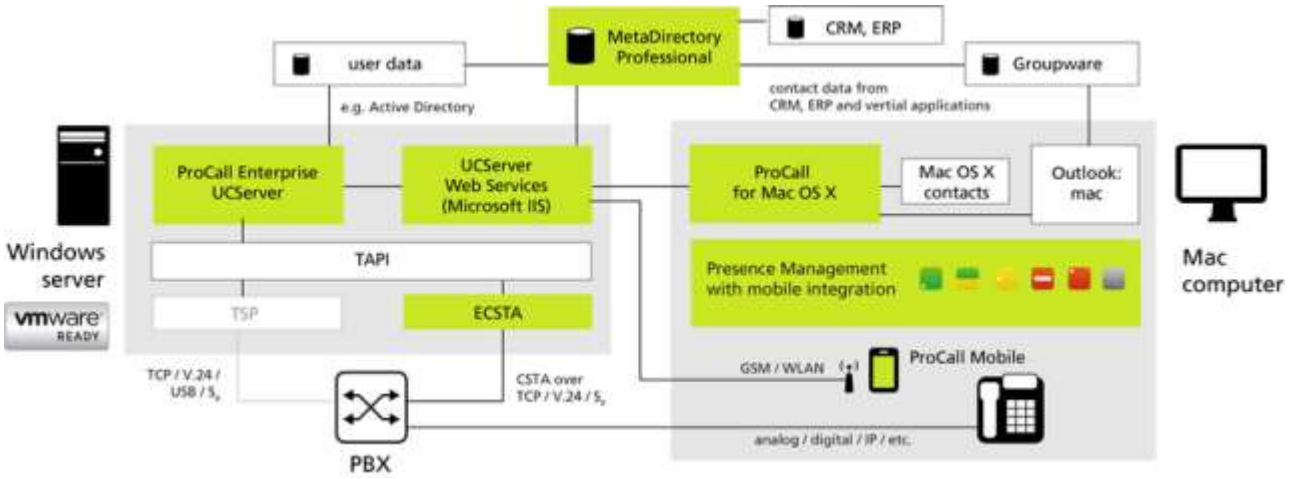
estos UCServer Web Services

5.1.50.44786

1 Willkommen zu den estos UCServer Web Services

Für eine schnelle erfolgreiche Installation lesen Sie bitte die Hinweise zur Installation

Die UCServer Web Services stellen für die Clients eines estos UCServer ein Internet kompatible Schnittstelle bereit. Der Dienst wird hierbei als Bindeglied zwischen dem UCServer und mobilen Endgeräten sowie auch von ProCall for Mac® benötigt.



Die vorliegende Hilfe führt Sie durch Installation und Konfiguration der UCServer Web Services.

- Wie Sie die estos UCServer Web Services installieren, erfahren Sie im Kapitel Installation.
- Die einzelnen Einstellungsseiten der estos UCServer Web Services-Verwaltung sind im Kapitel Einstellungen beschrieben.

In dieser Hilfe werden die folgenden Symbole verwendet:

Symbol	Bedeutung
	Hinweis
	Warnung, Vorsicht
	Änderung gegenüber älteren Versionen

2 Installation der estos UCServer Web Services

2.1 Systemvoraussetzungen

2.1.1 Hardware

- PC mit mind. 2 GHz Taktfrequenz
- 2 GB Arbeitsspeicher
- 75 MB freier Festplattenspeicher, zzgl. Plattenplatz für Logfiles

2.1.2 Software

- Windows Server® 2008 R2
- Windows® Small Business Server 2011 Standard
- Windows Server® 2012
- Windows Server® 2012 R2

Die Installation auf einem nicht-Server Betriebssystem z. B. Windows® Vista, Windows® 7 oder Windows® 8 wird nicht unterstützt. Wird estos UCServer Web Services auf einem nicht-Server Betriebssystem installiert, kommt es ab einer geringen Anzahl gleichzeitiger Nutzer zu Verbindungsabbrüchen zum Microsoft® Internet Information Services (IIS). Es handelt sich dabei um eine technische Einschränkung des Microsoft® Internet Information Services (IIS) auf nicht-Server Betriebssystemen.

