Mitel TA7100

58014896 REV00

CONFIGURATION BACKUP AND RESTORE

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

Trademarks

Mitel TA7100 Configuration Backup and Restore
58014896 REV00 - May 2016

Configuration Backup and Restore

Performing a configuration backup allows you to have a copy of the entire configuration at the time the backup was performed.

The configuration backup can be used:

- to revert the running configuration to a valid configuration when the running configuration generates error messages or no longer works;
- to deploy a valid configuration on other units;
- to revert to a known configuration when too many changes were made to the running configuration;
- to deploy a backup configuration on a replacement unit.

The configuration backup includes every aspects of the configuration, i.e.

- the status and configuration parameters;
- the certificates;
- the Rulesets;
- any other files contained in the unit's file management system.

But the configuration backup does not include the File service files, except for the Rulesets.

The configuration backup is an XML file and can, if necessary, be encrypted.

Please note that you can use a backup file on a unit with a newer or same firmware version than what is was taken from. A backup file can not be restored on an older firmware version than the one it was taken from.

Backup made on firmware version vX	Unit firmware version	Possible
Backup.v3	Firmware version 3	YES
Backup.v1	Firmware version 3	YES
Backup.v1	Firmware version 1	YES
Backup.v3	Firmware version 1	NO

The Configuration Back and Restore performed on Dgw v2.0.31 includes all Rulesets. However, starting on Dgw v.2.0.32 only the Rulesets modified by the user will be included in the configuration backup and restore. If a configuration backup is performed on Dgw v2.0.31 and restored on a newer version of Dgw, all Rulesets existing in v2.0.31 will be copied as custom Rulesets i.e the system will not use the factory Rulesets of the newer version even if they were not modified.

File Servers

Configuring the FTP Server

Prerequisite If you are not familiar with the procedure on how to set the FTP root path, please refer to your FTP server's documentation.

Perform this procedure if you plan to use the FTP transport protocol.

Steps

1. Set a FTP service on the assigned server.
2. Make sure the FTP server can be reached by the Mitel unit.

NOTE: If the file server is located behind a firewall, make sure that port 21 is open.

Configuring the TFTP Server

Prerequisite If you are not familiar with the procedure on how to set the TFTP root path, please refer to your TFTP server's documentation.

Perform this procedure if you plan to use the TFTP transport protocol.

Steps

1. Set a TFTP service on the assigned server.
2. Make sure the TFTP server can be reached by the Mitel unit.

NOTE: If the file server is located behind a firewall, make sure that port 69 is open.

Configuring the HTTP Server

Prerequisite If you are not familiar with the procedure on how to set the HTTP root path, refer to your HTTP server's documentation.

Perform this procedure if you plan to use the HTTP transport protocol.

Steps

1. Set a HTTP service on the assigned server.
2. Make sure the HTTP server can be reached by the Mitel unit.

NOTE: If the file server is located behind a firewall, make sure that port 80 is open.

Configuring the HTTPS Server

Prerequisite If you are not familiar with the procedure on how to set the HTTPS root path, please refer to your HTTPS documentation.

Perform this procedure if you plan to use the HTTPS transport protocol.

Steps

1. Set a HTTPS service on the assigned server.
2. Make sure the HTTPS server can be reached by the Mitel unit.

NOTE: If the file server is located behind a firewall, make sure that port 443 is open.

3. Make sure that in the Management > Certificates tab, in the Certificate Import Through Web Browser table, there is a certificate that authenticates the HTTPS server selected in the Path field, and that Other is selected in the Type field.
4. Set the configuration parameters. Refer to the Parameters section.

Configuring the Mitel Unit to Use an SNTP Server

Prerequisite Make sure there is an SNTP server available.

