

# estos UCServer Web Services

---

5.1.50.44786

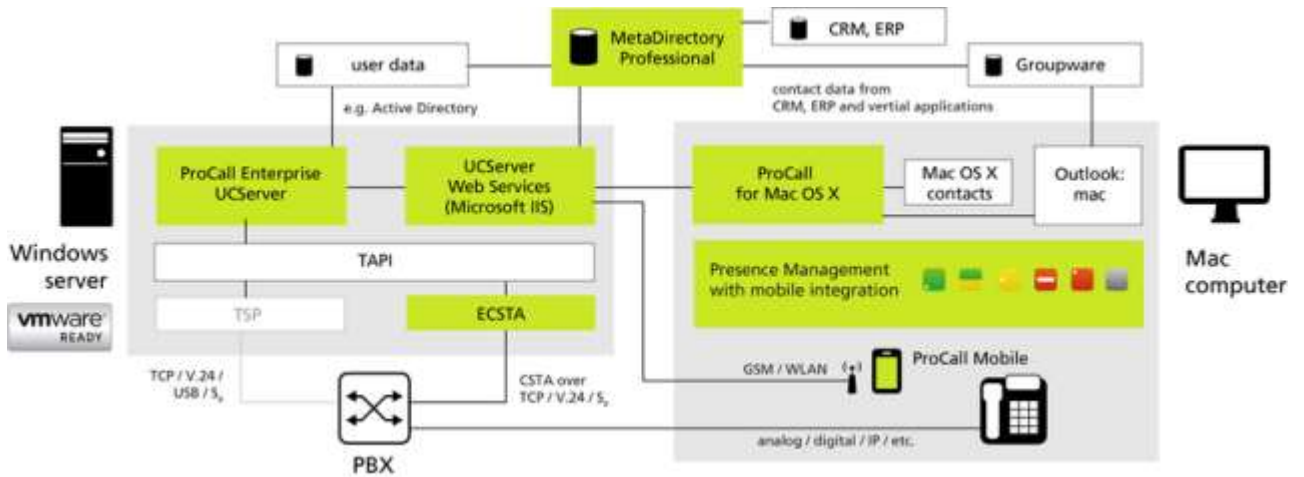
1	Welcome to estos UCServer Web Services .....	4
2	estos UCServer Web Services - Installation .....	5
2.1	System requirements.....	5
2.1.1	Hardware.....	5
2.1.2	Software.....	5
2.1.3	Environment.....	5
2.1.4	Required Knowledge.....	5
2.2	Preparation for installation.....	5
2.3	Performing the Installation .....	6
2.4	IISrequired features .....	6
2.5	Accessibility from the Internet (DMZ): Firewall Configuration .....	7
2.6	Server certificates .....	8
2.7	Optimizing the security settings in Microsoft® Internet Information Server (IIS) .....	8
2.8	Client scenarios for logging into estos UCServer Web Services .....	9
2.8.1	Simplified provision for estos ProCall desktop users.....	10
3	estos UCServer Web Services Administration .....	11
3.1	Overview.....	11
3.2	IISConfiguration.....	11
3.3	UCServer.....	12
3.4	Events.....	12
3.5	Active users .....	13
4	Frequently Asked Questions.....	14
4.1	An error message in the browser when testing accessibility: The web site cannot be displayed. ....	14
4.2	An error message in the browser when testing accessibility: 502 bad gateway.....	14
4.3	Contacts are missing or MetaDirectory records are not displayed .....	15
4.4	Scheduled calls are not displayed in the client application.....	15
4.5	A search for contacts that contain special characters (such as the umlauts: ä, ö or ü) from the client leads to a connection error.....	15
4.6	Functional Limitations.....	16
5	Info about estos UCServer Web Services .....	17



# 1 Welcome to estos UCServer Web Services

For a quick successful installation please read the instructions for installing.



The UCServer Web Services provide an Internet-compatible interface for the clients of a estos UCServer . The service can be seen as a link between UCServer and mobile devices as well as of ProCall for Mac® .



This help guides you through the installation and configuration of UCServer Web Services.

- How to install the estos UCServer Web Services, learn Installation chapter.
- The individual settings pages of estos UCServer Web Services management are described in the section settings.

