DOMINO

Domino D-Series
Pharma ユーザーガイド

D120i

D320i

D620i

このページは意図的に空白にしています。

目次

ページ

このページは意図的に空白にしています。

はじめに

この Pharma ユーザーガイドでは、D-Series レーザーマーキングシステムについて説明します。このシステムは、リモートのタッチパネルか、QuickStep ソフトウェアがインストールされた Microsoft Windows 7® または Microsoft Windows 8® を実行中の PC から操作します。

このガイドでは、D-Series レーザーマーキングシステムの Pharma バージョンに特有の機能について説明します。このシステムには、ユーザー ID およびパスワードシステム、電子署名および電子記録機能が含まれています。

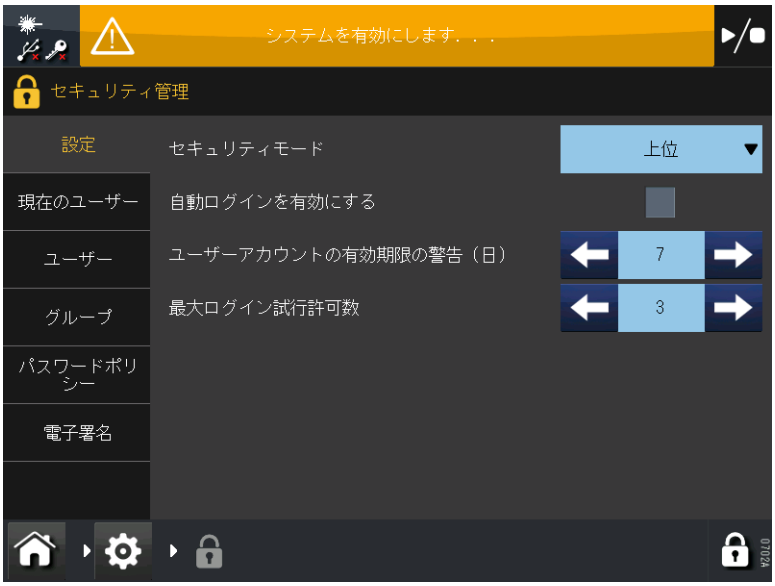
注記：　ユーザー ID、パスワード、電子署名および電子記録機能を有効にするには、Domino Pharma Key をコントローラーに差し込み、[セキュリティモード] を [上位] に設定します。

