren des HTTPS-Zugriffs auf den FortiAuthenticator. Nach diesen Einstellungen konnten wir über die IP-Adresse im Webbrowser auf die Webansicht des FortiAuthenticators zugreifen und uns mit unserem User anmelden.

## 4.2 Konfiguration der virtuellen Maschine

Nachdem wir die virtuelle Maschine erfolgreich eingerichtet hatten, begannen wir mit ihrer Konfiguration. Der erste Schritt bestand darin, eine Verbindung zu unserem Domaincontroller herzustellen. Im Bereich User Management/Remote Auth. Servers/LDAP fügten wir unseren Domaincontroller hinzu, um Userdaten in den FortiAuthenticator zu übertragen. Die Verbindung zum Domaincontroller wurde über dessen IP-Adresse und einen Admin-Zugang mit Lese- und Schreibberechtigungen hergestellt.

Unser Ziel war es, die Userkonten direkt aus der AD in den FortiAuthenticator zu synchronisieren. Dazu erstellten wir zunächst eine Sicherheitsgruppe in unserer Active Directory. Anschließend definierten wir eine Synchronisationsregel, die alle fünf Minuten die User aus dieser Gruppe mit dem zuvor eingebundenen Domaincontroller abgleicht. Da wir zu diesem Zeitpunkt noch mit einer Testlizenz arbeiteten, war die Anzahl der User auf fünf begrenzt.

## 4.3 Einrichtung des Mailservers

Anschließend konfigurierten wir unter dem Menüpunkt „SMTP Server“ unseren lokalen Exchange Server. Hier legten wir fest, was im Betreff der E-Mail stehen soll und unter welcher E-Mail-Adresse der FortiAuthenticator Nachrichten versenden soll. Um dem FortiAuthenticator das Versenden von E-Mails über unseren Exchange Server zu ermöglichen, hinterlegten wir die IP-Adresse des FA im Exchange als Relay. Dies erlaubt es dem FortiAuthenticator, E-Mails über den Exchange Server zu senden. Es war außerdem notwendig, die Standard-Mail-Option auf unseren lokalen Exchange einzustellen, damit E-Mails auch tatsächlich darüber versendet werden. Wir konfigurierten alle User so, dass ihr Token – also ihr zweites Passwort – per E-Mail verschickt wird. Dies ermöglichte es uns, während der Testphase so umfassend wie möglich zu testen, bis wir die Lizenzen erhielten. Da der FortiAuthenticator über eine Token-Testfunktion verfügt, konnten wir bestätigen, dass sowohl der E-Mail-Versand über den Exchange als auch die Token-Funktionalität einwandfrei funktionieren.

## 4.4 Einrichtung der Firewall

Unser erstes Ziel war die Einrichtung der VPN-Verbindungen über Multi-Faktor-Authentifizierung (MFA). Da unsere Serverinfrastruktur am Verwaltungsstandort in Emstek zentralisiert ist, benötigten wir lediglich eine VPN-Verbindung zu diesem Netzwerk, um die Arbeit unserer Mitarbeiter und uns selbst zu ermöglichen. Zunächst integrierten wir die vorhandene Fortigate in Emstek als Radius-Client in den FortiAuthenticator. Dies ermöglichte es dem FortiAuthenticator, Radius-Anfragen von der Fortigate zu verarbeiten.

Anschließend konfigurierten wir auf der Fortigate den FortiAuthenticator als neuen Radius-Server. Dies war notwendig, damit die Fortigate weiß, wohin sie Radius-Anfragen senden soll. Der nächste Schritt war die Erstellung einer Radius-Service-Policy im FortiAuthenticator. In dieser Policy definierten wir, wie der FortiAuthenticator mit den Radius-Anfragen der Fortigate umgehen soll. Es war wichtig festzulegen, für welche Radius-Clients die Policy gilt und wie die Authentifizierung genau ablaufen soll. Wir entschieden uns dafür, dass die Policy das Token – also das zweite Passwort – abfragen soll, um eine effektive MFA zu gewährleisten.

Weiterhin legten wir auf der Fortigate eine Gruppe an, die den Zugang zur VPN-Verbindung regelt. In den Firewall-Richtlinien stellten wir sicher, dass diese Gruppe auch Zugriff auf unser Netzwerk hat. Danach richteten wir Remote-Radius-User ein, die den zuvor konfigurierten Radius-Server und die erstellte Gruppe nutzen. Sobald wir nun versuchten, die VPN-Verbindung auszuwählen, erschien ein zusätzliches Feld, in das wir unser Token eingeben konnten. Nach erfolgreicher Eingabe beider Passwörter wurde die Verbindung hergestellt.

## 4.5 Aktivierung der Lizenz

Als nächster Schritt stand die Aktivierung der Lizenzen für den FortiAuthenticator an. Zuerst mussten wir uns in unseren FortiAccount einloggen, wo wir eine Übersicht über alle unsere Fortinet-Geräte im Netzwerk sowie Informationen zum FortiCare-Support finden. Für die Lizenzierung erhielten wir einen spezifischen Code. Diesen Code trugen wir in unserem FortiAccount ein, um den FortiAuthenticator zu registrieren. Nach der Registrierung konnten wir eine Lizenzdatei herunterladen und diese in unseren FortiAuthenticator hochladen, wodurch die Lizenz aktiviert wurde.

Insgesamt verfügten wir über vier Lizenzen: Eine Lizenz für die virtuelle Maschine des FortiAuthenticators, die 100 User unterstützt, zwei weitere Lizenzen, um die Useranzahl auf insgesamt 300 zu erhöhen, und eine Lizenz für das FortiCare-Paket, um sicherzustellen, dass

der FortiAuthenticator stets die neuesten Updates erhält. Zusätzlich erwarben wir 200 FortiToken Mobile Lizenzen für die Nutzung mit der mobilen App. Somit hatten wir einen FortiAuthenticator für 300 User mit 200 mobilen FortiTokens im Einsatz.

## 4.6 Einrichtung der Handy APP und Push Benachrichtigungen

Als nächsten Schritt planten wir, die FortiToken Mobile App zu testen, eine spezielle Anwendung von Fortinet. Zuvor hatten wir für die Testphase Token per E-Mail verwendet, entschieden uns nun jedoch für den Wechsel zu mobilen Token. Sobald einem User ein FortiToken Mobile zugewiesen wird, erhält er einen QR-Code an seine hinterlegte E-Mail-Adresse. Diesen QR-Code kann der User dann in seiner FortiToken Mobile App scannen, wodurch der Token in der App verfügbar wird.

Ein wesentlicher Grund für unsere Entscheidung, den FortiAuthenticator (FA) zu nutzen, waren die verbesserten Schnittstellen zu unseren anderen Produkten sowie die Möglichkeit, Push-Benachrichtigungen zu verwenden. Unser Ziel war es, die MFA für die User so komfortabel wie möglich zu gestalten. Die Bestätigung einer Push-Benachrichtigung auf dem Smartphone ist für viele Nutzer angenehmer und einfacher als das Eingeben eines sechsstelligen Codes.

## 4.7 Push-Benachrichtungen

Wir setzten uns das Ziel, die Funktionalität der VPN-Verbindung mit dem Token aus der FortiToken Mobile (FTM) App zu testen und zu vergleichen, ob sie genauso effektiv ist wie die Verwendung des Tokens, den wir zuvor per E-Mail erhalten hatten. Erfreulicherweise funktionierte der Code aus der FTM App genauso zuverlässig wie der per E-Mail versendete Code.

Anschließend wollten wir die Funktionsweise der Push-Benachrichtigungen überprüfen. Dazu aktivierten wir die Push-Benachrichtigungsfunktion im FortiAuthenticator und führten einen weiteren Test durch. Bei der Anmeldung an der Fortigate hatten wir nun die Wahl, entweder das Token manuell einzugeben oder uns eine Push-Benachrichtigung senden zu lassen. Wir stießen jedoch auf ein Problem: Obwohl die Push-Benachrichtigungen auf unserem Handy ankamen, führte das Akzeptieren der Benachrichtigung zu einem Timeout der App. Interessanterweise funktionierten die Push-Benachrichtigungen einwandfrei, sobald das Handy mit unserem Firmen-WLAN verbunden war. Daraus schlossen wir, dass die Push-Benachrichtigungen von unserer Fortigate-Firewall blockiert und nicht an den FortiAuthenticator weitergeleitet wurden.

Gemäß der Fortinet-Dokumentation zu Push-Benachrichtigungen nutzen diese den Port 443. Da in unserem System bereits mehrere Dienste diesen Port für HTTPS-Anmeldungen verwenden, mussten wir eine Lösung finden, um den Port 443 an den FortiAuthenticator weiterzuleiten, ohne die bestehenden Systeme zu beeinträchtigen. In der Dokumentation fanden wir eine Option, um den Push-Benachrichtigungen einen speziellen Port und eine spezielle IP-Adresse zuzuweisen. Wir wählten einen freien Port – Port 15235 – und gaben die WAN-IP unserer Fortigate an. Die Push-Benachrichtigung wurde somit an unser Handy gesendet und von dort über Port 15235 an unsere öffentliche IP-Adresse weitergeleitet. Anschließend richteten wir eine Portweiterleitung von der öffentlichen IP-Adresse am Port 15235 zur IP-Adresse unseres FortiAuthenticators am Port 443 ein. Diese Konfiguration ermöglichte es uns, die Push-Benachrichtigungen erfolgreich zu empfangen und zu bestätigen, selbst wenn das Handy nicht mit unserem Firmennetzwerk verbunden war.

