

CaseCenter 2.9 Administrator's Guide

June 5, 2018 Rev. 1

CC29-AG-EN Rev1

For research and education uses only, not for use in diagnostic procedures.

Contents

Disclaimer	4
Character Types and Symbols	6
Terms and Abbreviations	7
1 Introduction	8
1.1 Structure of the CaseCenter	8
1.2 HUB	9
1.3 Service Unit	9
1.4 CaseCenter Network Diagram	9
1.5 CaseCenter Logical Network Configuration	10
1.6 CaseCenter Site Requirements	17
2 Folder hierarchy	18
2.1 Folder Color Markings	18
2.2 Folder Operations	
2.3 Special folders	23
3 Managing Users and Groups	24
3.1 User Levels	24
3.2 Add User or Group	26
3.3 Edit User or Group Data	27
3.4 Remove User or Group	29
3.5 LDAP Users and Groups	29
4 CaseCenter Lightweight Directory Access Protocol (LDAP) Implementation	31
4.1 LDAP user import	31
4.2 LDAP group import	33
4.3 LDAP user login and function	34
5 Login Queue and Automatic Logout	36
6 Service menu	38
6.1 Statistics	
6.2 Service Units	
6.3 Problematic slides	40
6.4 Slides in progress	40
6.5 Log	41

	6.6 HIS Log	41
	6.7 Enums	42
	6.8 Settings	43
	6.8.1 Basic Settings	43
	6.8.2 Pathonet settings	
	6.8.3 Database Settings	
	6.8.4 Network settings 6.8.5 SMTP settings	
	6.8.6 LDAP settings	
	6.9 Column customization	
	6.10 Database Backup	55
	6.11 Slide Transfer Queue	56
	6.12 Integration Settings	56
	6.13 Edit Report Template	57
7	Manage Service Units	58
	7.1 Add SU	58
	7.2 Edit SU	58
	7.3 Remove SU	FO
8	Manage Slides	
8		60
8	Manage Slides	60 60
8	Manage Slides 8.1 SU storage management 8.1.1 Add new storage 8.1.2 NAS storage usage	60 60 62 62
8	Manage Slides	60 60 62 62 63
8	Manage Slides	60 62 62 63 63
8	Manage Slides. 8.1 SU storage management. 8.1.1 Add new storage. 8.1.2 NAS storage usage. 8.1.3 DAS, SAN or local storage usage. 8.1.4 Storage editing. 8.1.5 Moving of slides to another Storage folder within the SU.	60 62 62 63 63 64
8	Manage Slides	60 62 62 63 63 64 64
8	Manage Slides. 8.1 SU storage management. 8.1.1 Add new storage. 8.1.2 NAS storage usage. 8.1.3 DAS, SAN or local storage usage. 8.1.4 Storage editing. 8.1.5 Moving of slides to another Storage folder within the SU. 8.1.6 Requirements and recommendations.	60 62 63 63 64 64 65
	Manage Slides. 8.1 SU storage management. 8.1.1 Add new storage. 8.1.2 NAS storage usage. 8.1.3 DAS, SAN or local storage usage. 8.1.4 Storage editing. 8.1.5 Moving of slides to another Storage folder within the SU. 8.1.6 Requirements and recommendations. 8.2 Scan to Server.	60 62 63 63 64 64 65 66
9	Manage Slides. 8.1 SU storage management. 8.1.1 Add new storage. 8.1.2 NAS storage usage. 8.1.3 DAS, SAN or local storage usage. 8.1.4 Storage editing. 8.1.5 Moving of slides to another Storage folder within the SU. 8.1.6 Requirements and recommendations. 8.2 Scan to Server. 8.3 Import slides.	60 62 63 63 64 64 65 65 66
9 10	Manage Slides. 8.1 SU storage management. 8.1.1 Add new storage. 8.1.2 NAS storage usage. 8.1.3 DAS, SAN or local storage usage. 8.1.4 Storage editing. 8.1.5 Moving of slides to another Storage folder within the SU. 8.1.6 Requirements and recommendations. 8.2 Scan to Server. 8.3 Import slides. Slide consistency checker, Lost and Found folder.	60 62 63 63 64 64 65 66 66 67
9 10 11	Manage Slides. 8.1 SU storage management. 8.1.1 Add new storage. 8.1.2 NAS storage usage. 8.1.3 DAS, SAN or local storage usage. 8.1.4 Storage editing. 8.1.5 Moving of slides to another Storage folder within the SU. 8.1.6 Requirements and recommendations. 8.2 Scan to Server. 8.3 Import slides. Slide consistency checker, Lost and Found folder. Secondary Service Unit.	60 62 63 63 64 64 65 66 66 67 69 70

Disclaimer

Copyright © 2001-2018 3DHISTECH Ltd. All Rights Reserved

Intellectual property related to the 3DHISTECH products are as follows:

EP 1,789,831; US 7,663,078; EP 2,024,772; JP 2009-512685; US 12/301,781; EP 1,644,767; JP 2007-516451; US7,327,515; EP 1,994,398; JP 2008-557835; US 12/281,566; U0700210; US 6,246,785; HU0900142; HU0700404; PCT/HU2007/000065; EP 08762668.5; US 12/663,537; PCT/AT2006/000492; JP 2008-542552; EP 06817469; US 12/095,545; PCT/AT2006/000493; EP 06817470.5; US 12/095,596; HU0900741; US 61/264,732; US 11/826,752; P0401870; PCT/IB2005/050344; US 11/662,976; HU0700409; US 12/042,050; US 77/636,144 and 007502032.

The above mentioned granted patents, granted utility model, registered trademarks, pending international and national patent applications and the other corresponding IP are the sole properties of the 3DHISTECH Ltd.

CAUTION

For research and education uses only, not for use in diagnostic procedures. This product has not been approved or cleared as a medical device by the U.S. Food and Drug Administration, nor any other regulatory authority. The data and images obtained or viewed using this product are not intended for clinical or diagnostic use.

For performance evaluation only, the performance characteristics of this product have not been established.

Further Information

For the latest information on 3DHISTECH products and services, please visit our website at: <u>http://www.3dhistech.com</u>.

Or contact the distributor:

Richard Allan Scientific Co. Subsidiary of Thermo Fisher Scientific 4481 Campus Drive Kalamazoo Mi 49008, USA US Toll Free 1(800) 522-7270

Tudor Road, Manor Park Runcorn, WA7 1TA United Kingdom +44 (0) 800 018 9396

+44 (0) 1928 534 000

Character Types and Symbols

Example	Abbreviation or term that is explained in section <u>Terms and Abbreviations</u> .
Example	Words or characters that appear on the screen. These include field names, screen titles, pushbuttons and menu names, paths or options.
	Keys on the keyboard. For example, function keys (such as F11) or the Ctrl+O key combination.
Example	Cross-references to other documents or sections within this document.
Warning! Indicates that you need an additional module to use the feature or the there are prerequisites for the task.	
Important!Contains an important piece of information or a recommendation. application will work if you choose not to follow the recommendati its performance might be less than optimal.	
() Tip!	Contains a suggestion about using the application in some other way or to some interesting purpose.

Terms and Abbreviations

Annotation	A particular detail of a digitized slide.
Host	User who uploaded the digital slide to CaseCenter and who initiates the Teleconsultation about the slide.
CaseCenter user group	Group created by a CaseCenter administrator.
LDAP	Lightweight Directory Access Protocol – an Internet protocol for accessing distributed directory services that act in accordance with X.500 data and service models.
OLDAP	OpenLDAP – open source implementation of the LDAP
Participant	User invited to participate in the evaluation of a slide stored on a CaseCenter server.
Teleconsultation	Provides access to digitized slides for several users and supports their collaboration in inspecting and evaluating the virtual slide.
Teleconsultation group	Group created by the Host for a Teleconsultation session independently of the user groups that exist on CaseCenter.
	Several Teleconsultation sessions (and therefore several Teleconsultation groups) can be activated on a CaseCenter server in parallel.
Telepathology	Teleconsultation in the field of pathology: pathologists exchange information and evaluate a slide together via Teleconsultation.

1 Introduction

The system supports the following two protocols for accessing the slides:

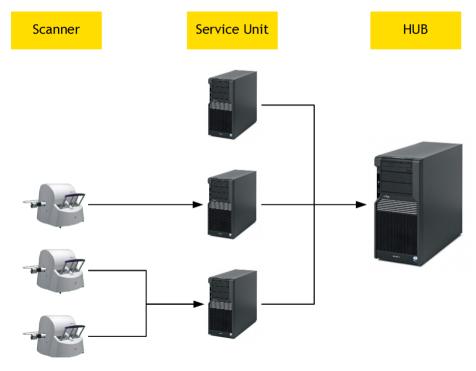
- 1. Microsoft Network protocol (SMB/CIFS), if the connection satisfies the standards below:
 - If using IPV4: <u>RFC 1918</u> standard, section <u>Private IPV4 address spaces</u>, or the IPs are different only in their class D addresses.
 - If using IPV6: <u>RFC 4193</u> standard, section <u>Unique local address</u>.
- 2. HTTP/HTTPS

Install the *scanner* – SU (as an external storage) – *client* within the same facility, and this order if possible, since the HTTP overhead can highly decrease the speed of scanning and communication.

It is recommended that you connect through HTTPS (HyperText Transfer Protocol over SSL) that is a TCP/IP protocol used by Web servers to transfer and display Web content securely. The data transferred is encrypted so that it cannot be read by anyone except the recipient.

1.1 Structure of the CaseCenter

CaseCenter is part of the 3DHISTECH and Thermofisher Scientific's product family that supports tasks in the educational or research workflow of pathologists. It is a platform for managing slides, cases, and other documentations. The figure below demonstrates how slides can be stored and managed on a designated CaseCenter server.



Important!

Operating system components in different time zones are not supported.

1.2 HUB

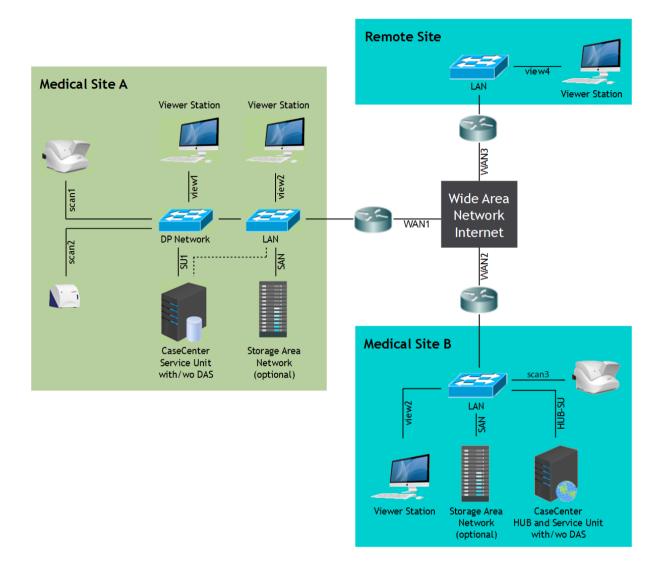
The HUB itself consists of two main parts: a database and the web surface. Database is for storing metadata of slides, the web surface is through which you can access and manage slide metadata. Accordingly, the **VIMMEET.EXE** application, which enables the usage of the Teleconsultation function, runs from the HUB as well.

1.3 Service Unit

A Service Unit (SU) is an element of CaseCenter where slides can be physically stored and slide processes take place. Storage can be added to the SUs on the network. Users who have registered on the server (registration is performed by the server administrator) can manage and use their slides on the server in the following ways:

- Upload slides or scan directly to the server.
- Arrange slides in folders, for example, group slides according to their staining types or your research projects.
- Share slides with other users who:
 - have account on the same CaseCenter (and can therefore access your slide on the server or if you share the slide with them explicitly)
 - can access the slide via E-School
 - are not registered CaseCenter users (Public Share Users), but can access publicly shared slides via a share URL
- Invite other users into *Teleconsultation* sessions to discuss slides.
- Participate in *Teleconsultation* sessions initiated by another user.
- Search for slides.

1.4 CaseCenter Network Diagram



1.5 CaseCenter Logical Network Configuration

This section describes the basic logical network configuration of CaseCenter digital slide manager server application in a typical network environment. It describes the simpler single site installation (all elements connected to the same LAN, and optionally some client components are connected from the public Internet) as well as geographically distributed multi site installation (more sites connected to each other through the public Internet).

Abbreviations used in this section:

HUB: Central component of the CaseCenter (hub, noun)

SU: Service Unit, Slide Storage and Slide Server component of the CaseCenter

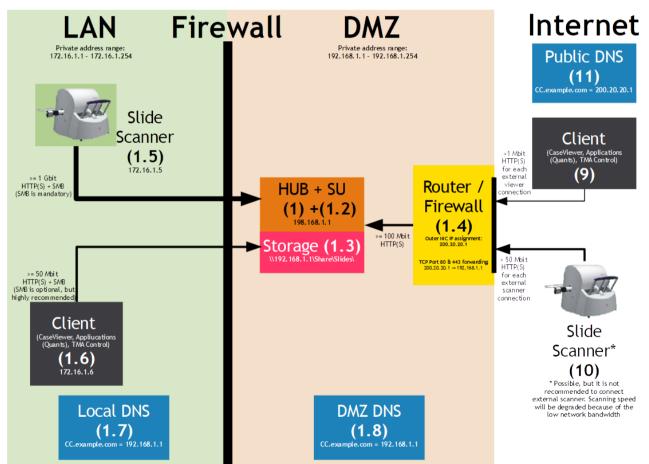
DNS: Domain Name Server

DMZ: Demilitarized Zone

FQDN: Fully Qualified Domain Name

Single site with public access

This use case enables to have access for digital slides stored in the CaseCenter from both the internal network (LAN) and optionally from the public Internet as well. The general network configuration is shown on the below figure.