2.1.3 Umgebung

- Microsoft® .NET Framework ab Version 4 (full edition). Das vollständige Downloadpaket steht bei Microsoft® zur Verfügung: (http://www.microsoft.com/en-US/download/details.aspx?id=17718)
- Microsoft® Internet Information Server (IIS) ab Version 7
- TCP-Netzwerkverbindung zum estos UCServer
- (optional) estos MetaDirectory (Professional) ab Version 3.5

2.1.4 Vorausgesetzte Kenntnisse

UCServer Web Services werden innerhalb des Microsoft® Internet Information Services (IIS) eines Microsoft® Server Betriebssystems installiert und stellt Anwendungen eine sichere Schnittstelle über offene Standardprotokolle zur Kommunikation mit dem estos UCServer zur Verfügung.

Während der Installation der UCServer Web Services wird der Microsoft® Internet Information Services (IIS) auf Ihrem Betriebssystem aktiviert und vorkonfiguriert. Für die Installation und den Betrieb des UCServer Web Services benötigen Sie daher Kenntnisse in:

- Konfiguration einer Firewall
- Installation und Konfiguration des Microsoft® Internet Information Services (IIS) auf Windows Server® Betriebssystemen
- Erstellung und Einrichtung von SSL-Zertifikaten zur Verschlüsselung der Kommunikation

2.2 Vorbereitung der Installation

Bitte überprüfen Sie vor einer Installation die nachfolgenden Punkte:

1. Stellen Sie sicher, dass die letzten Betriebssystem-Updates auf dem Zielrechner installiert sind.

2. estos UCServer ist installiert und gestartet.
3. Für eine sichere Nutzung der UCServer Web Services und um Ihre internen Daten (LAN) vor unerlaubten, externen Zugriffen zu schützen, empfehlen wir das Aufsetzen einer DMZ mit einem zweistufigen Firewall-Konzept. Eine schematische Darstellung zum Aufbau einer DMZ finden Sie im Kapitel Demilitarisierte Zone (DMZ).
4. Zwischen den UCServer Web Services und estos UCServer (Standard Port 7222) kann eine TCP Verbindung hergestellt werden. Das ist z. B. der Fall, wenn beide Dienste gemeinsam auf dem selben Betriebssystem installiert sind. Alternativ können Sie die Verbindung auch über den estos ProCall überprüfen.
5. Möchten Sie die Apps auf Ihrem mobilen Endgeräten oder ProCall for Mac® auch von Unterwegs aus nutzen, so müssen Sie sicherstellen, dass der Microsoft® Internet Information Services (IIS) aus dem Internet erreichbar ist. Lesen Sie hierzu das Kapitel Erreichbarkeit aus dem Internet (Demilitarisierte Zone (DMZ)). Wie Sie Ihren Router bzw. Ihre Firewall entsprechend konfigurieren, erfragen Sie bitte beim Hersteller der jeweiligen Systemkomponente.
6. Empfohlen: Um eine verschlüsselte Datenkommunikation zwischen ihren Clients und den UCServer Web Services aufbauen zu können, wird ein gültiges Serverzertifikat benötigt. Welche Anforderungen an ein solches Zertifikat bestehen, entnehmen Sie bitte dem Kapitel Server-Zertifikate.
7. Empfohlen: Deaktivieren Sie die Verwendung der mittlerweile als unsicher geltenden Verschlüsselungsprotokolle SSL v2 und SSL v3 und aktivieren Sie TLS. Details hierzu finden Sie im Kapitel Optimierung der Sicherheitseinstellungen im Microsoft® Internet Information Services (IIS).
8. Optional: Stellen Sie sicher, dass der Zielrechner eine Verbindung zum MetaDirectory aufbauen kann. Um Ihre Daten gegen externen Zugriff zu schützen, empfehlen wir dringend die Übertragung via LDAPs zu verschlüsseln. Voraussetzung hierfür ist eine MetaDirectory Professional-Lizenz.

2.3 Ausführen der Installation

estos UCServer Web Services werden als Setup Paket (.exe) im AddOns-Verzeichnis der estos UCServer Distribution ausgeliefert und müssen separat installiert werden. Führen Sie das Installationspaket (.exe) in der richtigen Sprache auf dem Zielsystem aus. Wir empfehlen dringend den Einsatz eines Server-Betriebssystems mit 64bit-Architektur.

Während der Installation werden alle notwendigen Komponenten des UCServer Web Services installiert. Nach Abschluss der Installation klicken Sie bitte auf "Fertigstellen". Der estos UCServer Web Services-Einrichtungsassistent startet automatisch im Anschluss an die Installation.

