

Universal Login Manager

Guida all'installazione e alla configurazione

ULM V4.5 SR3



Declinazione di responsabilità

NT-ware Systemprogrammierungs-GmbH, tutte le sue affiliate, i suoi partner e i suoi concessionari di licenza non riconoscono alcuna garanzia, comprese, a titolo puramente esemplificativo, le garanzie relative all'accuratezza o completezza delle dichiarazioni contenute nel presente sito/documento o rispetto al contenuto di qualsiasi sito o sito esterno per uno scopo particolare. Il presente sito/documento e i materiali, le informazioni, i servizi e i prodotti inclusi nel sito/documento, compresi, a titolo puramente esemplificativo, testo, grafica e collegamenti, sono forniti "tali quali" e senza garanzie di alcun tipo, espresse o implicite.

Tutti i diritti riservati. Nessuna parte di questo lavoro può essere riprodotta in qualsiasi forma o con qualunque mezzo (grafico, elettronico o meccanico, inclusi i dispositivi di fotocopiatura, registrazione, memorizzazione su nastro e i sistemi di archiviazione e recupero dei dati) senza il previo consenso scritto di NT-ware Systemprogrammierungs-GmbH (di seguito indicata anche semplicemente come NT-ware).

I nomi di società e di prodotti menzionati nella presente documentazione sono marchi registrati o non registrati dei rispettivi titolari. La citazione di prodotti di terzi ha scopo esclusivamente informativo e non costituisce in alcun modo un'approvazione o raccomandazione di tali prodotti. NT-ware non si assume alcuna responsabilità relativamente alle prestazioni di tali prodotti. Inoltre, NT-ware non si assume alcuna responsabilità per questi marchi commerciali. Qualsiasi utilizzo di marchi commerciali, logo, marchi di servizio, nomi commerciali e nomi di prodotti è proibito senza il consenso scritto dei rispettivi titolari.

Adlib, Express and Express Server sono marchi registrati o marchi commerciali di Adlib Publishing Systems Inc.; Adobe®, Adobe® Reader®, Acrobat®, Distiller®, PostScript® e i prodotti CREATIVE SUITE sono marchi registrati o marchi commerciali di Adobe Systems Incorporated negli Stati Uniti e/o altri paesi; Android è un marchio commerciale di Google Inc.; Apple®, the Apple® logo, Mac®, Mac OS®, Macintosh®, iPhone®, iPad® e AirPrint® sono marchi commerciali di Apple Inc. registrati negli Stati Uniti e in altri paesi; Box di Box Inc.; Blackboard Transact™ di Blackboard Inc.; CANON, imageRUNNER, imageRUNNER ADVANCE, MEAP, CPCA, AMS, iW AMS, iW Desktop, iSend, iW SAM sono marchi commerciali o registrati di Canon Inc.; CardSmith® è un marchio commerciale di CardSmith LLC; CBORD CS Gold® di CBORD Group Inc.; Crystal Reports e altri prodotti e servizi Business Objects citati nel presente documento nonché i rispettivi loghi sono marchi commerciali o marchi registrati di Business Objects Software Ltd. Business Objects è una società SAP; Dropbox di Dropbox Inc.; eCopy™, eCopy ShareScan® e eCopy ScanStation™ sono marchi o marchi commerciali di Nuance Communications, Inc.; Evernote® di Evernote Corporation; FileNet® di IBM Corporation; Foxit®SDK e Foxit® Reader di Foxit Corporation; Google Docs di Google Inc.; il servizio di stampa web Google Cloud Print™ è un marchio commerciale di Google Inc.; Helix™ Production Workflow è un marchio commerciale di NT-ware Systemprogrammierungs-GmbH; HP, HEWLETT-PACKARD, PCL e LASERJET sono marchi registrati appartenenti a Hewlett-Packard Development Company; KONICA MINOLTA è un marchio registrato di KONICA MINOLTA Inc.; iOS® di Cisco Technology Inc.; iDRS™ SDK e IRISConnect™ sono marchi commerciali non registrati di I.R.I.S. Group S.A.; JAWS pdf courier™ sono marchi commerciali di Global Graphics SA.; Microsoft®, Windows®, Windows Server®, Internet Explorer®, Internet Information Services, Microsoft® Word, Microsoft® Excel, Microsoft SharePoint®, Microsoft SharePoint® Online, OneDrive®, One Drive® for Business, SQL Server®, Active Directory®, Hyper-V® sono marchi registrati o marchi commerciali di Microsoft Corporation negli Stati Uniti e/o in altri paesi; Neevia Document Converter Pro™ di Neevia Technology; NetWare®, Novell®, Novell eDirectory™ di Novell Inc. sono marchi registrati/non registrati di Novell Inc. negli Stati Uniti e in altri paesi; MobileIron® di Mobile Iron Inc., Océ, Océ PlotWave®, Océ ColorWave® e PRISMA sono marchi commerciali o marchi registrati di Océ Technologies B.V. Océ è una società Canon, OpenOffice.org™ di Oracle Corporation; PAS™ è un marchio commerciale di Equitrac Corp.; PosterJet è un marchio registrato a livello internazionale e tutelato da