CaseCenter is installed in the DMZ (or the LAN if no DMZ exists). The Router / Firewall (1.4) is configured to give HTTP(S) access to CaseCenter from the public Internet. The simplest way is to configure the Router / Firewall (1.4) to forward HTTP and / or HTTPS network traffic comes to the outer interface(s) of the device to the interfaces of the HUB (1) and SU(s) (1.2).

The Router / Firewall (1.4) has to forward the incoming traffic to the same TCP port of the internal servers. This means it has to forward the TCP 80 traffic (HTTP) to the port TCP 80 of the internal server(s) as well as the TCP 443 (HTTPS) traffic to the port TCP 443. No port cross forwarding is allowed (for example forward TCP 8080 to TCP 80).

To access digital slides stored in the CaseCenter clients must have access both the HUB (1) and SU(s) (1.2) because each SU does not only store slides but also serves directly them to the client (client has to be able to connect to all SUs). This requirement and the port forwarding requirement above imply that the Router / Firewall (1.4) should have as many public IP addresses as many internal servers exist. If the HUB (1) and the SU (1.2) components are installed on the same server only 1 public address is required.

If the HUB (1) and the SU (1.2) are installed on 2 different servers 2 public addresses are required. If CaseCenter has more than one SU components (each high performance scanner is highly recommended to be connected to a distinct SU) any further SU requires one more public IP address on the Router / Firewall (1.4). (Only one SU can be installed on the HUB server. Any further one should be installed on a separated server.). It is also required that any public IP address has to be assigned to a FQDN (Fully Qualified Domain Name).

Single scanner – single SU configuration

In the simplest case there is only one Slide Scanner (1.5) installed. This scanner requires only one SU (1.2). In this case the HUB (1) and the SU (1.2) could be installed on a single server. This single server might have an internal storage (a bunch of HDD configured as a RAID array) or might have attached an external storage (DAS or SAN). (The SU prefers DAS or SAN over NAS.). The Storage (1.3) is a SMB network share served by the underlying operating system of the single server.

Both of three components (HUB, SU and Storage) are accessible through one single IP address. In the Router / Firewall (1.4) there is only one public IP address and one FQDN is required. The HUB (1) and the SU (1.2) will be configured with this single FQDN. (There is no working solution to configure them with neither the private nor the public IP address. This setup *requires* FQDN.) This FQDN have to be configured in a public DNS to resolve it to the single public IP address of the Router / Firewall (1.4). This enables for the Client (9) to access the HUB (1) and the SU (1.2) – through the Router / Firewall (1.4) – from the public Internet. Client (9) need not have access to the Storage (1.3). This client will have access for the digital slides through the SU. Client (1.6) resides on the LAN should have access for the HUB (1), the SU (1.2) and the Storage (1.3). There should be a Local DNS (1.7) in the LAN and might be a DMZ DNS (1.8) in the DMZ which resolve the FQDN to the local IP of the single server. This resolution enables for LAN clients (Slide Scanner (1.5) and Client (1.6)) to have direct access to the HUB (1) and the SU (1.2).

This configuration can serve further lower throughput scanners, for example Pannoramic Desk, Midi or Confocal.

Multiple high-throughput scanners – multiple SU configuration

In this more demand case there are two or more high throughput Slide Scanners (1.5) installed in the local LAN. Each high throughput scanner requires one separated SU (1.2). In this case the HUB (1) and one of the SU (1.2) could be installed on a single server. Any further SU (1.2) have to be installed on a separated server. All servers might have an internal storage (a bunch of HDD configured as a RAID array) or might have attached an external storage (DAS or SAN). (The SU prefers DAS or SAN over NAS.). In the case of shared external storage the high I/O demand should be considered. All SU will have an own Storage (1.3) which is a SMB network share served by the underlying operating system of each SU server.

In this case there are number N servers exist, where N is the number of high throughput scanners as well as the number of SUs and storages. Each server will have a private IP address and an FQDN (summary number N FDQN together with one public IP address for each).

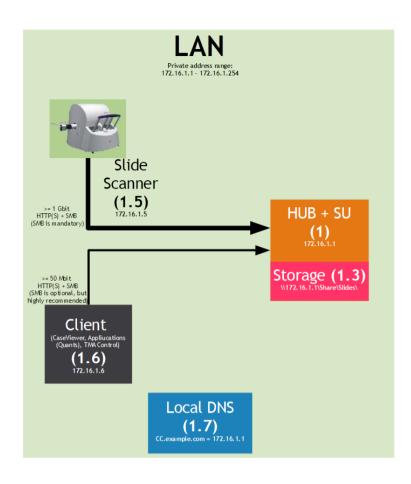
All of these public IP addresses have to be assigned for the outer interface of the Router / Firewall (1.4), and all FQDN have to be registered in a public DNS.

Each client (either it resides in the local LAN (1.6) or the public Internet (9)) should have access for the HUB (1) as well as all of existing SUs. For LAN (1.6) clients should also have access to all Storages (1.3).

Any further configuration is similar to the Single scanner – Single SU configuration.

Single site without public and VPN access

This use case enables to have access for digital slides stored in the CaseCenter only from the internal network (LAN). No slide access available from outside of the LAN. This use case also has same subcases as described in "Single site with public access" section. This use case has similar network configuration as described in "Single site with public access" section. This modified configuration is shown on the below figure.



There is no need to have DMZ and internal firewall between the LAN and the DMZ as well. All servers might be installed in the LAN and all clients can have direct access to them. (If the local IT policy requires, servers can be installed in a DMZ or behind a local firewall.) These restrictions enable not to have public IP addresses as well FQDN(s). Without FQDN, no DNS needed. CaseCenter components (HUB and SU(s)) could be configured with private IP addresses.

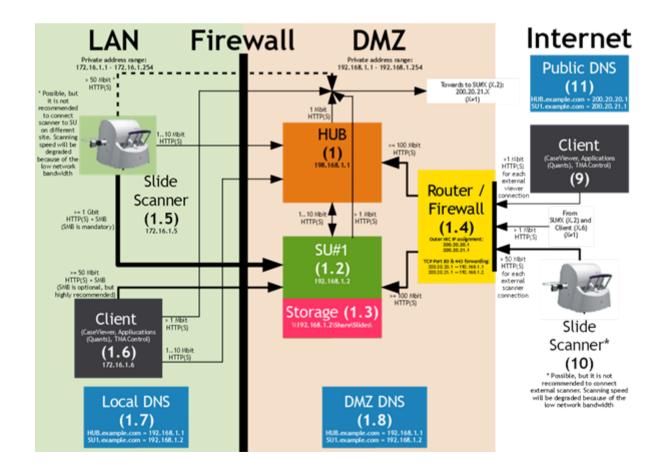
Single site with VPN access and without public access

This use case enables to have access for digital slides stored in the CaseCenter only from the internal network (LAN) and from the public Internet through VPN. No slide access available from outside of the LAN and the VPN. This use case also has same sub-cases as described in "Single site with public access" section.

Because of the VPN connection virtually takes the VPN user into the member of the LAN the required configuration is similar to the "Single site without public and VPN access". If the VPN user has restrictions in accessing LAN resources (servers), the IT has to enable HTTP(S) access for the HUB (1) server and for all SUs (1.2).

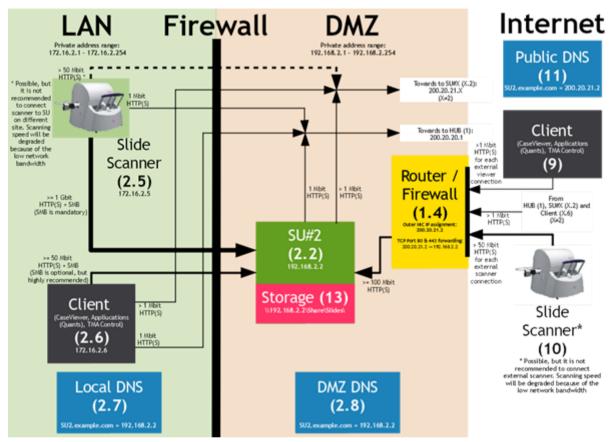
Multi site with public access

This use case enables a geographically distributed CaseCenter configuration. In this case at least two sites exist far from each other. Each site has an own LAN network which connects to the public Internet. No VPN connection available / required between any two sites (LANs), but through the Internet they are able communicate to each other. The first site has the very similar network configuration as described in "Single site with public access" section. This slightly modified configuration is shown on the below figure.



June 5, 2018 – Rev. 1

The main differences are that server components (the HUB (1) and the SU (1.2)) should have access to SU (2.2, see below figure) at the other site (as well as to any other SUs at further sites) and Client (1.6) should have access to SU (2.2) at the other site (as well as to any other SUs at further sites). Slide Scanner (1.5) need not have access to SU (2.2) because it is not optimal to scan to SUs at other sites due to network bandwidth limitations.



All further sites have network configuration shown in the above figure. These sites do not have their own HUBs but only SUs (2.2). From these sites all Clients (2.6), Slide Scanners (2.5) and SUs (2.2) must have network access to the HUB (1) at the first site through the Router / Firewall (1.4) of that site. Clients (2.6) and SUs (2.2) must also have network access to the SU (1.2) at the first site as well as SUs of other sites through Router / Firewall of those sites. Slide Scanner (2.5) need not have access to SU other than this site (2.2) because it is not optimal to scan to those SUs due to network bandwidth limitations.

If there is more than one high performance scanner at one of the sites it is recommended to have as many SUs as many scanners exist. This requirement is the same as in the case of single site configuration.

In no public access required (there is no Client (9) nor Slide Scanner (10)) the public Internet access theoretically can be replaced by permanent VPN connection between all sites. This requirement indicates either many-to-many point-to-point VPN connection between sites or star topology. If we use star topology Client (9) is able to connect through VPN to this CaseCenter as well.

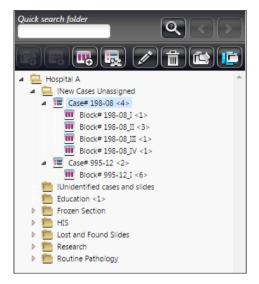
1.6 CaseCenter Site Requirements

Recommended Network Bandwidth		
Scan1, Scan2, Scan n	1 Gb/s	
View1, View2, View n	10/100 Mb/s	
SU1, SU2, SU n, SAN (in case of 1 scan)	At least 1 Gb/s	
SU1, SU2, SU n, SAN (in case of multiple scan)	10 Gb/s	
Wan3 (remote viewer station)	At least 500 kb/s for every concurrent viewer session Optimal 2-5 Mb/s for every concurrent viewer session	
Wan1, Wan2 (Broadband access)	At least 500 kb/s for every concurrent viewer session Optimal 10-20 Mb/s	

Storage capacity planning (Service Unit / Storage)		
Avg tissue single layer with 20x (15mmx15mm)	~ 1GB	
Avg tissue single layer with 40x (15mmx15mm)	~ 2,5 - 3GB	
Avg tissue with n x Z-layers	n x single layer GB	

2 Folder hierarchy

The tree structure of the server can be seen on the left side of the panel, where the actual folder is marked with blue background.



Hierarchically, the Case is a sub-level element within a folder, and the Block is a sub-level element of a Case. You can create several cases within a folder and several blocks in a case. Each folder, case, or block can directly contain slides.

Important!

The recommended maximum number of sub-level elements is 200 folders within a parent folder, 200 cases per folder, and 20 blocks per case (50000 elements total).

For slides the recommended counts are: 50 slides per folder, 10 slides per block, and 100 slides per case (in different blocks).

2.1 Folder Color Markings

User access rights are presented in different colors of folders in the tree panel. A folder name appears in black characters when it contains slides to which you have read and write access, blue if the slides are read only, and gray if the slides in the folder are hidden because the slides in it are not accessible.

Folder color marking and the tasks according to the different access rights are listed below:

- Black *Read/Write* access
- Blue Read only access
- Gray No access permission, but a sub-folder can be visible if you have *Read only* or *Read/ Write* access rights for that specific sub-folder, case, or block.

2.2 Folder Operations

•

•

This section details available folder operations. Folder operations are represented by buttons above the folder tree panel, and may be inactive depending on folder-related permissions.