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

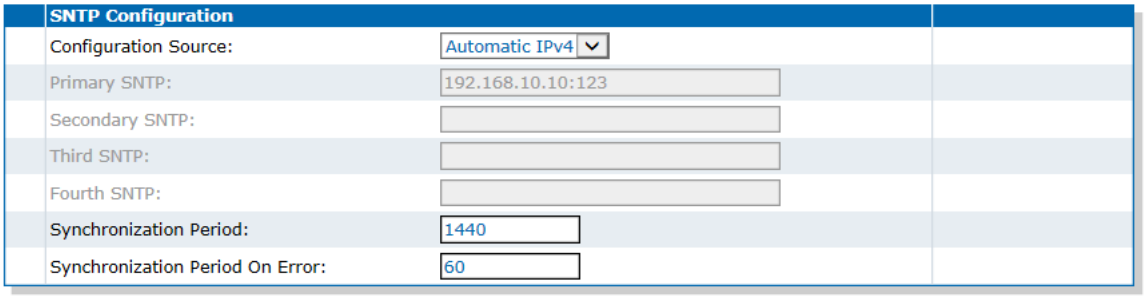
1. Go to Network/Host.
2. In the SNTP Configuration table, from the Configuration Source selection list, select the connection type from which you wish to obtain the SNTP parameters.

NOTE: Complete Step 3 only if you are using static SNTP server(s), otherwise go to step 4.

3. Provide an IP address or domain name and port numbers for each SNTP server you are using.
4. If necessary, change the displayed default value of the Synchronisation Period.

5. If necessary, change the displayed default value of the Synchronisation Period on Error.
6. Click Apply.

Result: The SNTP host name and port will be displayed in the Host Status table under Network/Status.



Simple Network Time Protocol (SNTP)

The Simple Network Time Protocol (SNTP) is used to update and synchronise the clock of the Mitel unit (day, month, time) when it is restarted.

Mitel units do not all include a real time clock allowing them to maintain accurate time when they are shutdown. Your system needs to have access to accurate time, for instance, if you are using HTTPS or for the caller ID feature. In these cases, an SNTP client with an available SNTP server will need to be configured to allow the system to update and synchronise its time to the local clock.

SNTP is used to synchronise an SNTP client with an SNTP or NTP server by using UDP as transport. The Mitel unit implements an SNTP version 3 client.

Backup

Performing a Configuration Backup to a File Server

Prerequisite Depending on the type of transport protocol used, one of the following procedures must be completed:

- Configuring the FTP Server
- Configuring the TFTP Server
- Configuring the HTTP Server
- Configuring the HTTPS Server

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

1. Go to Management > Backup / Restore.
2. In the Image Configuration table, in the File Name field, indicate the name of your backup.

NOTE: The file name is case sensitive. As a best practice, add the *.xml extension. Make sure to indicate the firmware version the backup was made from because a backup file can not be restored on an older firmware version than the one it was taken from.

NOTE: Remember, if you have several units with several configurations and plan to reuse the configuration on another unit, the name must be explicit. Indicate the date of your backup, the interfaces used, the device model, etc.

3. From the Transfer Protocol selection list, select the type of protocol you wish to use to transfer your backup.

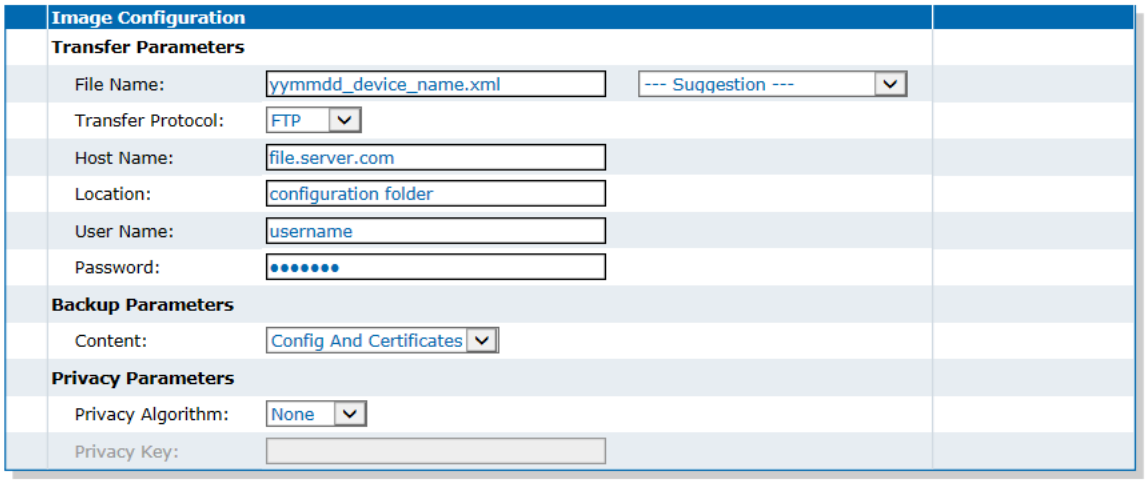
NOTE: This must be consistent with the file server you have configured.