In this help, the following symbols are used:

Symbol	meaning
	hint
	caution
	Changes from previous versions

## 2 estos UCServer Web Services - Installation

### 2.1 System requirements

#### 2.1.1 Hardware

- PC 2 GHz
- 2 GB RAM
- 75 MB free hard disk space, additional required some disk space for log files

#### 2.1.2 Software

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



Installation on a non-server operating system, for example. Windows® Vista, Windows® 7 or Windows® 8 is not supported. estos UCServer Web Services is installed on a non-server operating system, it comes from a small number of concurrent users to disconnections for Microsoft® Internet Information Services (IIS). This is a technical limitation of the Microsoft® Internet Information Services (IIS) on non-server operating systems.

#### 2.1.3 Environment

- Microsoft® .NET Framework version 4 (full edition). The full download package is available from Microsoft®: (<http://www.microsoft.com/en-US/download/details.aspx?id=17718>)
- Microsoft® Internet Information Server (IIS) version 7 or newer
- Network connection to estos UCServer
- (optional) estos MetaDirectory (professional edition) version 3.5 or newer

#### 2.1.4 Required Knowledge

UCServer Web Services be installed inside the Microsoft® Internet Information Services (IIS) of a Microsoft® server operating system and provides applications with a secure interface via open standard protocols for communication with the estos UCServer.

Upon installation, the Microsoft® Internet Information Services (IIS) is set up so that the UCServer Web Services is only available to applications from the company network. In order to install and operate the UCServer Web Services you will need to be familiar with how to:

- Firewall configuration
- Installing and Configuring the Microsoft® Internet Information Services (IIS) on Windows Server® operating systems
- Create and configure SSL certificates to encrypt communications

## 2.2 Preparation for installation

Please check the following points before installation:

1. Make sure that the latest operating system updates are installed on the target system.
2. estos UCServer is installed and started.

3. For a safer use of UCServer Web Services and your internal data (LAN) to protect against unauthorized external access, we recommend setting up a DMZ with a two-stage firewall concept. A schematic representation of the DMZ structure is available in chapter demilitarized zone (DMZ).
4. Between UCServer Web Services and estos UCServer (default port 7222), a TCP connection can be established. Alternatively, you can check the connection via the estos ProCall.
5. For using the apps on your mobile devices or ProCall for Mac® outside LAN environment, so you must make sure that the Microsoft® Internet Information Services (IIS) is accessible on the Internet. Refer to the chapter accessible on the internet (demilitarized zone (DMZ). How to configure your router or your firewall accordingly, please contact the manufacturer of the system component.
6. Recommended: To establish an encrypted communication between their clients and the UCServer Web Services, a valid server certificate is required. Please check the requirements for such a certificate and refer to section server certificates.
7. Recommended: Disable the use of the now considered to be insecure encryption protocols SSL v2 and SSL v3 and enable TLS. For details, refer to the chapter optimize the security settings in Microsoft® Internet Information Services (IIS).
8. Optional: Make sure that the target machine can connect to MetaDirectory. To protect your data against external access, we strongly recommend encrypted data transmission via LDAPs. This requires an MetaDirectory Professional license.

### 2.3 Performing the Installation

estos UCServer Web Services be delivered as a setup package (.exe) in the AddOns directory of estos UCServer distribution and must be installed separately. Run the installation package (.exe) in the right language on the target system. We strongly recommend the use of a server operating system with 64 bit architecture.

During installation, all necessary components of the UCServer Web Services will be installed. After installation is complete, click "Finish". The estos UCServer Web Services Setup Wizard starts automatically after the installation.