2.4 IIS benötigte Leistungsmerkmale

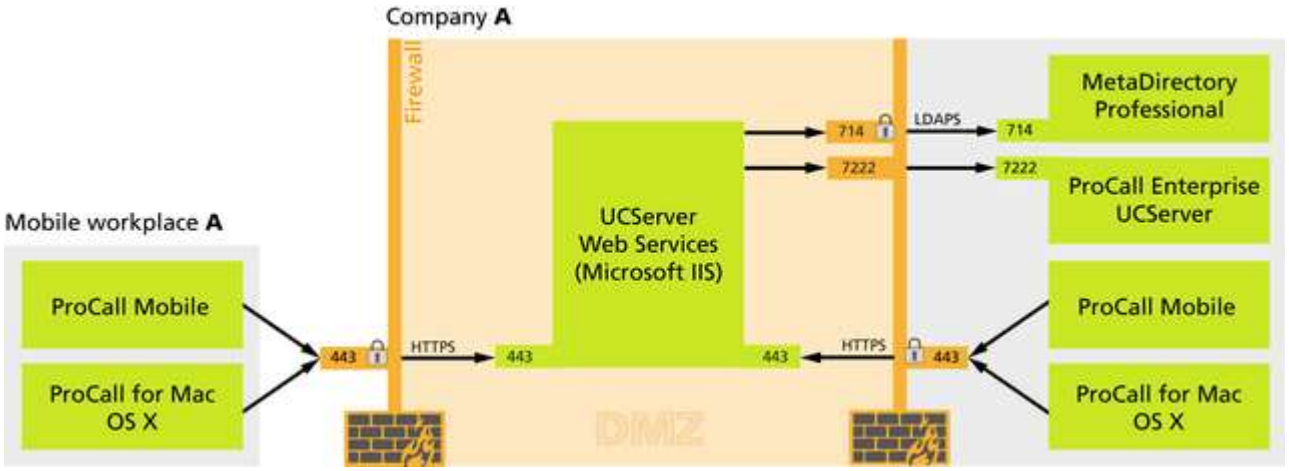
System	benötigte Leistungsmerkmale
Windows Server® 2008 R2 und alle anderen Systeme	IIS-WebServerRole, IIS-WebServer, IIS-StaticContent, IIS-DefaultDocument, IIS-HttpErrors, IIS-HttpRedirect, IIS-HealthAndDiagnostics, IIS-HttpLogging, IIS-HttpCompressionStatic, IIS-HttpCompressionDynamic, IIS-WebServerManagementTools, IIS-ManagementConsole, IIS-RequestFiltering
zusätzlich für Windows® Small Business	IIS-CommonHttpFeatures, IIS-DirectoryBrowsing, IIS-ApplicationDevelopment, IIS-ASP, IIS-CGI, IIS-ServerSideIncludes, IIS-RequestMonitor, IIS-HttpTracing, IIS-CustomLogging, IIS-ODBCLogging, IIS-Security, IIS-BasicAuthentication, IIS-IPSecurity, IIS-Performance, IIS-ManagementScriptingTools, IIS-ManagementService, IIS-IIS6ManagementCompatibility, IIS-Metabase, IIS-WMICompatibility, IIS-LegacyScripts,

Server 2011	IIS-LegacySnapIn, WAS-WindowsActivationService, WAS-ProcessModel, WAS-NetFxEnvironment, WAS-ConfigurationAPI
zusätzlich für Windows Server® 2012	NetFx4Extended-ASPNET45, IIS-NetFxExtensibility45, IIS-ISAPIExtensions, IIS-ISAPIFilter, IIS-ASPNET45, NetFx3ServerFeatures
zusätzlich für Windows Server® 2012 R2	NetFx4Extended-ASPNET45, IIS-NetFxExtensibility45, IIS-ApplicationDevelopment, IIS-ISAPIExtensions, IIS-ISAPIFilter, IIS-ASPNET45

2.5 Erreichbarkeit aus dem Internet (DMZ): Firewall-Konfiguration

Für die Nutzung von mobilen Endgeräten oder ProCall for Mac® von unterwegs über das Internet ohne ein Virtual Private Network (VPN) sind weitere Konfigurationsschritte in Ihrer IT-Infrastruktur notwendig. In der Verwaltung können diese Konfigurationsschritte nicht vorgenommen werden. Hier kann es z. B. notwendig sein, die Firewall Konfiguration Ihres Routers dahingehend zu ändern, dass Verbindungen aus dem Internet zu den UCServer Web Services weitergeleitet werden (port forwarding).

Um Ihre sensitiven Daten vor dem Zugriff durch Dritte zu schützen, empfehlen wir grundsätzlich, die UCServer Web Services auf einer separaten Einheit innerhalb einer DMZ mit einem zweistufigen Firewall-Konzept zu installieren. Nähere Informationen zur DMZ finden Sie auch http://en.wikipedia.org/wiki/DMZ_(computing).