Pharma バージョン以外の機能については、詳しくは『D-Series 製品マニュアル』を参照してください。

セットアップ

(1) 管理者ユーザー名とパスワードを使用してログインします。

(2) [設定] > [セキュリティ] > [設定] を選択します。



(3) [セキュリティモード] のドロップダウンの矢印をクリックし、[上位] を選択します (選択されていない場合)。

自動ログインを有効にする:選択したユーザーの自動ログインを許可したい場合のみ、チェックボックスをオンにします。

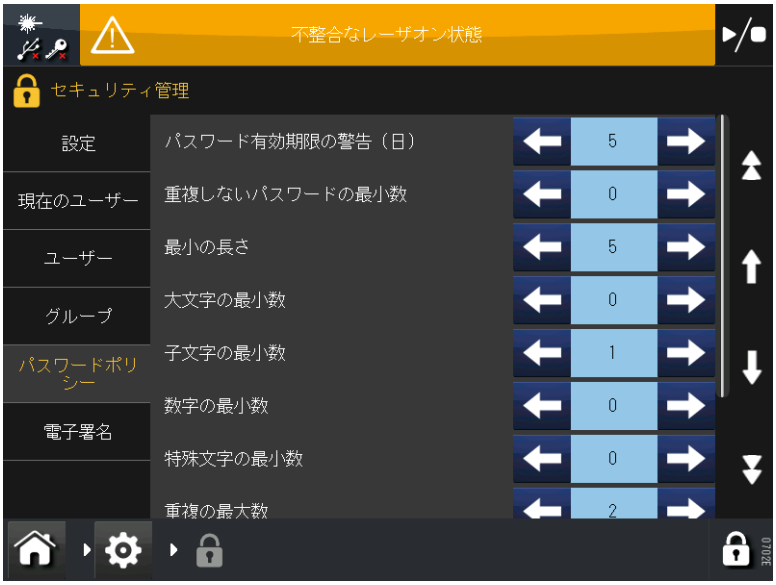
自動ログインユーザー:ドロップダウンリストからユーザーを選択します。

ユーザーアカウントの有効期限の警告 (日):ユーザーアカウントの有効期限が切れるまでの日数を入力します。この日数は画面上に通知として表示されます。

最大ログイン試行許可数：ログイン失敗回数の許容範囲を入力します。この回数を超えるとアカウントがロックされます。

パスワードポリシー

[設定] > [セキュリティ] > [パスワードポリシー] を選択します。



以下の設定が可能です。

- [パスワード有効期限の警告 (日)] — 指定した日数前に、パスワードの有効期限切れを警告。
- [重複しないパスワードの最小数] — 指定した回数より前に使用されていたパスワードは、新規パスワード設定時に重複の判定対象になりません。
- [最小の長さ]
- [大文字の最小数]
- [子文字の最小数]
- [数字の最小数]
- [特殊文字の最小数] — パスワードに最低限使用する必要がある特殊文字の数。
- [重複の最大数] — 1 つのパスワードの中に含めることができる重複文字の数。
- [最大 ID 文字数] — 1 つのパスワードの中に含められる ユーザー ID 文字列に一致する文字の数。
- [特殊文字] — 必ず含めなければならない特殊文字を入力します (キーボード上の任意の文字を選択可能)。

グループ

1 つのグループは、指定した数のユーザー承認によって構成されます。D-Series の出荷時設定では、デフォルトで管理者、ログアウト、オペレーター、スーパーバイザーの 4 つのグループが存在します。それぞれ、あらかじめ承認が選択されています。ただし、各グループに付与されている承認を、必要に応じて変更することもできます。

新しいユーザーおよび既存ユーザーは、1 つ以上のグループに関連づけられることにより、承認を継承します。

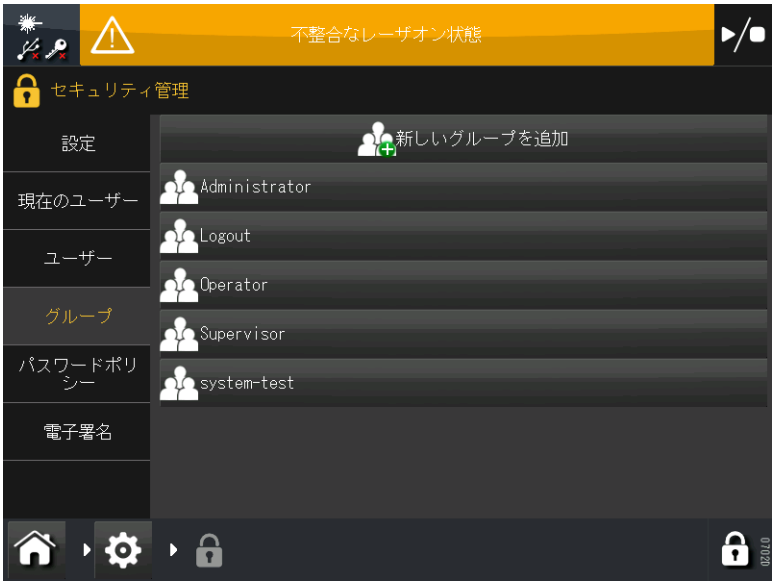
新しいグループを追加して、必要な承認を付与することもできます。

新しいグループの追加

以下で説明する機能を使用すると、選択し承認で新しいグループを作成できます。1 つまたは複数のグループと関連づけられたユーザーは、それらのグループの承認を継承します。

