Projektdokumentation

Anbindung des Standorts Vakuumhalle an die IT-Infrastruktur der
Hugo Vogelsang Maschinenbau GmbH

ENGINEERED TO WORK

Name	Bernd Abeln[redacted]
Geburtsdatum / -ort	[redacted]
Ausbildungsberuf	Fachinformatiker für Systemintegration
Ausbildungsbetrieb	Hugo Vogelsang Maschinenbau GmbH Essen (Oldenburg)
Ausbilder	[redacted]
Prüfung	Sommer 2015
Azubi-Ident-Nr	[redacted]

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Projektdefinition

1.1. Projektumfeld/Ausbildungsbetrieb

Die Hugo Vogelsang Maschinenbau GmbH, 1929 von Hugo Vogelsang gegründet, entwickelt innovative Produkte zur Ver- und Entsorgung im Bereich der Landwirtschaft und Industrie. Das Kernprodukt ist dabei die Drehkolbenpumpe. Durch konsequente Weiterentwicklung und Erschließung neuer Marktsegmente wächst das Produktportfolio stetig. Die Vakuumtechnik für den Abwasser- und Hygienebereich bewährt sich immer mehr als umweltfreundliche und kostensparende Alternative für den Einsatz auf Schiffen, Fahrzeugen und Gebäuden. Basierend auf der bewährten Drehkolbenpumpe hat die Hugo Vogelsang Maschinenbau GmbH eine kompakte, zuverlässige und wirtschaftliche Vakuum-Entsorgungstechnik entwickelt.

Zum 1. April hat die Abteilung Vakuumtechnik ihre Arbeit in der neuen Produktionshalle aufgenommen. Die 1.000m² große Halle, welche 500m Luftlinie (siehe Abbildung 1) vom Hauptstandort Holthöge entfernt liegt, bietet mehr Lagerplatz und flexiblere Montagemöglichkeiten, wodurch die Produktion größerer Anlagenteile nun möglich ist. Zudem machen großzügige Büro- und Aufenthaltsräume die Arbeit für die 15 Mitarbeiter der Vakuumabteilung noch angenehmer. In den Büroräumen befinden sich drei Arbeitsplätze, welche je mit einem PC ausgestattet sind. Eine Netzwerkanbindung zum Hauptstandort ist nicht vorhanden.

Abbildung 1: Anzeige beider Standorte (Google Maps)

1.2. Projektziel

Der Standort Vakuumhalle soll in das Netzwerk des Hauptstandortes integriert werden. Die Kommunikation zwischen den Standorten soll über einen zu konfigurierenden VPN-Tunnel realisiert werden. Im derzeitigen Hauptstandort wird die VoIP-Telefonanlage „Swyx“ eingesetzt. Diese soll ebenfalls am Standort Vakuumhalle genutzt werden. In der

Vakuumhalle soll darüber hinaus ein DECT-Netz ausgestrahlt werden, damit die Mitarbeiter vor Ort mit schnurlosen Telefonen in jedem Bereich der Halle telefonieren können.

Wenn sich ein Mitarbeiter des Hauptstandorts heute in der Vakuumhalle aufhält, ist dieser nicht unter seiner Firmenrufnummer zu erreichen. Ebenfalls ist ein Mitarbeiter der Vakuumhalle nicht unter seiner Rufnummer zu erreichen, wenn er sich am Hauptstandort aufhält.

Die Erreichbarkeit am Standort Vakuumhalle ist aufgrund dieser Gegebenheit verbesserungsbedürftig. Im Zuge dieser Anbindung wird das ERP-System, welches von der Hugo Vogelsang Maschinenbau GmbH eingesetzt wird, für die Mitarbeiter in der Vakuumhalle ausgerollt.

2. Projektplanung

2.1. IST-Analyse

Der Standort Vakuumhalle besteht aus einer Produktionshalle der Hugo Vogelsang Maschinenbau GmbH. In dieser Halle befinden sich zwei Teamleiter-Büros. Der Standort ist bezüglich Netzwerk und Telefonie vom Hauptstandort isoliert. Vor Ort befindet sich eine strukturierte Netzwerkverkabelung mit drei Windows-Clients, einem Multifunktionskopierer und einem Switch [redacted]. Eine „AVM FRITZ!Box 7390“ dient als Router und Telefonanlage. Der ADSL-Anschluss hat eine Geschwindigkeit von 6.000kbit/s.

Die „FRITZ!Box“ strahlt in der Halle ein DECT-Netz aus, mit dem drei schnurlose Telefone (Aastra DT390) verbunden sind.

Die Mitarbeiter der Vakuumhalle haben im Moment keine Möglichkeit auf die Anwendungen des Unternehmens zuzugreifen, da keine direkte Netzwerkverbindung bzw. VPN-Verbindung zum Hauptstandort besteht. Der Datenaustausch wird über externe Datenträger realisiert, wodurch die Informationen am nächsten Tag per Hand in die Warenwirtschaft eingetragen werden müssen. Dies ist eine sehr zeitintensive und fehleranfällige Arbeit.

2.2. Soll-Konzept

Ziel des Projektes ist die Integration des Standortes Vakuumhalle in die Telefonanlage, um damit die Erreichbarkeit der Mitarbeiter zu verbessern. Darüber hinaus ist eine Integration in die bestehende Netzwerkinfrastruktur notwendig, um später den Mitarbeitern die benötigten Anwendungen über „Citrix XenApp“ zur Verfügung zu stellen.

Die Kommunikation zwischen den Standorten soll über einen VPN-Tunnel realisiert werden. Am Standort Vakuumhalle wird eine Firewall konfiguriert und eingesetzt, womit eine Standort-zu-Standort-VPN-Verbindung aufgebaut werden kann. Auf den vorhandenen Clients wird die Software „Citrix Receiver“ installiert und konfiguriert, wodurch die Mitarbeiter auf die XenApp-Anwendungen des Unternehmens zugreifen können. Die zur Telefonanlage zugehörige Software „SwyxIt!“ ist eine dieser Anwendungen. Zahlreiche Leistungsmerkmale der Software wie Konferenz, Präsenzinformation und Desktop-Sharing ermöglichen anschließend eine zielgerichtete und effiziente Zusammenarbeit der Mitarbeiter und eine Steigerung der Produktivität.

Mit Hilfe von zwei Basisstationen soll ein DECT-Netz ausgestrahlt werden, welches im ganzen Gebäude eine Verbindung für die schnurlosen Telefone bietet. Das DECT-Netz vom Standort Vakuumhalle soll identisch mit dem DECT-Netz am Hauptstandort sein. Dies hat den Vorteil, dass die Schnurlostelefone an beiden Standorten funktionstüchtig sind. Um dies

zu ermöglichen, müssen die Basisstationen am Standort Vakuumhalle über den zu konfigurierenden VPN-Tunnel mit den Basisstationen am Hauptstandort kommunizieren. Externe Gespräche für die Vakuumhalle werden ebenfalls über die VPN-Verbindung zugestellt. Dadurch können die Mitarbeiter der Vakuumhalle eine Nebenstellennummer aus dem gleichen Nummernbereich wie die Mitarbeiter des Hauptstandorts erhalten.

2.3. Projektphasen

Die folgende Tabelle zeigt eine grobe Zeitplanung für die einzelnen Phasen des Projektes. Eine detaillierte Auswertung der Zeitplanung und dessen Bewertung befindet sich im Abschlussbereich der Projektdokumentation.

Projektphase	**Geplante Zeit** (in h)
Vorbereitung	3,0
Planung	7,0
Realisierung	10,0
Testphase	6,0
Abnahme des Projektes	3,0
Erstellung der Dokumentation	6,0
Gesamt	**35,0**

Tabelle 1: Zeitplanung Projektphasen SOLL

2.4. Recherche und Informationsbeschaffung

Im Rahmen des Projektes war es wichtig zu verstehen, wie eine VPN-Verbindung aufgebaut wird und was dabei beachtet werden muss. Informationen und das benötigte Know-how konnten durch externe Dienstleister, welche bei Rückfragen zur Seite standen, und die im Literatur- und Quellenverzeichnis aufgeführten Webseiten gesammelt werden.

Des Weiteren war es wichtig zu verstehen, wie die Telefonanlage Swyx funktioniert. Dazu gehört zum Beispiel die Konfiguration der Basisstationen und auch die Kommunikation der Stationen untereinander zu verstehen. Die benötigten Informationen konnten ebenfalls von externen Dienstleistern und aus Handbüchern der Produkte gesammelt werden.

2.5. Produktevaluierung

Zum Aufbau der Standort-zu-Standort-VPN-Verbindung wird eine Firewall eingesetzt. Es wurden einige Produkte verglichen. Zum Schluss sind zwei Produkte in Frage gekommen, welche in einer Entscheidungsmatrix miteinander verglichen wurden.

Produkt		[redacted]		[redacted]	
Kriterium	Gewichtung (1-3)	Leistungspunkte (1-10)	Erreichte Punkte	Leistungspunkte (1-10)	Erreichte Punkte
VPN-Durchsatz	2	7	14	6	12
Schnittstellen/ Anschlüsse	2	8	16	8	16
Erweiterbarkeit	1	7	7	1	1
Anzahl IPsec VPN-Tunnel	3	6	18	4	12
Anschaffungs-kosten	2	6	12	6	12
Gesamt			**67**		**53**

Tabelle 2: Produktevaluierung Firewall

Aus der Entscheidungsmatrix geht hervor, dass das Produkt [redacted]-Firewall für diese Situation und dieses Umfeld besser geeignet ist. Ein großer Vorteil der [redacted] Firewall gegenüber der [redacted] ist die Erweiterbarkeit. Es gibt zusätzliche Einschübe für weitere Module, wodurch ein Modem direkt in die [redacted]-Firewall integriert werden kann. So wird kein zusätzlicher Router benötigt wird. Zudem wird am Hauptstandort ebenfalls eine Firewall der [redacted]-Serie eingesetzt, sodass sichergestellt ist, dass diese beiden Firewalls einwandfrei miteinander kommunizieren können. Weitere technische Leistungsdaten sind in den Datenblättern der Firewalls im Anhang zu finden.