Im Rahmen einer DMZ sind grundsätzlich folgende Ports zu konfigurieren um die estos UCServer Web Services zwar von extern (WAN) erreichbar zu machen, Ihr lokales Netzwerk (LAN) hingegen vor externem Zugriff zu schützen:

Ursprung	Ziel	Port	Protokoll	Richtung
extern / Smartphone	UCServer Web Services	443	HTTPs	inbound
UCServer Web Services	estos UCServer	7222	ASN1	inbound

UCServer Web Services	estos MetaDirectory (optional)	714	LDAPS	inbound

Als zusätzliche Sicherheitsmaßnahme empfehlen wir ferner in der Firewall zum internen Netzwerk hin nur die IP-Adresse des Rechners zuzulassen, auf dem die UCServer Web Services aktiv sind.

Nachdem Sie die DMZ und die jeweiligen Firewall-Einstellungen vorgenommen haben, sollten die UCServer Web Services von extern erreichbar sein.

	Die gemachten Angaben beziehen sich auf Standardporteinstellungen und können ggf. abweichen, wenn Sie diese manuell konfiguriert haben.
	Die zu konfigurierenden Ports von UCServer Web Services zum estos UCServer bzw. estos MetaDirectory werden zur internen Kommunikation verwendet und sollten nicht extern (Internet, WLAN) erreichbar sein.
	Den LDAPS-Port 714 müssen Sie nur bei der Verwendung von estos MetaDirectory freischalten.

2.6 Server-Zertifikate

Für die verschlüsselte Kommunikation über TLS (Transport Layer Security) wird ein Server-Zertifikat benötigt.

Server-Zertifikat:
Ein Server-Zertifikat dient zur eindeutigen Identifizierung eines Servers. Das Zertifikat muss von einer vertrauenswürdigen Instanz auf den FQDN (fully qualified domain name) des Servers ausgestellt sein. Der Client muss den Server über den FQDN kontaktieren, nicht über eine IP-Adresse.
Sollen die UCServer Web Services unter "https://services.company.net/ws/" bereitgestellt werden, muss das Zertifikat auch auf den FQDN "services.company.net" ausgestellt sein.

Zertifikat-Speicher:
Für einen korrekten Zugriff auf die benötigten Zertifikate, müssen diese auf dem entsprechenden Server im Speicher "Lokaler Computer" - "Eigene Zertifikate" abgelegt sein. Das Zertifikat muss einen privaten Schlüssel enthalten (zu erkennen am Schlüssel Symbol am Zertifikats Icon). Den Zertifikatspeicher "Lokaler Computer" öffnen Sie mit der MMC-Konsole.

- Aus dem Windows® Start Menü, wählen Sie *Ausführen...* und geben *mmc.exe* ein.
- Wählen Sie Datei - *SnapIn hinzufügen/entfernen...*
- Wählen Sie *Hinzufügen*. Aus der Liste der verfügbaren SnapIns wählen Sie *Zertifikate*. Wählen Sie *Computerkonto*, auf der folgenden Seite *Lokaler Computer* und klicken Sie Fertigstellen.
- In der Liste gehen Sie zu *Zertifikate (Lokaler Computer) - Eigene Zertifikate - Zertifikate*.

	Ein passendes Serverzertifikat erhalten Sie beispielsweise bei Verisign bzw. Thawte. Bevor Sie ein Zertifikat bestellen, empfehlen wir Ihnen, dies vorher zu testen. Viele Hersteller bieten Test-Zertifikate mit einem limitierten Testzeitraum an.

2.7 Optimierung der Sicherheitseinstellungen im Microsoft® Internet Information Services (IIS)

In den Grundeinstellungen verwendet der Microsoft® Internet Information Services (IIS), je nach zugrundeliegenden Betriebssystem, noch das SSL Verfahren in technisch überholten Versionen, welche als unsicher eingestuft werden müssen.