copyright di Eisfeld Datentechnik GmbH & Co. KG; RedTitan EscapeE of RedTitan Limited; NETAPHOR®, SiteAudit™ sono marchi commerciali di NETAPHOR SOFTWARE Inc.; SAMSUNG è un marchio commerciale di SAMSUNG negli Stati Uniti o in altri paesi; Therefore™, Therefore™ Online di Therefore; UNIX® è un marchio registrato di The Open Group; uniFLOW®, uniFLOW Serverless Secure Printing®, Helix Production Workflow®, MIND®, microMIND®, MiCard® e uniFLOW Service for AirPrint® sono marchi registrati di NT-WARE Systemprogrammierungs-GmbH; pcProx®, AIR ID® sono marchi registrati di RFIdeas Inc. Readers; CASI-RUSCO® è un marchio registrato di ID Card Group; Radio Key® è un marchio registrato di Secura Key; GProx™ II è un marchio non registrato di Guardall; HID® ProxHID è un marchio registrato di HID Global Corporation; Indala® è un marchio registrato di Motorola; ioProx™ è un marchio non registrato di Kantech; VMware vSphere® e VMware vSphere® Motion® sono marchi registrati di VMware; Xerox, Xerox and Design nonché Fuji Xerox and Design sono marchi registrati o marchi commerciali di Xerox Corporation in Giappone e/o in altri paesi.

Tutti gli altri marchi commerciali, nomi commerciali, nomi di prodotti e marchi di servizio appartengono ai rispettivi titolari e sono riconosciuti in questa sede.

Benché il presente documento sia stato preparato con la massima cura, NT-ware non si assume alcuna responsabilità relativamente a possibili errori o omissioni oppure a danni derivanti dall'uso delle informazioni contenute nel presente documento o dall'uso dei programmi e del codice sorgente eventualmente forniti con esso. NT-ware non si assume alcuna responsabilità relativamente a eventuali malfunzionamenti o perdite di dati conseguenti all'uso di almeno un prodotto NT-ware in combinazione con un sistema operativo e/o prodotti di terze parti. In nessun caso NT-ware potrà essere ritenuta responsabile di qualsiasi perdita di profitto o di qualunque altro danno commerciale causato o possibilmente causato direttamente o indirettamente dal presente documento.

Inoltre, il presente manuale contiene collegamenti ai siti web di società affiliate o indipendenti e di alcune altre aziende. NT-ware non è responsabile dell'esame o della valutazione del contenuto di tali siti web né delle offerte presentate dalle aziende o dagli individui collegati a tali siti e non fornisce alcuna garanzia in merito. NT-ware non si assume alcuna responsabilità relativamente ad azioni, prodotti e contenuti di tali terze parti o di eventuali altre terze parti. Leggere attentamente le dichiarazioni sulla privacy e le condizioni d'uso di tali terze parti.

Tuesday, October 10, 2017, Bad Iburg (Germania)

Nota importante

Si possono verificare problemi seri se si modifica il registro di sistema di Windows in maniera non corretta. Potrebbe essere addirittura necessario reinstallare il sistema operativo. Si consiglia vivamente di creare sempre una copia di backup del registro di sistema di Windows prima di modificarlo, per prevenire problemi di questo tipo. NT-ware non si assume alcuna responsabilità relativamente alle conseguenze sul sistema operativo delle modifiche apportate al registro di sistema. L'utente comprende e accetta di utilizzare queste informazioni e modificare il registro di sistema di Windows a proprio rischio.

uniFLOW e i relativi componenti come Web Submission e Internet Gateway dipendono significativamente dai relativi database SQL per il loro funzionamento. Si consiglia vivamente di evitare di modificare questi database SQL manualmente senza consultare preventivamente il team dell'assistenza NT-ware. NT-ware non si assume alcuna responsabilità relativamente alle possibili conseguenze sull'ambiente uniFLOW di modifiche apportate ai database SQL.