## 4.8 Fortiauthenticator Windows Agent

Nachdem wir die VPN-Verbindung über den FortiAuthenticator (FA) mit Push-Benachrichtigungen konfiguriert hatten, richteten wir unser Augenmerk auf die Multi-Faktor-Authentifizierung (MFA) für die Windows-Anmeldung. Im FortiAuthenticator gab es einen Bereich, in dem man den FortiAuthenticator Windows Agent (FAWA) herunterladen und installieren konnte. Nach der Installation erschien eine zusätzliche Option unter der Windows-Anmeldung, in der man sein zweites Passwort, also den Token, eingeben konnte. Zu diesem Zeitpunkt war die MFA jedoch noch nicht aktiviert.

Der erste Schritt bestand darin, den FAWA mit dem FortiAuthenticator zu verbinden. Wir erstellten einen speziellen Admin-Zugang auf dem FA und wiesen diesem die Rolle eines Web-Admins zu, wodurch ein Schlüssel generiert wurde, den wir für die Verbindung zum FA nutzen konnten. In den Einstellungen des FAWA trugen wir den Web-Admin und den Schlüssel ein, um eine Verbindung zum FA herzustellen. Wir stießen jedoch auf ein Problem: In den Logs des FA gab es keine Hinweise darauf, dass sich der FAWA mit dem FA verbunden hatte oder versucht hatte, eine Verbindung aufzubauen. Nach Durchsicht der Fortinet-Dokumentation fanden wir heraus, dass wir zunächst den API-Zugang für den FA freischalten mussten, damit der FAWA eine Verbindung herstellen kann.

Um die MFA im FAWA zu aktivieren, mussten wir festlegen, bei welchen Domänen sie aktiviert werden soll. Wir aktivierten also die MFA für die GUG-Domäne und testeten anschließend, ob die Anmeldung mit dem Code funktioniert. Nachdem dies erfolgreich war, testeten wir auch die Push-Benachrichtigungen, die ebenfalls funktionierten. Es ist erwähnenswert, dass der FAWA standardmäßig eine Sicherheitsoption aktiviert hat, die es ermöglicht, die MFA zu umgehen und sich dennoch normal mit den Anmeldedaten einzuloggen. Diese Funktion dient dazu, den FAWA zunächst zu testen und zu konfigurieren und Möglichkeiten einzurichten, um Zugang zum Rechner zu erhalten, falls beispielsweise das zweite Passwort nicht funktioniert.

## 4.9 Möglichkeiten für die MFA

Um eine reibungslose Implementierung der MFA zu gewährleisten, haben wir verschiedene Möglichkeiten in dem FAWA konfiguriert, um den User bei Anmeldeproblemen zu helfen und den normalen Betrieb so wenig wie möglich zu stören.

**1. Ausgenommene User und Gruppen (Exempted Users/Groups):** Wir haben eine Gruppe in der Active Directory (AD) erstellt, die von der MFA ausgenommen ist. Diese Gruppe ermöglicht es bestimmten Usern, sich ohne ein zweites Passwort anzumelden. In diese Gruppe haben wir unsere Admin-Accounts aufgenommen, um im Notfall immer Zugriff zu haben. Wenn ein User sein zweites Passwort nicht zur Hand hat, können wir ihn temporär dieser Gruppe hinzufügen. Nach der Synchronisation mit der AD kann sich der User wieder anmelden.

**2. Administrator-Override:** Wir haben einen speziellen Administrator-Account in der AD eingerichtet, der es uns ermöglicht, uns bei Bedarf mit einem Administrator-Token bei einem Userkonto anzumelden. Jedes Mitglied unserer IT-Abteilung erhielt den Token dieses Admin-Accounts, um im Notfall einen User über diesen Weg anzumelden.

**3. Anmeldemöglichkeiten außerhalb des Firmennetzwerks:**

- **Lokaler Administrator:** Da die MFA-Richtlinie für Domänenuser der GUG-Domäne gilt, aber nicht für den lokalen Administrator, können wir uns über den lokalen Admin-Account anmelden. Dank unserer Verwaltung der lokalen Administrator-Passwörter über LAPS (Local Administrator Password Solution) haben wir stets Zugriff auf diese Passwörter.
- **Vorgecachte Passwörter (Offline Token):** Der FAWA kann zukünftige Passwörter vorspeichern, sodass sich User auch dann anmelden können, wenn keine Verbindung zum FA besteht. Diese Funktion muss aktiviert werden, und ein gemeinsamer Schlüssel, der im FA generiert wurde, muss eingegeben werden. Sobald der FAWA mit dem FA verbunden ist, lädt er die nächsten Passwörter herunter, was die Anmeldung auch offline ermöglicht.
- **Emergency Code:** Jeder User, dem ein Token zugewiesen wurde, erhält einen Emergency Code, der alle 30 Tage generiert wird. Dieser Code kann als zweites Passwort verwendet werden, um Zugang zum Rechner zu erhalten, falls der User keinen Zugriff mehr auf sein reguläres Token hat. Diese Funktion ist allerdings nur aktiv wenn der FAWA nicht in Verbindung mit dem FA steht.

Diese vielfältigen Möglichkeiten stellen sicher, dass die Einführung der MFA den Arbeitsablauf der User so wenig wie möglich beeinträchtigt und wir effektiv auf Probleme mit dem zweiten Passwort reagieren können.

# 5 Rollout auf die Mitarbeiter

## 5.1 Planung des Rollouts

Nachdem wir den FortiAuthenticator Windows Agent (FAWA) ausgiebig getestet hatten und genügend Möglichkeiten zur Verfügung standen, um den Usern bei Anmeldeproblemen zu helfen, begannen wir mit der Planung des Rollouts auf die User. Wir entschieden uns dafür, den Sicherheitsmechanismus des Windows Agents aktiviert zu lassen, um eine Testphase zu ermöglichen, in der die Mitarbeiter den Agenten testen können, aber jederzeit die Möglichkeit haben, diesen zu umgehen, falls Probleme auftreten. Solange dieser Sicherheitsmechanismus aktiviert ist, können sich die User über die Windows-Funktion „Andere Benutzer“ mit ihren normalen Anmeldedaten einloggen und somit die MFA des FAWA umgehen.

Unser Rollout-Plan sah vor, zunächst unsere gesamte IT-Abteilung mit der neuen Windows-Anmeldung vertraut zu machen, um eine erste Testphase zu durchlaufen. Anschließend planten wir, den Rollout auf jeweils eine Person aus jeder Abteilung auszuweiten. Ziel war es, alle Abteilungen einzubeziehen und sicherzustellen, dass bei auftretenden Problemen jeweils nur eine Person pro Abteilung betroffen ist. Wir erstellten eine Liste der Mitarbeiter, bei denen wir den Rollout durchführen wollten. Indem wir jeweils eine Person pro Abteilung auswählten, wollten wir sicherstellen, dass sich die Mitarbeiter auf das Kommende einstellen können und dass in jeder Abteilung jemand als Ansprechpartner zur Verfügung steht, der bereits Erfahrung mit dem neuen System hat.

Der dritte Schritt wäre dann der vollständige Rollout am gesamten Standort in Emstek, gefolgt von den weiteren Standorten nach demselben Prinzip. Wir entschieden uns gegen einen Rollout per Gruppenrichtlinie, da wir es bevorzugten, persönlich mit den einzelnen Personen zu sprechen. So konnten wir gemeinsam die neue Anmeldung durchgehen und sicherstellen, dass sich niemand überfordert fühlt.

## 5.2 Erstellen der Batch Datei

Um den Installations- und Konfigurationsprozess des FortiAuthenticator Windows Agents (FAWA) zu vereinfachen und zu standardisieren, haben wir eine Batch-Datei erstellt, die alle erforderlichen Einstellungen automatisch vornimmt. Diese Datei enthält alle wichtigen Konfigurationen, die wir am FAWA vorgenommen haben, und basiert auf den CLI-Befehlen, die wir aus den Fortinet-Dokumenten entnommen und an unsere Bedürfnisse angepasst haben. Die Batch-Datei umfasst folgende Einstellungen:

1. **Zeile 3:** Startet das Setup für den FAWA und sorgt für eine stille Installation (Silent Installation).
2. **Zeilen 4/5/6:** Beinhalten die IP-Adresse des FA und die Admin-Zugangsdaten mit dem Pre-Shared Key (PSK), um die Verbindung zum FA herzustellen.
3. **Zeilen 7/8/9:** Beinhalten Einstellung über das Zeitlimit die Anzahl der Wiederholungsversuche bei Fehlern und welche Aktion bei Fehler ausgeführt werden soll
4. **Zeile 10:** Gibt den Zeitraum in Stunden, für den Anmeldeinformationen im Cache gespeichert werden.
5. **Zeilen 11/12:** Aktivieren die Administrator-Override-Funktion und legen die Admins fest, die diese Funktion nutzen können.
6. **Zeile 13:** Fügt die Gruppe „Forti Windows Agent“ zu den ausgenommenen Gruppen (Exclude Groups) hinzu.
7. **Zeilen 14/15:** Aktivieren die Offline-Token-Funktion und geben das Passwort an, damit der FAWA die Passwörter herunterladen und vorspeichern kann. Dies ist wichtig für die Anmeldung, falls die Verbindung zum FA unterbrochen ist.
8. **Zeilen 16/17/18:** Fügen die Domäne „gug.local“ hinzu und setzen sie als Standarddomäne, sodass User die Domäne nicht jedes Mal auswählen müssen.

Durch die Verwendung dieser Batch-Datei können wir den FAWA effizient mit allen wichtigen Einstellungen installieren. Dies minimiert menschliche Fehler, wie das Vergessen einer Einstellung, und stellt sicher, dass alle FAWA-Installationen in unserem Unternehmen einheitlich konfiguriert sind.

## 5.3 Durchführung des Rollouts

Für die Durchführung des Rollouts des FortiAuthenticator Windows Agents (FAWA) entschieden wir uns für einen persönlichen Ansatz statt einer automatisierten Verteilung per Gruppenrichtlinie. Dies erforderte eine effektive Planung und Koordination. Wir verteilten die Liste der für die Testphase ausgewählten Personen unter den Teammitgliedern, um den Rollout möglichst effizient durchzuführen.