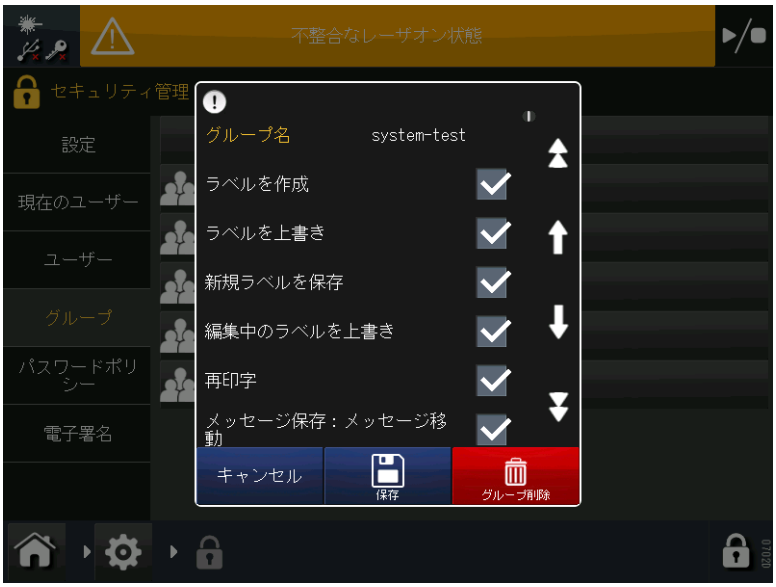
(1) [設定] > [セキュリティ] > [グループ] を選択します。

(2) [新しいグループを追加] を選択します。



(3) 新規グループ名を入力し、[保存] を選択します。

(4) グループに必要な承認のチェックボックスをオンにします。



(5) [保存] を選択すると、グループリストに新しく作成されたグループが表示されます。

グループの削除

(1) [設定] > [セキュリティ] > [グループ] を選択します。

(2) 削除するグループをグループリストから選択し、[グループ削除] を選択します。

(3) [OK] を選択して、削除を確認します。

承認の変更

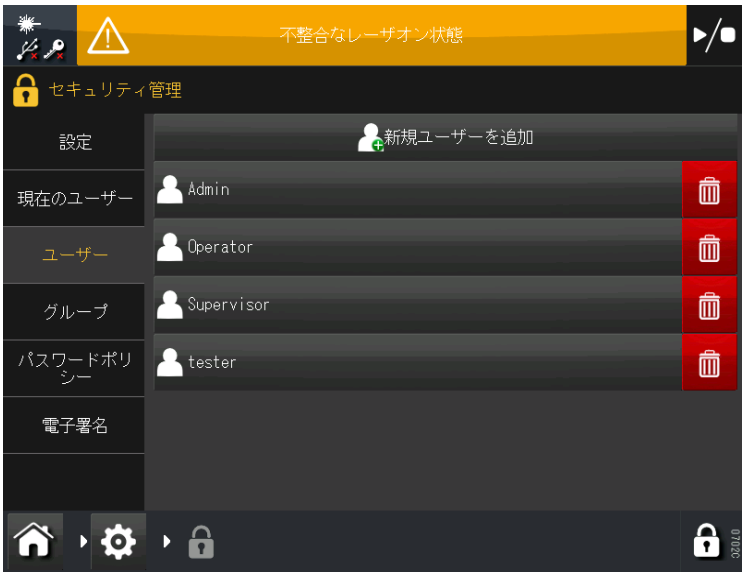
(1) [設定] > [セキュリティ] > [グループ] を選択します。

(2) 目的のグループを選択し、承認を必要に応じて変更します。

(3) [保存] を選択し、変更を確認します。

新しいユーザーの追加

(1) [設定] > [セキュリティ] > [ユーザー] を選択します。



(2) [新規ユーザーを追加] を選択します。

ユーザー名 : 目的のユーザー名 (ユーザー ID) を入力します。

パスワード : パスワードを入力します。

新しいパスワードの再入力 : パスワードを確認します。

グループ : ドロップダウンリストから、新しいユーザーに必要な承認を持つグループを 1 つまたは複数選択します。

ステータス : ドロップダウンリストから、[アクティブ]、[休止] または [ロック中] を選択します。

新しいユーザーに対して初回ログイン時のパスワード変更を強制するには、[パスワード変更が必要] チェックボックスをオンにします。

必要に応じて、新しいユーザーの [名]、[姓]、[部門] を入力します。

数分間の無反応タイムアウト : 必要に応じて、操作を行わない場合にユーザーが強制的にログアウトするまでの時間を分数で指定します。

有効期限報告有効 : チェックボックスを選択するとオンになります。

有効期限報告 : 必要に応じて、ユーザーアカウントの有効期限が自動的に切れる日付を入力します。

パスワード有効期限 : ユーザーのパスワードが無効になり、新しいパスワードの作成が必要になるまでの日数です。

ユーザーの削除

注記：　　削除した場合、元に戻すことはできませんので注意してください。

(1) [設定] > [セキュリティ] > [ユーザー] を選択します。

(2) 目的のユーザーの削除アイコン を選択します。