Um diese Einstellungen zu ändern, und TLS als aktuell sicher geltendes Protokoll zu aktivieren, verändern Sie am Host-System die nachfolgenden Registry-Werte:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Protocols]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Protocols\TLS 1.1]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Protocols\TLS 1.1\Client]
"DisabledByDefault"=dword:00000000
"Enabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Protocols\TLS 1.2]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Protocols\TLS 1.2\Client]
"Enabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHA
NNEL\Protocols\TLS 1.1\Server]
"Enabled"=dword:00000001
"DisabledByDefault"=dword:00000000
```

Sie können den abgebildeten Textblock speichern und über regedit in die Registry importieren.

Diese Einstellungen wirken ab Windows Server® 2008 R2 und Internet Information Services (IIS) 7.5. Nach dem Setzen der Registry-Werte muss das Betriebssystem neu gestartet werden. Bitte beachten Sie in diesem Zusammenhang auch den Microsoft® Knowledgebase Artikel unter http://support.microsoft.com/kb/245030.

Um die vom Server verwendeten Verschlüsselungsmethode zu prüfen kann der Internet Explorer® nach Anpassung folgender Einstellungen verwendet werden:
Systemsteuerung - Internetoptionen - Erweitert - Sicherheit
SSL 2.0/3.0 verwenden deaktivieren
TLS 1.2 verwenden aktivieren

Damit kann eine über https ausgelieferte Webseite nicht mehr über die unsicheren Technologien SSL2.0/3.0, sondern nur noch über TLS geöffnet werden.

Öffnen Sie anschließend in Ihrem Browser die Seite des estos UCServer Web Services unter der im Admin angegebenen URL.

2.8 Anmelde-Szenarien der Clients am estos UCServer Web Services

Damit sich Clients über die UCServer Web Services an einem UCServer anmelden können, sind neben dem Benutzernamen und dem Passwort die URL des UCServer Web Services anzugeben. Sind mehrere UCServer über einen UCServer Web Services erreichbar, muss in der Anmeldung der Servername des UCServer enthalten sein.

Die Client-Applikation bietet Ihnen hierzu drei Felder an:

- Servername: URL, über die estos UCServer Web Services erreichbar sind, z.B. https://services.company.net/ws/
- Benutzerkennung: Benutzerkennung zur Authentifizierung am UCServer
- Kennwort: Kennwort zur Authentifizierung am UCServer

Die Kombination aus Benutzerkennung und Passwort hängt von der Art der im UCServer konfigurierten Benutzeranmeldung ab. Der jeweilige Benutzername entspricht dem Inhalt des Feldes "Benutzername" der UCServer Benutzerverwaltung. Falls Sie mehr als einen estos UCServer konfiguriert haben, so müssen Sie ggf. zusätzlich dessen Servername im Login angeben.

	UCServer verwendet Benutzerverwaltung mit Active-Directory Server	UCServer verwendet die lokale Benutzerverwaltung
UCServer (als Default konfiguriert) oder einzig verwendeter UCServer	Login: muster.mann@company.local	Login: muster.mann
UCServer (nicht als Default konfiguriert)	Login: ucservername\muster.mann@company.local	Login: ucservername\muster.mann

2.8.1 Einfache Bereitstellung für estos ProCall Desktop Benutzer

Um Ihren Benutzern die Einrichtung der Mobilgeräte zu erleichtern können Sie alle notwendigen Informationen direkt in estos ProCall Desktop anzeigen lassen. Die Informationen werden hierbei sowohl im Klartext als auch in Form eines QR-Codes, der direkt mit der App eingescannt werden kann, bereitgestellt).
Erstellen Sie hierzu einen benutzerdefinierten "Tab" in der estos UCServer Verwaltung unter:
Konfiguration - Benutzerverwaltung - Profile (Profil auswählen) - Custom Tabs
Tragen Sie folgende Informationen ein:

Feld	Inhalt
Titel	Mobile
URL	<Öffentliche Adresse des UCServer Web Services>/Addons/Startup/ Beispiel: *https://services.company.net/ws/Addons/Startup/*

Internet Explorer® Sicherheitszonen deaktivieren	Ja (Haken setzen)

3 estos UCServer Web Services Verwaltung

Die estos UCServer Web Services Verwaltung unterteilt sich in die folgenden Bereiche

Bereich	Erläuterung
Übersicht	Überblick und Funktionsprüfung der wichtigsten Einstellungen