### 2.4 IIS required features

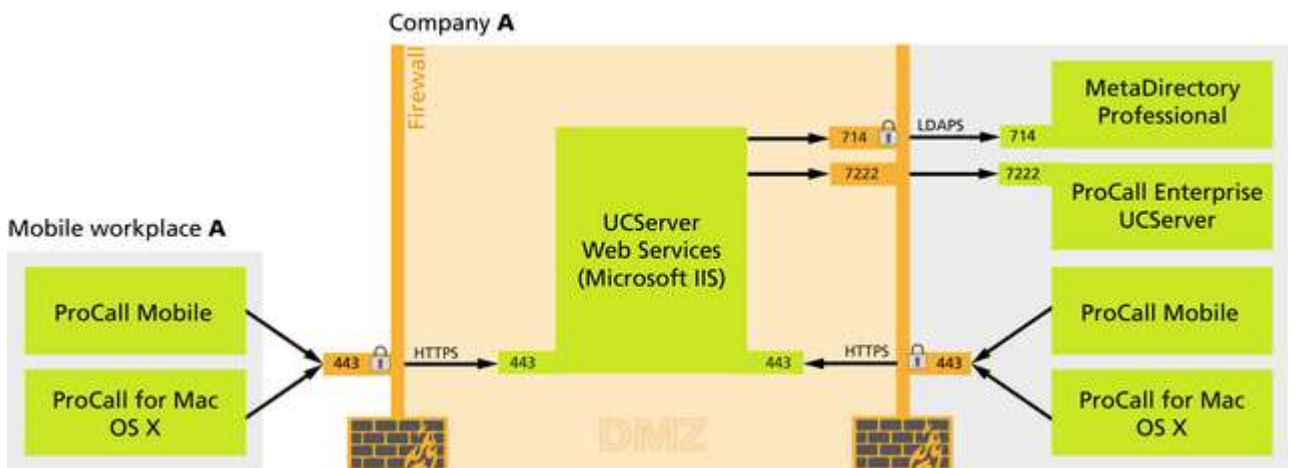
System	required Features
Windows Server® 2008 R2 and all other systems	IIS-WebServerRole, IIS-WebServer, IIS-StaticContent, IIS-DefaultDocument, IIS-HttpErrors, IIS-HttpRedirect, IIS-HealthAndDiagnostics, IIS-HttpLogging, IIS-HttpCompressionStatic, IIS-HttpCompressionDynamic, IIS-WebServerManagementTools, IIS-ManagementConsole, IIS-RequestFiltering
in addition to Windows® Small Business Server 2011	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, IIS-LegacySnapIn, WAS-WindowsActivationService, WAS-ProcessModel, WAS-NetFxEnvironment, WAS-ConfigurationAPI
in addition to Windows	NetFx4Extended-ASPNET45, IIS-NetFxExtensibility45, IIS-ISAPIExtensions, IIS-ISAPIFilter, IIS-ASPNET45, NetFx3ServerFeatures

Server® 2012	
in addition to Windows Server® 2012 R2	NetFx4Extended-ASPNET45, IIS-NetFxExtensibility45, IIS-ApplicationDevelopment, IIS-ISAPIExtensions, IIS-ISAPIFilter, IIS-ASPNET45

## 2.5 Accessibility from the Internet (DMZ): Firewall Configuration

Additional configuration steps in your IT infrastructure will be necessary for the use of mobile devices or ProCall for Mac® on the road through the Internet without a Virtual Private Network (VPN). These configuration steps cannot be taken from the Administration tool. To do this, it may be necessary, for example, to make changes to the configuration of your firewall, so that connections from the Internet will be forwarded to UCServer Web Services.

To protect your sensitive data against access by third parties, we recommend that you install UCServer Web Services on a separate unit inside of a DMZ with a two-layer firewall concept in principle. You will also find more detailed information at [http://en.wikipedia.org/wiki/DMZ\\_\(computing\)](http://en.wikipedia.org/wiki/DMZ_(computing)).






The following ports should be configured as part of a DMZ in principle, in order to make estos UCServer Web Services accessible from external networks (WAN), while protecting your Local Area Network (LAN) in contrast against external access.

Source	Target	Port	Protocol	Direction
External or Smart Phone	UCServer Web Services	443	HTTPS	Inbound
UCServer Web Services	estos UCServer	7222	ASN1	Inbound
UCServer Web Services	estos MetaDirectory (optional)	714	LDAPS	Inbound

As an additional security measure, we further recommend only allowing the IP address of the computer that is running UCServer Web Services through the firewall for the internal network.

Once you have made the DMZ settings and the respective firewall settings, UCServer Web Services should be accessible from outside of the network.

	The entries made are related to the default port settings and may deviate as needed, when you have configured them manually.
	The ports from UCServer Web Services to estos UCServer and estos MetaDirectory to be configured will be used for internal communication and should not be accessible from outside of the network (Internet or WLAN).
	You will only have to release Port 714 for LDAPS when using estos MetaDirectory.

## 2.6 Server certificates

A server certificate is required for encrypted communication via TLS (Transport Layer Security).

Server certificate:


A server certificate serves to uniquely identify a server. The certificate must be issued to the Fully Qualified Domain Name (FQDN) of the server by a trusted authority. The client must contact the server through the FQDN, not through an IP address.