Zuvor erstellten wir eine umfassende Anwenderdokumentation. Diese sollte den Usern helfen, die verschiedenen Möglichkeiten ihrer 2FA zu verstehen und bei Problemen selbstständig Lösungen zu finden, um wieder Zugang zu ihren Computern zu erhalten. Während der Testphase ließen wir den Sicherheitsmechanismus des FAWA aktiviert, empfahlen den Usern jedoch, diesen nur im Notfall zu umgehen.

Nachdem wir die 2FA für die VPN-Verbindung und den Windows Agent bei unseren Testusern eingerichtet hatten, ließen wir die Testphase zunächst für zwei Wochen laufen. Dies sollte uns helfen, mögliche Probleme frühzeitig zu identifizieren und sicherzustellen, dass bei größeren

Problemen nur ein Teil der Belegschaft betroffen ist. Die meisten User bevorzugten die Nutzung des Handys und der mobilen App für die Anmeldung, da dies für sie der einfachste Weg war.

Während der Testphase traten nur wenige Probleme auf. Einige User hatten Schwierigkeiten mit den Push-Benachrichtigungen, insbesondere wenn sie ihr Passwort falsch eingegeben hatten und sich zu schnell erneut anmelden wollten. Zudem gab es Verwirrung darüber, warum die Push-Benachrichtigungen nicht funktionierten, wenn sich die Laptops der User im Homeoffice befanden. Abgesehen von diesen kleineren Problemen gab es keine größeren Funktionsstörungen des Systems.

Aufgrund des erfolgreichen Verlaufs der Testphase entschieden wir uns, den Rollout auf den gesamten Standort Emstek auszuweiten. Nachdem der Standort Emstek vollständig auf MFA umgestellt war, planten wir, die anderen Standorte nach demselben Prinzip umzustellen.

# 6. Projektabschluss

## 6.1 Projektübergabe

Das Projekt wurde im Rahmen eines Meetings mit allen IT-Administratoren übergeben. Dabei wurden erneut die Funktionalität und Anwendung des Systems besprochen. Zusätzlich wurden weitere Aspekte der Ausfallsicherheit erörtert, einschließlich der Maßnahmen, die im Falle eines Systemausfalls zu ergreifen sind.

## 6.2 Projektziel

Das Ziel unseres Projekts wurde weitgehend erreicht. Wir haben ein neues System implementiert, das die Multi-Faktor-Authentifizierung (MFA) unterstützt und uns ermöglicht, die verschiedenen Zugänge zu kontrollieren. Zudem ist es uns gelungen, unsere Windows-Anmeldung mit MFA zu sichern, wie ursprünglich geplant.

Allerdings hat der Rollout auf alle Standorte mehr Zeit in Anspruch genommen als erwartet. Bislang wurde nur ein Großteil des Hauptstandortes Emstek umgestellt, während die anderen Standorte noch auf den Rollout warten. Ebenso steht die vollständige Ablösung des aktuell aktiven Radius-Servers noch aus, da die externe Anmeldung bei Citrix momentan noch über diesen Server läuft.

Wir haben nicht so viele Authentifizierungsmethoden implementiert, wie ursprünglich geplant, da wir uns gegen die Verwendung der Forti Hardware Token entschieden haben. Trotzdem konnten wir die meisten der gesteckten Projektziele erfolgreich umsetzen. Die verbleibenden Aufgaben, wie der Rollout an den anderen Standorten und die Umstellung des externen Zugangs auf unsere Citrix-Umgebung, werden in naher Zukunft angegangen, um das Gesamtziel des Projekts vollständig zu erreichen.

Die Dauer der Projektphasen hat sich im Laufe des Projektes verändert. Hier eine Übersicht der Änderungen in den Projektphasen

| Phase | Geplante Zeit in Stunden | Tatsächliche Zeit | Differenz |
|---|---|---|---|
| Analyse | 6 | 7 | +1 |
| Planung | 7 | 9 | +2 |
| Implementierung | 23 | 20 | -3 |
| Abschluss | 4 | 5 | +1 |

*Tabelle 4: Projektphasen Geplant/Tatsächlich*

## 6.3 Fazit des Projektes

Das Projekt hat wertvolle Lernerfahrungen mit sich gebracht, insbesondere in Bezug auf die Einrichtung und Integration des FortiAuthenticators (FA) sowie die Konfiguration des Windows Agents. Darüber hinaus habe ich wichtige Erkenntnisse über das Projektmanagement und mögliche Fehlerquellen gewonnen.

Ein wesentlicher Fehler in meinem Ansatz war die Zeitplanung. Ich konzentrierte mich oft nur auf den nächsten Schritt, ohne die notwendigen Vorbereitungen für die folgenden Schritte zu bedenken. Ein Beispiel hierfür ist die Umstellung des externen Zugangs für unsere Citrix-Umgebung. Da wir normalerweise mit externen Dienstleistern zusammenarbeiten, die Expertise im Bereich Citrix bieten, sind wir auch für diese Umstellung auf ihre Unterstützung angewiesen. Durch unsere schrittweise Vorgehensweise haben wir die Anfrage für einen Umstellungstermin zu spät gestellt, was dazu führte, dass der Dienstleister keinen passenden Termin mehr vor der Abgabe unserer Projektdokumentation anbieten konnte.

Auch die für den Rollout eingeplante Zeit war zu knapp bemessen, was zu einer Verzögerung des gesamten Prozesses führte. Die Entscheidung, den Rollout in Testphasen zu unterteilen und den Usern die Möglichkeit zu geben, sich an das neue System zu gewöhnen, war jedoch sehr positiv. Dieser Ansatz verhinderte eine Überlastung der Mitarbeiter und potenzielles Chaos, das durch eine gleichzeitige Umstellung aller User hätte entstehen können.

Für zukünftige Projekte werde ich eine realistischere Zeitplanung anstreben und dabei Erfahrungen aus vorherigen Projekten einfließen lassen. Eine effektive Zeitplanung sollte nicht nur die theoretisch schnellstmögliche Umsetzung des Projekts berücksichtigen, sondern auch Faktoren wie Krankheit, Urlaub oder unerwartete Schwierigkeiten einplanen, um Verzögerungen zu vermeiden.

## 6.4 Ausblick

In naher Zukunft planen wir, in Zusammenarbeit mit unserem Dienstleister, den externen Zugang zu unserer Citrix-Umgebung auf den FortiAuthenticator (FA) umzustellen. Dies ermöglicht es uns, die Multi-Faktor-Authentifizierung (MFA) über ein einheitliches System zu verwalten. Zusätzlich ist der Rollout der MFA auf alle anderen Standorte vorgesehen, um unternehmensweit eine umfassende Sicherheit zu gewährleisten und alle Sicherheitslücken zu schließen. Ferner erwägen wir, weitere Authentifizierungsmethoden zu integrieren, um den Usern noch mehr Komfort zu bieten und die IT-Sicherheit zu stärken, ohne dass die User sich dadurch beeinträchtigt fühlen.

## A.1 Abkürzungsverzeichnis

| | |
|---|---|
| AD | Active Directory |
| API | Application Programming Interface |
| App | Applikation |
| CPU | Central Processing Unit |
| E-Mail | Electronic Mail |
| ESX | Elastic Sky X |
| EWE | Energieversorgung Weser-Ems |
| FA | Fortiauthenticator |
| FAWA | Fortiauthenticator Windows Agent |
| FTM | FortiToken Mobile |
| GmbH | Gesellschaft mit beschränkter Haftung |
| HTTPS | Hypertext Transfer Protocol Secure |
| IHK | Industrie- und Handelskammer |
| IP-Adresse | Internet Protocol Adresse |
| IT | Informationstechnologie |
| KG | Kommanditgesellschaft |
| LAPS | Local Administrator Password Solution |
| LDAP | Lightweight Directory Access Protocol |
| MFA | Multi-Faktor-Authentifizierung |
| MPLS | Multi-Protocol Label Switching |
| OTP | One-Time Password |
| OVF | Open Virtualization Format |
| PSK | Pre-Shared Key |
| QR Code | Quick Response Code |
| RADIUS | Remote Authentication Dial-In User Service |
| SMS | Short Message Service |
| SMTP | Simple Mail Transfer Protocol |
| USB | Universal Serial Bus |
| VM | Virtuelle Maschine |
| VMDK | Virtual Machine Disk |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| 2FA | Zweifaktorauthentifizierung |

## A.2 Quellenverzeichnis:

[1]https://www.softwareexpress.de/hersteller/watchguard/authpoint/#:~:text=%2A%20Preisstaffel%20251,Brutto%3A%2045%2C84%20%E2%82%AC%0A%0ANetto%3A%2038%2C52%20%E2%82%AC [Zugriff am 28.11.2023

[2]https://www.protectimus.com/de/pricing/#:~:text=,Kostenlos%0A%0A%240%2000%20im%20Monat[Zugriff [Zugriff am 28.11.2023]

[3]https://docs.fortinet.com/product/fortiauthenticator/6.5 [Zugriff am 03.12.2023]

[4]https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-FortiToken-Push-on-FortiAuthenticator-operation/ta-p/190810 [Zugriff am 01.12.2023]

[5]https://www.ihk.de/oldenburg/ [Zugriff am 05.12.2023]

[6]https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/759080/configuring-a-radius-server [Zugriff am 03.12.2023]

[7]https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9283bc66-f6d2-11eb-8f3f-00505692583a/FortiAuthenticator_Agent_for_Microsoft_Windows-3.8-Install_Guide.pdf [Zugriff 29.11.2023]