2.6. Kosten-Nutzen-Analyse

2.6.1. Kosten

Zur Realisierung des Projektes sind einige Kosten zu betrachten. Zum einen werden die Personalkosten berechnet, welche sich aus dem gegebenen durchschnittlichen Stundensatz und der Projektzeit ergeben.

- Durchschnittlicher Stundensatz Personal: [redacted] EUR/Std.

Die Hardwarekosten setzen sich aus der Firewall [redacted], dem benötigten Modul [redacted] und die beiden Basisstationen [redacted] der Telefonanlage zusammen.

- [redacted]
- [redacted]
- [redacted]

Zusätzlich fallen einige Kosten für Lizenzierungen an. Zum einen setzen sich die Lizenzkosten für die Citrix-Nutzung aus den Kosten für XenDesktop als auch für Remotedesktoplizenzen für den Terminalserver zusammen. Außerdem werden noch Windows Server CALs (User CALs) benötigt.

- 3x Citrix XenDesktop-Enterprise Lizenz [redacted] EUR
- 3x RDS (TSCAL) [redacted] EUR
- 3x Windows Server CAL (User CAL) [redacted] EUR

Für die Telefonanlage „Swyx“ müssen ebenfalls Lizenzen beschafft werden. Neben den Userlizenzen für „SwyxWare“ zur Benutzerverwaltung werden auch Lizenzen für die „SwyxProfessional“-Optionen benötigt. Da die Mitarbeiter am Standort Vakuumhalle nur schnurlose Telefone benutzen, werden nochmal zusätzlich drei „CTI+“-Lizenzen fällig.

- 3x SwyxWare-Userlizenz [redacted] EUR
- 3x SwyxProfessional-Option [redacted] EUR
- 3x „CTI+“-Lizenz [redacted] EUR

Menge	Kostenpunkt	Einzelkosten (in EUR)	Kosten (in EUR)
35	Personalkosten	[redacted]	[redacted]
1	[redacted]	[redacted]	[redacted]
1	[redacted]	[redacted]	[redacted]
3	Citrix XenDesktop-Enterprise Lizenzen	[redacted]	[redacted]
3	Remote Desktop Services (TSCAL)	[redacted]	[redacted]
3	Windows Server CAL (User CAL)	[redacted]	[redacted]
2	SwyxDECT 800 Basisstation	[redacted]	[redacted]
3	SwyxWare Userlizenz	[redacted]	[redacted]
3	SwyxProfessional Option	[redacted]	[redacted]
3	CTI+ Lizenzen	[redacted]	[redacted]
	Gesamtkosten		**5513,00**

Tabelle 3: Berechnung Gesamtkosten

2.6.2. Nutzen

- Zugriff auf die Anwendungen des Unternehmens: Über „Citrix XenApp“ werden die Anwendungen den Clients zur Verfügung gestellt
- Steigerung der Produktivität: Über die Telefonie-Software „SwyxIt!“ besteht die Möglichkeit mit jedem Kollegen, der ebenfalls diese Software installiert hat, den Desktop zu teilen und über Sachverhalte zu diskutieren oder gemeinsam Probleme zu lösen. Zuvor mussten die Mitarbeiter zu dem jeweiligen Standort fahren um einen Sachverhalt zu klären
- Geringerer Administrationsaufwand: Anwendungen müssen lediglich auf dem Terminalserver aktualisiert werden
- Die Mitarbeiter des Standort Vakuumhalle arbeiten nun in Echtzeit im ERP-System und die Informationen müssen nicht mehr am nächsten Tag per Hand in die Warenwirtschaft eingetragen werden
- Telefonische Erreichbarkeit steigt: Die Mitarbeiter sind mit den Schnurlostelefonen an beiden Standorten unter der gleichen Rufnummer zu erreichen
- Zufriedenere Mitarbeiter

3. Projektrealisierung

3.1. Konfiguration Standort-zu-Standort-VPN-Verbindung

Die Standort-zu-Standort-VPN-Verbindung wird am Hauptstandort mit einer [redacted]- und am Standort Vakuumhalle mit einer [redacted]-Firewall ausgehandelt. Da die [redacted]-Firewall kein integriertes Modem enthält und am Standort Vakuumhalle ein ADSL-Anschluss vorhanden ist, wird ein zusätzliches Modul für diese Firewall benötigt. Das Modul [redacted] wird in einen freien Slot der Firewall eingesteckt und dann automatisch als DSL-Modem erkannt. Zwischen den beiden Geräten wird ein IPsec-Tunnel aufgebaut. Beide Standorte besitzen eine feste öffentliche IP-Adresse. Für IPsec dient das IKEv1 (Internet Key Exchange-Protokoll) der automatischen Schlüsselverwaltung. Das IKE-Protokoll definiert, wie Sicherheitsparameter vereinbart und gemeinsame Schlüssel ausgetauscht wurden. IKE arbeitet in zwei Phasen. In Phase 1 wird die SA (Security Association) über den Main Mode ausgehandelt. Die SA ist eine Vereinbarung zwischen beiden Kommunikationspartnern, in diesem Fall die [redacted]- und die [redacted]-Firewall, und legt die Sicherheitsparameter fest. Im Proposal werden Verschlüsselung- und Hash-Algorithmen festgelegt. Als Verschlüsselungsalgorithmus wird [redacted] und als Hash-Algorithmus [redacted] gewählt. Dieses muss bei beiden Firewalls eingestellt werden damit diese mit den gleichen Algorithmen arbeiten. Zur Authentifizierung wird das Pre-Shared-Key-Verfahren (PSK) eingesetzt. Dieser Schlüssel wird ebenfalls bei beiden Geräten eingetragen. Es wird das PSK-Verfahren ausgewählt, da dieses einfacher zu konfigurieren ist. Im Moment werden im Unternehmen kaum Standort-zu-Standort-VPN-Verbindungen verwendet. Daher bleibt die Konfiguration übersichtlich. Zur Sicherheit wird ein Schlüssel mit vielen Zeichen ausgewählt. Nachdem nun die Phase 1 vorüber ist, werden erneut SAs in Phase 2 erzeugt, welche zum eigentlichen Datenaustausch benutzt werden. Für diese SAs werden wieder Proposal ausgewählt und an beiden Geräten eingestellt. Es werden in diesen SAs keine Schlüsselinformationen aus Phase 1 genutzt. Somit ist die Sicherheit der Phase 2 unabhängig von Phase 1. Zusätzlich wird in Phase 2 noch zwischen AH (Authentication Header) und ESP (Encapsulating Security Payload) gewählt. Da die Nutzdaten verschlüsselt werden sollen, kommt nur ESP in Frage. Allgemein stellt ESP Mechanismen zur Sicherstellung der Authentizität, Integrität und Vertraulichkeit der übertragenen IP-Pakete bereit. Da es sich hierbei um eine Standort-zu-Standort-VPN-Verbindung handelt, wird diese Verbindung im Tunnelmodus aufgebaut.

Zusätzlich wird die [redacted]-Firewall als DHCP-Server am Standort Vakuumhalle dienen, sodass alle angeschlossenen Netzwerkgeräte, die Netzwerkkonfiguration (IP-Adresse, Subnetzmaske etc.) zugewiesen bekommen.

3.2. Festlegung der eingehenden und ausgehenden Verbindungsberechtigungen

Um die Netzwerksicherheit am Standort Vakuumhalle zu erhöhen, werden die ein- und ausgehenden Verbindungen über fest definierte Regeln kontrolliert. Auf deren Grundlage wird entschieden, ob Datenpakete durchgelassen werden oder nicht.

Grundsätzlich werden alle Verbindungen erst einmal abgelehnt um dann später die wirklich benötigten Dienste freizuschalten. Dieses muss sowohl an der Firewall in der Vakuumhalle als auch an der Firewall des Hauptstandortes durchgeführt werden.

Um eine bessere Fehleranalyse zu ermöglichen werden ICMP-Pakete erlaubt. Auch die Anfragen über den NTP-Dienst, um eine zuverlässige Zeitangabe im Netzwerk zu erhalten, werden freigeschaltet.

Da es vor Ort keinen DNS-Server gibt, werden die DNS-Anfragen über die DNS-Server des Hauptstandortes aufgelöst. Die übrigen Regeln werden für den Aufbau der Citrix XenApp zuständig sein.

Damit die Administratoren die Möglichkeit haben, den Standort Vakuumhalle zu verwalten und bei auftauchenden Problemen reagieren zu können, wird die Kommunikation vom Hauptstandort in das Vakuumnetz nicht eingeschränkt.

3.3. Installation und Konfiguration des Citrix-Zugangs

Es befinden sich drei Arbeitsplätze am Standort Vakuumhalle. Alle drei Arbeitsplätze sind mit je einem PC (Dell Optiplex 360) ausgestattet. Die PCs nutzen das Betriebssystem Windows 7. Als zusätzliche Software wird „Citrix Receiver“ auf allen PCs installiert. Jeder Arbeitsplatz wird seinen eigenen Benutzer erhalten, welcher im Active Directory angelegt wird.

Auch die Rechte- und Richtlinienverwaltung wird im Active Directory durchgeführt. Die drei Benutzer werden die Berechtigungen erhalten, die benötigten Programme über „Citrix XenApp“ starten zu können.