4. In the Host Name field, enter the file server IP address or FQDN.
5. In the Location field, enter the path relative to the root of the file server where the backup will be saved.
6. If your server requires authentication, enter your username and password.
7. From the Content selection list, choose the elements you wish to include to the backup.
8. If you wish to use encryption for backup operations, complete the Privacy Parameters.

NOTE: Mitel strongly recommends to use a privacy algorithm (encryption) to protect certificates and passwords.

9. Make sure the file server is started.
10. Click Apply and Backup Now.

Result: The configuration will be saved on the selected file server.



Performing a Configuration Backup to the Unit File Management System

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

1. Go to Management > Backup / Restore.
2. In the File Name field, indicate the name of your backup.

NOTE: The file name is case sensitive. As a best practice, add the *.xml extension. Make sure to indicate the firmware version the backup was made from because a backup file can not be restored on an older firmware version than the one it was taken from.

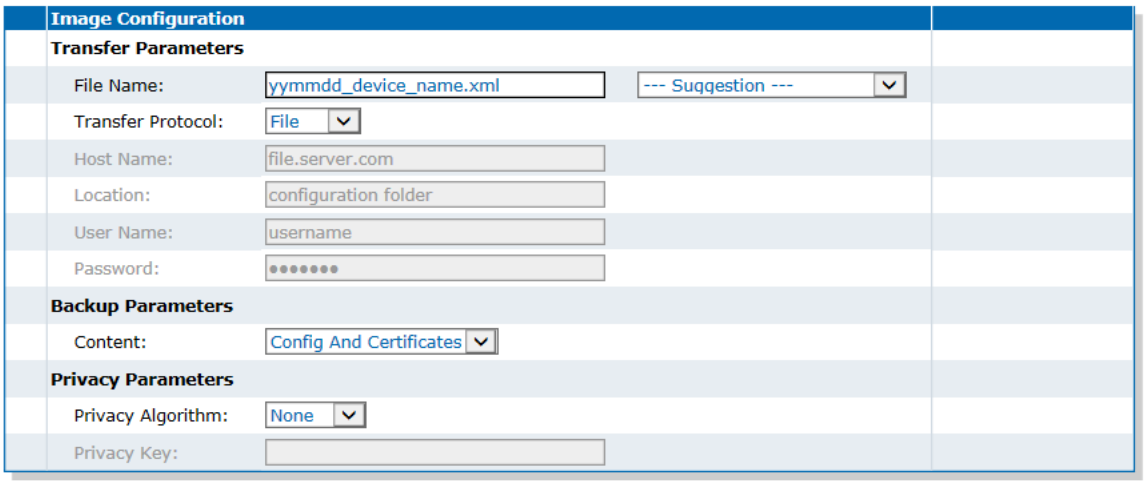
NOTE: Remember, if you have several units with several configurations and plan to reuse the configuration on another unit, the name must be explicit. Indicate the date of your backup, the interfaces used, the device model, etc.

3. From the Transfer Protocol selection list, select File.
4. From the Content selection list, choose the elements you wish to include to the backup.
5. If you wish to use encryption for backup operations, complete the Privacy Parameters.