## A.3 Abbildungsverzeichnis

### A.3.1 Phasen des Projektes

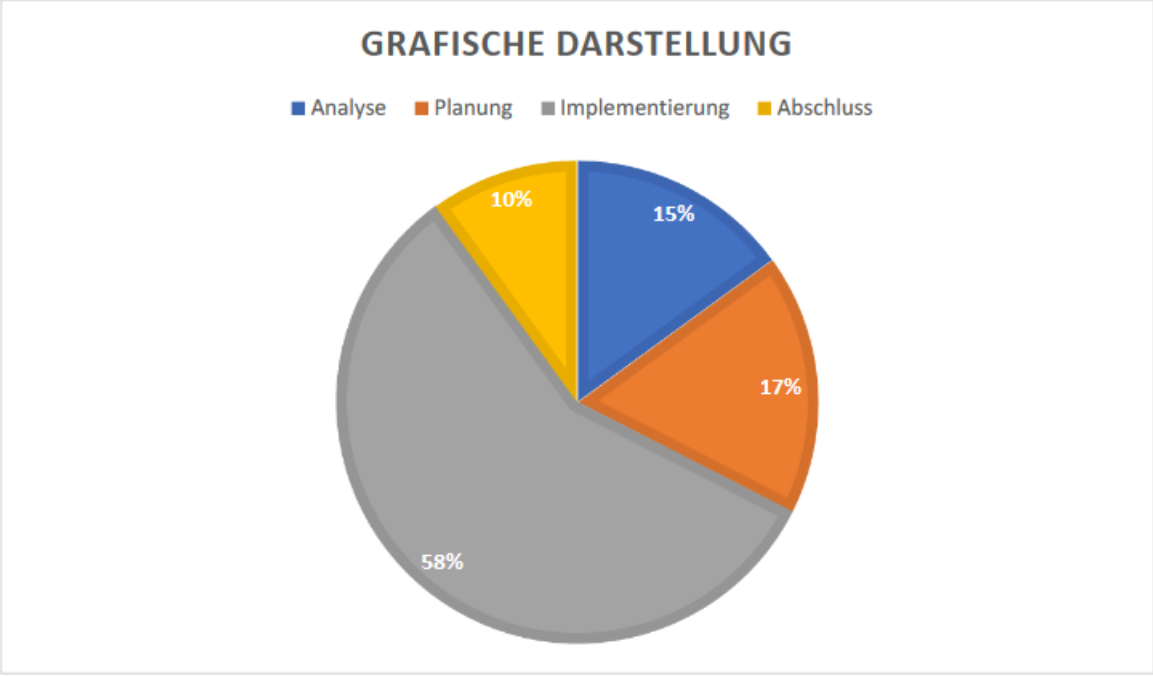



*Abbildung 3.1.1: Projektphasen*

## A.3.2 Übersicht der Zugriffe

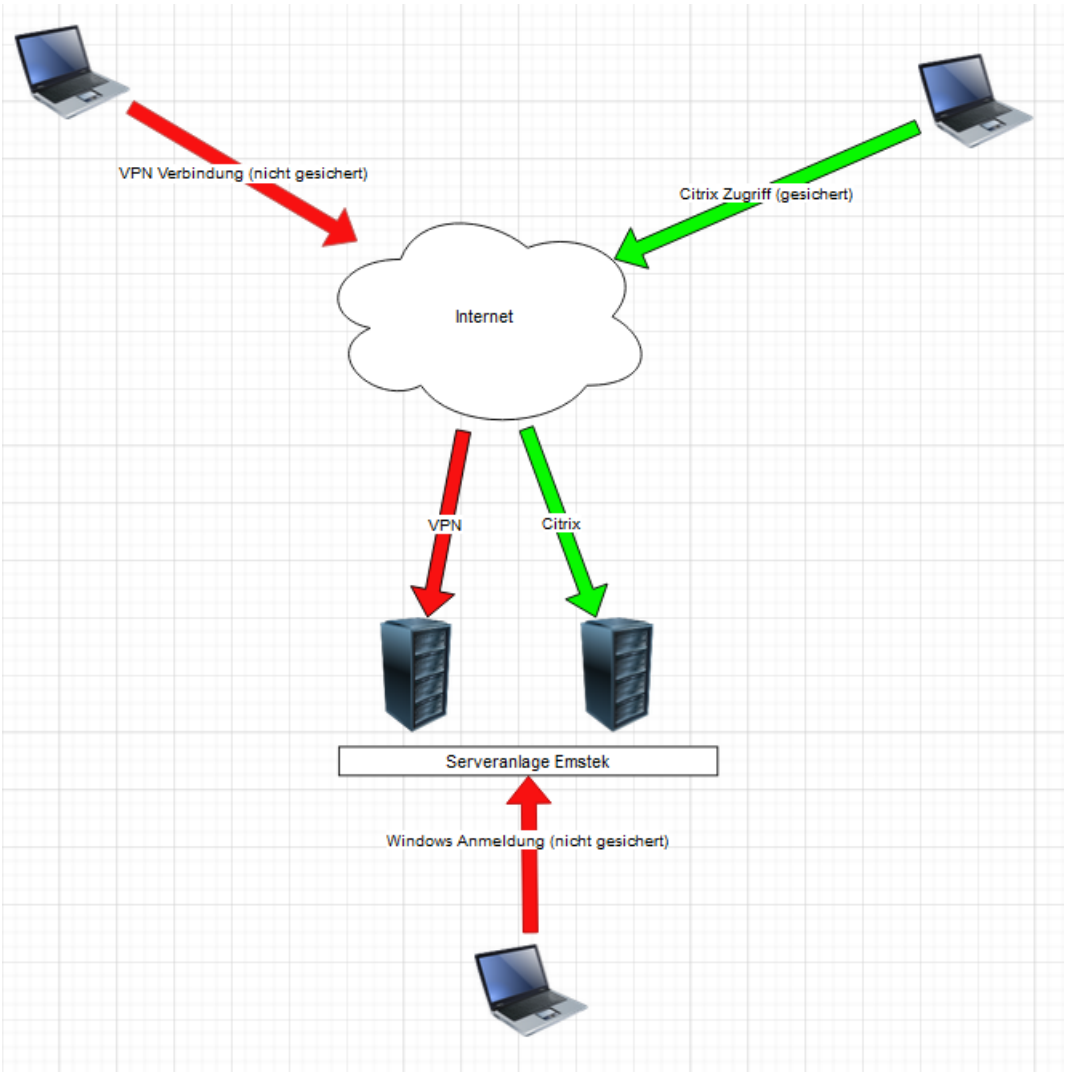



*Abbildung 3.2.1 Übersicht der Zugriffe*

## A.3.3 Nutzwertanalyse

| Kriterien | Gewichtung | Fortinet | | Watchguard | | Protectismus | |
|---|---|---|---|---|---|---|---|
| | | Bewertung (ungewichtet) | Bewertung (gewichtet) | Bewertung (ungewichtet) | Bewertung (gewichtet) | Bewertung (ungewichtet) | Bewertung(gewichtet) |
| Preis | 0,15 / 15 % | 5 | 0,75 | 3 | 0,45 | 4 | 0,6 |
| Zentrale Oberfläche | 0,15/ 15% | 4 | 0,6 | 5 | 0,75 | 4 | 0,6 |
| Zuverlässigkeit | 0,3/ 30 % | 5 | 1,5 | 5 | 1,5 | 5 | 1,5 |
| Implementierung | 0,15/ 15 % | 4 | 0,6 | 3 | 0,45 | 3 | 0,45 |
| Kompatibilität | 0,25/ 25 % | 4 | 1,0 | 3 | 0,75 | 3 | 0,75 |
| SUMME | | | 4,45 | | 3,9 | | 3,9 |

Bewertungen von 5 Sehr gut bis 1 nicht gut

*Abbildung 3.3.1 Nutzwertanalyse*

Preisvergleich der 3 Anbieter

Fortinet:

Fortiauthenticator mit 300 Usern 250 Lizenzen kosten **9.683,14€**

Protectimus:

2€ pro Nutzer pro Monat, also 24€ pro Jahr pro User

300 User * 24€ = 7200€ pro Jahr

Für 3 Jahre: 7200€ * 3 = **21600€**

WatchGuard:

38,52 € pro Jahr pro Nutzer

300 User * 38,52€ = 11.556 Euro pro Jahr

Für 3 Jahre: 11.556€ * 3 = **34.668€**

*Abbildung 3.3.2 Preisvergleich der 3 Anbieter*

*Abbildung 3.3.3 Angebot von Fortinet*

## A.3.4 Konfigurieren des Fortiauthenticators

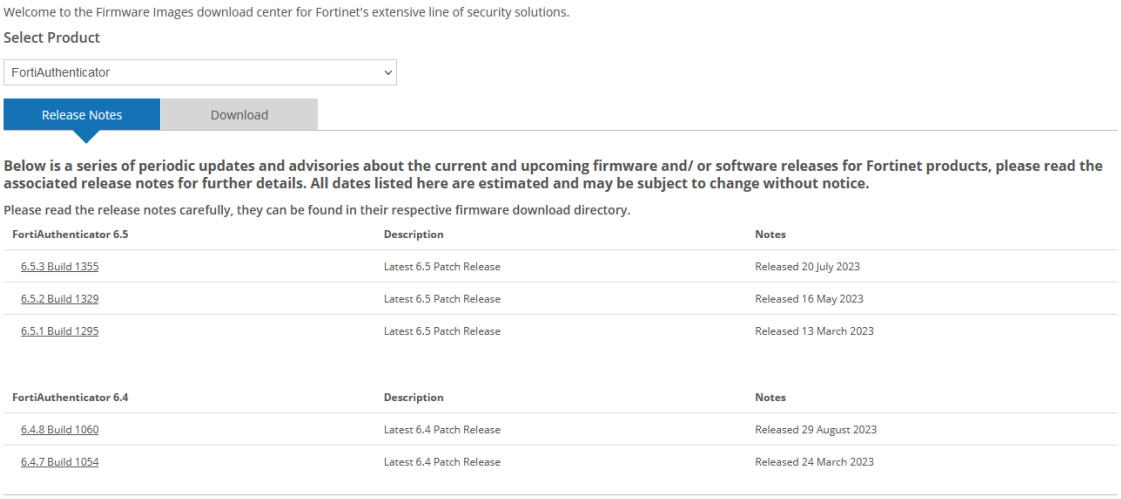



*Abbildung 3.4.1 Herunterladen der Installtionsdatein*

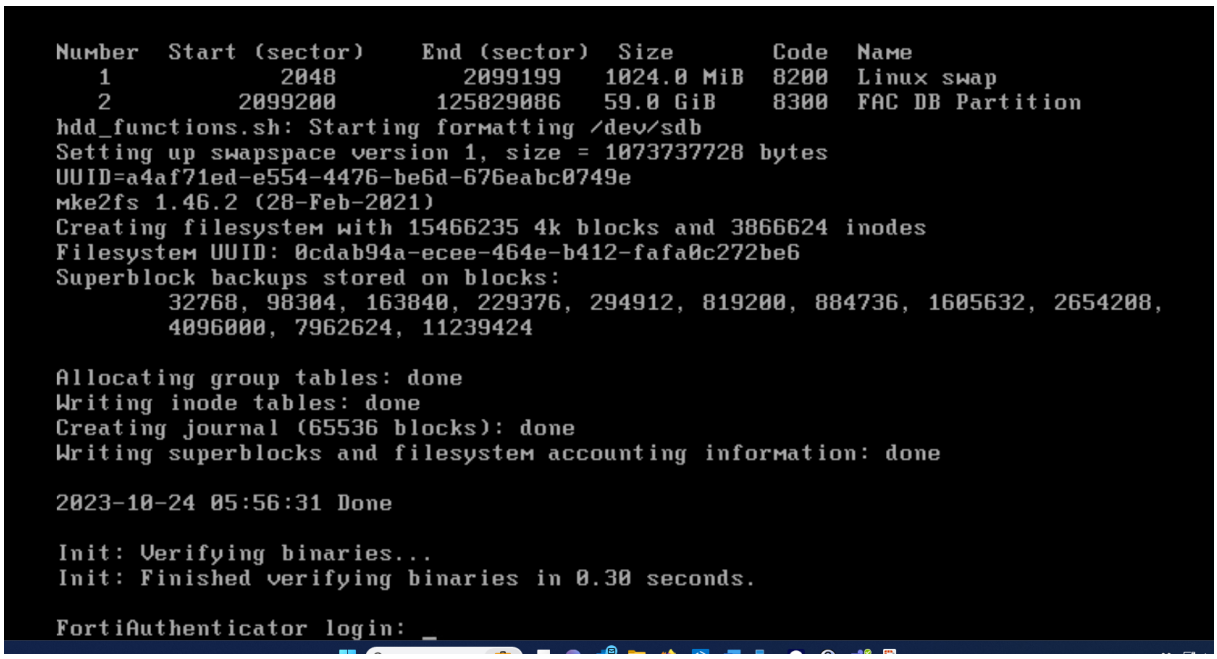



*Abbildung 3.4.2 Erste Konfiguration per Kommandozeile*

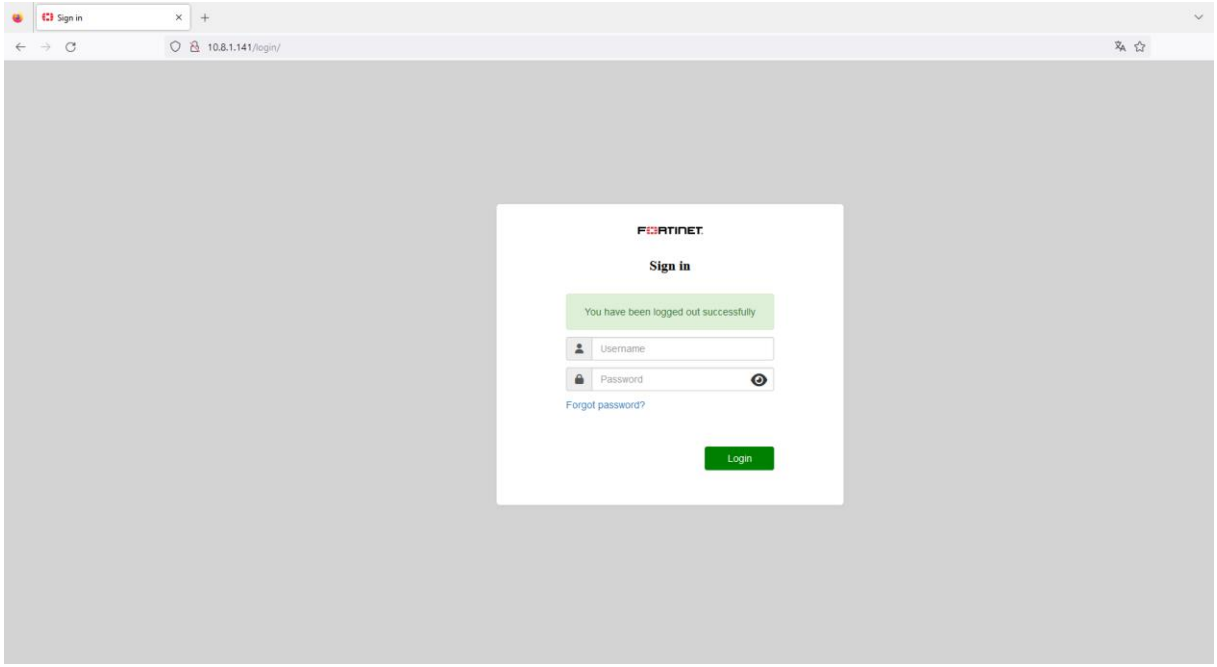



*Abbildung 3.4.3 Zugang zum Fortiauthenticator per Webzugriff*

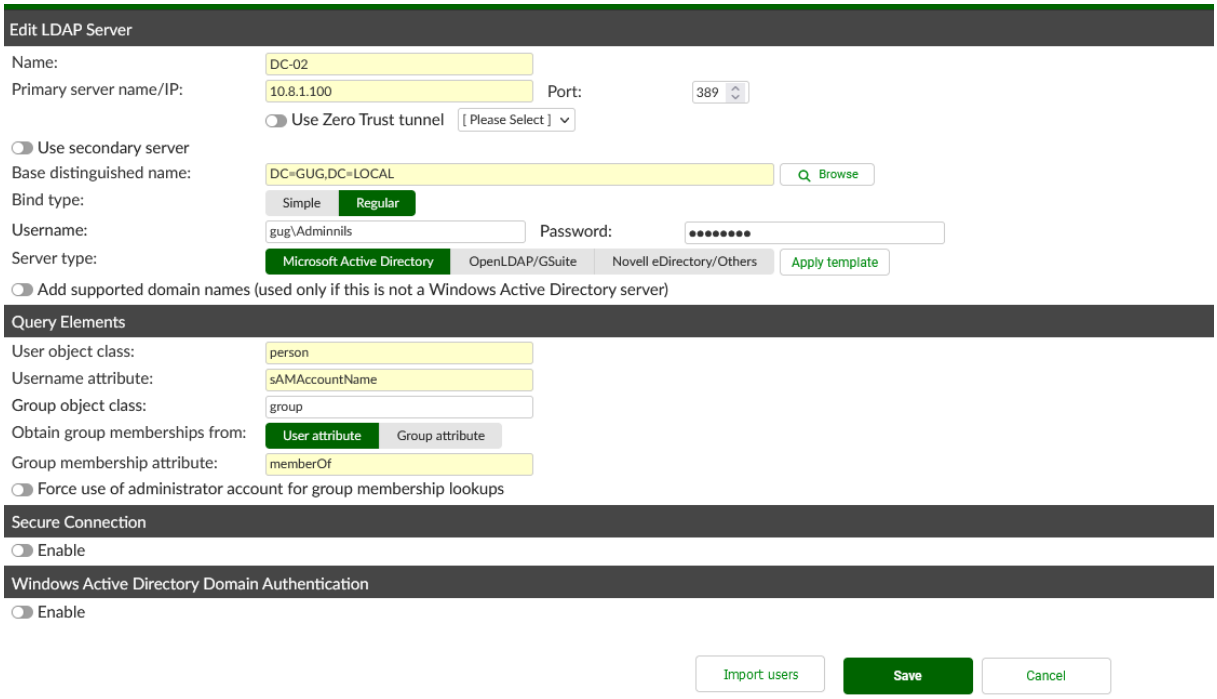



*Abbildung 3.4.4 Einrichten der Verbindung zum Domain Controller*