Im „Citrix Receiver“ wird die IP-Adresse des Citrix Webinterfaces angegeben, damit die PCs über den VPN-Tunnel die Möglichkeit haben auf den Server zugreifen zu können. Nur so können die Programme zur Verfügung gestellt werden.

Der Multifunktionskopierer ist ebenfalls am LAN angeschlossen. Damit der Multifunktionskopierer über „Citrix XenApp“ genutzt werden kann, wird die zusätzliche Software „ScrewDrivers“ auf jedem PC installiert. Diese Software sorgt dafür, dass keine speziellen Druckertreiber mehr auf den Citrix Servern installiert und verwaltet werden müssen. Die Druckertreiber machen immer wieder Schwierigkeiten in Citrix Umgebungen, wenn der Druckertreiber nicht für Citrix zertifiziert wurde. Im Endeffekt werden durch „ScrewDrivers“ Supportaufwand und damit anfallende Kosten gespart.

3.4. Konfiguration und Aufstellung der Basisstationen

Es werden zwei „Ascom/SwyxDECT 800“-Basisstationen für den Standort Vakuumhalle vorgesehen, damit die DECT-Netzausstrahlung für das ganze Gebäude ausreichen wird. Zusätzlich muss beachtet werden, dass die Basisstationen eine „On-air“-Synchronisation aufbauen können, d.h. die Basisstationen müssen im Sichtkontakt stehen. Die optimalen Standorte für die Basisstationen werden mit unserem Dienstleister erarbeitet. Die

Erweiterung der strukturierten Verkabelung für den Anschluss der Basisstationen wird von unserem Betriebselektriker durchgeführt.

Im Vorfeld der Konfiguration wird mit unserem Dienstleister geprüft, welche Firmware für die Basisstationen von Swyx für den DECT-Betrieb vorausgesetzt wird. Diese Version wird auf beiden Basisstationen installiert.

Eine der beiden Basisstationen wird als Sync-Master konfiguriert. Dieser Sync-Master wird sich in Sichtkontakt mit den dort vorhandenen Basisstationen befinden und wird als Bindeglied zwischen Basisstationen am Standort Vakuumhalle und dem sogenannten Top-Master am Hauptstandort dienen. Der Top-Master wird alle Basisstationen verwalten und wird ebenfalls als Mittelsmann zur Kommunikation zwischen dem Swyx-Server und den Basisstationen dienen. Durch diese Lösung wird Roaming unter den Standorten möglich sein und ein schnurloses Telefon kann an jedem Standort Gespräche annehmen und durchführen. Über die VPN-Verbindung zwischen den beiden Standorten werden die beiden Basisstationen der Vakuumhalle mit dem Top-Master kommunizieren und werden so die benötigten Informationen erhalten um das gleiche DECT-Netz ausstrahlen zu können.

Damit die Kommunikation der Telefonanlage, Basisstationen und der schnurlosen Telefone zwischen den beiden Standorten über die VPN-Verbindung reibungslos funktioniert, werden die Firewall-Regeln erweitert. Auf der [redacted]-Firewall werden zwei weitere Regeln angelegt, die die Kommunikation vom Swyx-Server und vom VOIP-Netz zum Netz der Vakuumhalle erlauben. Diese Einstellungen müssen ebenfalls an der Firewall in der Vakuumhalle vorgenommen werden. Eine weitere Regel für die Basisstationen muss nicht angelegt werden, da sich die Basisstationen des Hauptstandortes im VOIP-Netz befinden.

Zusätzlich wird bei all diesen Regeln die Einstellung „Quality of Service“ aktiviert. Der Datenverkehr für die Telefonanlage wird in der höchsten Priorität über den VPN-Tunnel übertragen. Ohne diese Einstellung könnte anderer Datenverkehr die Datenübertragung der Telefonie stören, da der VPN-Tunnel nur eine bestimmte Bandbreite zur Verfügung hat.

3.5. Anlegen der Benutzer in der Telefonanlage

Am Standort Vakuumhalle sind drei Aastra DT390-Schnurlostelefone vorhanden. Folgerichtig werden drei Benutzer auf dem Swyx-Server über die „SwyxWare Administration“ angelegt. Jeder Benutzer wird seine eigene Durchwahl und eine externe Rufnummer erhalten, mit der Benutzer intern und extern telefonieren können. Aufgrund der Übersicht werden die Benutzer der Vakuumtechnik drei aufeinanderfolgende Durchwahlen erhalten über die sie zu erreichen sein werden [redacted]. Die Schnurlostelefone werden ihre Verbindungen über das SIP-Protokoll (Session Initiation Protocol) aufbauen. SIP ist ein Netzprotokoll zum Aufbau, zur Steuerung und zum Abbau einer Kommunikationssitzung zwischen zwei oder mehr Teilnehmer. Es arbeitet auf der OSI-Schicht 5 und verwendet die Transport-Protokolle TCP und UDP für die Übertragung.

3.6. Verbindung der Schnurlostelefone mit dem DECT-Netz

Im Top-Master, welcher die Basisstationen und Schnurlostelefone verwaltet, werden die drei neuen Schnurlostelefone angelegt. Dafür wird die jeweilige IPEI des DT390-Schnurlostelefons benötigt. Die IPEI (International Portable Equipment Identifier) ist eine „Seriennummer“ für DECT-Mobilteile, welche weltweit eindeutig ist. Im Webinterface des Top-Masters unter dem Menüpunkt „Users“ werden die Schnurlostelefone neu hinzugefügt. Folgende Daten werden dafür benötigt: Long Name, Display Name, SIP-Benutzer-ID, SIP-Kennwort, IPEI, Idle Display sowie den Authorisation Code, welcher bei der Anmeldung der Schnurlostelefone am Gerät benötigt wird.

Zuerst werden die drei Schnurlostelefone als „Benutzer“ auf dem Top-Master bekannt gemacht und anschließend konfiguriert. Unter „Einstellungen → System → Anmelden“ wird das Schnurlostelefon am DECT-System angemeldet. Als Systemname wird nach Vogelsang Richtlinie „VGS“ eingetragen. Im nächsten Schritt der Konfiguration wird die „PARK“-Nummer des Top-Masters und der zuvor genutzte „Authorisation Code“ eingetragen. Die „PARK“-Nummer befindet sich im Webinterface des Top-Masters. Diese dient der eindeutigen Identifizierung des DECT-Netzes und ist vergleichbar mit der SSID eines WLAN-Netzes. Das Schnurlostelefon wird eine Verbindung zum DECT-Netz aufbauen und unter der eingetragenen Durchwahl zu erreichen sein.

4. Testphase

4.1. Test der Standort-zu-Standort-VPN-Verbindung

Der Test der Standort-zu-Standort-VPN-Verbindung verlief reibungslos. Mit dem „Ping“-Befehl wurde getestet, ob alle benötigten Ressourcen zu erreichen sind und die beiden Firewalls miteinander kommunizieren können. Die Firewall arbeitet mit einem Paketfilter. So konnte anhand der gesetzten Firewall-Regeln getestet werden, ob die jeweiligen Anfragen geblockt oder weitergeleitet werden. Durch einen Belastungstest (alle Clients arbeiten zur gleichen Zeit im ERP-System über „Citrix XenApp“) wurde getestet, ob die Performance des Netzwerkes ausreicht, da die Geschwindigkeit des ADSL-Anschlusses lediglich 6.000kbit/s beträgt.

4.2. Test der Telefonie und Funktionalität der Software

Nachdem sich die Schnurlostelefone im DECT-Netz angemeldet haben, werden Testanrufe durchgeführt. Hierbei wird kontrolliert, ob alle Sprachdaten reibungslos übertragen werden und keine Störungen während des Telefonats auftreten. Zusätzlich wird die Ausleuchtung des DECT-Netzes im Gebäude getestet und geschaut ob die Übergänge zwischen den Basisstationen funktionieren. Dies ist mit einer Funktion des schnurlosen Telefons nachvollziehbar. Diese Funktion zeigt zum Beispiel an, wie groß die Fehlerrate der erhaltenen Datenpakete ist.

Bei der „SwyxIt!“-Software wird getestet, ob Anrufe über die Anwendung getätigt werden können. Darüber hinaus wird die Desktop-Sharing-Funktion getestet. Kleine Verzögerungen werden zu erkennen sein, was auf die Geschwindigkeit des ADSL-Anschlusses zurückzuführen ist.

5. Projektabschluss

5.1. Fazit

Zum Abschluss des Projektes wurde noch einmal überprüft, ob die Zeitplanung, welche zu Beginn aufgestellt wurde, eingehalten werden konnte.

Projektphase	**Geplante Zeit** (in h)
Vorbereitung	3,0
Planung	7,0
Realisierung	**11,0**
Testphase	**5,0**
Abnahme des Projektes	3,0
Erstellung der Dokumentation	6,0
Gesamt	**35,0**

Tabelle 4: Zeitplanung Projektphase IST

In der Realisierungsphase ist eine Stunde Zeit mehr benötigt worden, da die Konfiguration der Firewall mehr Aufwand benötigte als zuvor erwartet. Da jedoch die Tests reibungslos verliefen konnte hier wiederum eine Stunde eingespart werden. Somit ist das Projekt bei einer Gesamtstundenanzahl von 35 Stunden wie erwartet verlaufen.

Im Allgemeinen ist das Projekt sehr gut verlaufen und es sind kaum Probleme aufgetreten. Die Kommunikation mit den Mitarbeitern am Standort Vakuumhalle war sehr gut. Es kam lediglich zu kleinen Projektverzögerungen aufgrund von Reaktionszeiten der externen Dienstleister (z.B. Anbieter der VoIP-Telefonanlage). In diesem Projekt fiel auf, wie wichtig die Kommunikation mit den Kollegen und den Entscheidungsträgern ist, damit ein Projekt erfolgreich abgeschlossen werden kann. So gab es immer mal wieder aufkommende Fragen, die nur nach Rücksprache mit den Kollegen beantwortet werden konnten.