	Quick search folder	
Quick sea	arch folder	
1.	Enter a string of characters (as a part textbox, then click .	of a slide/block/case/folder name) into the
2.	A message appears at the top of the v found items related to your search:	window informing you about the number of Vitems found using QuickSearch: 8
3.	To move between items click 💽 or	<u>></u>
i	New folder	
	Create new folder	۲
	Folder name New Folder Folder description	
	Add User(s) Subfolders inherit the permissions o demo, demo Dep 1, D Dep 2, D Dr. Jones, David Restricted, User Dr. Scott, Brian Dr. Smith, John Add Group(s) Administration department	f the parent folder. Read & Write Prof. A, A Dr. Anderson, James Prof. B, B Prof. C, C dep3, dep3 doe, jane
	Student department	Read only Demo Department 1 Department 2 Normal

- 1. In the folder tree, click the desired folder in which you would like to create the subfolder, and if active, click this button.
- 2. The **Create new folder** window opens. Type in the **Folder name**. Add some information in the **Description** field if necessary.
- 3. Select users and/or groups you would like to give access to this folder, and set their permissions. Click the right arrow buttons to add them to the selection list. Click the left arrow button to remove items from the lists.

By default, users are displayed with the given permissions for the parent folder, and will be marked with red if you modify their permissions.

NOTE: Only moderator and administrator users are allowed to set user permissions.

Each user type is marked with an avatar of a unique color:

- Moderator user is displayed with green
- Normal user is displayed with blue
- Restricted user is displayed with red

🐻 – New case

Creates a case under the actual folder. Note, that a case cannot be created under an other case or block. Similarly to the **Create new folder** window, description can be added to the case as well as users and groups and their access rights to the case.

Click Accept to create the case.

🔣 – New block

Creates a block under the actual case. Note, that you cannot create a block under an other block. Description can be added to the block as well as determining users and groups and their access rights to the block.

Click **Accept** to finalize block creation.

- 🔙 – Share Case

Click this button to share selected Case with others. Add users and/or groups with whom the Case should be shared.



• 🗾 – Edit folder

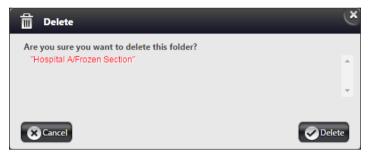
By default, you can modify the folder description only. Moderator and administrator users are allowed to change user permissions. Administrators are listed with green avatars.

Click Accept to confirm changes.

💼 – Delete folder

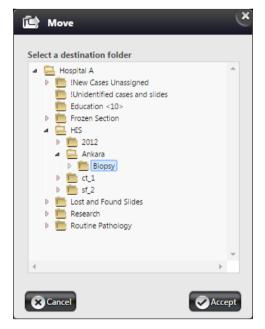
Upon clicking the **Delete Folder** button a dialog window opens. Click the checkbox to delete folder recursively. Select **Accept** to confirm the removal of the folder.

NOTE: Recursive folder deletion is available only for Administrators and the option is set to active by default. The maximum number of folders that can be deleted recursively is 1000, and for slides is 5000.



Move folder (for administrator users only)

Creates an exact copy of the selected folder and its content to a desired location in the tree; the original folder and its components will be completely removed from the server.



III – Move slide(s) to SU (available for administrator users only)

This button is active only if at least two SUs have been defined. All of the slides within the selected case or block can be moved to another SU.

Click the drop-down arrow first, then select the destination SU from the list.

NOTE: On how to add an SU or manage SUs, see sections 7.1 and 7.2.

Move slide(s) to SU				
Total size of slides	Slide count			
27.46 MB	2			
Server storage IP				
ug2.3dh.local/su_local (48.32 G	B Free -bytes move: 0 B)	•		
Cancel		Accept		

2.3 Special folders

- **Root directory** Root folder containing all the sub-folders. It cannot be deleted (neither by the user, nor the administrator), but can be renamed if needed.
- **HIS Root directory** A folder for storing folders and cases created during HIS integration. It cannot be deleted (neither by the user, nor the administrator), but folder role can be modified and set to another folder under Integration settings.
- Unidentified slides A folder for storing slides created during scanning without a specified destination folder, and another folder cannot be identified as destination based on HIS integration. It cannot be deleted (neither by the user, nor the administrator), but folder role can be modified and set to another folder under Settings.
- Lost and found slides A folder for storing slides not having location information identified by consistency checker. It cannot be deleted (neither by the user, nor the administrator), but folder role can be modified and set to another folder under Settings.

3 Managing Users and Groups

The **Users & Groups** window displays information about registered users and groups created by administrators. The Users and Groups information is separately displayed on two different panels. For group data click the **Groups** tab on the left side of the panel.

To search for users or groups scroll down the list in this window, and you can also narrow search results by entering text in the **Quick search** textbox. Adding, removing, and managing users and groups is also available for you in these two panels.

Selected users can be logged off from the server by clicking the **Kick selected users** or all the users logged in can be logged out by clicking the **Kick all users** button.

If LDAP settings are correctly set in the Service/Settings panel, then **Get LDAP user list** and **Get LDAP** group list buttons are displayed and active on both Users and Groups panels.

Users & Groups		×)								i 0
Users Quick search			h Add us	🚴 Add user 🔪 🔊 Kick selected users 🕵 Kick all users 🔍 🧟 Get LDAP user list						
Groups		User	User name	User title	Given name	Family name	User last logged in at	User level	User type 🖨	Edit
	2		jamesanderson	Dr.	James	Anderson	2015-10-29 13:10:06	Normal user	CaseCenter user	<u>×</u>
	C		research		R	Research	2012-02-06 10:07:22	Moderator user	CaseCenter user	<u>×</u>
	C		awest		Abraham	West		Public share user	CaseCenter user	2
			Public Share User 01		Public	Public Share User 01	2015-04-16 15:54:49	Public share user	CaseCenter user	<u>×</u>
	C		RestrictedUser		User	Restricted	2016-02-04 10:36:49	Restricted user	CaseCenter user	2



3.1 User Levels

To categorize users with different access rights, separate user levels have been introduced in CaseCenter. One user level is assigned to each user. If a user is imported as a member of a group from LDAP, the highest user level set for the group is assigned to the user.

The following User levels are available in the system to be set for users:

- Moderator Green avatar
- Normal Blue avatar
- Restricted Red avatar
- Public Share Purple avatar

The Moderator user level is hierarchically above the other in a way that the Moderator is allowed to modify folder access rights (to which they have Read&Write permission). Besides, users get in the Login queue based on their user level, which means the higher the level is, the sooner they are allowed to log in (the higher ranked user is put forward, but behind the users of the same level). The other function of user leveling is to define which menus (and, also which columns of a list within a menu) would be visible for a user of a specific level.

Public Share User can be created by a Normal user when sharing a single slide, or VS/VT with a Public Share User or a user who does not have a CaseCenter account.

If not creating a Public Share User prior sharing, after selecting the item(s) to be shared, a URL for the slide(s) can be generated for a newly created Public Share User upon clicking . In the Public Share Slide window, first type the name of the user in the **..or Create User** field, then click **Create**. The URL pointing to the shared slides is now displayed in the **Share URL** field. Copy the URL and send it to the user with whom you want the selected slide(s) to share with. Choose one of the available user rights (**Read & Write** or **Read only**) and finish the procedure by clicking **Accept**.

Public Share User is allowed to access the **Share** panel only (without having a CaseCenter account they cannot access the entire content of a CaseCenter server). Shared slides are listed under the **Shared by me** panel of the **Share** menu. If deleting a Public Share User the URL of the share will be invalid. The share URL opens the slide(s) with the platform-independent InstantViewer, but Pannoramic Viewer can be used as well if the user has installed the software (version 1.15.4) prior opening the link.

The default view of tables can be set for each user level uniquely. These settings can be performed within the **Column customization** panel on the **Service** menu window (see *section 9.9* for more information).

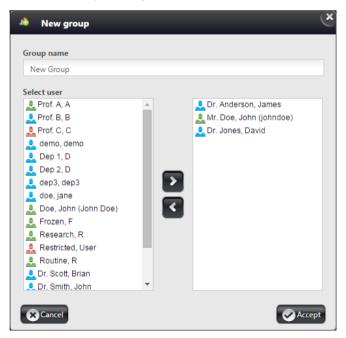
NOTE: Although the Administrator takes up a license but is not shown as a user logged in. Besides, an Administrator cannot be invited to Teleconsultation sessions but is allowed to create one, and is able to share slides as well.

3.2 Add User or Group

Users can be added by clicking the Adduser button on the **Users** panel. Fill in the data fields in the New user window. Check the **Can change profile** option to allow the user to modify their profile settings, and select the user level from the drop-down list.

👌 New user	×		
User title Family name	User name		
New	New User		
Given name	Password		
User	•••••		
E-mail	•••••		
new_user@aaa.com	Can change profile		
Server storage IP	User level		
ug2.3dh.local(su_local)	👤 Normal user 🔍		
Other contact	Specialities		
	Open slides in		
	Application •		
Cancel	Accept		

Additional Group can be created by clicking the standard group button on the Groups panel.

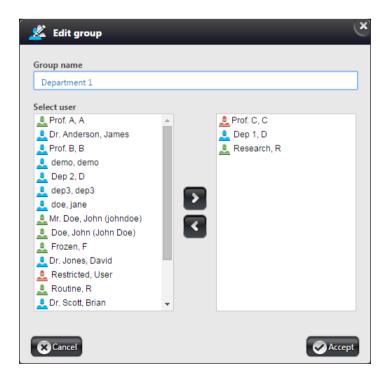


- Type in the name of the new group into the **Group name** field.
- Select the users you want to add as members of the group to the right column by clicking or remove by clicking , then click Accept when finished.

3.3 Edit User or Group Data

To access user or group data, click the $\stackrel{\frown}{\simeq}$ or the $\stackrel{\frown}{\simeq}$ button at the far right column of a user or group. All the information can be modified both in the Edit User and the Edit Group windows. Click **Accept** if modifications are done, or exit the window without saving the changes by clicking the **Cancel** button.

👱 Edit user	×		
User title Family name Dr. Anderson	User name jamesanderson		
Given name	Password		
James			
E-mail			
jamesanderson@email.com	Can change profile		
Server storage IP	User level		
ug2.3dh.local/su_local 🗨	👤 Normal user 🔍		
Other contact	Specialities		
	Open slides in		
	Application		
Cancel	Accept		



LDAP users cannot edit their full profiles, they only are able to edit some of the data in the CaseCenter interface, other data can be modified on the LDAP server only.

👱 Edit user		×
User title	Family name	User name
Dr.	Scott	brianscott
Given name		Password
Brian		
E-mail		
brianscott@m	ail.com	Can change profile
Server storage	IP	User level
ug2.3dh.local/	su_local	▼ Normal user ▼
Other contact		Specialities
		Open slides in
		Application
Cancel		Accept

When editing group data of an imported LDAP group, only storage IP, default user level, and the default viewer can be modified.

Group name		
Student department		
Default server storage IP		Default user level
ug2.3dh.local/su_local	-	👤 Normal user 🔍 👻
Open slides in		Import members when they log
Application	-	
Select user		
🔔 Prof. A, A	-	
👤 Dr. Anderson, James		
💄 Prof. B, B		
🔔 Prof. C, C		
👤 demo, demo		2
👤 Dep 1, D		
👤 Dep 2, D		
👤 dep3, dep3	_	_
🤳 doe, jane		
Mr. Doe, John (johndoe)		

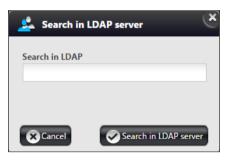
3.4 Remove User or Group

Selected user or users can be removed by clicking **Selected** on the **Users** panel. To delete a group or groups, click **Selection** on the **Group** panel after making the selection.

Important!
Users logged in cannot be removed. If the user status icon is lit, it means that the user is logged in, therefore you cannot put a check mark into the selection box.

3.5 LDAP Users and Groups

To search for LDAP users and groups in LDAP server click the **Get LDAP user list** or **Get LDAP group list** buttons respectively. A window is then displayed in which LDAP users/groups can be filtered based on the settings.



As a result, the first 500 list items are shown on the displayed list.

Sea	List of LDAP users										
	User name 🖨	User title	Given name	Family name	User E-mail	LDAP user status	Convert or bind user				
	brianscott	Dr.	Brian	Scott	brianscott@mail.com	User deleted from LDAP	Convert to CC user				
	davidjones	Dr.	David	Jones	davidjones@domain.com	User deleted from LDAP	Convert to CC user				
	johnsmith	Dr.	John	Smith	johnsmith@domain.com	User deleted from LDAP	Convert to CC user				
	teszt0		t_given_0	t_family_0	teszt0@3dhistech.com	User not imported	Please choose				
	teszt1		t_given_1	t_family_1	teszt1@3dhistech.com	User not imported	Please choose				
	teszt10		t_given_10	t_family_10	teszt10@3dhistech.com	User not imported	Please choose Bind				

If the LDAP user or group you have searched for is not present on the list, use the **Search** field at the top of the pop-up window to further narrow down search results. Click **Search users** or **Search groups** to start search.

For more information on LDAP user import **4.1 LDAP user import**, on group import see section **4.2** LDAP group import.

4 CaseCenter Lightweight Directory Access Protocol (LDAP) Implementation

CaseCenter LDAP protocol implementation is compatible both with OpenLDAP (multi-platform – for example, Linux) and Microsoft Active Directory (Microsoft Windows) servers.