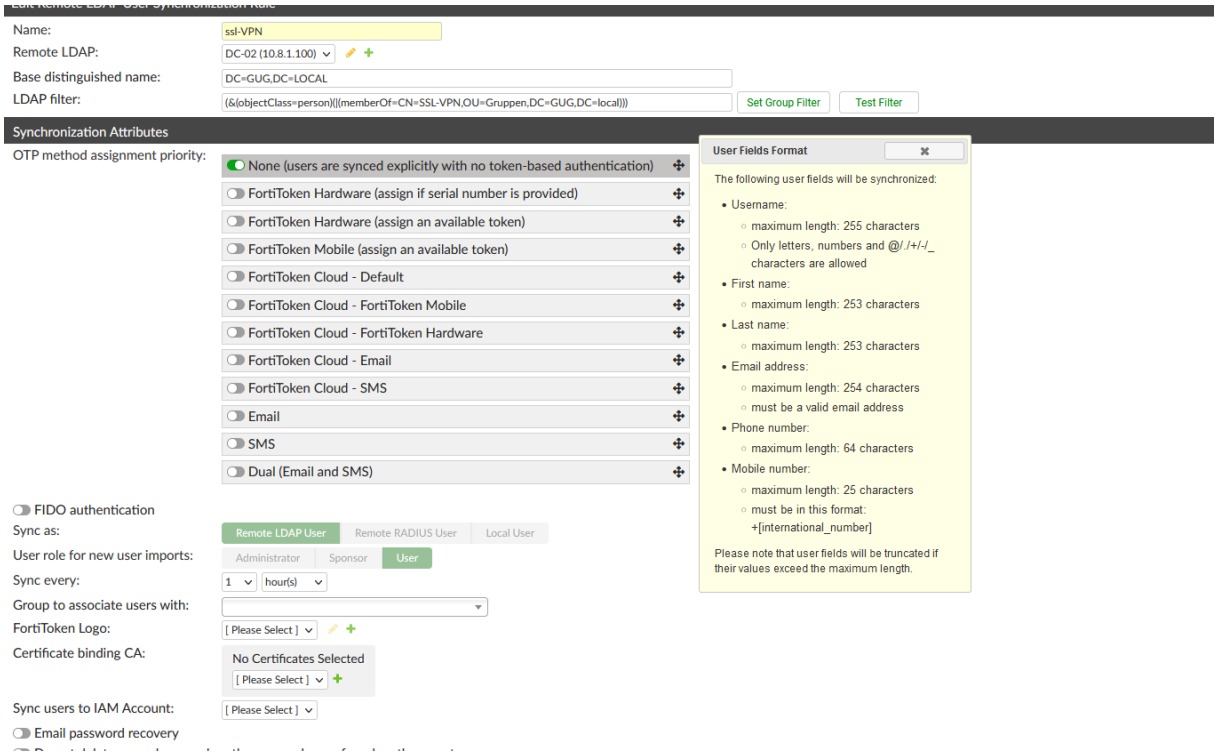



*Abbildung 3.4.5 Einrichten der Synchronisationsregel*

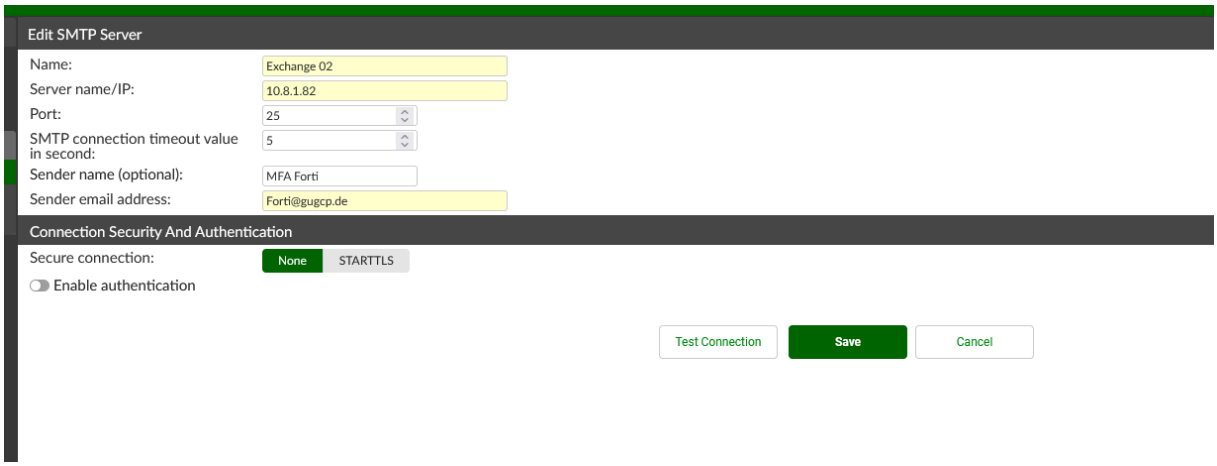



*Abbildung 3.4.6 Einrichtung des Exchange Servers*


*Abbildung 3.4.7 Fortigate Firewall als Radius Client anlegen*

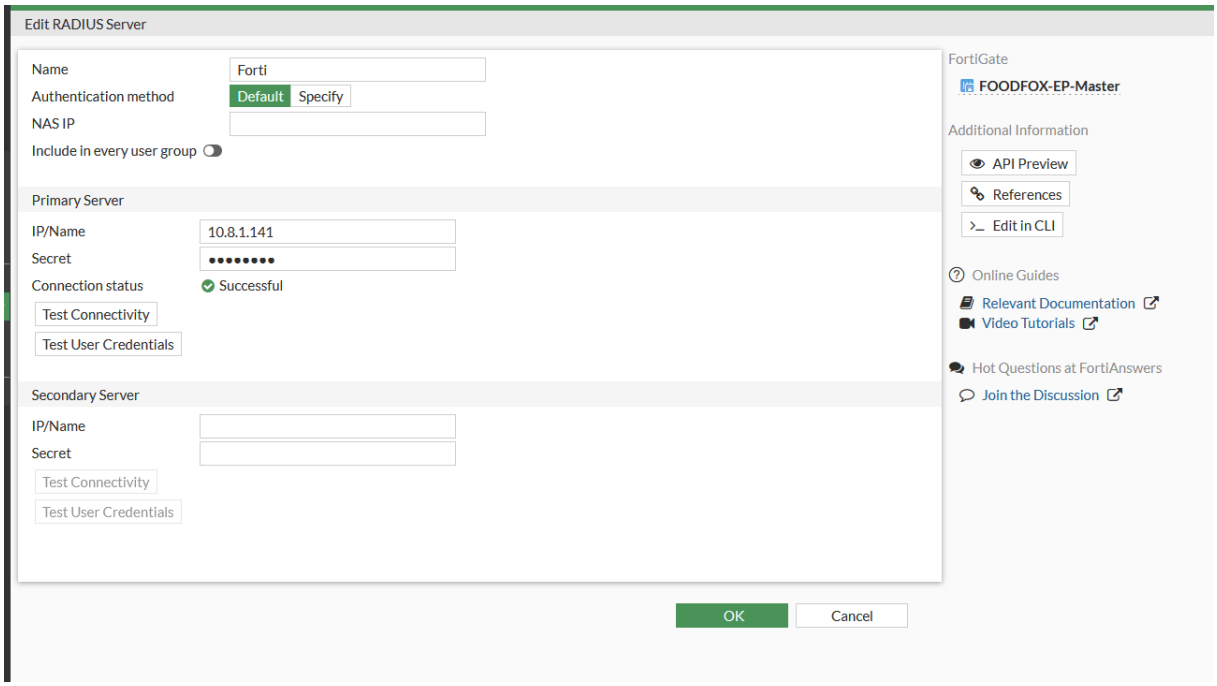



*Abbildung 3.4.8 Fortiauthenticator als Radius Server auf der Firewall anlegen*

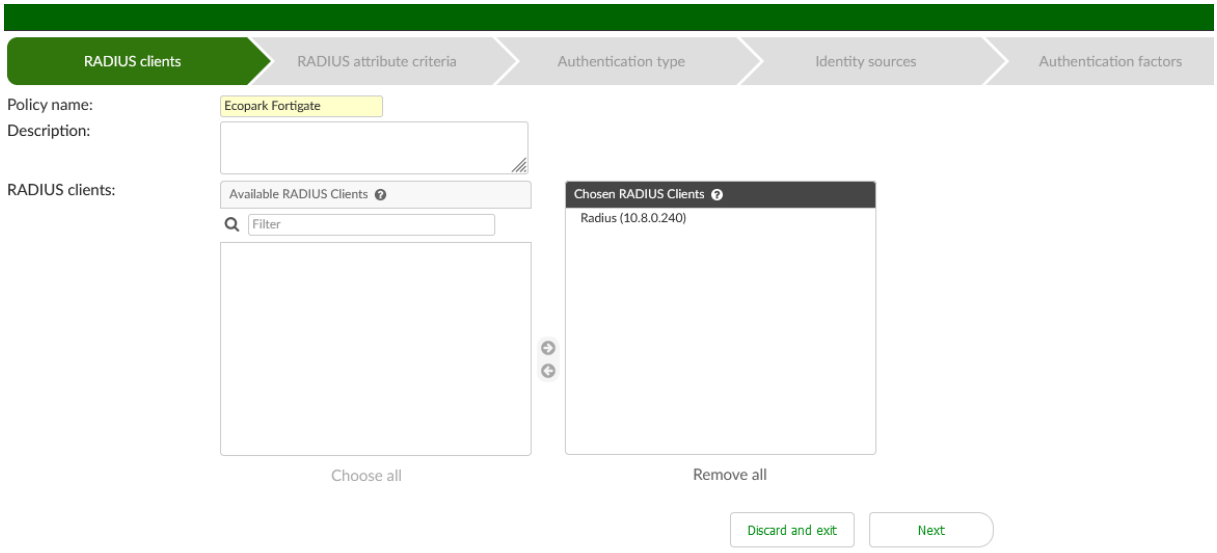



*Abbildung 3.4.9 Einrichtung einer Radius Server Policy auf dem Fortiauthenticator*

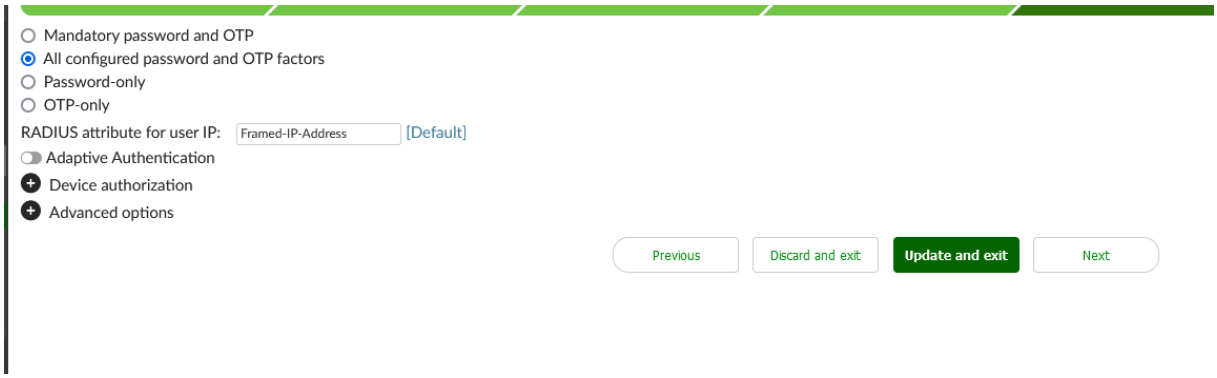



*Abbildung 3.4.10 Einrichtung einer Radius Server Policy auf dem Fortiauthenticator*