Die Mitarbeiter am Standort Vakuumhalle sind sehr zufrieden mit dem Verlauf und dem Ergebnis des Projektes. Hierbei ist vor allem wichtig, dass sie nun selbst die Möglichkeit haben Änderungen im ERP-System eintragen zu können. Somit sind sie nicht mehr darauf angewiesen, dass ein Mitarbeiter des Hauptstandortes die Änderungen nachträgt. Des Weiteren sind die Mitarbeiter der Vakuumabteilung, sehr zufrieden mit der Desktop-Sharing-Funktion. Mit dieser können sie bei Problemen und unklaren Sachverhalten sehr schnell Hilfestellung leisten, ohne den Standort wechseln zu müssen. Dies erspart ihnen viel Zeit und dem Betrieb zusätzliche Kosten.

6. Literatur- und Quellenverzeichnis

Internetquellen

- Allgemeines VPN-Verbindungen
  - http://www.nwlab.net/know-how/VPN/
  - Stand vom 20.03.2015

- Funktionsweise IPsec
  - http://www.ping.de/~christian/IPSec.pdf
  - Stand vom 20.03.2015

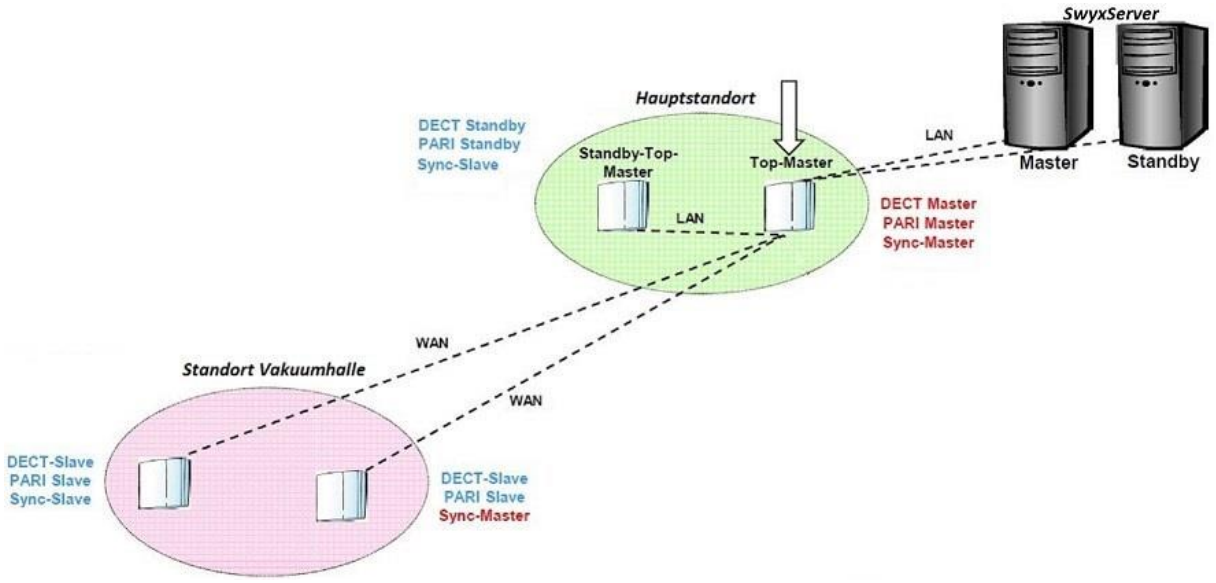
- Allgemeines SwyxIt!
  - http://www.swyxdownload.com/download/SwyxIt!_german.pdf
  - Stand vom 01.04.2015

- Funktionsweise Ascom IP-DECT
  - http://www.swyxdownload.com/download/ip-dect_sd_92375gb_2011-10-28%20Ver%20L.pdf
  - Stand vom 01.04.2015

- Personal-Service GmbH: Personalkostenrechner
  - http://www.personalservice-alpha.de/unternehmen/personalkostenrechner
  - Stand vom 16.04.2015

7. Anhang

Übersichtsplan Kommunikation Basisstationen



Anwenderdokumentation

Anbindung des Standorts Vakuumhalle an die IT-Infrastruktur der
Hugo Vogelsang Maschinenbau GmbH

ENGINEERED TO WORK

Verfasser Bernd Abeln
Kontakt [redacted]
Unternehmen Hugo Vogelsang Maschinenbau GmbH Essen (Oldenburg)

Inhaltsverzeichnis

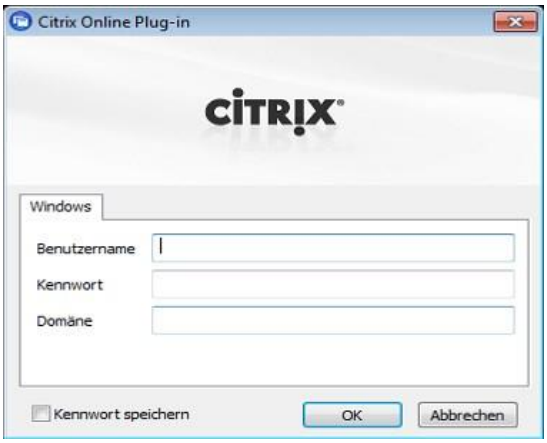
1. Einführung

In dieser kurzen Anleitung werden Ihnen „Citrix Online Plug-in“ und die Telefonsoftware „SwyxIt!“ mit den wichtigsten Funktionen näher gebracht. „Citrix Online Plug-in“ ist dafür zuständig, dass Sie die benötigten Anwendungen Ihres Unternehmens (proALPHA, SwyxIt!) an Ihrem PC nutzen können.

„SwyxIt!“ ist eine Telefonsoftware, die Ihnen die Möglichkeit bietet aus der Software heraus Anrufe zu tätigen oder aber auch Ihren Bildschirm mit Ihren Kollegen teilen zu können. Mit dieser Desktop-Sharing-Funktion können sie bei Problemen und unklaren Sachverhalten sehr schnell Hilfestellung erhalten bzw. leisten.

1.1 Nutzung von Citrix Online Plug-in

Nachdem Sie sich mit Ihren Windows-Anmeldedaten am PC eingeloggt haben, erscheint auf dem Desktop die Aufforderung zur Anmeldung am „Citrix Online Plug-in“.



Benutzername: [redacted]

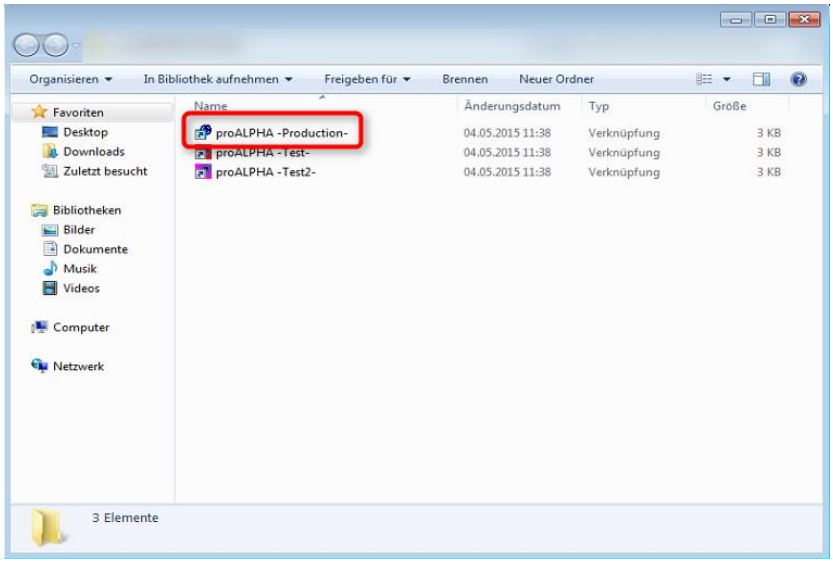
Kennwort: [redacted]

Domäne: [redacted]

Bestätigen Sie Ihre Eingaben mit „OK“. Wenn Ihre Eingaben akzeptiert worden sind, haben Sie nun Zugriff auf die bereitgestellten Anwendungen. Diese Anwendungen befinden sich auf Ihrem Desktop.

1.2 Starten von proALPHA und SwyxIt!

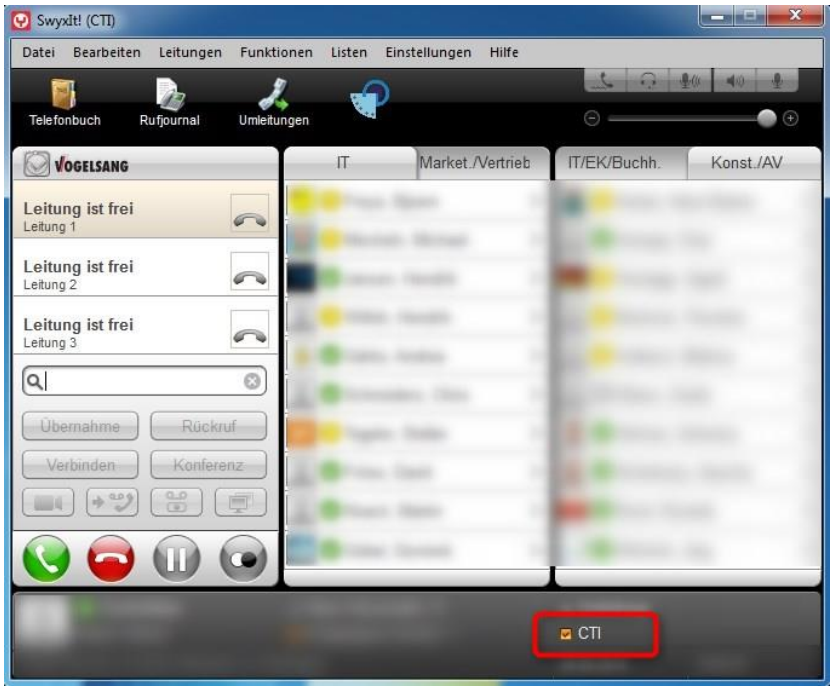
Um „proALPHA“ zu starten, öffnen Sie den Ordner „proALPHA [redacted] Client auf ihrem Desktop. In dem Ordner werden drei Versionen von „proALPHA“ zur Verfügung gestellt. Sie arbeiten in der „proALPHA –Production-“-Version. Mit einem Doppelklick auf die Verknüpfung starten die Anwendung.