If UCServer Web Services should be provided from "https://services.company.com/ws/", the certificate must also have been issued for the "services.company.com" FQDN.

Certificate storage:

The certificates used must be stored under Local Computer/Own Certificates and contain a private key. The Local Computer certificate store can be opened with the MMC console.

- Select *Run...* from the Windows® Start Menu and enter *mmc.exe*.
- Select: File - *Add/Remove SnapIn...*
- Click the *Add* button. Then, select *Certificates* from the list of available snap-ins. Select *Computer account* on the subsequent *Local computer* tab and click the *Finish* button.
- Select the *Certificates (Local Computer)*, *Personal* and *Certificates* nodes in the treeview.

	You can receive an appropriate server certificate, for example, from Verisign or Thawte. Before ordering a certificate, we recommend that you test this in advance. Many manufacturers provide test certificates with a limited test period.
---	--

## 2.7 Optimizing the security settings in Microsoft® Internet Information Server (IIS)

Depending on the version of the underlying operating system, Microsoft® Internet Information Server (IIS) still uses versions of the SSL procedure that have been deprecated by later versions and must be categorized as insecure in the default settings.

Change the following registry values on the host system in order to change these settings and enable TLS as the protocol currently considered as secure.



```

REGEDIT4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]

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

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

The depicted text blocks can be saved and imported into the registry using RegEdit.

These settings will work from Windows Server® 2008 R2 and Internet Information Server (IIS) 7.5. Once the registry values have been set, the operating will have to be re-booted. In this context, also read the Microsoft® Knowledgebase Article at <http://support.microsoft.com/kb/245030>.

To verify the encryption method used by the server, the Internet Explorer® can be used after adapting the following settings:

*Control Panel - Internet Options - Advanced - Security*  
 Use SSL 2.0/3.0 Disable  
 Use TLS 1.2 Enable

With these changes, a web page delivered by HTTPS can no longer be opened using the insecure SSL2.0 & 3.0 protocols, but rather only using TLS.

Afterwards, open the estos UCServer Web Services page using the URL specified in the Administrator in your browser.

## 2.8 Client scenarios for logging into estos UCServer Web Services

So that clients can log into a UCServer system using UCServer Web Services, the UCServer Web Services URL must be specified in addition to the user name and password. If several UCServer systems can be accessed through one UCServer Web Services system, the UCServer server name must be contained in the login information.

The client application will provide you with three fields for this:

- Server name: The URL through which estos UCServer Web Services can be accessed, such as: <https://services.company.com/ws/>
- User name: The user name for UCServer authentication
- Password: The password for UCServer authentication

The combination of user name and password will depend on the user login type configured on the UCServer system. The respective user name will correspond to the content of the User Name field in the UCServer user management. If you have configured more than one estos UCServer system, you will also have to specify its server name during login as needed.

	UCServer uses the Active Directory® Server user management system	UCServer uses the local user management system
UCServer (configured as the Default) or the only UCServer in use	Login: muster.mann@company.local	Login: muster.mann
UCServer (not configured as the default)	Login: ucservername\muster.mann@company.local	Login: ucservername\muster.mann

### 2.8.1 Simplified provision for estos ProCall desktop users

You can permit all necessary information to be displayed directly on the estos ProCall desktop to make setting up mobile devices easier for your users. The information will be provided both as plain text as well as in the form of a QR codes, which can be scanned directly using the app). To do this, create a user-defined tab on the estos UCServer Administrator dialog:

*Configuration - User Management - Profile (choose the profile) - Custom Tabs*

Enter the following information:

Field	Content
Title	Cell phone
URL	<UCServer Web Services's public address>/Addons/Startup/ Example: <a href="https://services.company.com/ws/Addons/Startup/">https://services.company.com/ws/Addons/Startup/</a>
Disabling Internet Explorer® security zones	Yes (check)

### 3 estos UCServer Web Services Administration

The estos UCServer Web Services Administration system is divided into the following sections

Area	Explanation
Overview	Overview and Function Check of the Most Important Settings
IIS Configuration	DNS Name, IP Address, Security and Certificates
UCServer	UCServer that can be accessed through UCServer Web Services
Events	Logging and Problem Analysis, Creating the Service Support file
Active users	A list of all users currently actively logged in.
About	Version Information

You will also find additional information in the Frequently Asked Questions.

#### 3.1 Overview

You will see the significant settings and information about the accessibility of UCServer Web Services on the overview.