(3) [OK] を選択してユーザーを削除します。

ユーザーパスワードの変更

(1) [設定] > [セキュリティ] > [ユーザー] へ進み、目的のユーザーを選択します。

(2) 新しいパスワードを入力して、さらにもう一度入力します。

(3) [変更] を選択し、次に [保存] を選択して、パスワードを変更します。

ユーザーステータスの変更

ユーザーステータスを現在のステータス (「ロック中」など) から新しいステータス (「アクテイブ」など) へ変更することができます。

(1) [設定] > [セキュリティ] > [ユーザー] へ進み、目的のユーザーを選択します。

(2) [ステータス] ドロップダウンリストから、新しいステータスを [アクティブ]、[休止] または [ロック中] *から選択します。*

(3) [保存] を選択します。

電子署名 & 電子記録

電子署名の使用および電子記録の作成がサポートされています。

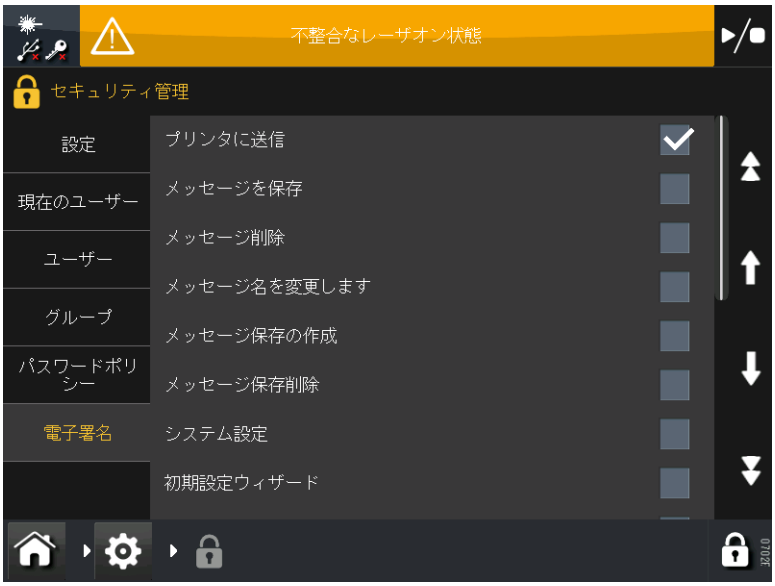
電子署名を要求するよう設定した操作を試みるたびに、ユーザーはパスワードの入力を要求されます (つまり、その操作にユーザー ID とパスワードを関連づけるように要求されます)。パスワードを入力すると、電子記録が作成されます。

ユーザーの操作の一覧はアクションログとして保存されます。このログは .db ファイルとしてエクスポートできます。

実際の例

以下では、電子署名および電子記録の機能について、実際の例を挙げて説明します。

(1) 「管理者」としてログインし、[設定] > [セキュリティ] > [電子署名] を選択します。



(2) 電子署名の入力を要求する承認を選択し、[OK] を選択します。この例では、[プリンタに送信] の承認を選択したところです。

(3) これで、すべてのユーザーは、上記のリストで選択された操作を実行する前にパスワードの入力を要求されるようになります。この操作の内容と、操作を行った時間および日付は、ユーザーの名前と関連づけられて監査証跡ログに記録されます。それが電子記録を構成することになります。

注記 :　電子署名の要求に関する設定は、管理者を含むすべてのユーザーに適用されます。

(4) メッセージエディタへ進み、新しいメッセージを作成し、「メッセージ 1」というテキストを入力します。

(5) 任意の名前を付けてメッセージを保存します。

(6) [プリンタに送信] を選択すると、パスワードの入力を要求されます。入力すると、メッセージがプリンタに送信されます。この操作は、監査証跡ログに電子記録として記録されます。