Die Software „SwyxIt!“ befindet sich direkt auf dem Desktop. Um „SwyxIt!“ zu starten, machen Sie einen Doppelklick auf die folgende Verknüpfung:

2. Funktionen von SwyxIt!

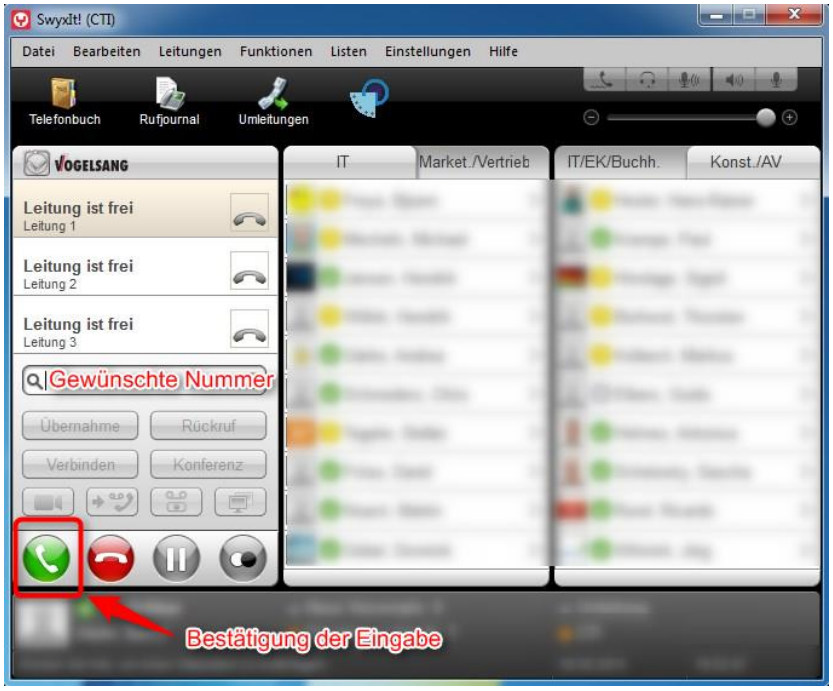
Damit Sie einen Anruf mit „SwyxIt!“ tätigen oder Ihren Bildschirm mit Ihrem Gesprächspartner teilen zu können, muss die CTI-Funktion für Sie aktiviert sein. Dies erkennen Sie daran, dass auf der Benutzeroberfläche von „SwyxIt!“ ein Haken beim Punkt „CTI“ unten in der Leiste gesetzt ist.



Ist dieser Haken nicht gesetzt, springen Sie zum Punkt 3 „Fragen und Probleme“.

2.1 Anruf mit „Swxylt!“ tätigen

Einen Anruf mit „SwyxIt!“ können Sie tätigen, indem Sie die Nummer des gewünschten Gesprächspartners in das Suchfeld eintragen und Ihre Eingabe mit einem Klick auf den grünen Hörer bestätigen.



Wenn Sie die Rufnummer des gewünschten Gesprächspartners nicht zur Hand haben, können Sie ebenfalls den Vor- oder Nachnamen in das Suchfeld eintragen. „SwyxIt!“ wird Ihnen dann aufgrund Ihrer Eingabe alle möglichen Gesprächspartner vorschlagen.

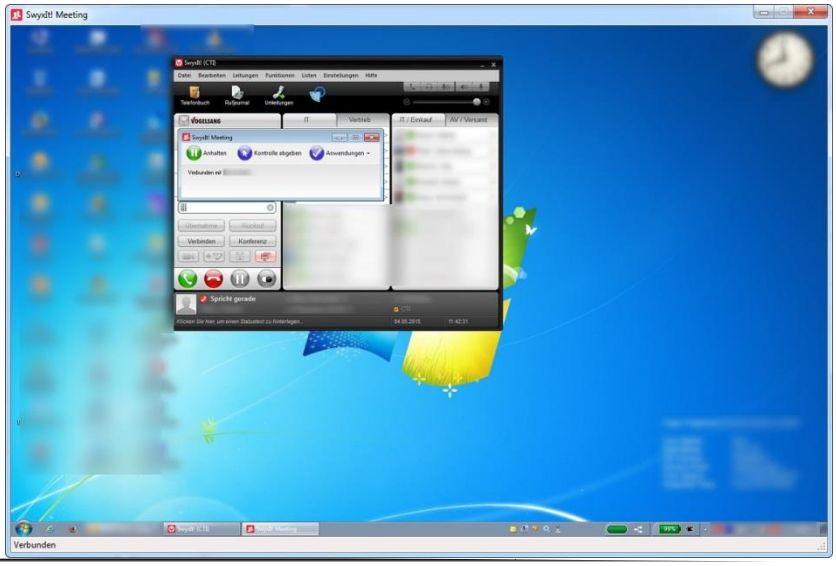
Wenn Sie Ihre Eingabe bestätigt haben, erhalten Sie auf Ihrem Telefon einen Anruf. Nachdem Sie den Anruf angenommen haben, beginnt der Rufaufbau zu Ihrem gewünschten Gesprächspartner.

2.2 Desktop-Sharing-Funktion

Während eines Anrufes haben Sie die Möglichkeit den Bildschirm zu übertragen. **Wichtig:** Eine Übertragung des Bildschirms ist nur möglich, wenn der Gesprächspartner ebenfalls „SwyxIt!“ nutzt und die „CTI“-Verknüpfung aktiviert hat..

Um den Bildschirm zu übertragen, wählen Sie die Schaltfläche „Collaboration“ mit den beiden Monitoren aus. Nun wird Ihr Bildschirm an Ihren Gesprächspartner übertragen.

Bei Ihrem Gesprächspartner öffnet sich ein neues Fenster „SwyxIt! Meeting“. In diesem Fenster wird Ihr Bildschirm angezeigt und Ihr Gesprächspartner bekommt Ihren Desktop zu sehen.



Sie haben nun zusätzlich zwei Einstellungsmöglichkeiten:

1) Sie können Ihrem Gesprächspartner die Kontrolle über die Maus erteilen.

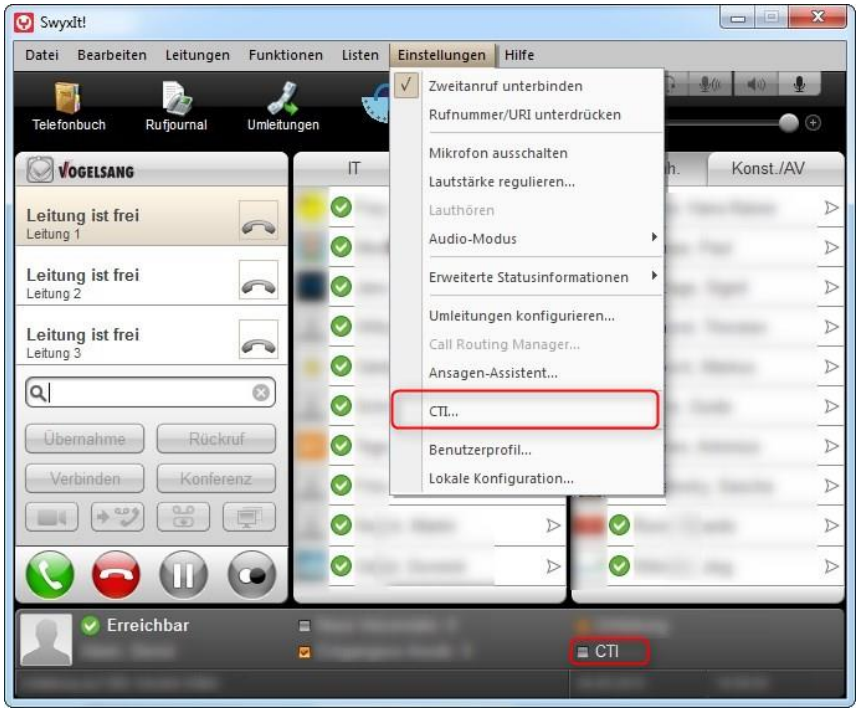
2) Sie können entscheiden, was Ihr Gesprächspartner zu sehen bekommt.