Terms and abbreviations

- *CC user*: a user, created in CaseCenter, and can enter with password stored in CaseCenter
- *Import user*: CC user imported from LDAP user list, can log in with password stored in LDAP.
- *Temporary user*: a user that is not imported, or existing in CaseCenter, but is a member of a LDAP group that has already been imported, therefore, access with LDAP password is granted for this user. The user temporarily has been created in CaseCenter when logging in and it has become deleted when logging out.
- Permanent user: a user that is not imported, or existing in CaseCenter, but is a member of a LDAP group that has already been imported and the attribute "Import members when they log in" of the group has been set. The access with LDAP password is granted for this user. This kind of user has been handled and acting identical as the type of "import user" after the first logging in.
- LDAP user: user object existing in LDAP
- *AD*: Microsoft Active Directory
- OLDAP: OpenLDAP
- LDAP server: LDAP server in use (can be either AD, or OLDAP)

4.1 LDAP user import

LDAP users imported from LDAP to CaseCenter but currently not existing/inactive in LDAP are displayed on the list with red background. These users cannot log into CaseCenter, unless they are reregistered in LDAP or converted to CaseCenter user (by clicking **Convert to CC user** at the right of the row). If this type of user can be freely erased, select the checkbox at the left of the row and click **Delete users** button.

Each LDAP user having the same name as an existing CaseCenter user is marked with yellow background on the list. If a matching user name is found, choose one of the following options:

• Binding LDAP user to CaseCenter user is available for you by clicking the **Bind** button. This way, LDAP user becomes an imported user, and the data of the existing CaseCenter will be overwritten with the data queried from LDAP. When logging in, these users will be able to use their LDAP password only.

• Deleting CaseCenter user on the Users tab panel, then the user will be displayed with gray background on the LDAP list (see below).

Users displayed with blue background are LDAP users imported from LDAP to CaseCenter. Such users can be either removed from CaseCenter only, or converted to CaseCenter users. If converted, the user is able to log in with the password he/she used the last time to access CaseCenter (i.e. if in the meantime, the user's LDAP password has been changed, the user can log in with the password used previously).

If the user is converted to CaseCenter user right after importing and before the first login, then password can be set for the user on the Users tab by clicking **Edit**, otherwise user login will be denied.

Users marked with gray background are LDAP users that are not yet imported. Import is possible in two ways:

- Select the user/users by ticking the checkbox at the left side of the row then click **Import users**.
- At the right side of the row select the CaseCenter from the drop-down list to which the LDAP user is to be bound, then click **Bind**. CC user data will be overwritten with the data queried from LDAP, and only the user's LDAP password is accepted during login.

Tick checkboxes at the left side of the rows to select multiple users. If selecting a user that is not imported yet, the only available option is to import this user by clicking the **Import users** button. If the selected user has already been imported from LDAP, then it can be removed from CaseCenter by clicking **Delete users**.

If users of both types are selected, then upon clicking **Import users** only the importable users will be processed, and removable users (already imported from LDAP) will be deleted after clicking **Delete users** (users cannot be removed from LDAP). Imported users are listed with blue background on the Users tab panel, and can be deleted, but you have limited data editing capabilities for such users – you cannot modify personal data (as data are queried from LDAP), only the SU settings and user level is modifiable.

Temporary users are marked with red on the list. User data of such users cannot be modified, moreover, the user cannot be deleted, since it was imported from LDAP or queried from LDAP group data. SU and user level settings must be configured during editing the related imported LDAP group data.

Each time querying for LDAP user list, the data of every LDAP user imported to CaseCenter will be updated.

Instead of batch importing users, it is easier to import groups from LDAP.

4.2 LDAP group import

In the Users & Groups menu, on the Groups tab click the **Get LDAP group list** button to open a window in which LDAP groups can be filtered based on the settings. As a result, the first 500 list items are shown on the displayed list. If the LDAP group searched for is not presented on the list, use the field at the top of the pop-up window to further narrow down search results. Click **Search groups** to start search.

Imported groups are listed with blue background, and gray represent groups that have not been imported yet. LDAP groups with a name identical with the one of a CaseCenter group is marked with yellow background. These groups can be imported only if the CaseCenter group is deleted previously.

Tick checkboxes at the left side of the rows to select multiple groups. If selecting a group that is not imported yet, the only available option is to import this group by clicking the **Import groups** button. If the selected group has already been imported from LDAP, then it can be removed from CaseCenter by clicking **Delete groups**.

If groups of both types are selected, then upon clicking **Import groups** only the importable groups will be processed, and removable groups (already imported from LDAP) will be deleted after clicking **Delete groups** (groups cannot be removed from LDAP itself via this CaseCenter administrator function).

Imported groups are listed with blue background on the Groups tab panel, and can be deleted, but you have limited data editing capabilities for such groups – you cannot modify groups name or personal data of the members (as data are queried from LDAP). The SU settings, the user level and default viewer of the group member logged in to CaseCenter and the type of user (temporary or permanent) after the user first logged in, can only be modified. Modified settings will be applied for each group member who have not been created in CaseCenter as an Import or Permanent user yet.

If the user is a member of more than one imported group, then:

- The "User level" of the created user has been set to as the highest level "Default user level"
- If in any group the "Import members when they log in" has been set, then the user will have been created as "Permanent user" when logging in, otherwise as "Temporary user".
- The values of SU and "Default slide viewer" will have been set randomly from the values of the potential groups.

When giving any CaseCenter permission to the imported groups (folder permission, TC requests, share, etc.), Import, Permanent and Temp users of this specific group in LDAP will inherit these permissions. Temp user is added to the imported groups during each login, Import and Permanent user is added at the first login, and added and removed each time according to his/her actual LDAP group membership.

4.3 LDAP user login and function

Import user

A user gets into CaseCenter database during import. When logging in, the user uses LDAP name and password. At each login the encoded actual password, together with other personal data are updated in the CaseCenter database.

If the imported LDAP user is a member of a LDAP group imported, the user will be the member of that group as well. If in the meantime the user is removed from a LDAP group that has been imported to CaseCenter, then the user has to be removed from the CaseCenter group as well. If you remove a user from LDAP, then he/she cannot log in to CaseCenter any longer.

If the user password is modified in LDAP, access is available only with the updated password. While the LDAP server is inaccessible, the LDAP user cannot log in to CaseCenter.

If the Import user uses cookie during login (the **Remember me** checkbox is activated in the login window), then user existence is checked by an LDAP query with LDAP admin user. If the user does exist, access is granted (without password, using cookie) and their data is updated in the CaseCenter database; but if the user does not, access will be denied, and also the cookie will be deleted. This type of users can be freely removed from CaseCenter, SU and user level data can be modified.

Temp user

An LDAP user can connect to CaseCenter (without being imported) with LDAP username and password only if he/she is a member of an LDAP group already imported to CaseCenter. At each login a Temp user is created in CaseCenter (SU and user level settings can be performed during editing data of that specific imported LDAP group), and bound to the imported LDAP groups in which the user is a member. Temp users cannot have CaseCenter rights (folder, TC request, share, etc.).

Temp user rights can be set by giving CaseCenter rights for the imported LDAP group in which the user is a member. Temp user is removed from the CaseCenter database after the user is logged out. Temp users cannot be removed from CaseCenter, nor their data can be modified, as they are always online when present in the CaseCenter database.

If you want to set measures to rights of a user, first the user has to be removed from the LDAP group to which he/she belongs in LDAP, or groups must be removed from CaseCenter to which the user belongs (if so, it can occur that other users lose their access rights, if they were members of the imported LDAP group that has been deleted, and they are not imported).

Permanent user

An LDAP user can connect to CaseCenter (without being imported) with LDAP username and password only if he/she is a member of an LDAP group already imported to CaseCenter and the value of "Import member when they log in" has been set. Upon first logging in the user will have been created as "Import user" (SU and user level settings can be maintained when editing data of that specific imported LDAP group), and bound to the imported LDAP groups in which the user is a member. After first logging in the behaviour of "Permanent user" will be identical as it is written in "Import user" section.

Permanent user rights can be set by giving CaseCenter rights (folder, TC request, share, etc.) for the imported LDAP group in which the user is a member. After the first logging in (when the user has been created as "Import user") individual CaseCenter rights can be set.

5 Login Queue and Automatic Logout

Login queue has been introduced in CaseCenter to handle the shortage of free licenses.

An administrator is always able to log in to CaseCenter, but when there is no more free license is left, then only one Administrator is permitted to access CaseCenter. If another Administrator wants to log in, then a message is displayed stating that there already is an Administrator logged in who can be kicked from the server and he or she will be able log in to CaseCenter.



So, if there is no more free license is left, no one can access CaseCenter except an Administrator. In this case users are directed to the queue side. Users get in the queue according to their user level (users with higher rank are put forward in the queue) and their queue number (position in the queue) is displayed and is automatically updated.



The user may leave the queue by clicking Cancel, and every other user beside will be placed forward.

If users take the first position in the queue and a license is set free, then they are notified that the system is accessible, and log in is available within two minutes (this value is set as default, but it can be modified in the Settings panel).

	DHISTECH	CaseCenter 2.9	3DHISTECH
	ueue length: 1	You can log in now. 01: Password	51 minutes left
Password		Remember my login on th	is computer
Remember my login on this comput UNNAMED	er Login ►	Cancel	Login 🕨

If the user does not log in, will be removed from the queue, and the possibility of logging in is given to the user next in line.

Users of a specific level and below may be kicked from the server after a determined amount of time can be set in the Settings panel. In this case the user will be logged out anyway, thus providing an opportunity for the next user in queue to log in.



Furthermore, it is available for the Administrator to log users out after a specified time of inactivity. Login queue is worth using together with automatic logout at systems with lots of users (above the number of free licenses).

6 Service menu

The maintenance functions can be found on the **Service** panel, and can be accessed by the administrator only.

6.1 Statistics

I Service	v	iC
Statistics	Statistical data	Statistical value
Service units	Slides	42
Problematic slides Slides in progress	Total size of slides on SUs	7.01 GB
Log (?)	Free space on SUs	77.17 GB
HIS log (?)	Used space	8 %
Enums Settings	Folders	92
Column customization	Users	36
Database backup	Active user account	1
Slide transfer queue Integration settings	Moderator users	6
Edit report template	Normal users	12

This panel contains statistical information on the following CaseCenter-related data:

- Total number of uploaded slides
- Total size of slides on SUs
- Free space on SUs
- Used space
- Number of Folders
- Number of Users
- Number of Active Users
- Number of Moderators
- Number of Normal users
- Number of Restricted Users
- Number of Administrators
- Number of Groups
- Number of Attachments
- Number of Active Sessions

- Number of Shares
- Number of Teleconsultations

6.2 Service Units

In this panel, the list of the SUs connected to the HUB is displayed. Their name, IP, port, protocol, free space available on the SU, status, and SU version data are presented on the list.

Service	Ŧ											(iC
Statistics	Quick sea	rch											
Service units	SU ID 🔶	SU name	SU IP	SU port	SU protocol	SU virtual folder	SU slide number	Free space on SU	Total size of slides on SU	SU state	SU version	SU details	Transfer SU
Problematic slides	1	su_local	ug2.3dh.local	80	http	CaseCenter	40	48.32 GB	6.97 GB	SU online	2.0700060956	K	ic;
Slides in progress	2	su2		80	L.U	CaseCenter	2	28.85 GB	45.36 MB	CH Contraction	2.0502057265		
Log (?)	2	su2	ccsunpa	80	http	CaseCenter	2	28.83 GB	45.30 MB	SU disabled	2.0603057266	14	
HIS log (?)													
Enums													
Settings Column customization													
Database backup													
Slide transfer queue													
Integration settings													
Edit report template													

Click 🔢 to display details of that particular SU you have selected.

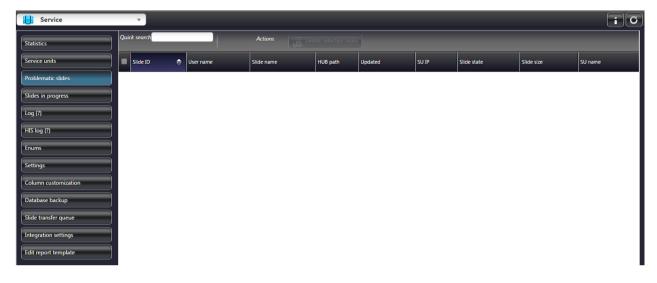
[SU a	details					e
SU name su_local Storage p						
Activity	Availability	Storage path	Free space	Used space	Slide count	User name
Active	Available	C:\Program Files (x86)\3DHISTECH\CaseCenter\Slides	48.32 GB	6.97 GB	40	ug2.3dh.local\CaseCenter_User

Click 🖳 to transfer slides contained on the selected SU to another SU. Select destination SU from the drop down list, then click **OK**.

Move slide(s) to SU		(x)
Total size of slides	Slide count	_
6.97 GB	33	
Server storage IP		
ug2.3dh.local/su_local (48.31 G	B Free -bytes move: 0 B)	•
Cancel		Accept

6.3 Problematic slides

Those slides are displayed in this panel that have some defect, for example slides that are being processed, but their status has not changed during the past half hour. The main reason for this is that processes are terminated, interrupted, or an error occurred in the system operation, or in the network connection.



