System Log

Panduan Modul: System Log (User Login Logout)

Lokasi Modul
Pengaturan > Pengaturan Sistem > System Log

Tujuan Modul
Modul System Log berfungsi sebagai catatan audit keamanan yang merekam semua aktivitas login dan logout pengguna di dalam sistem. Tujuannya adalah untuk memberikan jejak digital yang jelas mengenai siapa saja yang mengakses sistem, kapan mereka masuk dan keluar, serta dari mana mereka mengaksesnya. Ini adalah alat penting untuk pemantauan keamanan dan analisis aktivitas pengguna.

Penjelasan Tampilan dan Fitur

Halaman utama modul ini adalah antarmuka untuk melihat dan memfilter data log.

- **Filter Pencarian**:
    - **User ID**: Memungkinkan administrator untuk memfilter log dan hanya menampilkan aktivitas dari satu pengguna spesifik.
    - **Mulai Tanggal** dan **Hingga Tanggal**: Filter rentang waktu untuk melihat aktivitas login atau logout dalam periode tertentu.

- **Cari**: Tombol untuk menerapkan filter yang telah dipilih.
- **Tampilkan semua**: Tombol untuk menghapus semua filter dan menampilkan kembali seluruh catatan log.

- **Tabel Daftar Log**:
  - **No**: Nomor urut.
  - **User ID**: ID unik dari pengguna yang melakukan aktivitas.
  - **ID Karyawan**: ID karyawan yang terkait dengan akun pengguna tersebut.
  - **Nama User**: Nama akun pengguna.
  - **Employee Name**: Nama lengkap karyawan.
  - **Alamat IP**: Alamat IP dari mana pengguna tersebut melakukan login.
  - **Tanggal Log**: Tanggal dan waktu pasti saat aktivitas login atau logout terjadi.
  - **Waktu(ms)**: Kemungkinan besar mencatat durasi sesi atau waktu respons sistem dalam milidetik.

- **Tombol Aksi**:
  - **Hapus**: Tombol untuk menghapus catatan log yang dipilih. Tindakan ini harus dilakukan dengan sangat hati hati.

Alur Kerja dan Proses Bisnis Terintegrasi

- **Audit Keamanan**: Fungsi utama modul ini adalah untuk audit keamanan. Administrator dapat secara rutin meninjau log untuk mendeteksi aktivitas yang mencurigakan, seperti upaya login dari alamat IP yang tidak dikenal atau aktivitas di luar jam kerja normal.

- **Pemantauan Aktivitas Pengguna**: Membantu memantau kepatuhan pengguna terhadap kebijakan perusahaan. Misalnya, untuk memastikan pengguna melakukan logout di akhir hari kerja.

- **Investigasi Insiden**: Jika terjadi insiden keamanan atau kesalahan data, System Log adalah titik awal yang krusial untuk investigasi. Administrator dapat melacak siapa yang aktif di sistem pada saat kejadian untuk mempersempit kemungkinan penyebabnya.

- **Analisis Kinerja Sistem**: Kolom Waktu(ms) dapat memberikan wawasan awal mengenai kinerja dan kecepatan respons sistem saat pengguna berinteraksi. Waktu yang sangat tinggi secara konsisten mungkin mengindikasikan adanya masalah performa.

Tips dan Catatan Penting

- **Kebijakan Retensi Log**: Perusahaan harus memiliki kebijakan yang jelas mengenai berapa lama data log ini harus disimpan. Menghapus log yang terlalu cepat dapat menghambat investigasi, sementara menyimpannya terlalu lama dapat membebani database.

- **Keamanan Alamat IP**: Perhatikan alamat IP yang tidak biasa. Jika perusahaan Anda menggunakan jaringan internal, semua login seharusnya berasal dari rentang IP internal. Login dari IP eksternal yang tidak terduga harus segera diselidiki.

- **Tindakan Hapus**: Menghapus catatan log harus dibatasi dan diatur dengan ketat. Dalam banyak standar kepatuhan, penghapusan log audit tanpa alasan yang jelas merupakan pelanggaran serius.

Revision #2
Created 22 October 2025 08:25:38 by Sayu
Updated 23 October 2025 14:26:45 by Sayu