3. Fragen und Probleme

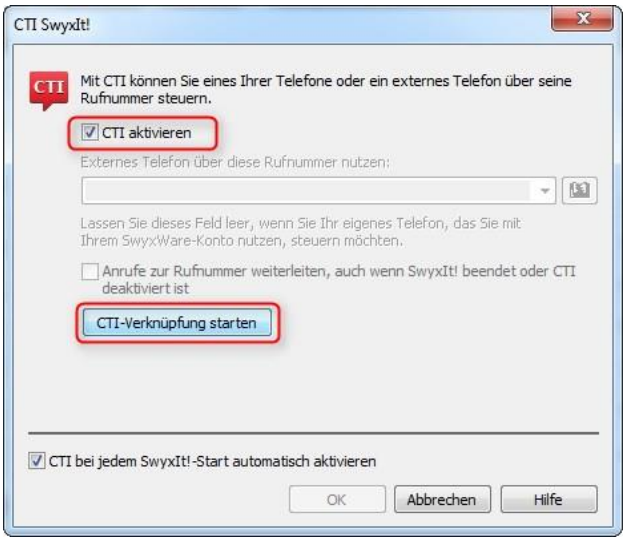
„CTI“-Verknüpfung nicht hergestellt

Damit Sie Anrufe mit „SwyxIt!“ tätigen können, muss die „CTI“-Verknüpfung in „SwyxIt!“ aktiviert sein. Wenn diese Verknüpfung nicht gesetzt ist, sind Ihr Telefon und „SwyxIt!“ nicht miteinander gekoppelt. Um eine Kopplung herzustellen, gehen Sie wie folgt vor:

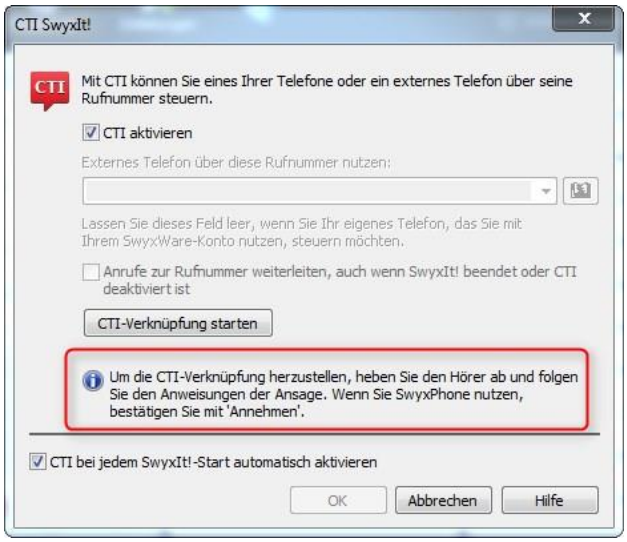
Über „Einstellungen → CTI…“ gelangen Sie in die Konfiguration zur CTI-Verknüpfung.

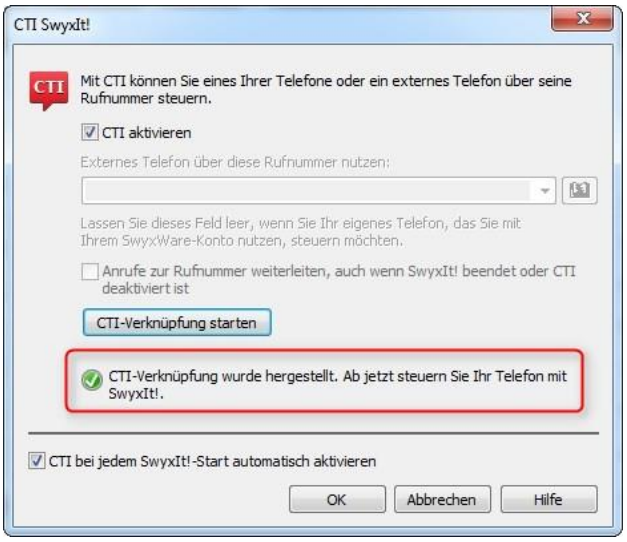


Im neuen Fenster setzen Sie einen Haken bei „CTI aktivieren“ und klicken daraufhin die „CTI-Verknüpfung starten“-Schaltfläche.



Sie erhalten nun einen Anruf auf Ihrem Telefon. Diesen Anruf nehmen Sie an und sorgen so dafür, dass Ihr Telefon mit „SwyxIt!“ gekoppelt wird.





Bestätigen Sie den Vorgang mit „OK“. Nun können Sie „SwyxIt!“ mit allen Funktionen nutzen.

„Citrix Online Plug-in“-Anmeldung fehlgeschlagen

Wenn Sie diese Fehlermeldung nach mehrmaliger Eingabe Ihrer Anmeldedaten erhalten, melden Sie sich bitte bei Ihrer verantwortlichen IT-Abteilung. Die Kontaktdaten befinden sich im Punkt 4 „Kontakt“

4. Kontakt

Bei Fragen oder Problemen bei der Verwendung vom „Citrix Online Plug-In“ oder von „SwyxIt!“, melden Sie sich bei Ihrer Vogelsang IT-Abteilung. Wir helfen Ihnen gerne!

[redacted]

- Herr Abeln: [redacted]

Betriebsdokumentation

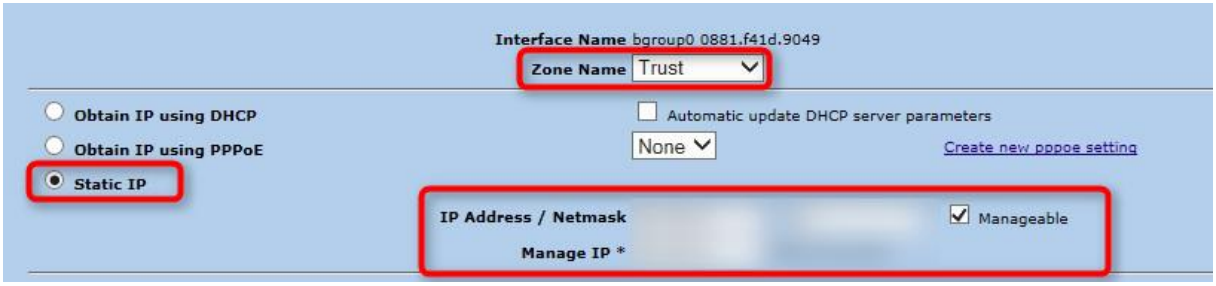
Anbindung des Standorts Vakuumhalle an die IT-Infrastruktur der
Hugo Vogelsang Maschinenbau GmbH

ENGINEERED TO WORK

Verfasser Bernd Abeln
Kontakt [redacted]
Unternehmen Hugo Vogelsang Maschinenbau GmbH Essen (Oldenburg)

Konfiguration [redacted]

Zu Beginn muss der Firewall eine statische IP für das LAN zugeordnet werden. In der Benutzeroberfläche der [redacted]-Firewall über „Network→Interfaces→List“ an der LAN-Schnittstelle erhält die Firewall die lokale IP [redacted], wodurch die Firewall von allen lokal angeschlossenen Geräten zu erreichen ist. Über „Edit“ gelangt man in das Konfigurationsmenü und es können alle benötigten Einstellungen gesetzt werden. Dabei zu beachten ist, dass die Zone als „Trust“-Zone deklariert wird.



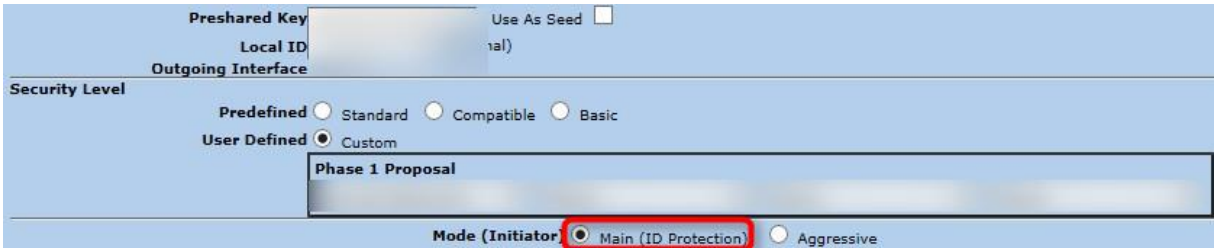
Da die Firewall ebenfalls als DHCP-Server dient, müssen zusätzlich die DHCP-Einstellungen an der lokalen Schnittstelle gesetzt werden. Unter „Network→DHCP“ an der lokalen Schnittstelle wird die Option für den DHCP-Server ausgewählt. Weitere Einstellungen die gesetzt werden müssen sind die Lease-Time, sowie der Adressbereich, welcher für die angeschlossenen PCs zur Verfügung stehen soll. Da lediglich drei PCs im LAN angeschlossen sind, wird auch nur ein kleiner Adressbereich [redacted] festgelegt.

Zwischen der [redacted] (Standort Vakuumhalle) und der [redacted] (Hauptstandort) wird ein IPsec-Tunnel aufgebaut. Beide Standorte besitzen eine feste öffentliche IP-Adresse. Unter „VPNs→AutoKey Advanced→Gateway“ wird eine neue Verbindung erstellt.

Der Gateway Name heißt [redacted] und als IP-Adresse muss die WAN-IP der [redacted] vom Hauptstandort eingetragen werden.

Dieser Punkt wird auch bei der [redacted] wiederholt. Der Gateway Name bekommt nun aber die Bezeichnung [redacted] und als IP-Adresse muss die WAN-IP der [redacted] des Standortes Vakuumhalle eingetragen werden.

Unter „VPNs→AutoKey Advanced→Gateway→Edit→Advanced“ wird nun an beiden Firewalls der gleiche PSK (Pre-Shared-Key) und auch die gleichen Phase 1 Proposals ausgewählt, sodass der Schlüsselaustausch zwischen beiden Standorten ohne Probleme funktioniert. Zusätzlich wird noch der Main Mode ausgewählt.



Um die Phase 2 des IKEv1-Protokolls zu konfigurieren, wird unter „VPNs→AutoKey IKE“ ebenfalls einen neue Verbindung erstellt. Als Remote Gateway wird die vorhin vordefinierte [redacted]-Schnittstelle ausgewählt.