Copyright e contatti

NT-ware Systemprogrammierungs-GmbH
Niedersachsenstraße 6
49186 Bad Iburg
Germania

www.nt-ware.com

Tel: +49 - 54 03 - 7243 - 0

Fax: +49 - 54 03 - 78 01 03

E-mail: info@nt-ware.com

Registro delle società: Amtsgericht Osnabrück
N. di registrazione nel Registro delle società: HRB 110944
Amministratore delegato: Karsten Huster
Responsabile in base a § 6 MDStV: Karsten Huster
N. di partita IVA in base a §27 Umsatzsteuergesetz: DE 230932141
©1998-2017 NT-ware Systemprogrammierungs-GmbH.

Commenti

Qualora si riscontrassero errori particolari oppure se si desidera inviare dei suggerimenti, contattare documentation@nt-ware.com o utilizzare il pulsante *Invia commento* della Guida in linea di uniFLOW.

Supporto tecnico

Il servizio di supporto tecnico viene fornito in prima istanza dal rivenditore. Prima di contattare il rivenditore per richiedere assistenza, leggere bene questo documento.

Informazioni licenza Open Source

La seguente dichiarazione di copyright e la licenza si applicano ai componenti software opensv che vengono utilizzati da Universal Login Manager.

Licenza Apache - Versione 2.0, gennaio 2004 - <http://www.apache.org/licenses/>

TERMINI E CONDIZIONI PER L'USO, LA RIPRODUZIONE E LA DISTRIBUZIONE

1. Definizioni.

"Licenza" si riferisce ai termini e alle condizioni per l'uso, la riproduzione e la distribuzione, così come definiti nelle sezioni da 1 a 9 del presente documento.

"Licenziatario" indica il titolare del copyright o l'entità autorizzata dal titolare del copyright che concede la Licenza.

"Entità legale" indica l'unione dell'entità operativa e di tutte le altre entità che controllano, o sono controllate da, o sono sotto controllo comune con tale entità. Ai fini di questa definizione, per "controllo" si intende (i) la capacità, diretta o indiretta, di determinare la direzione o la gestione di tale entità, per contratto o altrimenti, oppure (ii) la proprietà del cinquanta per cento (50%) o oltre delle azioni in circolazione, oppure (iii) la proprietà effettiva di tale entità.

"Voi" (o "Vostro") indica un individuo o un'entità legale che esercita i diritti concessi dalla presente Licenza.

Per formato "Sorgente" si intende il formato preferenziale per l'effettuazione di modifiche quali, a titolo esemplificativo ma non esaustivo, modifiche del codice sorgente del software, del sorgente della documentazione e dei file di configurazione.

Per formato "Oggetto" si intende qualsiasi formato risultante dalla trasformazione meccanica o dalla traduzione di un formato Sorgente quale, a titolo esemplificativo ma non esaustivo, il codice oggetto compilato, la documentazione generata e le conversioni in altri tipi di supporto.

Per "Lavoro" si intende un lavoro d'autore, in formato Sorgente o Oggetto, reso disponibile ai sensi della Licenza, così come indicato nelle note sul copyright incluse nel lavoro o ad esso accluse (un esempio è riportato nell'Appendice del presente documento).

Per "Lavori derivati" si intende qualsiasi lavoro, in formato Sorgente o Oggetto, basato sul Lavoro (o da esso derivato) e per il quale le revisioni redazionali, le annotazioni, le elaborazioni o altre modifiche rappresentano, nel loro complesso, un lavoro d'autore originale. Ai fini della presente Licenza, i Lavori derivati non includono quei lavori che rimangono separabili dal Lavoro e dai relativi Lavori derivati, o sono semplicemente collegati a (o associati tramite il nome) alle relative interfacce.