6.4 Slides in progress

Those slides are displayed here, that are under processing (for example, they are being scanned, uploaded, duplicated, or removed).

Service		 Slide is under duplication 						x	iG
Statistics	Qui	ck search	Actions						
Service units		Slide ID 🔶	User name	Slide name	HUB path	Updated	SU IP	Slide size	SU name
Problematic slides		222c025c63aa2da0eebb9295e3ffe5e2	Administrator Administrator	198-08 G I Duplicating (destination): 28 %	Hospital A/HIS/Ankara/Biopsy/14	2016-02-05 13:08:52	ug2.3dh.local	31.11 MB	su_local
Slides in progress		67b5b7977b457a4932b9bad294f7af9a	Administrator Administrator	198-08 G I Duplicating (destination): 70 %	Hospital A/HIS/Ankara/Biopsy/14	2016-02-05 13:08:52	ug2.3dh.local	31.86 MB	su_local
HIS log (?)		a8d6e19754238d63830bb3794ae308d3	Administrator Administrator	198-08 G I Duplicating (source): 70 %	Hospital A/Education	2016-02-05 13:08:52	ug2.3dh.local	45.35 MB	su_local
Enums Settings		ecd2f628fc87f9f8ffe732387ff79a54	Administrator Administrator	198-08 G I Duplicating (source): 28 %	Hospital A/Education	2016-02-05 13:08:52	ug2.3dh.local	111.67 MB	su_local

6.5 Log

User and server activity is logged and displayed on the Log panel of the CaseCenter.

Service	v)				iG
Statistics Service units	Search user o			Date from 2016-02-05 0 Date to	00:00:00 Saved searches
Problematic slides Slides in progress	 ✓ Login / Log ✓ User Rights 	Group TC	Share Email (unsuccessful) Service unit Email (unsuccessful) Admin	Q Today	Not set
Log (14)	Log date	User name	Client IP	Log Tag	Log entry details
HIS log (?)	2016-02-05 06:30:59	Mr.Doe, John	172.16.253.1	.0	Login (johndoe, 6579e96f76baa00787a28653876c6127) success.
Enums	2016-02-05 06:32:59	Mr.Doe, John	172.16.253.1	.0	Logout: success.
Column customization	2016-02-05 06:33:06	Prof.C, C	172.16.253.1	.0	Login (profc, b933a375f92fc9b0d026c77e87fc4185) success.
Database backup	2016-02-05 06:34:27	Prof.C, C	172.16.253.1	.0	Logout: success.
Slide transfer queue Integration settings	2016-02-05 06:34:32	Mr.Doe, John	172.16.253.1	.0	Login (johndoe, 6579e96f76baa00787a28653876c6127) success.
Edit report template	2016-02-05 06:45:46	Mr.Doe, John	172.16.253.1	.0	Logout: success.

At the upper section of the window the search parameters can be set. After all the necessary parameters are set, click **Search**. Search criteria can be saved when a name is given at the **Save as** field prior clicking the **Save** button, and loaded from the **Saved search parameters** drop down list.

Click the **Delete** button to remove the selected item.

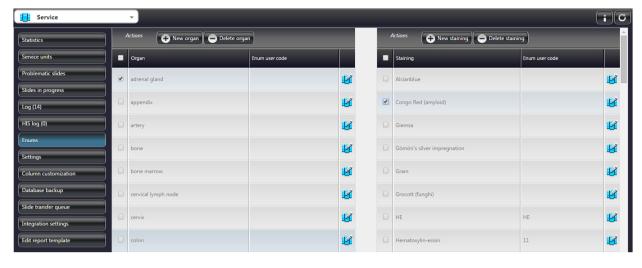
6.6 HIS Log

This tab includes search options regarding incoming and outgoing HIS/LIS logs. Various parameters can be switched ON/OFF to customize search and summary criteria. Additional options, such as printing HIS log, free text search and search within a given time-frame, are available on this tab.

Service	Ŧ						i
Statistics	User name	Case name	 Response slide Slide scanned (reply) 	 Request slide Slide scanned 	Date from	Q Search	
Service units	Barcode	Slide ID	Delete slide (reply)	Delete slide	Date to	🧒 Reset	
Problematic slides Slides in progress	 Search incoming log Incoming OK Incoming failed 	 ✓ Search outgoing log Outgoing OK ✓ Outgoing failed 		 Opened slide Send Report 	Q Today Q Last hour	E Show report	
Log (14)	Command 🔶 HIS	user name Casi	eCenter user name	Log time	Status (0=OK) Case ID	Error code	XML details
HIS log (0)							
Enums							
Settings Column customization							
Database backup							
Slide transfer queue							
Integration settings							
Edit report template							

6.7 Enums

Manage Organ, Staining, Site (medical institutes), and Case type lists on this panel if needed.



- Click Over organ / Over staining / Over site / Over case type to add a new item to the particular list.
- Type the name of the item to the upper textbox, then define an Enum in the lower textbox that is needed for barcode parsing.

NOTE: Organ, staining, and slide name can be as long as 255 characters.

An Enum, based on a defined rule, is identified from the barcode string of a slide. For more information on barcode parsing, read the related sections of *CaseCenter 2.7 Integration Guide*.

Click O Delete organ / O Delete staining / O Delete site / O Delete case type to remove selected items.

You can select items one by one, or tick their selection box (first row of columns) to select all the entries on the list.

• Click 🗹 to edit list item details.

NOTE: When entering **Site name** or **Case type** the character string cannot be longer than 60, and only include "\" as separator if you want to add sub-level elements (the name string cannot be longer than 32 characters after the separator.

NOTE: If more than one administrator is working on the same server, lists will not automatically be updated, therefore it is advised to hit F5 after creating or modifying an item.

6.8 Settings

In this panel, important settings can be accessed and modified related to database, network, SMTP, LDAP, and barcode parsing. Upon modifying a setting, its row background turns green. After modification to the settings click the **Save settings** button.

6.8.1 Basic Settings

E	Basic settings
Default language	Henglish 🗨
Default theme	Black Jelly
Institute name *	UNNAMED
Header logo picture	
Default directory for unidentified slides *	Root directory/Unidentified Slides
Lost and Found folder *	Root directory/Lost and Found Slides
Enable cookies *	۲
Cookie expiration time (seconds) *	2592000
Save login password *	۲
Opening Instant Viewer in new tab *	0
Lowest user level to delete folders	Restricted user
Lowest user level to delete slides	Legendreited user
Session timeout (minutes) *	30
Session auto logout (user level)	Moderator user
Session auto logout (minutes) *	0
Login queue timeout (minutes) *	2
Table refresh time (seconds) *	1
Secondary SU	No secondary SU
Attachment directory *	attachments
Macrostation name	
Macrostation um/pixel X *	250
Macrostation um/pixel Y *	250

- **Default language** set the default language of the web interface (choose a list item from the drop-down list)
- Default theme set the default GUI skin (choose a list item from the drop-down list)
- Institute name name of Institute displayed in the header of CaseCenter window
- Header logo picture add a logo of the Institute displayed in the header of CaseCenter window

Browse for logo file	×
Slide name	
Upload file Select file	👿 Logo reset
Cancel	Lupicad logo

- Default directory for unidentified slides folder in which slides without barcodes will be automatically stored
- Lost and Found folder folder set to which Lost and Found slides will be stored
- Enable cookies cookies can be enabled to automatically retrieve user password on the login window
- Cookie Expiration Time (seconds) the time in seconds after the cookie expires
- Save login password if checked, it enables to store the password for the browser
- **Opening Instant Viewer in new tab** if checked, InstantViewer opens in a new tab
- Lowest user level to delete folders folder deletion function is available for users of a specified user level (and above) set on the Settings panel in the Service window, irrespective of the user's basic RW folder permission. If, according to the set user level, the user is permitted to delete a folder (RW folder permission), then the folder (only when empty) can be deleted, otherwise the delete button is inactive. The default user level enabling users to delete a folder is "Restricted user".

- Lowest user level to delete slides slide deletion function is available for users of a specified user level (and above) set on the Settings panel in the Service window, irrespective of the user's basic RW folder permission. If, according to the set user level, a user is permitted to delete a folder (RW folder permission), then the user is allowed to:
 - delete slides within the folder
 - modify slide deletion time
 - execute the DeleteSlide command on the HIS interface
 - set deletion date of slides included in a Case by executing the *CloseCase* command on the HIS interface

The default user level enabling users to delete a folder is "Restricted user".

NOTE: If user level is set higher than "Restricted", and HIS integration is activated (also, user level is not set to "Restricted"), HIS may not execute slide deletion

- Session timeout (minutes) the set value determines the time of inactivity in minutes after the user will be disconnected from the server
- Session auto logout (user level) the selected user level and below will be logged out after the specified amount of time of inactivity
- **Session auto logout (minutes)** specify the time of inactivity after which users will be logged out from the server (remaining time is displayed in the user label on the header bar)
- Login queue timeout (minutes) users waiting in the login queue will be removed after the set period of time
- Table refresh time (seconds) set the time-frame after which tables will be updated

For more information on login queue and automatic logout see section **11** Login Queue and Automatic Logout.

• Secondary SU – the selected SU will be used as an auxiliary SU if the primarily used one is unavailable

For more information on secondary service unit see section **11** Secondary Service Unit.

- Attachment directory uploaded attachments are stored in the specified folder
- Macrostation name the name of the Macrostation device attached to the computer
- Macrostation µm/pixel X resolution value of the X-axis
- Macrostation µm/pixel Y resolution value of the Y-axis

6.8.2 Pathonet settings

	Pathonet settings			
Pathonet address				
Pathonet secure connection				
Pathonet session cookie id				
Public key for OpenCenter				
Pathonet users root folder	Root directory/Pathogate			

This panel includes CaseCenter-Pathonet connection settings.

6.8.3 Database Settings

Database settings				
Database host *	127.0.0.1			
Database username *	cc_lpuser			
Database password				
Database name *	casecenter			
Save database after how many days *	3			
Save database at *	01:00:00			
Save database to				

Overwrite data if necessary, for example either the IP address of the host, the user credentials, or the database name has changed.

- Database host host address of database
- Database username name of the user of the database
- Database password password of the database user
- Database name name of the database

- Save database after the number of days after which the database is saved, the location and exact time can be set in Save database to and Save database at fields
- Save database at create backup at the specified date
- Save database to save backup at the set destination

If not set, the destination is the following by default: C:\Program Files\ 3DHISTECH\CaseCenter\BackupRestore\Backup[date of saving]

6.8.4 Network settings

The settings within this section are related to TC and HUB servers, the web interface, HIS communication and logging, and SU/HUB database.

	Network settings
HUB server address *	ug2.3dh.local
HUB virtual folder *	CaseCenter
HUB server protocol (http/https)	Prefer HTTP
TC server address *	ug2.3dh.local
TC server module name *	CaseCenter

• TC server address, TC server module name, HUB server address, HUB virtual folder, and HUB server protocol (http/https) fields contain data specified during the installation.

Warning!

If HTTP is used during HIS communication, passwords will **NOT** be encrypted.

6.8.5 SMTP settings

These fields contain settings for *Simple Mail Transfer Protocol*. Fields on SMTP settings panel are uneditable by default. Tick the **Enable e-mail sending to users** selection box, and the fields turn editable so settings (except for SMTP user credentials) can be modified.

	SMTP settings
Enable e-mail sending to users *	
SMTP server address *	
SMTP port *	
SMTP SSL	
SMTP TLS	
SMTP username	
SMTP password	
SMTP from address *	
SMTP settings test e-mail address *	admin@example.com
SMTP SU status e-mail address	
Sending time of SMTP SU daily status	
SMTP SU disabled e-mail address	

- SMTP server address
- SMTP port
- SMRP SSL
- SMTP TLS
- SMTP username
- SMTP password
- SMTP from address

• SMTP settings test e-mail address

• SMTP SU status e-mail address

The administrator receives an e-mail about the SU status including date, SU name, total, free and used spaces, and storage path. This mail is sent to the address specified on the **Settings** panel, but if not set, the e-mail sending function is inactive.

• Sending time of SMTP SU daily status (HH:MM:SS)

The system sends an e-mail (to the address specified on the **Settings** panel) on the statuses of SUs to the administrator on a daily basis. If the address is not set, the e-mail sending function becomes inactive.

After 3 unsuccessful attempts, the system tries to resend the e-mail at the specified time on the following day, and logs once only, may the result of sending be unsuccessful or unsuccessful.

SMTP SU disabled e-mail address

If an SU becomes disabled, an e-mail is sent to this address.

NOTE: If a SMTP has been defined during upgrade, these settings must be revised and modified if necessary.

6.8.6 LDAP settings

These fields contain options for Lightweight Directory Access Protocol settings.