IIS Konfiguration	DNS-Name, IP-Adresse, Sicherheit, Zertifikate
UCServer	Über die UCServer Web Services erreichbare UCServer
Ereignisse	Protokollierung und Problemanalyse, Service-Support-Datei erzeugen
Angemeldete Benutzer	Liste aller Benutzer, die derzeit aktiv angemeldet sind.
Info über	Versionsinformationen

Weiterführende Informationen finden Sie auch im Kapitel Häufig gestellte Fragen.

3.1 Übersicht

In der Übersicht sehen Sie wesentlichen Einstellungen und Informationen über die Erreichbarkeit der UCServer Web Services.

Web Services
Zeigt Ihnen ob der Dienst läuft, über welche URL er erreichbar ist und ob Verbindung zum Dienst verschlüsselt sind. Sie können die Erreichbarkeit des UCServer Web Services aus dem Internet überprüfen lassen und den Dienst starten und stoppen.

UCServer
Zeigt die Liste der konfigurierten UCServer und ob diese aktuelle vom UCServer Web Services erreichet werden können. Eine Aktualisierung der Anzeige können Sie manuell über den Button *Prüfen* anstoßen.

3.2 IIS Konfiguration

Hier wird konfiguriert, wie die UCServer Web Services erreichbar sein soll. Diese Einstellungen führen zum entsprechenden Anlegen des UCServer Web Services Eintrages im Internet Information Service (IIS).

DNS-Name / IP-Adresse
Bitte geben Sie an dieser Stelle den DNS-Namen ein, über den die UCServer Web Services von extern erreichbar sein wird (Ohne vorangestellten Protokollheader http/https). Beispiel: *services.company.net*
Sollten Sie die UCServer Web Services nur intern nutzen, z.B. innerhalb eines Virtual Private Networks (VPN), so verwenden Sie den internen Namen des Zielrechners. Sollten Sie eine verschlüsselte Verbindung einrichten wollen, muss der hier angegebene DNS Namen mit dem Namen im Zertifikat übereinstimmen. Die Angabe einer IP-Adresse ist in Verbindung mit gewünschter Verschlüsselung nicht sinnvoll.

Virtuelles Verzeichnis
Die UCServer Web Services werden im Internet Information Service (IIS) unterhalb eines virtuellen Verzeichnisses bereitgestellt. Ein virtuelles Verzeichnis wird an die URL angehängt, die im Client für die Verbindung zur UCServer Web Services einzugeben ist (Beispielsweise: https://services.company.net/ws/ - ws entspricht dem virtuellen Verzeichnis). Eine Bereitstellung der UCServer Web Services im Root-Verzeichnis Ihrer Domain (z.B. https://services.company.net/) ist möglich, bedarf jedoch entsprechenden Kenntnissen.

Verbindungstyp
Definiert ob die UCServer Web Services über eine gesicherte verschlüsselte Verbindung (https:) erreichbar sein soll oder über eine unverschlüsselte (http:). Für eine verschlüsselte Verbindung benötigen Sie ein Server-Zertifikat. Details welche Anforderungen bezüglich des Zertifikates gelten, woher Sie dieses beziehen können und wie Sie dieses im System hinterlegen müssen sind im Kapitel Server-Zertifikate beschrieben.
Sie können den Port für http/https Verbindungen manuell verändern, wir empfehlen mit den Default Einstellungen zu arbeiten.

Serveradresse für Clients
Zeigt die URL, die in den Applikationen zum Zugriff auf die UCServer Web Services verwendet werden muss.

	Das Übernehmen der Einstellungen (Installation der Applikation im IIS) kann, abhängig von den im IIS bereits installierten Websites bzw. Applikationen, mehrere Minuten in Anspruch nehmen.
	Wir empfehlen dringend die Verwendung einer gesicherten Verbindung. Speziell wenn Sie über den UCServer Web Services den Nutzern Zugriff auf Kontaktdaten im Unternehmen ermöglichen sollte die Verbindung ausschließlich verschlüsselt aufgebaut werden.

3.3 UCServer

Tragen Sie hier die estos UCServer ein, die über die UCServer Web Services erreichbar sein sollen. Falls Sie mehrere UCServer verwenden, so muss einer als Standard-Server gekennzeichnet sein. Dieser Default-UCServer wird immer dann verwendet, wenn bei der Anmeldung kein UCServer angegeben wird.

Hinzufügen...
Über Hinzufügen können Sie einen weiteren Server in die Liste der UCServer aufnehmen.
Hierbei werden folgende Informationen abgefragt:

- UCServer:
  Geben Sie hier den DNS Namen oder die IP-Adresse des hinzuzufügenden Servers ein.
- Port:
  Geben Sie hier den Port ein über den der hinzuzufügende Server für ProCall Clients erreichbar ist. Default ist dies 7222.
- Domäne:
  Tragen Sie hier die Präsenzdomäne ein für die der hinzuzufügende Server zuständig ist. Über den Button *Domäne ermitteln* kann dies auch automatisch erfolgen.
- Diesen Server als Standard-Server verwenden
  Wenn bei der Anmeldung kein UCServer angegeben wurde wird dieser UCServer kontaktiert. Solange nur ein UCServer konfiguriert ist, bleibt diese Option dauerhaft aktiviert.

3.4 Ereignisse

Zur Analyse von Fehlermeldungen oder unerwartetem Verhalten kann die Protokollierung der UCServer Web Services angepasst werden.

Falls Probleme mit den UCServer Web Services auftreten sollten, können Sie hier eine ZIP-Archiv (Support-Datei) mit allen Informationen zur weiteren Analyse des Sachverhalts erstellen. Zudem haben Sie die Möglichkeit, die Protokolldateien manuell zu löschen, um konkrete Fehlerszenarien zu protokollieren.

3.5 Angemeldete Benutzer

Zeigt welche Nutzer aktuell am UCServer Web Services angemeldet sind und mit welchem UCServer diese verbunden wurden. Die Anzeige aktualisiert sich nicht automatisch, sie kann aber manuell über den Button *Aktualisieren* angestoßen werden.

4 Häufig gestellte Fragen

In diesem Abschnitt finden Sie Antworten auf häufig gestellte Fragen sowie Hinweise zu funktionalen Einschränkungen.

Wir haben für Sie auch Hinweise für den Anmeldeprozess zusammengestellt.

4.1 Fehlermeldung im Browser bei der Erreichbarkeitsprüfung: "Die Website kann nicht angezeigt werden"

	Erläuterung
Problembeschreibung	Nach der Installation und Konfiguration möchten Sie in der UCServer Web Services-Verwaltung die Erreichbarkeit überprüfen. Dazu klicken Sie auf den angezeigten Link, worauf sich ein Browserfenster öffnet mit der Bitte um Benutzername/Passwort. Nach erfolgter Authentifizierung wird die Meldung "Die Website kann nicht angezeigt werden" ausgeliefert.
Hintergrund	• Die UCServer Web Services Website konnte nach der Installation nicht gestartet werden, da der angegebene Port z.B. durch eine andere Applikation verwendet wird. Dies ist häufig der Fall wenn Sie den Webserver des MetaDirectory nutzen, der standardmäßig auf Port 80 lauscht. Die Folge ist, dass die Website, unter der der UCServer Web Services installiert ist, nicht gestartet werden konnte. • Für einen bereits im Vorfeld installierten IIS wurde die anonyme Authentifizierung nicht aktiviert. Dies führt dazu, dass der IIS selbst versucht, mit den angegeben Benutzerinformationen eine Authorisierung vorzunehmen, was fehlschlagen muss.
Lösungsansatz	Überprüfen Sie zunächst in der IIS-Verwaltung, ob die anonyme Authentifizierung für die Website und Applikation aktiviert ist. Falls das Problem immer noch auftritt, ändern Sie zunächst den Port des UCServer Web Services durch erneutes Installieren und Ausführen des Konfigurationsassistenten bzw. durch manuelles Konfigurieren im IIS (Änderung der Port-Bindung). Anschließend sollten Sie in der Lage sein, die entsprechende Website zu starten und die Erreichbarkeitsprüfung zu wiederholen.

4.2 Fehlermeldung im Browser bei der Erreichbarkeitsprüfung: "502 Bad Gateway"

	Erläuterung
Problembeschreibung	Nach der Installation und Konfiguration möchten Sie in der UCServer Web Services-Verwaltung die Erreichbarkeit überprüfen. Dazu klicken Sie auf den angezeigten Link, worauf sich ein Browserfenster öffnet mit der Bitte um Benutzername/Passwort. Nach erfolgter Authentifizierung wird die Meldung "502 Bad Gateway" ausgeliefert.

Hintergrund	Die ausgelieferte Fehlermeldung deutet darauf hin, dass der estos UCServer vom UCServer Web Services nicht erreicht werden kann oder keine entsprechenden Lizenzen zur Verfügung stehen.