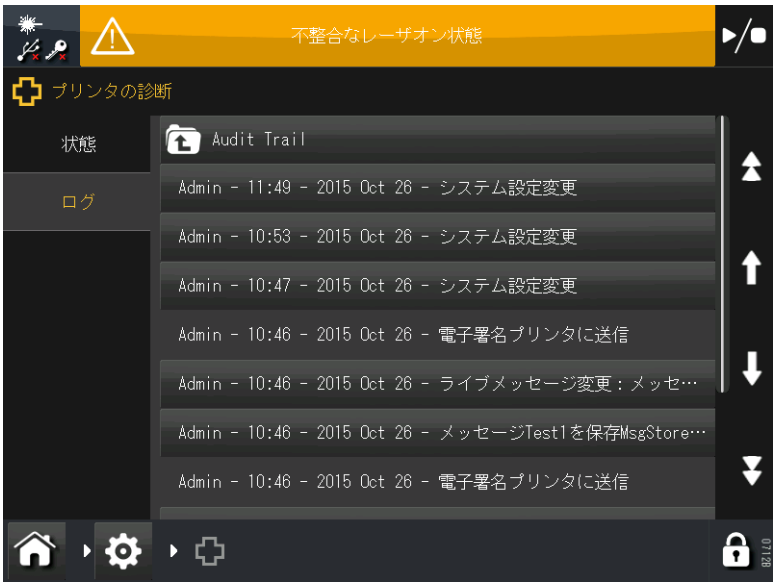
(7) メッセージを数回印字します。

(8) メッセージを編集し、上記のテキストを「メッセージ 2」に変更します。

(9) メッセージを保存してプリンタに送信しようとすると、前回と同じように電子署名を要求するメッセージが表示されるので、パスワードを入力します。メッセージを数回印字します。

(10)[設定] > [診断] > [ログ] > [監査証跡ログ] を選択します。画面上に過去の操作が一覧表示されます。一覧には、日付、時間、実行したユーザー ID、操作の説明が記載されています。

(11)「オブジェクトテキスト 1 変更」を選択します



(12)テキスト変更の詳細が表示されます。

監査証跡ログ

システム動作の最適化のために、アクションログは毎日アーカイブされ、古い記録がライブデータベースからアーカイブデータベースへ移動します。

監査証跡ログでは、最近 300 件の記録に加えて、アーカイブ化を最後に行った時点よりも後に作成されたすべてのエントリーが表示されます。

監査証跡ログはいつでもエクスポートすることができます。ただし既定では、ログが作成されてから 183 日が経過した場合、ログがエクスポートされるまでユーザーはマーキングを有効にすることができなくなります。

既定では、ログが作成されてから 153 日が経過した場合、監査証跡ログのエクスポートを促す警告メッセージが表示されます。

警告およびエラーメッセージが表示されるまでの日数を変更するには、[ホーム] > [設定] > [警報の設定] > [警報の範囲] を選択します。

監査証跡ログをエクスポートするには

(1) コントローラーの USB ポートか、使用中のリモートアクセス手段 (例えばタッチスクリーンパネル) に付属している USB ポートに、USB メモリを差し込みます。

(2) [ホーム] > [設定] > [ファイルマネージャ] > [プリンタディスク] > [ログ] を選択します。

(3) 監査証跡ログの鉛筆アイコンを選択し、[コピー] を選択します。

(4) [ファイルマネージャ] を選択し、次に対象の USB メモリを選択します。

(5) [貼り付け] を選択し、USB メモリにログをコピーします。

監査証跡ログファイル (拡張子 : .log) が USB メモリのファイル一覧に表示されます。

Domino Dyn3LogViewer

エクスポートすると、.NET framework 3.5 がインストールされた MS Windows PC 上で Domino Dyn3LogViewer ユーティリティーを使用して、監査証跡ファイル (ライブおよびアーカイブ済みの記録) を閲覧することができます。このユーティリティーは、Domino への申し込み後に使用可能になります。

Domino Dyn3LogViewer ユーティリティーを使用すると、アクションログをテキストファイル形式でエクスポートすることもできます。

監査証跡ログの閲覧 :

Dyn3LogViewer ユーティリティーを開き、[ファイル] > [開く] を選択し、適切な場所で対象の監査証跡ログを選択します。

ログの記入に使用される言語を変更するには、[言語] を選択し、ドロップダウンリストから対象の言語を選択します。

監査証跡ログをテキストファイル形式でエクスポート :

Dyn3LogViewer ユーティリーティーを [ファイル] > [開く] > [テキストファイルにエクスポート] を選択し、ファイルの保存場所を指定して、[保存] を選択します。

監査証跡ログの削除

(1) [設定] > [診断] > [ログ] > [監査証跡ログ] を選択します。

(2) 赤い  アイコンを選択し、[(日数) 前より古い入力を削除] の値を確認します。必要に応じて [日数] の設定値を修正し、[OK] を選択します。