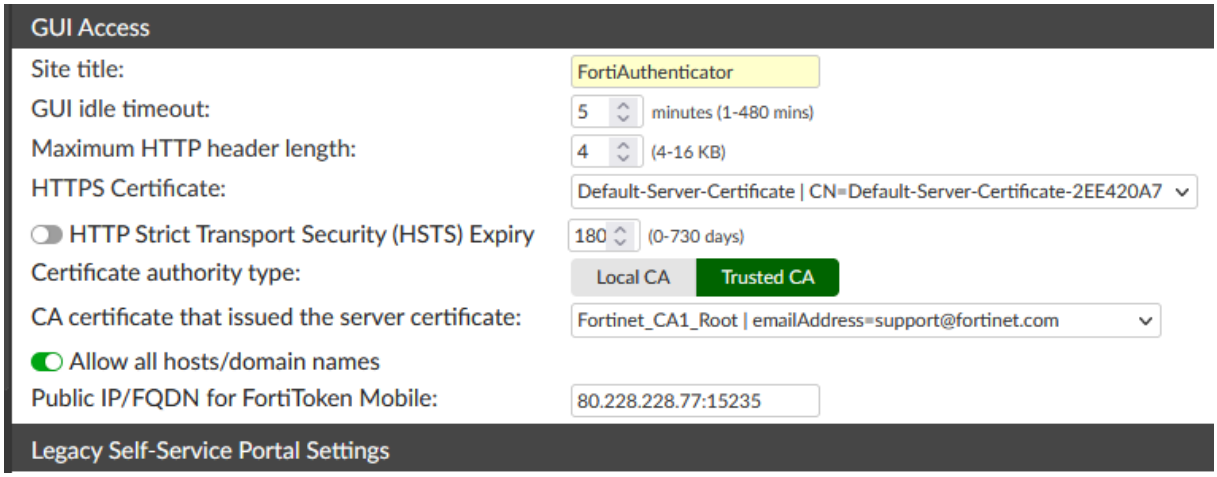



*Abbildung 3.4.11 Festlegung des Ports und der IP-Adresse für die Push Benachrichtigungen*