Unter dem Punkt „Advanced“ werden wieder die gleichen Phase 2-Proposals an beiden Firewalls ausgewählt.

Festlegung der eingehenden und ausgehenden Verbindungsberechtigungen

Allgemeine Firewall-Regeln am Standort Vakuumhalle [redacted]:

Trust	→	Untrust	Service	Status
Firewall Vakuumhalle	→	ANY	ICMP+NTP	Permit
Firewall Vakuumhalle	→	DNS-Server	DNS	Permit
Firewall Vakuumhalle	→	Citrix Webserver	HTTP+HTTPS	Permit
Firewall Vakuumhalle	→	Citrix Terminalserver	Citrix Session Reliability + Citrix ICA	Permit
ANY	→	ANY	ANY	Deny

Untrust	→	Trust	Service	Status
Firewall Hauptstandort	→	Firewall Vakuumhalle	ANY	Permit
ANY	→	ANY	ANY	Deny

Allgemeine Firewall-Regeln am Hauptstandort [redacted]:

Untrust	→	Trust	Service	Status
Firewall Vakuumhalle	→	Firewall Hauptstandort	ICMP	Permit
Firewall Vakuumhalle	→	DNS-Server	DNS	Permit
Firewall Vakuumhalle	→	Citrix Webserver	HTTP+HTTPS	Permit
Firewall Vakuumhalle	→	Citrix Terminalserver	Citrix Session Reliability + Citrix ICA	Permit
ANY	→	ANY	ANY	Deny

Trust	→	Untrust	Service	Status
Firewall Hauptstandort	→	Firewall Vakuumhalle	ANY	Permit
ANY	→	ANY	ANY	Deny

Zu den allgemein gesetzten Firewall-Regeln, werden zusätzlich für die Telefonanlage „Swyx“ Regeln gesetzt, damit eine Kommunikation zwischen den Basisstationen am Standort Vakuumhalle und dem Top-Master bzw. dem Swyx-Server stattfinden kann.

Zu setzende Firewall-Regeln am Standort Vakuumhalle [redacted]:

Trust	→	Untrust	Service	Status
Firewall Vakuumhalle	→	IP Swyx-Server	ANY	Permit
Firewall Vakuumhalle	→	VOIP-Netz	ANY	Permit

Untrust	→	Trust	Service	Status
IP Swyx-Server	→	Firewall Vakuumhalle	ANY	Permit
VOIP-Netz	→	Firewall Vakuumhalle	ANY	Permit

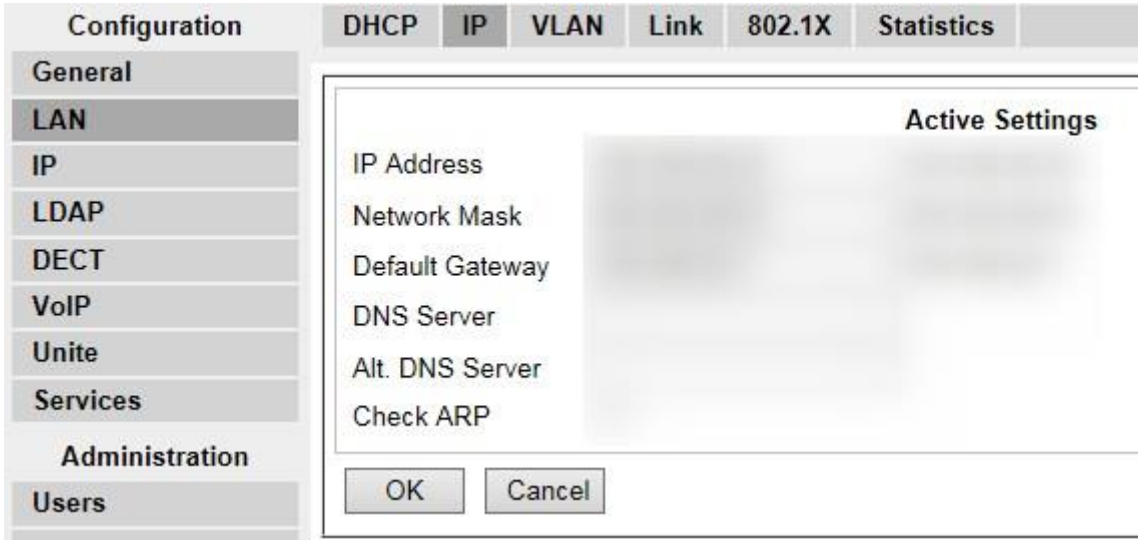
Zu setzende Firewall-Regeln am Hauptstandort [redacted]:

Trust	→	Untrust	Service	Status
IP Swyx-Server	→	Firewall Vakuumhalle	ANY	Permit
VOIP-Netz	→	Firewall Vakuumhalle	ANY	Permit

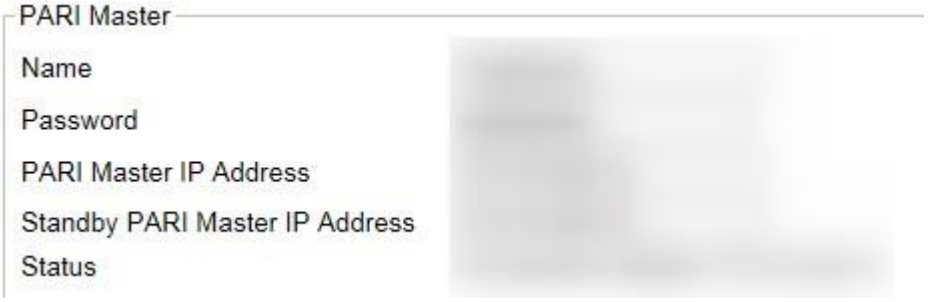
Untrust	→	Trust	Service	Status
Firewall Vakuumhalle	→	IP Swyx-Server	ANY	Permit
Firewall Vakuumhalle	→	VOIP-Netz	ANY	Permit

Konfiguration der Basisstationen

Zu Beginn erhalten die Basisstationen jeweils eine feste IP-Adresse. Unter „LAN→IP“ werden diese den Stationen zugeteilt. Der DHCP-Mode wird deaktiviert unter „LAN→DHCP“. Nach der Änderung der IP sollte ein Neustart der Geräte erfolgen, sodass diese die Netzwerkeinstellungen übernehmen.



Anschließend sind die Basisstationen über die neue IP-Adresse erreichbar. An beiden Basisstationen wird unter „DECT→Radio“ der Top-Master vom Hauptstandort eingetragen, wodurch diese ihre, vom Top-Master zugewiesenen, RFPIs (Radio Fixed Part Identity) erhalten.

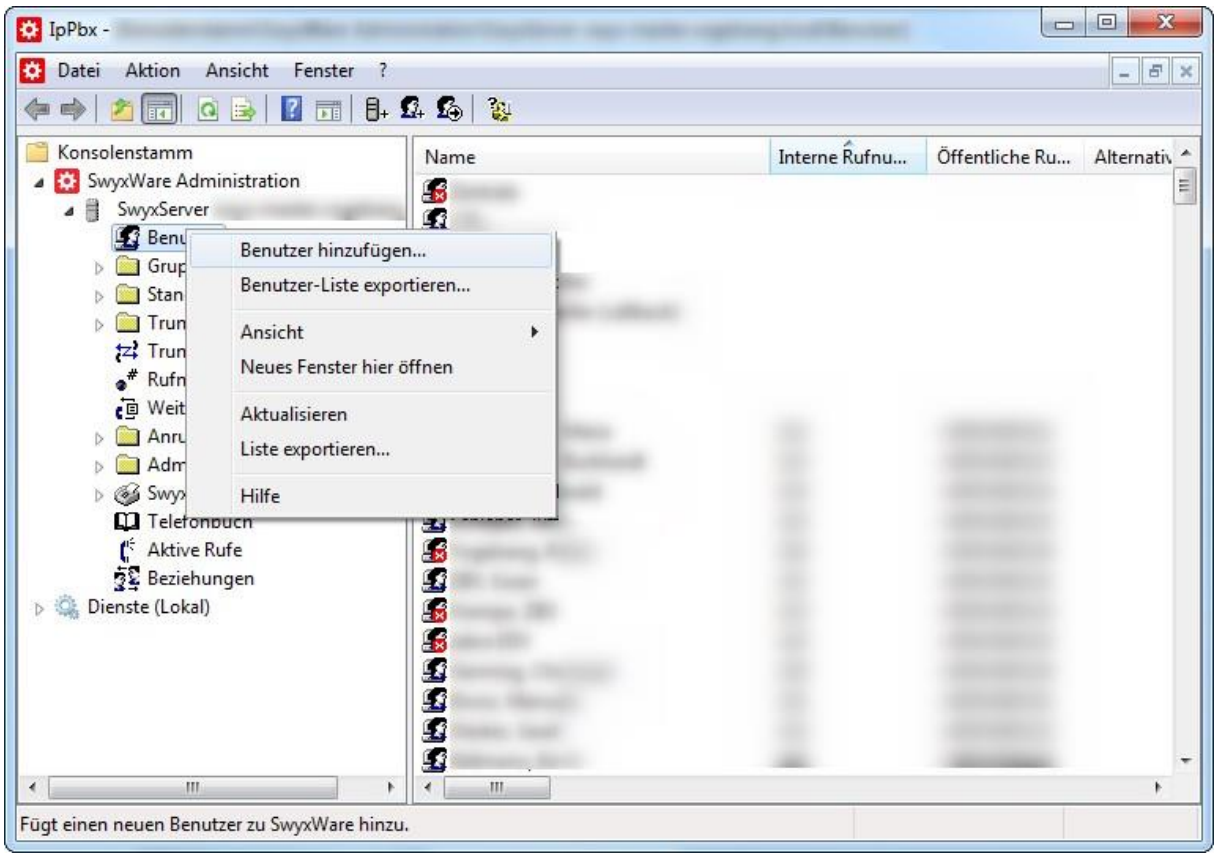


Zusätzlich muss der Sync-Master unter „DECT→Air Sync“ den „Sync Mode“ als „Master“ und die andere Basisstation als „Sync Mode“ „Slave“ gesetzt haben. Die „Sync Region“ bei beiden Basisstationen muss identisch sein.