##### Web Services

Will indicate if the service is running, the URL to use for access and if the connection with the service is encrypted. You can let accessibility to UCServer Web Services be checked from the Internet and start and stop the service.

##### UCServer

Displays the list of the configured UCServers and if they can currently be accessed from UCServer Web Services. You can manually update the display by clicking the *Check* button.

#### 3.2 IIS Configuration

How UCServer Web Services should be accessed can be configured from here. These settings will lead to the creation of a UCServer Web Services entry in Internet Information Server (IIS).

##### DNS Name & IP Address

Enter the DNS name here, through which UCServer Web Services will be accessible from outside the network (without a prefixed protocol header, such as http/https). Example: *services.company.com* If you use the UCServer Web Services only internally, for example, within a Virtual Private Networks (VPN), use the internal name of the target computer. If you want to set up an encrypted connection, the DNS specified here must match code name with the name of the certificate. Specifying an IP address is not useful in conjunction with the desired encryption.

##### Virtual Directory

UCServer Web Services will be provided by Internet Information Server (IIS) using a virtual directory. A virtual



directory will be attached to the URL, which must be entered in the client for connection with UCServer Web Services (For example: <https://services.company.com/ws/> where: ws corresponds to the virtual directory). UCServer Web Services can be provided in your domain's root directory (such as: <https://services.company.net/>), however requires corresponding knowledge.

#### Type of Connection

Defines if UCServer Web Services should be accessed using a secure, encrypted connection (https:) or using an unencrypted connection (http:). You will need a server certificate for an encrypted connection. Details about the requirements regarding the certificate that will apply, where you can get the certificate and how you must store the certificate in the system will be described in the Server Certificate section. You can manually change the port for http & https connections. We recommend working with the default settings.

#### Server Address for Clients

Shows the URL that must be used for accessing UCServer Web Services.

	Depending on the web sites and applications already installed in IIS, accepting the settings (Application Installation in IIS) take several minutes.
	We highly recommend using a secured connection. Especially when you permit users access to company contact information through UCServer Web Services, the connection should be setup exclusively in encrypted mode.

### 3.3 UCServer

Enter the estos UCServer that should be accessible through UCServer Web Services. If you are using several UCServer systems, one will have to be set as the default server. This default UCServer will always be used if a UCServer is not specified for Login.

Add...

You can add additional servers to the list of UCServer systems by clicking Add. The following information will be request for this.

- UCServer:  
Enter the DNS name or the IP address for the server to be added.
- Port:  
Enter the port through which the server should be accessible to ProCall clients. The default is 7222.
- Domains:  
Enter the presence domain for which the server to add will be responsible. This can be done automatically by clicking the *Determine Domain* button.
- Use this server as the default server  
If a UCServer system was not specified during Login, this UCServer will be contacted. As long as only one UCServer has been configured, this option will remain permanently enabled.

### 3.4 Events

The UCServer Web Services log files can be adjusted for analysis of error messages or unexpected behavior.

If problems should arise with UCServer Web Services, you can create a ZIP archive (support file) with all of the information for further analysis of the behavior. In addition, you can delete the log files manually in order to log specific error scenarios.

### 3.5 Active users

Overview of the users active in UCServer Web Services and logged into UCServer. This information can be used, for example, to select an appropriate time for your maintenance work. The display does not update automatically, but it can be initiated manually via the *Update* button.

## 4 Frequently Asked Questions

You will find answers to frequently asked questions as well as note about Functional Limitations.

We have also collected notes about the Login Process.

### 4.1 An error message in the browser when testing accessibility: The web site cannot be displayed.

	Explanation
Description of the Problem	You will want to check accessibility from the UCServer Web Services Administration window after installation and configuration. To do so, click the displayed link, which will open a browser that will request a user name and password. The message, the web site cannot be displayed, is returned after successful authentication.
Reason	<ul style="list-style-type: none"> <li>The UCServer Web Services web site could not be started after installation, because the specified port may, example, be in use by another application. This is often the case, when you use the MetaDirectory web server, which listens to Port 80. As a consequence the web site where UCServer Web Services has been installed cannot be started.</li> <li>Anonymous authentication has not been enabled for an IIS system that was installed in advance. This will lead to IIS itself attempting authentication using the specified user information, which must fail.</li> </ul>