	LDAP Settings	
LDAP enabled *	۲	
LDAP server address *	cclinux	
LDAP port *	389	
LDAP user RDN *	cn=_USERNAME_,dc=cclinux,dc=local	
LDAP user search filter *	(&(objectClass=inetOrgPerson)(uid=_	
LDAP user search RDN *	dc=cclinux,dc=local	
LDAP group search filter *	(&(objectClass=groupOfNames)(cn=_	
LDAP group search RDN *	dc=cclinux,dc=local	
Group filter of LDAP user *	(member=_USERDN_)	
LDAP admin group	csoport_abc	
LDAP admin user	teszt0	
LDAP admin password		
LDAP user name attribute *	uid	
LDAP user title attribute *	initials	
LDAP user familiy name attribute *	sn	
LDAP user given name attribute *	givenname	
LDAP user e-mail attribute *	mail	
LDAP user other contact attribute *	telephonenumber	
LDAP user specialities attribute *	department	
LDAP group name attribute *	cn	
LDAP object guid attribute *	objectGUID	

- LDAP enabled: LDAP login is disabled (OFF) by default. LDAP users cannot, but only CC users (users managed by CaseCenter) can log in.
- LDAP server address: LDAP server host Empty by default. LDAP server can be either a Microsoft Active Directory server (henceforth: AD) or an Open LDAP server (henceforth: OLDAP).
- **LDAP port**: LDAP server port set to 389 by default.
- LDAP user RDN: Relative Distinguished Name format used in binding to LDAP.
 __USERNAME__ is a placeholder, and will be replaced by the current user name. Default AD is "_USERNAME_@domain". Default OLDAP: "uid=_USERNAME_,dc=domain,dc=com". Login is granted to LDAP server by using LDAP server name and password.

It is advised to edit this setting before using CaseCenter with LDAP: for example, change 'domain' to the proper domain name where the user objects are present, but do **NOT** change the "__USERNAME__" placeholder. CaseCenter replaces "_USERNAME_" with the name of the specific user logging in.

LDAP user search filter: This filter expression is used to search either a specific user or all the users in LDAP. Default AD is "(&(objectCategory=user)(samaccountname=_USERNAME_))". Default OLDAP: "(&(objectClass=inetOrgPerson)(uid=_USERNAME_))".

Do **NOT** change the "__USERNAME__" placeholder. CaseCenter replaces "_USERNAME_" with the name of the specific user, or to "*" when CaseCenter queries all users from the LDAP. "objectCategory" and "objectClass" parameters specify the Class/Category of LDAP user-type objects in LDAP.

If OLDAP is used, LDAP user registration determines the Class the LDAP user gets into. The attributes "samaccountname" and "uid" of LDAP users are used to indicate the user's login name. These two settings relate with AD and OLDAP default settings.

 LDAP user search RDN: This RDN defines the LDAP server tree in which the search criteria 'LDAP user search filter' is run. Default AD is "cn=Users,dc=domain,dc=com". Default OLDAP is "dc=domain,dc=com". By defining an OU (Organizational Unit) for example, search results can be narrowed down, but only those users can be imported and logged in to CaseCenter, who meet this requirement (i.e. users belonging to other OU cannot).

With these two settings the whole domain tree can be searched. The "domain" and the "com" attributes identify the domain name ("dc" as "domain component") in which the specific LDAP user object is located.

The two settings above help to identify user objects in LDAP server, and query user data. CaseCenter replaces "_USERNAME_" in FILTER with the name of the user logging in (uses "*" during import to query all users). The user is searched for within RDN, and the necessary LDAP user object is filtered based on FILTER.

 LDAP group search filter: This filter expression is used to search either a specific group or all the groups in the LDAP. Default AD is "(&(objectCategory=group) (samaccountname=_GROUPNAME_))". Default OLDAP is "(&(objectClass=groupOfNames) (cn=_GROUPNAME_))".

Do **NOT** change the "__GROUPNAME__" placeholder. CaseCenter replaces "_GROUPNAME_" with the name of the specific group or to "*" when CaseCenter queries all groups from LDAP. Attributes "objectCategory" and "objectClass" give the Class/Category attributes of LDAP-type objects in LDAP. If OLDAP is used, the creation of LDAP group determines the Class of LDAP group. Attributes "samaccountname" and "cn" of LDAP groups to identify group name. These two settings work with default AD and OLDAP settings.

• **LDAP group search RDN**: This RDN defines the LDAP server tree in which "LDAP group search filter" search filter will run. Default AD is "cn=Users,dc=domain,dc=com". Default OLDAP is "dc=domain,dc=com". By defining an OU for example, search results can be narrowed down, but only those groups can be imported and logged in to CaseCenter, which meet this requirement (i.e. groups belonging to other OU cannot).

Based on these two settings the whole domain tree will be searched. "domain" and "com" attributes identify the domain name ("dc" as "domain component") in which the specific LDAP group object is located.

The two settings above help to identify group objects in LDAP server, and query group data. CaseCenter replaces "_GROUPNAME_" in FILTER with the name of the group (uses "*" during import to query all groups). The group is searched for within RDN, and the necessary LDAP group object is filtered based on FILTER.

Group filter of LDAP user: This filter expression is used to query group memberships of the user logged in. Default AD is "(member=_USERDN_)". Default OLDAP: "(member=_USERDN_)". LDAP user groups can be queried from LDAP by using this filter. If LDAP user object possesses a "member" attribute, then this setting is correct. CaseCenter replaces "_USERDN_" value to the user DN in LDAP (queried from LDAP). This setting works with the default settings of both AD and OLDAP.

NOTE: If AD is set, the admin user must be a member of a group created by another user, therefore being a member inclusively of default groups (for example, Users, Domain Users, etc.).

- **LDAP admin group**: Default: empty. A group whose members include the **LDAP admin user** in LDAP. It is needed only for checking group query when saving settings.
- LDAP admin user: Default: empty. A LDAP user with permission to query data and groups of other LDAP users, and LDAP groups. Permission is required only to execute queries specified by the user and group search filters in the specified RDNs. This user is also enabled (by using the 'LDAP admin password') to check all the LDAP settings you specified in this section.
- **LDAP admin password:** Default: empty. Password of the above LDAP user. Saved encoded into CaseCenter database.
- LDAP user name attribute: This is an attribute of a user-object in LDAP by which the login name of the user is denoted (see LDAP user search filter), and indicated as Username in CaseCenter. Default AD is "samaccountname". Default OLDAP is "uid".

- **LDAP user title attribute:** In LDAP, this is a user-object attribute denoting user initials. Default AD is "initials". Default OLDAP is "initials".
- LDAP user family name attribute: In LDAP, this is a user-object attribute denoting the family name of the user, and indicated as Family name in CaseCenter. Default AD is "sn". Default OLDAP is "sn".
- LDAP user given name attribute: In LDAP, this is a user-object attribute denoting the given name of the user, indicated as **Given name** in CaseCenter. Default AD is "givenname". Default OLDAP is "givenname".
- **LDAP user e-mail attribute:** In LDAP, this is a user-object attribute denoting the email address of the user. Indicated as **Email** in CaseCenter. Default AD is "mail". Default OLDAP is "mail".
- LDAP user other contact attribute: In LDAP, this is a user-object attribute denoting other contacts of the user (by default, the telephone number). Indicated as **Other contact** in CaseCenter. Default AD is "telephonenumber". Default OLDAP is "telephonenumber".
- LDAP user specialities attribute: In LDAP, this is a user-object attribute denoting user specialities (by default, the department the user works at). Indicated as **Specialities** in CaseCenter. Default AD is "department". Default OLDAP is "departmentNumber".

If the above fields are left empty, they will not be filled during importation of a CaseCenter user, or in that case a Temporary and Permanent user is logging in. Make sure to fill in the **LDAP user name attribute** field, because if it's left empty, the user will not be able to log in.

- LDAP group name attribute: In LDAP, this is an attribute of the group-object denoting group name (see LDAP group search filter). Indicated as Groupname in CaseCenter. Default AD is "samaccountname". Default OLDAP is "cn".
- **LDAP object guid attribute:** In LDAP, this is an attribute of the user-object and also groupobject denoting object ID. Default AD is "objectGUID". Default OLDAP is "entryUUID".

LDAP object attributes can be of "objectClass" or "objectCategory" types enabled through the template of the particular LDIF type.

NOTE: Make sure to edit RDN and FILTER settings in accordance with the valid LDAP query.

At those settings where "_USERNAME_", "_GROUPNAME_", or "_USERDN_" occur, these special strings must be used.

Except a few exceptions, the specification of the above settings is mandatory. Each LDAP user logging into CaseCenter must be able to log into LDAP (auth) and to query their own personal or group data from LDAP server (with at least read permission).

For more information on LDAP and user-related functions, see section **4** CaseCenter Lightweight Directory Access Protocol (LDAP) Implementation.

6.9 Column customization

This panel provides settings for each user category to define accessible menu items and their display options.

Service	·				iG
Statistics	Actions Sestore defaults	-	-	-	
Service units	Menu	Moderator user	Normal user	Restricted user	Public share user
Problematic slides	Slides & Folders	e /	•	· /	
Slides in progress				- ×	✓
Log (?)	Consultation	• //	• /	• 🖉	
HIS log (?)	Late Share	• /	• 🦻	• /	
Enums	Q Search (This menu requires the presence of Slides and folders menu.)	• /	• /	•	
Settings Column customization	Lusers & Groups (Read only)	• /	• /		
Database backup	CaseView page	· /	• /	· /	
Slide transfer queue					
Integration settings					
Edit report template					

To disable/enable menu items uncheck/check the checkboxes of that specific item. If any of the settings has been modified and is different from default, the corresponding field turns yellow. To edit panel options related to any of the user types click 2.

In the displaying window check/uncheck the checkboxes next to the column names to customize the selected panel for the specific user category. Click **Back** to return to the parent panel when finished, or click **Restore defaults** to ignore modifications.

Service	·		i
Statistics	eleconsultation (TC requests) (Normal user) Teleconsultation (TC invitation	ns) (Normal user)	
Service units			Restore defaults
Problematic slides			
Slides in progress	Checkbox 🖾 TC name 🖾 Start date 🖾	Expiration date 🗹	Edit 🗹
Log (?) HIS log (?)	Title	Start date Expiration da	te Edit TC
Enums	Sample Teleconsultation #0	2012-12-12 12:30 2013-02-12	12:30
Settings	Sample Teleconsultation #1	2012-12-12 12:30 2013-02-12	12:30
Database backup	Sample Teleconsultation #2	2012-12-12 12:30 2013-02-12	12:30
Slide transfer queue	Sample Teleconsultation #3	2012-12-12 12:30 2013-02-12	12:30
Integration settings Edit report template	Sample Teleconsultation #4	2012-12-12 12:30 2013-02-12	12:30

6.10 Database Backup

SU and HUB backup is fully automated based on the defined values of the following related settings: Save database after, Save database at, and Save database to. For more information, see section 9.8 Settings.

The information details of previous backup sessions are listed on this panel, including start and end time, type (manual or automatic), progress, and status.

The backup process can be performed manually as well, by simply clicking the **Start Backup** button at the top of this panel. You may cancel a running backup process with the **Stop Backup** button.

Service	×						iG
Statistics	Actior	as 🛛 🧭 Start Backup	G Stop Backup				
Service units	Backup status	Start time		Туре	Progress	Running	Status
Problematic slides	0	2017-02-20 01:00:42	2017-02-20 01:00:46	Automatic	100	Finished	Success
Slides in progress		Save path: C:\Program File	es\3DHISTECH\CaseCenter\Bac	kupRestore\Backu	0_20 <mark>17-02-2001</mark>	_00_42	
Log (?)							
HIS log (?)							
Enums							
Settings	0	2017-02-17 09:45:18	2017-02-17 09:45:25	Automatic	100	Finished	Success
Column customization		Save path: C:\Program File	es\3DHISTECH\CaseCenter\Bac	kupRestore\Backu	o_2017-02-1709_	_45_18	
Database backup							
Integration settings							_
Edit report template	0	2017-01-09 09:12:17	2017-01-09 09:12:20	Automatic	100	Finished	Success
		Save path: C:\Program File	es\3DHISTECH\CaseCenter\Bac	kupRestore\Backu	p_2017-01-0909_	_12_17	
		2016-12-01 08:50:39	2016-12-01 08:50:42	A. 41	100	Finished	Success
	0		2010-12-01 08:50:42	Automatic			→ Success

Important!

Modifications performed during the period between HUB backup and restoration will be lost.

6.11 Slide Transfer Queue

If moving a folder, a slide, or a batch of slides to another SU by clicking or the actual progress and the data of the transfer is visible on this panel.