Lösungsansatz	Bitte prüfen Sie zunächst, ob Sie den entsprechenden UCServer von dem Rechner aus erreichen können, auf dem die UCServer Web Services installiert sind. Dies können Sie beispielsweise durch Installation und Konfiguration eines estos ProCall verifizieren. Alternativ besteht die Möglichkeit, eine Erreichbarkeitsprüfung via telnet auf dem konfigurierten Port durchzuführen. Wenn Sie nicht vom Standard abgewichen sind, lautet das Kommando beispielsweise telnet serverName 7222. Alternativ können Sie auch mit der IP-Adresse Ihres UCServer arbeiten, um ein Problem bei der DNS-Auflösung des Namens auszuschließen. Bitte geben Sie diese in der UCServer Web Services Verwaltung im Reiter "Konfiguration" unter UCServer ein und wiederholen die Prüfung via Webbrowser, nachdem Sie die Einstellungen übernommen haben.

4.3 Fehlende Kontakte bzw. es werden keine MetaDirectory Datensätze angezeigt

	Erläuterung
Problembeschreibung	Die Suche auf dem angeschlossenen Client liefert weniger Treffer als die gleiche Suchanfrage auf meinem Desktop-Client. Suchergebnisse aus dem MetaDirectory werden nicht angezeigt.
Hintergrund	Für die Anbindung des MetaDirectory an den UCServer Web Services benötigen Sie mindestens MetaDirectory 3.5 oder höher.
Lösungsansatz	Bitte prüfen Sie die Versionsnummer Ihres MetaDirectory und laden sich gegebenenfalls die aktuellste Version auf unserer Website (http://www.estos.de/) herunter.

4.4 Geplante Anrufe werden in den Client-Applikation nicht angezeigt

	Erläuterung
Problembeschreibung	Obwohl in Ihrem estos ProCall Desktop-Client geplante Anrufe hinterlegt sind, werden diese in der Client-Applikation nicht angezeigt.
Hintergrund	Wird für die Planung von Anrufen Microsoft Outlook® und nicht der estos UCServer genutzt (Einstellung in estos ProCall), so werden geplante Anrufe nicht an den UCServer weitergeleitet. Da die Client-Applikation jedoch mit dem UCServer kommuniziert und nicht mit dem lokalen estos ProCall, werden keine geplanten Anrufe im Client angezeigt.

Lösungsansatz	Stellen Sie die Verwaltung von geplanten Anrufen in Ihrem Desktop-Client auf UCServer um.

4.5 Eine Kontaktsuche im Client, die u.a. Umlaute (z.B. ä ö ü) enthält, führt zu einem Verbindungsfehler

	Erläuterung
Problembeschreibung	Sie verwenden als Firewall ein Threat Management Gateway der Firma Microsoft®. Eine Kontaktsuche aus dem Client, die u.a. Umlaute enthält, führt zu folgender Fehlermeldung: "Verbindungsfehler! Bitte prüfen Sie Ihre Internetverbindung und versuchen Sie es erneut!"
Hintergrund	Der Suchbegriff wird bei einer Suchanfrage über die URL übergeben. Alle Sonderzeichen, insbesondere auch deutsche Umlaute, werden dort "URL-encoded". Wird als Firewall ein Threat Management Gateway der Firma Microsoft® eingesetzt (siehe hierzu auch http://www.microsoft.com/TMG), kann dies zur oben genannten Fehlermeldung führen, wenn die Konfigurationseinstellung der Firewall "HighByte-Zeichen" innerhalb der URL verbietet. Durch diese Einstellung wird jegliche Weiterverarbeitung mit einem Http-Result 500 abgelehnt.
Lösungsansatz	Deaktivieren Sie innerhalb Ihrer Microsoft® TMG Firewall die Option "Block high-bit characters".

4.6 Funktionale Einschränkungen

Beim Betrieb des estos UCServer Web Services in Verbindung mit Smartphones (iOS bzw. Android-Geräten) bestehen folgende funktionale Einschränkungen:

iOS	Android	Erläuterung
X	-	Da es technisch in iOS keine Möglichkeit gibt, innerhalb einer App auf die Telefonie-Ereignisse des iPhones zugreifen zu können, ist die Signalisierung *busy in a call* im estos ProCall derzeit nicht möglich, d.h. obwohl der Nutzer auf seinem mobilen Endgerät telefoniert, erscheint dieser in der Kontaktliste am Desktop Client als *verfügbar*.
X	X	Die Konfiguration und Anzeige von geplanten Anrufen funktioniert nur, wenn Sie diese innerhalb des estos UCServer und nicht in Microsoft Outlook® verwalten.
X	X	Derzeit ist es nur möglich, mit Kontakten zu chatten, die sich in den eigenen Favoriten befinden. Einen Chat starten aus der Suchergebnis-Liste heraus wird nicht unterstützt.

5 Info über estos UCServer Web Services

Die estos UCServer Web Services sind ein Produkt der estos GmbH.

Produkt Updates finden Sie unter http://www.estos.de/

Häufig gestellte Fragen und Antworten, sowie Support erhalten Sie unter http://support.estos.de