Solution	First, check if anonymous authentication has been enabled for the web site and the application in IIS Administration. If the problem continues to happen, first change the UCServer Web Services port by re-installing and running the configuration wizard or by manually configuring from IIS (change the port binding). You should finally be able to start the corresponding web site and repeat the accessibility test.

### 4.2 An error message in the browser when testing accessibility: 502 bad gateway.

	Explanation
Description of the Problem	You will want to check accessibility from the UCServer Web Services Administration window after installation and configuration. To do so, click the displayed link, which will open a browser that will request a user name and password. The message, 502 Bad Gateway, is returned after successful authentication.
Reason	The returned error message indicates that estos UCServer cannot be accessed from UCServer Web Services or that a corresponding license is not available.
Solution	First check if you can access the corresponding UCServer from the computer, where UCServer Web Services has been installed. For example, you can verify this by installing and configuring a estos ProCall. Alternatively, there is the option of testing accessibility

by using TelNet to access the configured port. If you have not deviated from the standard, the command would be: telnet servername 7222, for example. Alternatively, you can also use the IP address for your UCServer system in order to exclude a problem in the DNS resolution of the name. Enter this address from UCServer Web Services Administration on the Configuration tab under UCServer and repeat the test using a web browser, once you have accepted the settings.

#### 4.3 Contacts are missing or MetaDirectory records are not displayed

	Explanation
Description of the Problem	Searching the connected client returns fewer matches than the same query on my desktop client. Search results from MetaDirectory are not displayed.
Reason	You will need MetaDirectory 3.5 or later for integrating MetaDirectory into UCServer Web Services.
Solution	Check the version number for your MetaDirectory and download the most current version from our web site ( <a href="http://www.estos.de/">http://www.estos.de/</a> ).

#### 4.4 Scheduled calls are not displayed in the client application

	Explanation
Description of the Problem	Although scheduled calls have been saved in your estos ProCall desktop client, they are not displayed in the client application.
Reason	If you are using Microsoft Outlook® (user settings in the estos ProCall) instead of the estos UCServer to schedule calls, you will not be able to view your scheduled calls from within the client application. Your client application will use direct communication with UCServer instead of estos ProCall. Therefore UCServer could not manage your scheduled calls.
Solution	Change the management of scheduled calls in your desktop to UCServer.

#### 4.5 A search for contacts that contain special characters (such as the umlauts: ä, ö or ü) from the client leads to a connection error.

	Explanation
Description of the Problem	You are using a threat management gateway from Microsoft® as a firewall. Searches for contacts that contain special characters will lead to the following error message: Connection error: Please check your Internet connection and try again.

Reason	The search term is entered in a query via the URL. There, all special characters, including German umlauts, are "URL encoded". If you are using a Microsoft® Threat Management Gateway (TMG: <a href="http://www.microsoft.com/TMG">http://www.microsoft.com/TMG</a> ), this can lead to the indicated error message, if the configuration of the firewall forbids high-bit characters in URLs. That setting will cause any further processing to be rejected with a 500-range HTTP result.
Solution	Disable the Block High-bit Characters option in your Microsoft® TMG firewall.

## 4.6 Functional Limitations

When operating in conjunction with the estos UCServer Web Services smartphones (iOS or Android devices) has the following functional limitations:

iOS	Android	Explanation
X	-	Because iOS does not provide the technical ability to access an app from the iPhone's telephony events, the <i>Busy, in a Call</i> cannot be indicated in estos ProCall at this time. This means that, although the user is making a call with their mobile device, they will appear to be <i>available</i> in the desktop client's contact list.
X	X	Configuring and displaying scheduled calls will only work if you manage them from within estos UCServer and not from Microsoft Outlook®.
X	X	Currently, chats can only be conducted with contacts that are in the list of Favorites. Starting a chat with a contact from the search results list is supported.



## 5 Info about estos UCServer Web Services

estos UCServer Web Services are a product of estos GmbH.

Copyright (C) 2017 estos GmbH.

For product updates visit <http://www.estos.de/>

Frequently asked questions and answers, and for support navigate to <http://support.estos.de>

Mac® is either registered trademark or trademark of Apple Inc., registered in the U.S. and other countries.

Active Directory®, Internet Explorer®, Microsoft Outlook®, Microsoft®, Windows Server®, Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

MetaDirectory, ProCall are either registered products or products of estos GmbH in Germany and/or other countries.

All brands and product names used in this document are for identification purposes only and may be trademarks or registered trademarks of their respective owners.