Service	~											iG
Statistics	Actions 😿 Abort selected slide transfer											
Service units	Slide name	Slide size	SU source	SU destination	Start time	¢	Last updated	User name	Status	Abort	Error code	Error description
Problematic slides	<u>198-08 G I</u>	<u>107.13 MB</u>	su_local	su2	2016-02-08	09:41:10	2016-02-08 09:41:10	Administrator Administrator	Waiting	Not aborted	0	
Slides in progress										1		
HIS log (?)												
Enums												
Settings												
Column customization Database backup												
Slide transfer queue												
Integration settings												

6.12 Integration Settings

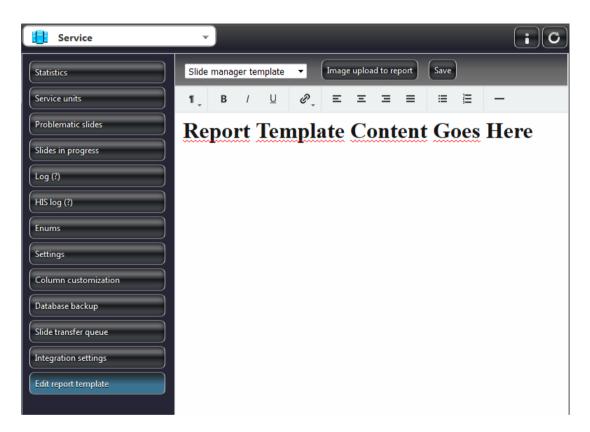
NOTE: Refer to section **3** *HIS Integration Settings in CaseCenter* in the *CaseCenter 2.8 Integration Guide* to read a detailed information on integration settings.

6.13 Edit Report Template

Report templates can be defined here for the following panels that can be selected from the dropdown menu:

- Slide manager
- Teleconsultation
- Share

NOTE: Group members are also allowed to attach a report to the shared case.



Additionally, users can add images for the templates by clicking the Image upload to report button.

NOTE: As an Administrator, you can view reports, but you cannot edit them.

7 Manage Service Units

7.1 Add SU

A SU can be connected to one HUB only!

After installing the SU, it has to be connected to the HUB through the **3DHISTECH CaseCenter Configuration** application, **HUB** tab panel.

- 1. Log in as administrator (user name: admin)
- 2. Add HUB address
- 3. Choose HUB server protocol (Secure connection means HTTPS)
- 4. Add SU name
- 5. Add SU self address
- 6. Choose used **SU protocol**

When it is done, the SU starts communicating with the HUB.

7.2 Edit SU

If the SU settings are changed, such as its name, address, or protocol, these values can be set in the SU through the **3DHISTECH CaseCenter Configuration** application, **HUB** tab panel.

NOTE: you cannot change the SU virtual folder.

On the SU side, start the **3DHISTECH CaseCenter Configuration** application and switch to the HUB tab panel:

- 1. Log in as administrator (user name: *admin*)
- 2. Change SU name
- 3. Change **SU self address**
- 4. Change SU protocol
- 5. Press Change button to save changes

See sections 8.4 Import Slides and 9. Slide- and user-related maintenance for more information.

Open a slide from the SU to check modifications are well performed.

7.3 Remove SU

Warning!

This function should be used only in reasonable cases. All slide-related data (name, staining, organ, scan date) are stored on the HUB, the unique identifiers (GUID) of slides are stored on the SU. Therefore, in a normal situation only that SU can be unregistered from the HUB, that does not contain slides. You can verify this on the **Settings** panel of the **3DHISTECH CaseCenter Configuration** application.

- 1. On the SU side, start the **3DHISTECH CaseCenter Configuration** application and switch to the **HUB** panel
- 2. Log in as administrator (user name: *admin*)
- 3. Click Remove

8 Manage Slides

8.1 SU storage management

The average size of a digital slide is 1GB (Z-Stack slides require multiple times more space). The size of a specific slide depends on the size of the scanned area, the scanning method (Brightfield, Fluorescent, Z-Stack), the selected compression algorithm, and the rate of the algorithm (JPG, JPG2000, BMP). For example, a Brightfield Z-Stack whole slide digitized in JPG 80 may require more than 30 GB space on the storage drive.

CaseCenter does not perform backup of slides (because of the huge amount of data) so it is the user's responsibility to ensure that storage of slides is secure. The most obvious solution is to use storage drives conform with security standards. Data security level can be increased if a backup copy of slides to a 3rd party device is created regularly. Expectation towards the storage device that is has to be compatible with Microsoft Windows Server 2012 R2 (operation system of CaseCenter Host).

Storage connection type is either NAS (Network Attached Storage), DAS (Direct Attached Storage) or SAN (Storage Area Network). If NAS connection is established, communication through a Microsoft SMB/CIFS protocol. DAS or SAN requires a proper Windows driver as the bare minimum. Ensure that storage server does provide Microsoft SMB file or printer share function towards CaseCenter clients, otherwise clients connected to storage server can access slides from CaseCenter through HTTP/HTTPS only. Outer storage has to be connected to SU (if NAS is preferred, the outer storage is connected to the LAN that includes the SU). NAS storage is in direct connection with clients of the same LAN (through SMB protocol) only if SMB access is enabled on the SU (enabled by default). If SAN or DAS is used, clients access storage through the SU. In such cases, slide storage folder on the SU must be shared (Windows Share), thus making it accessible for clients on the LAN (that includes the SU) through SMB.

				Service Unit Setting	gs			
JB Settings								
Slide Store								
Storage path	State 1	State2	# of slides	Allocated space [MB]	Reserved space for other SW's [MB]	Available space [MB]	User name	
C:\Program Files\3DHISTECH\CaseCenter\Slid	es Active	Available	0	0	1024	48920		
Add Reactivate Archive	Remove	Edit	Te	est				
Statistics								
] (0 slide(s))							
Total available space for new slides: 4892) [MB] (cca. 47 s	slide(s))						
Largest available space for one new slide: 4892) [MB]							
Status								
Operation status: Onlin	•							
Slide checking progress:pro	cess is running in	background						
								0
							Close	Cance

Storage drives can be set in Settings panel in CaseCenter Configuration application:

On the Settings panel of the **Service Unit Settings** window, the following columns are displayed:

- Storage path: slide storage directory
- State1: usability status of storage (modifiable by administrator) Values:
 - Active: new slide can be placed on the storage
 - **Archived**: additional slide cannot be placed on the storage, slides already present on the drive can be read/written
- State2: accessibility status of storage (shifts automatically)

Values:

- Available: storage can be accessed
- **Unavailable**: storage is temporarily inaccessible (for example, because of a network error)
- # of slides: number of slides momentarily stored on the storage
- Allocated space: total size of slides on the storage
- Reserved space for other SW's: smallest reservable free space on the storage
- Available space: free space on storage for storing slides
- User name: SMB (NTLM) user that can access storage path with Full control permission

Push buttons:

- Add: add a new storage path
- Archive: a storage in State1 = Active status can be set to Archived

Important!

Do **NOT** archive a storage if import is in progress.

- **Reactivate**: a storage in **State1 = Archived** status can be set to **Active**
- **Remove**: remove a storage (can be performed only if there is no slide on the storage)
- Edit: edit storage path data
- Test: check storage path (test result is displayed as a value in column State2)

Statistics:

• Summed up statistics of every storage path (slide number, size, total free space, largest continuous free space)

Status:

• If **Operation status** is online, slide checker runs automatically in the background.

8.1.1 Add new storage

	Storage data	x
Storage Path:	\\slidestorage.3dhistech.com\storage1\slides	
User Name:	3dhistech.com\su1_user	
Password:	**********	
Reserved Space [MB]:	1024	
🔽 Check folder secuti	ty	^
Information		
WARNING! Do not use	DFS share with replication to store slides, because it could cause loss of slide data!	
In this form you should	d give a valid (existing) storage path for storing slides.	
Currently, 2 paths are	available:	
In case using directory -not use the root fold -specify a valid user i -specify an existing d	k share (eg.: '\\Server\Share\Sildes') - SMB and HTTP(S) slide access will be available on a network share you should: for of the network share (eg. '\\Server\Share), but you should specify at least one of its subdirectories (eg. '\\Server\Share\Sildes'), name and password, who will be identified by the 'Server', irectory, S access rights on the folder (and its subfolder(s)) for the specified user.	
In the case of using lo -should not use the fi -should not use a roo -need not specify a u -can specify a non ex-	D: \Home\Sildes', where D is a 'fixed disk') - only HTTP(S) slide access will be available cal directory you: ollowing drive eg. removeable (floppy, CD/DVD, USB, etc.), RamDrive I folder of a drive (eg. D: ('), but you should specify at least one of its subdirectories (eg. 'D: \Sildes'), ser name and password, because the server will use 'CaseCenter_User' for access the directory, disting directory, because it will be created, edal NTFS access rights for the folder, because the required user privileges will be set for the 'CaseCenter_User'.	
Other path options are	e not supported (such as removable disk (floppy, CD/DVD, USB, etc.), RamDrive)!	
For 'Reserved Space'	we highly recommend to specify at least 1GB or 5% of unallocated free space on the storage!	
For further information	about storage requirements, please, refer to 'SU Storage management' section in the Administrator's guide.	
	OK Cancel	Ÿ

- Storage Path: storage access UNC Windows/NAS SMB share
- User Name: a Windows Domain user, or local user that exists on the storage, having Full Control permission on the Storage Path and the Windows Share (these access rights must be set before adding the storage).
- **Password**: user password
- **Reserved Space**: the minimum free space to be reserved (value in MB). Recommended free space is 5% of the total disk space, but at least 1 GB.
- Check folder security: check access rights of the folder specified at the Storage Path field.

8.1.2 NAS storage usage

- Storage Path is a valid UNC path in the following form: <u>\\SERVER_NAME\SHARE\SUBFOLDER</u>. The SUBFOLDER part must be included, one sub-folder path depth (for example, <u>\\</u> <u>SERVER_NAME\SHARE</u>) cannot be used as a folder for slide storage.
- Only one Storage Path can be added to the system from one logical volume.
- User Name: a valid user, that either exists on a domain server which includes SERVER_NAME and SU as members, or a local user on the SERVER_NAME machine. This user must have Full Control NTFS access permission to <u>\\SERVER_NAME\SHARE\SUBFOLDER</u> folder and to all of its sub-folders, as well as to <u>\\SERVER_NAME\SHARE</u> SMB share.

User permission setting must be performed prior to adding the storage by the storage administrator. Permission must be registered for the user explicitly, group permission is invalid.

 If several Storage Path is added to the system, each of them has to be set with the same User Name.

8.1.3 DAS, SAN or local storage usage

- The folder for storing slides must be shared (Windows share). Specification for the share created this way is the same as in section **NAS storage usage**.
- Although the system allows us to use local folder path as slide storage (for example, D\:Slides), slides stored in such folder can only be accessed through HTTP/HTTPS even from clients within the LAN of SU, that drastically decreases the speed of transfer, and has dramatic effect especially on the scanning speed.

8.1.4 Storage editing

	Storage data	x			
Storage Path:	\\\$lidestorage.3dhistech.com\storage1\\$lides				
User Name:	3dhistech.com\su1user				
Password:	*******				
Reserved Space [MB]:	2048				
Check folder secutit	у	^			
Information					
WARNING! Do not use	DFS share with replication to store slides, because it could cause loss of slide data!				
In this form you should	give a valid (existing) storage path for storing slides.				
Currently, 2 paths are	available:				
In case using directory -not use the root fold -specify a valid user r -specify an existing d	x share (eg.: '\\Server\Share\Slides') - SMB and HTTP(S) slide access will be available on a network share you should: er of the network share (eg. '\\Server\Share'), but you should specify at least one of its subdirectories (eg. '\\Server\Share\Slides'), name and password, who will be identified by the 'Server', rectory, S access rights on the folder (and its subfolder(s)) for the specified user.				
-Local directory (eg.: 'D: Home\Slides', where D is a 'fixed disk') - only HTTP(S) slide access will be available In the case of using local directory you: -should not use the following drive eg. removeable (floppy, CD/DVD, USB, etc.), RamDrive -should not use a root folder of a drive (eg. 'D:\'), but you should specify at least one of its subdirectories (eg. 'D:\Slides'), -need not specify a user name and password, because the server will use 'CaseCenter_User' for access the directory, -can specify a non existing directory, because it will be created, -need not set any special NTFS access rights for the folder, because the required user privileges will be set for the 'CaseCenter_User'.					
Other path options are	not supported (such as removable disk (floppy, CD/DVD, USB, etc.), RamDrive)!				
For 'Reserved Space' v	e highly recommend to specify at least 1GB or 5% of unallocated free space on the storage!				
For further information	about storage requirements, please, refer to 'SU Storage management' section in the Administrator's guide.				
	OK Cancel	×			

- Storage Path: path of storage, cannot be modified.
- User Name: a Windows Domain user, or a local user on the storage, who has Full Control permission to Storage Path and Windows Share (these permissions must be set prior to adding the storage).
- **Password**: user password
- Reserved Space [MB]: minimum reserved free space in MB
- Check folder security: check access rights of the folder specified at the Storage Path field.

8.1.5 Moving of slides to another Storage folder within the SU

- 1. Add new Storage folder with the Service Unit Settings program
- 2. Disable SU (end both SUSvc and SlideHandler2 service tasks)
- 3. Remove slides from SU database (table sudb/su_slides)
- 4. Move slide files to new folder
- 5. Start SU (launch both SUSvc and SlideHandler2 service tasks)
- 6. The Consistency Checker finds slides in the newly added folder, and builds up the database (table *sudb/su_slides*)
- 7. Since HUB registrations remain unchanged, slides can be opened in CaseCenter from their original locations, however slides are physically stored in another folder
- 8. Delete previously used Storage folder with the Service Unit Settings program

8.1.6 Requirements and recommendations

Each system component of CaseCenter (storage as well) is within the same – solely – Windows domain, in other words from network access, name resolution, and handling of user privileges points of view, are included in the scope of the same administration area; so they are mutually accessible and interoperable (including deactivation of occurrent bottlenecks such as firewalls, anti-virus applications, or security system limitations; otherwise – if these components are enabled – assure an absolutely transparent yet standard software interoperability.