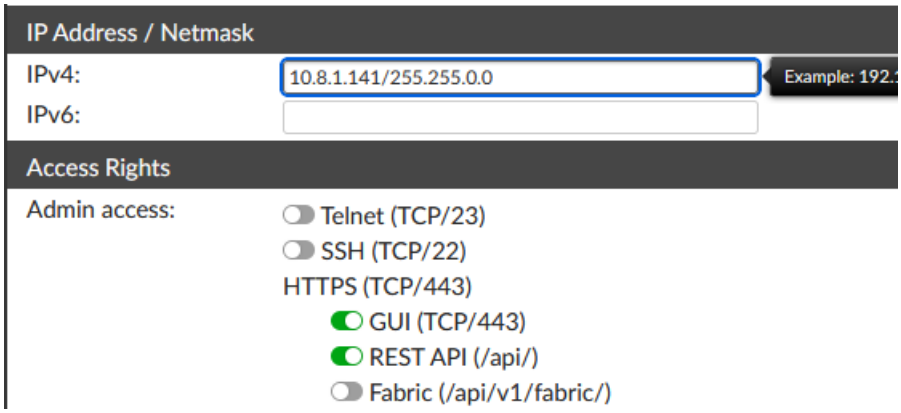



*Abbildung 3.4.12 Freischalten der API beim Fortiauthenticator*

## A.3.5 Einrichtung des FAWA

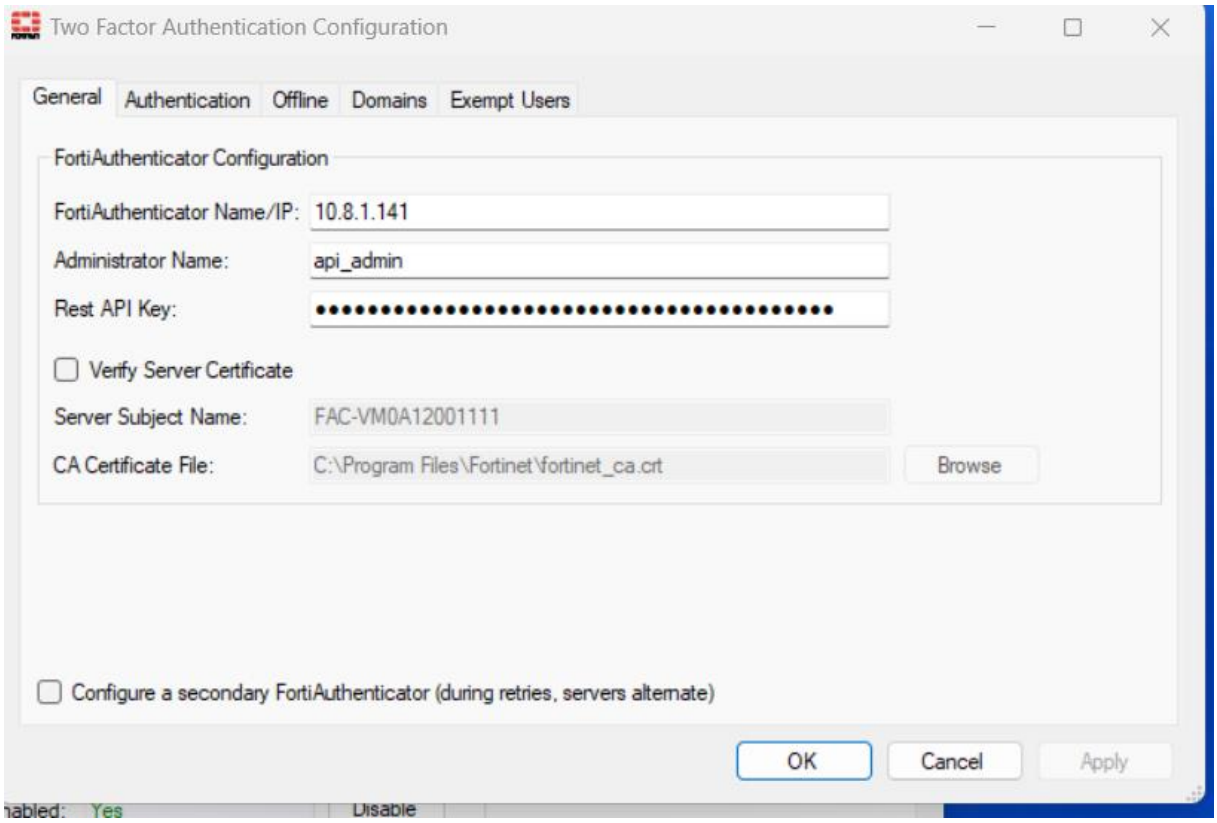



*Abbildung 3.5.1 Verbinden des FAWA mit dem FA*

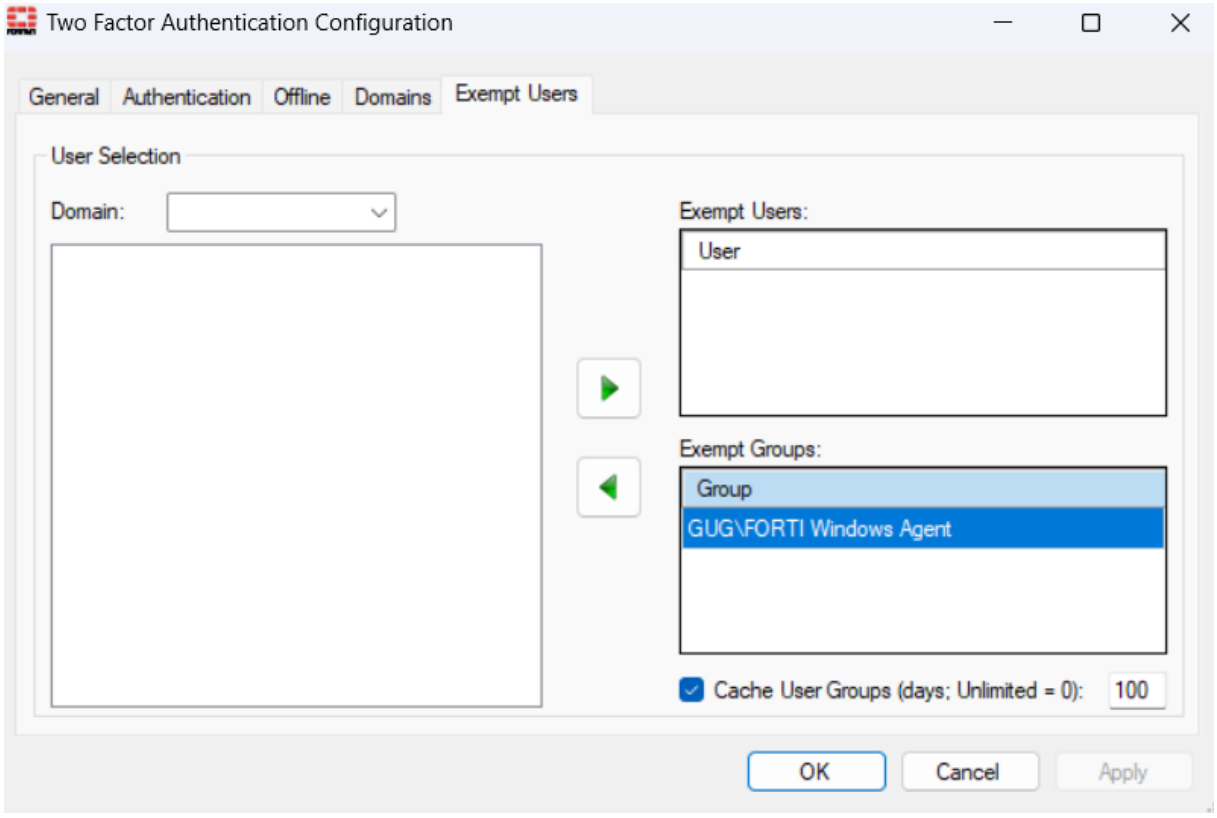



*Abbildung 3.5.2 Festlegen der „Exempted Groups“*

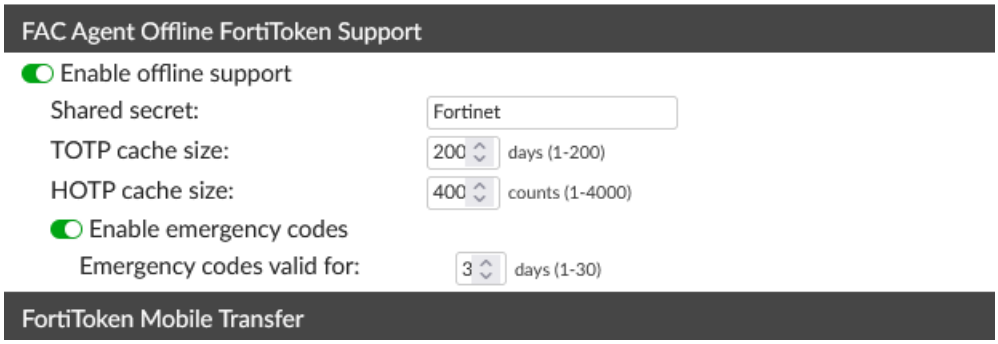



*Abbildung 3.5.3 Aktivierung der Offline FortiToken*

neu 1.txt | neu 1 | neu 2 | Fortiinstall.bat | Fortiinstall.bat

```
1   @echo off
2   REM FortiAuthenticator Agent Installation
3   FAC_Agent_Setup_v5.0.exe /VERYSILENT ^
4       /FACHOST=10.8.1.141^
5       /FACRESTADMIN=api_admin ^
6       /FACRESTKEY=l5HEEyDslMjDdBV019AhK65oEYYMxBtGsx8p6yMp ^
7       /AUTHNUMRETRIES=2 ^
8       /AUTHTIMEOUT=3 ^
9       /AUTHFAILACTION=1 ^
10      /AUTHCACHECREDPERIOD=23 ^
11      /AUTHALLOWADMINOTP ^
12      /AUTHADMINOVERRIDENAMES="Adminnils,AdminForti" ^
13      /EXCLUDEDGROUPS="GUG\FORTI Windows Agent" ^
14      /OFFLINEENABLED ^
15      /OFFLINESHAREDSECRET=Fortinet ^
16      /INCLUDEDDOMAINS="gug.local" ^
17      /DEFAULTDOMAINMODE=2 ^
18      /DEFAULTDOMAIN=GUG
19
20
21
22
23
24  echo Installation abgeschlossen.
25  pause
```

*Abbildung 3.5.4 FAWA Installtions Batch Datei*

A.3.6 Anwenderdokumentation

# Anwenderdokumentation für die Zweifaktorauthentifizierung.

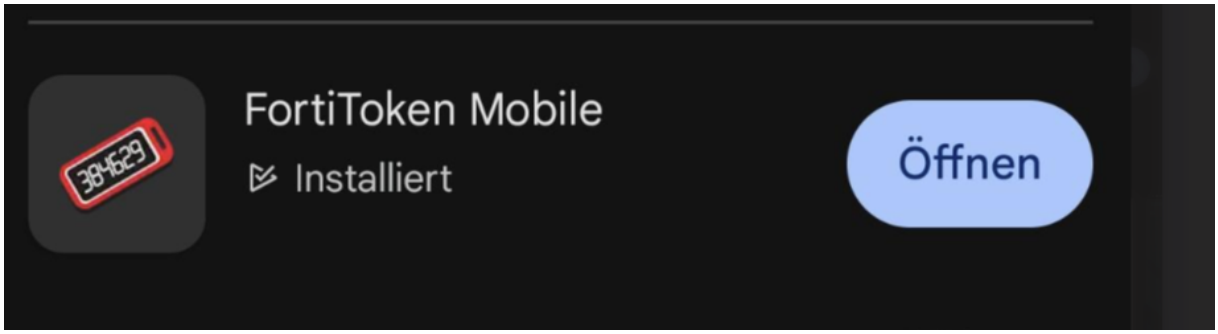
# Amoutec IT Solutions GmbH

# Einleitung:

Wir wollen die Anmeldungen an unser System vereinheitlichen und durch eine Zweifaktor-Authentifizierung absichern. Dies wird die Sicherheit unseres Systems erhöhen.

### 1.1 Einrichtung der FortiToken Mobile App

Zuerst müsst ihr euch die FortiToken Mobile App auf einem Handy installieren.




Danach müsst ihr die App öffnen und den von uns gescannten Barcode zur App hinzufügen

### 1.2 Wann findet die Zweifaktor-Authentifizierung statt?

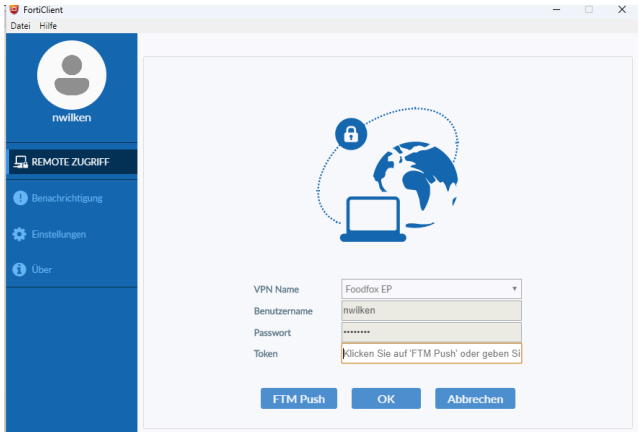
Wenn ihr eine VPN-Verbindung zu unserem System aufbaut.

Wenn ihr euch bei Windows anmeldet.

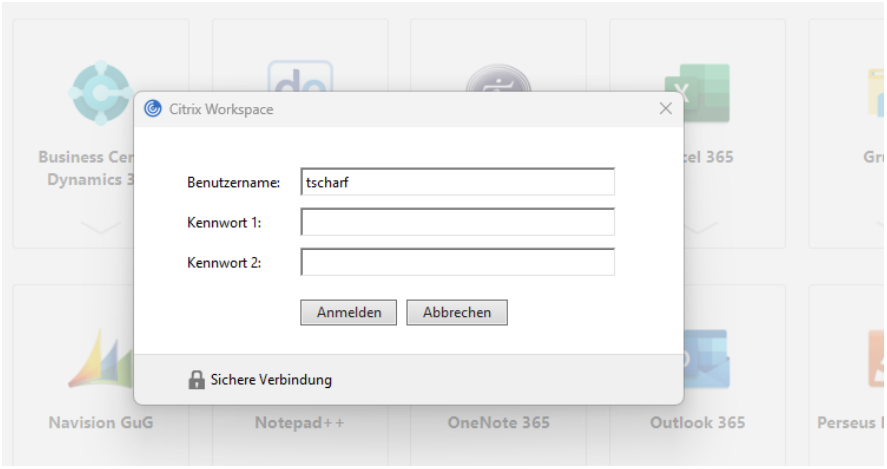
Wenn ihr euch von extern bei Citrix anmeldet.

### 1.3 VPN und Citrix

Bei der Anmeldung von Citrix oder per VPN müsst ihr einfach eure Windows-Anmeldedaten eingeben und in das zweite Feld euer Token-Passwort eingeben oder wenn ihr die App benutzt die Push Benachrichtigungen bestätigen.



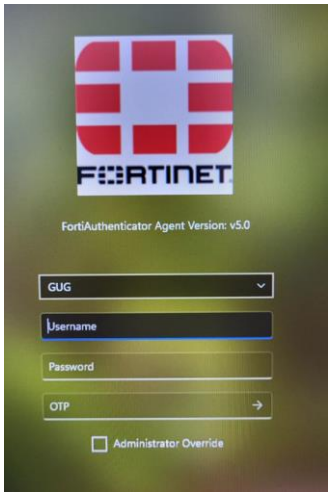

So sieht dann eure Anmeldemaske bei einer VPN-Verbindung aus.




Und so sieht eure Maske dann bei Citrix aus

### 1.4 Windows Anmeldung

So wird eure Anmeldung bei Windows dann aussehen:




Bei der Windowsanmeldung müsst ihr ebenfalls eure Windowsanmeldedaten eingeben und das zweite Passwort oder die Push-Benachrichtigung.

Sollte sich der Rechner nicht mehr im Firmennetzwerk befinden müsst ihr immer eine Windows-Anmeldedaten und das zweite Passwort eingeben. **Außerhalb des Firmennetzwerkes funktionieren die Push-Benachrichtigungen nicht.**

Solltet ihr euch nicht mehr anmelden können, meldet euch bei uns. Wir werden euch dann einen Emergency Code generieren, den ihr anstelle eures Tokens verwenden könnt. Bei weiteren Fragen könnt ihr euch gerne bei mir melden.

### A.3.7 Betriebsdokumentation

Die Seiten 7 bis 13 der Projektdokumentation sowie die Seiten iv bis xi des Anhanges gehören zur Betriebsdokumentation.