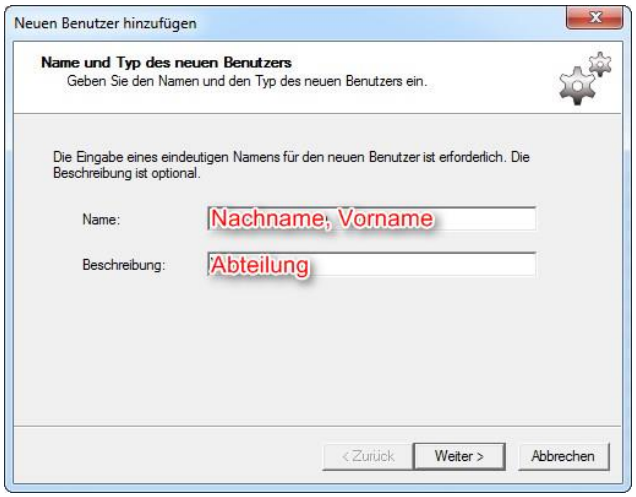
Anlegen der Benutzer in der Telefonanlage

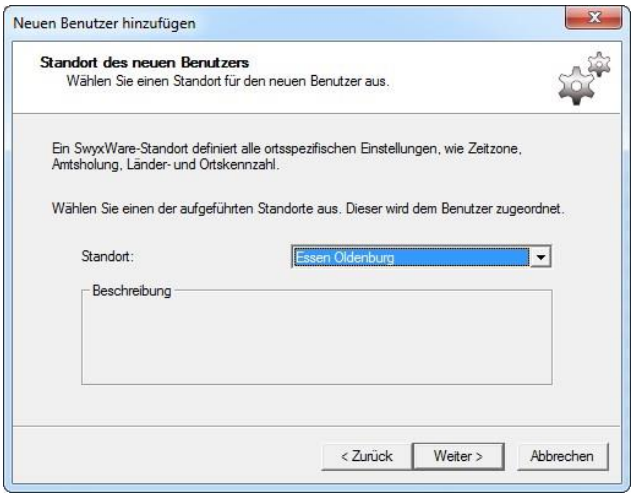
Über die Software „SwyxWare Administration“, welche auf dem Swyx-Server installiert ist, werden die drei neuen Benutzer angelegt.

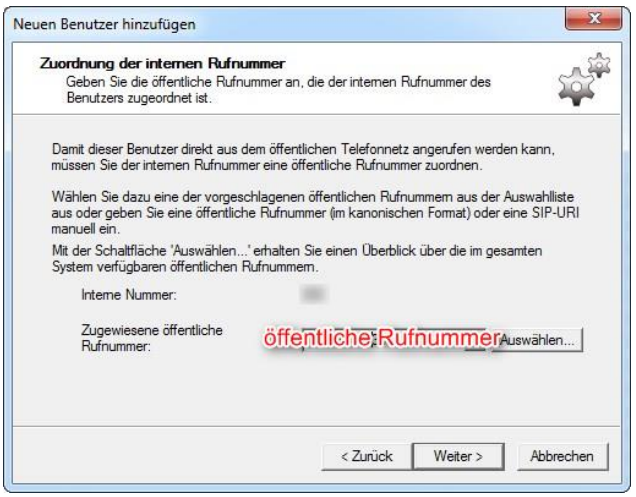
Mit Rechtsklick auf Benutzer öffnet sich ein Kontextmenü, wo die Option „Benutzer hinzufügen…“ ausgewählt wird.

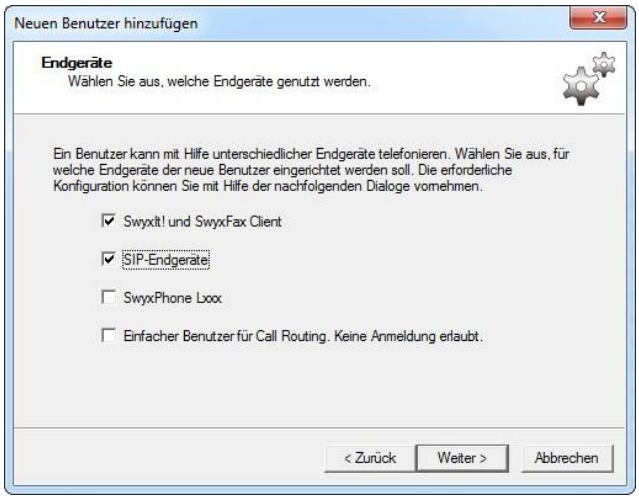


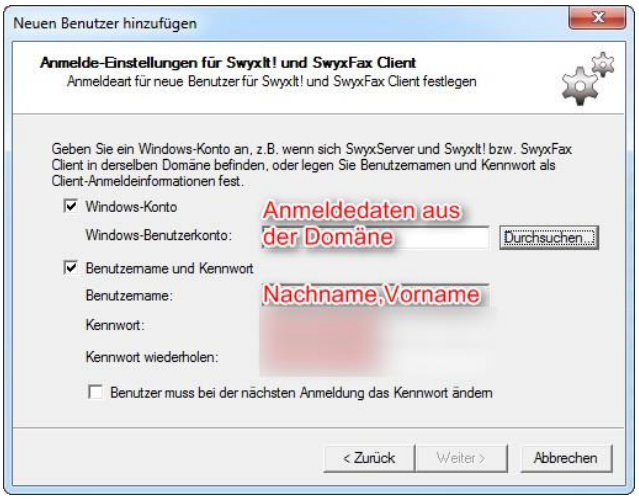
Es öffnet sich ein neues Fenster. Das Anlegen des Benutzers wird nach der Standardprozedur der Firma Vogelsang wie folgt ausgeführt:



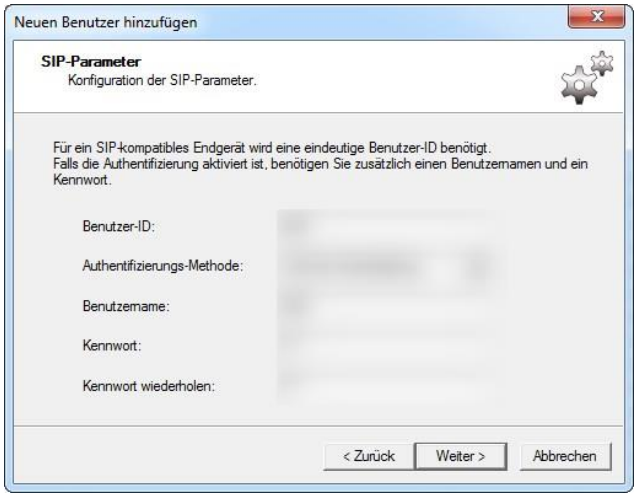






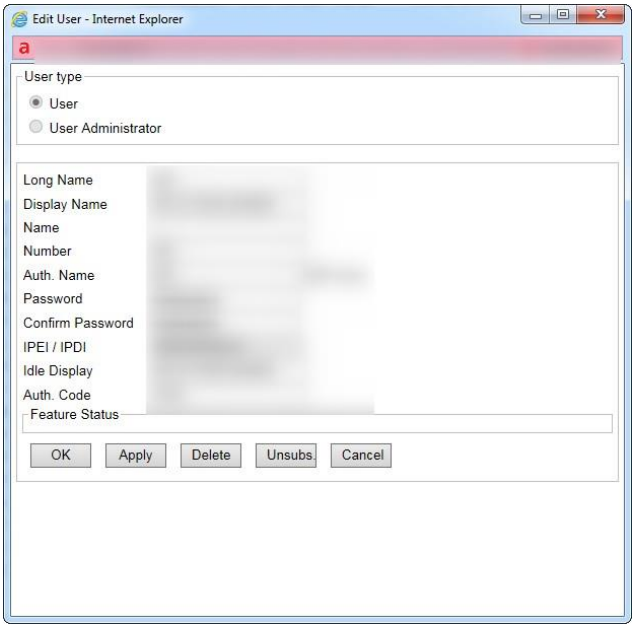


Die SIP-Parameter sind entscheidend für die schnurlosen Telefone. Diese Parameter werden beim Anlegen der Benutzer am Top-Master wieder benötigt.



Anlegen der Benutzer am Top-Master

Um die drei Benutzer am Top-Master anzulegen, wird das Webinterface des Top-Masters geöffnet. Zum Anlegen der Benutzer werden Administratorrechte benötigt. Unter „Users→new“ werden nun alle benötigten Informationen eingetragen.



Verbindung der schnurlosen Telefone mit dem DECT-Netz

Unter „Menü→Einstellungen→System→Anmelden“ im Aastra DT390 wird das Telefon mit dem DECT-Netz verbunden.

Die IPEI wird beim Anlegen des Benutzers am Top-Master benötigt.

Im nächsten Schritt werden die PARK vom DECT-Netz und der AC (Authentication Code) benötigt. Der PARK wird auf dem Top-Master-Webinterface mit angezeigt. Der AC wurde vorher beim Anlegen des Benutzers definiert.

Wenn die Daten übereinstimmen wird sich das schnurlose Telefon mit dem DECT-Netz verbinden und die Anmeldung wird erfolgreich sein.