セキュアエリア - ヘルプ

1. セキュアエリアの価値

- SAP からのシステムへのリモートログオン用アクセスデータの保存場所です。
- アクセスデータは、インシデントではなくシステムに関連付けられます（2007 年 Q1 以降）。
- アクセスデータはシステムにつき一度だけ登録する必要があり、このシステムを参照する各インシデントで使用されます。
- ユーザーのアクセスデータは、SAP に対してユーザーパスワードの表示を制限する目的で特定のインシデントに明示的に割り当てることができます（2007 年 Q4 以降）。
- アクセスデータは、いつでも変更できます。
- すべてのデータ変更およびセキュアエリアへのアクセスは、履歴ログで確認できます。
- インシデントは、システム用のアクセスデータが登録されているかどうかを示します。

2. 権限の定義

- 「カスタマーログオンデータ：個人」権限を持つ S ユーザーは、ログオンデータを保存できるほか、以前記録されたログオンデータを照会または変更できます。ただし、このユーザーはほかのユーザーが登録したパスワードの照会はできません（変更はできます）。
- 「カスタマーログオンデータ：管理者」権限を持つ S ユーザー（例：ユーザー管理者）は、あらゆる S ユーザーのすべての保存済みログオンデータを登録、変更、または照会できます。

3. セキュアエリアへのアクセス方法

次の方法でアクセスデータを更新します。

- [リモートログオンデータ更新]ボタンをクリックしてインシデントにより直接更新、または
- [カスタマーログオンデータ]ボタンをクリックしてシステムデータ管理機能から集中的に更新

注記：特定のユーザーを特定のインシデントに割り当てるオプションを使用できるのは、インシデントからセキュアエリアにアクセスした場合に限られます（セクション 5 を参照）。

4. セキュアエリアアプリケーション

このアプリケーションは、お客様が必要に応じて SAP サポートに「ユーザー」、「SAProuter」、「サーバー」、「コンタクト」、および「情報」のデータを提供する場合、またはこれらのデータをメンテナンスする場合にのみ使用します。可能な操作は、そのお客様に割り当てられたすべてのシステムのログオンデータのメンテナンスのみです。他のお客様の情報は提供されません。

- [インシデント]セクション - インシデントごとのユーザー表示をメンテナンスするために使用します。初期設定では、SAP サポートの処理担当者はメンテナンス対象のユーザー全員の情報を確認できます。
- [履歴ログ] - 各システムのすべてのデータ変更およびセキュアエリアへのアクセスは、履歴ログで確認できます。ログは Excel にエクスポートできます。

別のお客様に関連するシステムの表示またはメンテナンスを行うには、ヘッダーの [Related Options] ドロップダウンを選択します。

ログオンデータを入力したら、[ログオンデータの照会]をクリックします。入力済みのすべてのログオンデータが一目で分かるように照会モードで表示されます。これらのデータを更新したユーザーおよび「カスタマーログオンデータ:管理者」権限を持つユーザーのみが、保存されているパスワードを表示できます。「カスタマーログオンデータ:個人」権限を持つユーザーは、ほかのユーザーによって保存されたパスワードの照会はできませんが、変更はできます。

5. インシデントの制限ビュー

インシデントを登録または更新する場合は、特定のユーザーを特定のインシデントに割り当てることができます。したがって、SAP インシデント処理者に対して、この特定のインシデントが照会可能なユーザーを制限できます。インシデントを登録する場合、[制限ユーザビューの更新]ボタンをクリックして制限ビューにアクセスするには、インシデントを先に保存する必要があります。

- この制限は SAP システムユーザーのみを対象とし、SAProuter ユーザーや追加サーバーのユーザーなど、ほかのユーザーには影響しません。
- ほかのシステムまたはインストレーションからユーザーを選択することもできます。
- ユーザーが明示的にインシデントに割り当てられている場合、SAP は、この制限リストに含まれているユーザーのみを表示できます。ほかのすべてのユーザーは表示されません。
- ユーザーが明示的にインシデントに割り当てられていない場合、ログイン情報の可視性に関する制限はありません。そのため、すべてのユーザーおよびパスワードが SAP に対して表示されます。

注記: この内容を変更することで、お客様は、特定のインシデントにのみ有効なユーザーをシステムに対して登録できます。制限ビューを登録して画面を更新すると、対応するシステムの下で、このビューの構築対象であるインシデント番号とともにアイコンが表示されます。

特定のインシデントに有効なビューを削除するには、ビュー内のすべてのユーザーを選択して[ビューの削除]ボタンをクリックします。ビューに割り当てられているユーザーが存在しなくなると、そのビューは表示されなくなります。

6. 履歴ログの照会

すべてのデータ変更およびセキュアエリアへのアクセスは、履歴ログで追跡されます。インシデントからセキュアエリアが呼び出されると、インシデント番号もログに記録されます。

注記: 同じユーザーが、変更を加えることなくセキュアエリアを 1 日に複数回呼び出した場合は、ログが読みやすくなるように、最初のログインのみが追跡されます。