NOTE: Mitel strongly recommends to use a privacy algorithm (encryption) to protect certificates and passwords.

6. Click Apply and Backup Now.

Result: The configuration will be saved in the unit's file management system. The backup file will appear at the end of the list of the File page, under Management > File.



Restore

Restoring a Configuration From a File Server

Prerequisite Depending on the type of transport protocol used, one of the following procedures must be completed:

- Configuring the FTP Server
- Configuring the TFTP Server
- Configuring the HTTP Server
- Configuring the HTTPS Server

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

1. Go to Management > Backup / Restore.
2. In the File Name field, indicate the name of your backup or use the Suggestion selection list.

NOTE: The file name is case sensitive. Remember that a backup file can not be restored on an older firmware version than the one it was taken from.

3. From the Transfer Protocol selection list, select the type of protocol you wish to use to transfer your backup.

NOTE: This must be consistent with the file server you have configured.

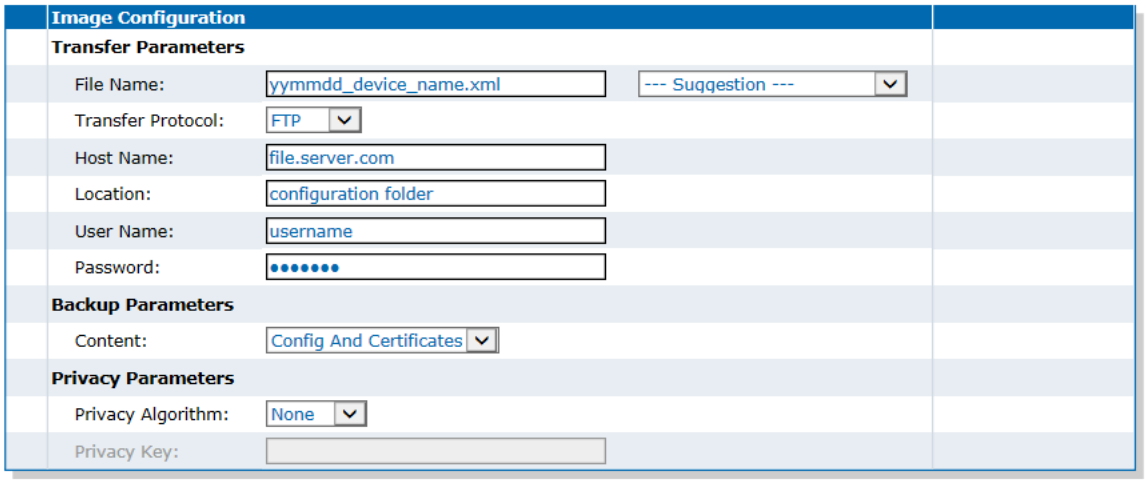
4. In the Host Name field, enter the file server IP address or FQDN.
5. In the Location field, enter the path relative to the root of the file server where the backup will be saved.
6. If your server requires authentication, enter your username and password.
7. Make sure the file server is started.
8. If the backup file is encrypted, complete the Privacy Parameters.

NOTE: The privacy key must match the privacy key used to encrypt the backup file.

9. Click Apply & Restore Now.

NOTE: A pop-up message will be displayed indicating that the unit will be automatically restarted once the restore procedure is completed.

Result: The unit will be restarted. The configuration will be restored from the configured file server, and used as the running configuration.



Restoring a Configuration from the Unit File Management System

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

1. Go to Management > Backup / Restore.
2. In the File Name field, indicate the name of your backup or use the Suggestion selection list.

NOTE: The file name is case sensitive. Remember that a backup file can not be restored on an older firmware version than the one it was taken from.