• All of the storages of the specific SU must be connected with the same (and the only one) domain user. For this user must have explicitly-granted full access permission (in addition to effective rights related to group membership) both for shares and the file system.

Accordingly, it is the person's responsibility who performs the installation, to ensure that the target computer of the storage is inaccessible by other users using a different user credentials via the SU (neither for establishing connection related to storage, software, nor services) than the one selected.

- If possible, the connection of storages to the SU units must be performed when putting CaseCenter in operation, but their modification during operation is avoidable. Any alteration requires special circumspection and attention, be performed on a system unit out of service, and in accordance with the guidance within the topic.
- Permissions required for the connection and usage of the SU unit must be guaranteed on connectable storage prior putting them in operation, and then continuously during their operation time (while in use).
- The storage connected to SU must be at service non-stop, and with great reliability during operation.
- Connection of more than one storage from the same volume (drive or file-system-level logical unit) to an SU is not supported.
- The folder used as slide storage neither can be a root folder of a drive (for example, *D*:) nor a root folder of a network share (for example, *D*:) or a DFS path pointing to a root folder (for example, *\server\share*). NOTE: HUB/SU backup could not be performed from these locations.
- Do not connect a storage through an administrative Windows share, exclusively by granting appropriate permissions on an explicitly shared folder (for example, \\<<machine_name>>\ C\$).

To assure convenient operation performance, we suggest to designate a storage in such a way that it is located on an independent physical drive using different code than any other operating unit of the CaseCenter runs. To meet higher performance needs, further (inner – from system point-of-view) resource decoupling or exclusive use might be necessary.

8.2 Scan to Server

The relevant feature documentation can be found in the device-specific User's Guide for Pannoramic scanners.

8.3 Import slides

To import slides to CaseCenter, use the Slide Converter software that is also installed on your computer. For more information on how to use and import slides, refer to *Slide Converter User's Guide*.

9 Slide consistency checker, Lost and Found folder

Slide consistency checker runs in the background each day from 2:00 a.m. for two hours on the SUs. It monitors slide accessibility/availability, and sends status report to the HUB. This is necessary because in the database slides are not stored together with their meta-data, on a separate file storage. Therefore, the consistency between the database and the storage cannot be guaranteed through the transactional method, and it can suffer damage.

The checker sends a "per slide" status about the consistency checking to the HUB. Statuses can be of the following:

- Existing slide normal state, everything is OK
- **Missing slide** not present on the SU (for example, because it has been deleted from the storage evasively, not through CaseCenter)
- Slide that is not included in the database restore database to a previous backup, that excludes those slides that have been scanned since then, but which are located on the storage. Such slides will be collected to the "Lost and Found" folder on the HUB.

If a slide is missing, HUB marks it as incomplete, and is listed on the specific folder on the Slides & Folders panel. Slide state is displayed on the Service panel, Problematic slides list where the type of issue is indicated. If the slide is not included in the database, the slide is moved to the Lost and Found folder where the slide can be further managed (move, delete, etc.).

The process checks states of the HUB database, SU database, and physical file slides; and after their comparison the following issues can be found:

- If a slide is missing only from the SU database (slide is present physically and also in the HUB database) then it will be fixed, no action is necessary from your side.
- If the slide is located only in the HUB database, it will be marked as missing, and its state is displayed on the CaseCenter HUB interface (Slides & Folders and Service/Problematic slides) indicating that both the file itself and SU database entry are, or any of them is missing. This situation typically results when SU database is not restored and if the storage is missing.
- When only the slide file is missing, it may be the result of the following:
 - The SU, where the slide is stored, is not accessible (server is offline). On the HUB
 interface of CaseCenter "Missing SU" is indicated next to the slide (Slides & Folders),
 and "offline" status is displayed for the specific SU on the Service Units list at the
 Service tab panel.
 - If both the SU and the storage folder where the slide should be located on the SU are accessible, but the slide is missing from this folder (for example, because slide file has been deleted), the slide receives a "Missing slide" stamp on the Slides & Folders panel, and it will be included on the Problematic slides list as well.

- SU is accessible, but the storage folder on the SU where the slide should be is not (for example, network storage is shut down/offline). In such cases, we receive information of the problematic slides on the CaseCenter interface, on the Slides & Folders panel. Problematic slides do not appear on the Problematic slides list, but on the Service Units list on the Service panel ("Missing storage" status is displayed next to the SU).
- If the slide is missing from the HUB but is present in the SU database, and also the slide file is
 existing, then based on the actual slide information, it will be listed in the Lost and Found
 folder. This issue may arise during HUB restoration or due to data loss or if using an SU
 connected to a different HUB. Such slides can be managed in the Lost and Found folder
 (where move, delete, etc. options are available for you).
- If the slide file is existing, but it cannot be found on the HUB, nor the SU databases, then the slide is displayed in the Lost and Found folder. This issue may arise when the storage has been used at different location. In such cases slides can be managed in the Lost and Found folder (where move, delete, etc. options are available for you).

Lost and Found folder

This folder includes those slides that have been found by the consistency checker, and did not exist in the HUB database yet. The Lost and Found folder is located in the Root folder by default, and named to 'Lost and Found'. To select a different folder as destination, select a new one on the Service/Settings panel.

The actual Lost and Found folder cannot be deleted, not even by administrators.

The slides stored in this folder are categorized the following way: the *Lost and Found* main folder contains an *su_X* folder (where X is the ID of the SU), and its sub-folder structure is based on the time and date the slide was scanned (ordered as 'hour.minute' sub-folder within the 'year-month-day' parent folder). Slides are named to their scanning date, as being the only data known of the slide that is found.

NOTE: The *Lost and Found* folder is worth checking periodically.

10 Secondary Service Unit

Operation

Slide types and creation methods in accordance with the different SU states are the following:

- Both the SU set for the user, and slide SU of VS/VT, and Project Slide are offline
 - Slides created with Macro slide upload, slide upload, slide scan, and project slide must be stored on the designated secondary SU
 - This status is not interpreted if slides are created with VS create or VT create, because these slides are created on an SU only if the source slides (or their majority) are stored on the actual SU
- There is not enough free space both on the SU set for the user, and on the SU for storing slides based on which VS/VT, and Project Slide items have been created
 - Except for VS create, each slide type creation is performed on the secondary SU
- Both the SU set for the user, and the storage of SU for storing slides based on which VS/VT, and Project Slide items have been created are inaccessible
 - Except for VS create, each slide type creation is performed on the secondary SU

Important!

Newly created slides generated with slide duplication and slide import cannot be stored on the secondary SU Irrespective of SU, storage status, and slide type. Therefore, if any problem occurs with the SU or its storage when performing such actions, slides cannot be generated.

11 HUB and SU version compliance

Since several SUs can connect to a HUB, after upgrading some of the components they not necessarily are able to work together. If two components are not compatible with each other, then SU status turns to *Disabled* that is also identified and logged by the HUB.

Compatibility check is performed during the following events:

- 1. At the early stage of upgrade conflicted components are listed and the system notifies you that one ore more of its modules become offline if you continue with the upgrade. You may cancel the actual upgrade, and every system module remain operable and accessible irrespective of which component you are upgrading (HUB or SU).
- 2. At the end of upgrade process components that incompatible with each other are listed and turned disabled.
- 3. Each time **Change** function is called.
- 4. When registering a new Service Unit.

The system uses the following methods to determine component conflicts:

- HUB version number is stored in the SU that is used as the required minimum for compatibility purposes. If version number of the HUB is smaller than of the minimum for HUB stored in the SU, then the SU identifies HUB as conflicted, incompatible.
- A required minimum SU version number is stored in the HUB that is referred to as compatible. If version number of the SU is smaller than of the minimum for SU stored in the HUB, then the HUB identifies SU as conflicted, incompatible.
- If any of the two components identifies the other as incompatible, then the HUB and the SU mutually account each other incompatible, so the status of both components becomes *Disabled*.

Possible SU states on the HUB and their effects are the following:

Disabled: All of the slides stored on the actual SU are marked a Missing SU label. Slides cannot be opened in this status, cannot be selected, and none of the slide actions can be performed. Scanning, uploading, and importing a slide to the specific SU also cannot be initiated. When saving database, the database of the disabled SU will not be saved. The SU can be toggled from the disabled status only after a successful *Change* operation. HUB does not ping the SU when disabled. The SU takes up the disabled status on the HUB if the actual SU is incompatible, becomes inaccessible during upgrade, or *Change* operation is unsuccessful.

- *Online*: The opposite status of *Disabled*, every operation is allowed and can be performed. The HUB pings the SU once in a minute to check its availability.
- UnderCheckBySU: Consistency checker runs with high priority on the SU. Slides stored on the SU cannot be opened or selected, therefore slide operations cannot be performed as well. After consistency checker process is completed, SU status should turn to Online. The HUB pings the SU once in a minute to check its availability.
- *NeedcheckSU*: The system may take up this status by either of the following ways:
 - SU is in *UnderCheckBySU* status when upgrade procedure is initiated.
 - System takes up this status after HUB database restore. The HUB commands the SU to perform a consistency check with high priority (SU status is *UnderCheckBySU*). After consistency checker is performed successfully the system will be online. The HUB pings the SU once in a minute to check its availability.
- *Offline*: The SU takes up this status if the SU is inaccessible by the HUB. Slides stored on the SU cannot be opened and none of the slide operations can be performed. The HUB pings the SU once in a minute to check its availability.

12 Troubleshooting

Windows Updates

Microsoft[™] releases updates for Windows Server 2012 R2 operation system used by CaseCenter server. These updates are followed up by the specialists and technicians at Thermo Fisher Scientific., however it may occur that a future update installed automatically on your server may cause restricted or erroneous server operation.

If you do not consider your CaseCenter server a critical element in terms of availability, and take accidental risks of Windows Updates, it is available for you to enable automatic updates for your operation system. Whenever an error comes from the Microsoft update, remove that specific update and contact Thermo Fisher Scientific support or your local distributor about the aspects and symptoms of the caused error.

Otherwise, do NOT enable the automatic installation of Microsoft updates on your server's operation system. On the other hand, your CaseCenter server will operate dispensing continuously enforced system safety offered by security updates, therefore you must ensure secure server operation and its security. For example, do not connect your server directly to the Internet, and ensure that the server is available through your own secure network.

Should we informed about a Microsoft update release is non-conform to the operation of our product, the round of duties will be announced to our partners and customers on our website promptly.

Important!

Do **NOT** run CaseCenter **AND** Windows updates at the same time.

SU Installation

Registration is unsuccessful

- Is the admin user name and password correct?
- Check in the browser that HUB is accessible and can be logged into it. If not then:
 - The SQL user defined during the installation of HUB does either not exist, its password is incorrect, or does not have the permission to access the HUB
 - License is invalid/expired (dongle or license file)

Installation of prerequisite files is unsuccessful

• Shut down running *vcredist* processes on **Windows Task Manager / Processes** panel.

Slide Storage

Multiple connection error – "Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again."

- 1. Remove all mapped network drives connected to the storage server.
- 2. Log off from CC/SU then log on again. If the problem still persists, then:
- 3. Close the network session on the storage, and if you did not succeed, then:
- 4. Restart storage

Storage management error – "The trust relationship between this workstation and the primary domain failed." OR "Logon failure: unknown user name or bad password." messages are received

• Disconnect SU from domain, then reconnect it

Server Upgrade

'Pure virtual function call' message is displayed during upgrade

Solution:

- 1. Open Windows Task Manager
- 2. End "SlideHandlerInsHelper.exe" process

For troubleshooting assistance, please contact us at Thermo Fisher Scientific .

Thumbnails are not visible

Thumbnail cannot be displayed after Windows upgrade

Solution:

• User must be granted access to the following folder:

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\

Index

В	
Block	
Brightfield	61
C	
Case	17, 19, 57, 58, 59, 60, 67
CaseCenter	7, 8, 9, 37, 40, 57, 58, 61, 68
E	
Edit	20, 26, 27, 31, 41, 52, 53, 57, 58, 59, 62
F	
Fluorescent	61
G	
Group7, 9, 19, 23, 25, 26, 27,	28, 29, 30, 31, 32, 33, 34, 37, 51, 52, 64, 65
н	
HIS	
HUB	9, 38, 46, 54, 57, 59, 60, 66, 70, 71, 75
1	
Import	29, 30, 31, 32, 33, 50, 51, 62, 67, 68, 69
LDAP7, 23, 27,	
LDAP object guid attribute	
Login queue	
S	
Search	
Server	7, 8, 9, 17, 21, 40, 44, 61, 66, 67, 75, 76
Service Unit	
Share	
SU8, 9, 31, 32, 33, 34, 37, 38, 46, 54,	59, 60, 61, 63, 64, 65, 66, 67, 70, 71, 75, 76
т	
Teleconsultation	7, 9, 24, 38
U	
Upload	