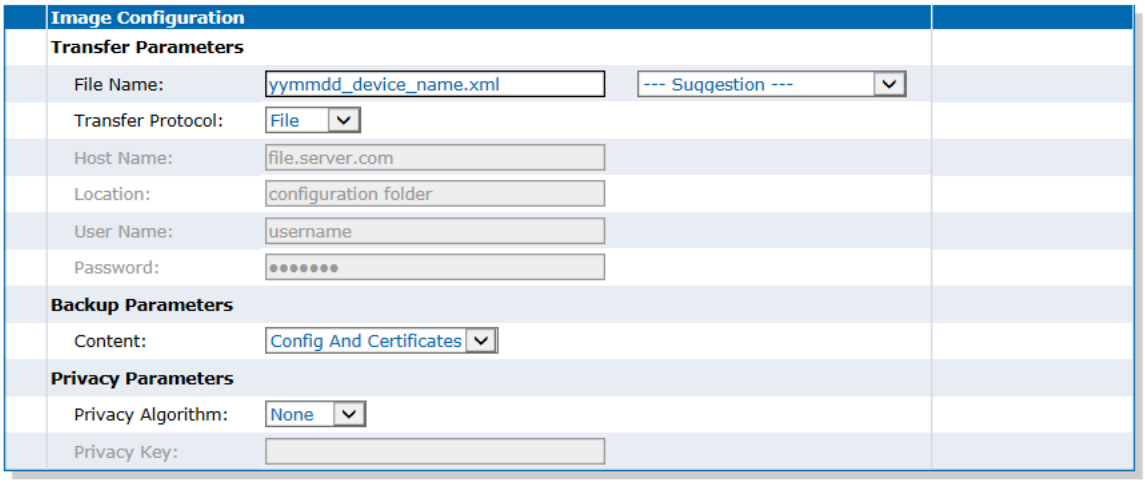
3. From the Transfer Protocol selection list, select File.
4. If the backup file is encrypted, complete the Privacy Parameters.

NOTE: The privacy key must match the privacy key used to encrypt the backup file.

5. Click Apply & Restore Now.

NOTE: A pop-up message will be displayed indicating that the unit will be automatically restarted once the restore procedure is completed.

Result: The unit will be restarted. The configuration will be restored from the system's file management system, and used as the running configuration.



Restoring a Configuration from Your PC

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

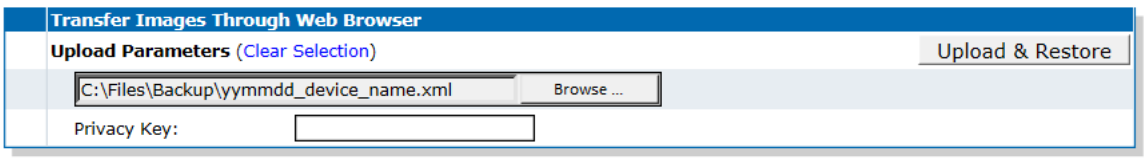
1. Go to Management > Backup / Restore.
2. If the Web pages are not encrypted (HTTPS), click Activate unsecure file transfer through web browser, located at the top of the tables.
3. In the Transfer Scripts Through Web Browser table, browse to the location of the file you wish to restore.

NOTE: The file name is case sensitive. Remember that a backup file can not be restored on an older firmware version than the one it was taken from.

4. Click Upload & Restore.

NOTE: A pop-up message will be displayed indicating that the unit will be automatically restarted once the restore procedure is completed.

Result: The unit will be restarted. The configuration will be restored from your PC, and used as the running configuration.



Parameters

Although the services can be configured in great part in the web browser, some aspects of the configuration can only be completed with the MIB parameters by :

- using a MIB browser, such as the Mitel Unit Manager Network (UMN);
- using the CLI;
- creating a configuration script containing the configuration parameters.

Conf > Configuration Parameters

Image Transfer Cipher Suite

Refer toConf.ImageTransferCipherSuite in the TA7100 Reference Guide.

Image Transfer Tls Version

Refer toConf.ImageTransferTlsVersion in the TA7100 Reference Guide.

Mitel
Powering connections

mitel.com