"Contributo" indica qualsiasi lavoro d'autore, compresa la versione originale del Lavoro ed eventuali modifiche o aggiunte apportate a tale Lavoro o ai suoi Lavori derivati, che sia intenzionalmente sottoposto al Licenziatario ai fini dell'inclusione nel Lavoro da parte del titolare del copyright o di un individuo o un'entità legale autorizzati a sottoporre lavori per conto del titolare del copyright. A fini della presente definizione, "sottoporre" si riferisce a qualsiasi forma di comunicazione elettronica, verbale o scritta, inviata al Licenziatario o ai suoi rappresentanti, incluso, a titolo esemplificativo ma non esaustivo, la comunicazione tramite liste di distribuzione elettroniche, sistemi di controllo del codice sorgente e sistemi di registrazione dei problemi che siano gestiti dal Licenziatario o per suo conto, allo scopo di discutere e migliorare il Lavoro, escludendo tuttavia qualsiasi comunicazione che sia chiaramente indicata o altrimenti definita per iscritto dal titolare del copyright come "Non un contributo".

"Collaboratore" indica il Licenziatario e qualsiasi individuo o entità legale per conto di cui sia stato ricevuto dal Licenziatario un Contributo successivamente incorporato nel Lavoro.

2. Concessione della Licenza di copyright.

In conformità con i termini e le condizioni della presente Licenza, ciascun Collaboratore concede a Voi una licenza di copyright perpetua, mondiale, non esclusiva, gratuita, esente da royalty e irrevocabile per la riproduzione, la preparazione di Lavori derivati, la pubblicazione, la presentazione in pubblico, la concessione in sublicenza e la distribuzione del Lavoro e dei Lavori derivati in formato Sorgente o Oggetto.

3. Concessione della Licenza di brevetto.

In conformità con i termini e le condizioni della presente Licenza, ciascun Collaboratore concede a Voi una licenza di brevetto perpetua, mondiale, non esclusiva, gratuita, esente da royalty e irrevocabile (fatta eccezione per i casi indicati nella presente sezione), che vi autorizza a effettuare, far effettuare da altri, utilizzare, offrire in vendita, vendere, importare e/o diversamente trasferire il Lavoro, laddove tale licenza è valida unicamente per le

rivendicazioni di brevetto concedibili in licenza da tale Collaboratore che siano necessariamente violate dai suoi Contributi o dalla combinazione dei suoi Contributi con il Lavoro per il quale i Contributi sono stati presentati. Se si dà inizio a una controversia sul brevetto contro qualsiasi entità (inclusa una domanda riconvenzionale in una causa legale) dichiarando che il Lavoro o un Contributo incorporato nel Lavoro costituisce una violazione del brevetto diretta o concomitante, qualsiasi licenza di brevetto a Voi concessa ai sensi della presente Licenza per tale Lavoro cesserà di essere valida nella data in cui la controversia viene depositata.

4. Ridistribuzione.

Potete riprodurre e distribuire copie del Lavoro o dei relativi Lavori derivati su qualsiasi supporto, con o senza modifiche e in formato Sorgente o Oggetto, a condizione che siano rispettate le condizioni seguenti:

Dovete dare a ogni altro destinatario del Lavoro o dei Lavori derivati una copia di questa Licenza;

Dovete indicare chiaramente nei file modificati che si tratta di copie;

Dovete mantenere, nel formato Sorgente di qualsiasi Lavoro derivato che distribuirete, tutte le comunicazioni di copyright, brevetto, marchio e attribuzione presenti nel formato Sorgente del Lavoro, fatta eccezione per le comunicazioni che non riguardano alcuna parte dei Lavori derivati;

(d) Se il Lavoro include, nel pacchetto in cui viene distribuito, un file di testo di "COMUNICAZIONI", tutti gli eventuali Lavori derivati che distribuite devono includere una copia leggibile degli avvisi di attribuzione contenuti in tale file di COMUNICAZIONI, fatta eccezione per le comunicazioni che non riguardano alcuna parte dei Lavori derivati, in almeno una delle seguenti posizioni: all'interno di un file di testo di COMUNICAZIONI distribuito insieme ai Lavori derivati; all'interno del formato Sorgente o della documentazione, se forniti con i Lavori derivati; oppure, all'interno di un avviso visualizzato nei Lavori derivati, se e dove tali avvisi di terzi vengono normalmente visualizzati. Il contenuto del file di COMUNICAZIONI è unicamente informativo e non modifica la Licenza. Potete aggiungere le Vostre comunicazioni di attribuzione all'interno dei Lavori derivati che distribuite, accluse oppure come addendum delle COMUNICAZIONI del Lavoro, a condizione che tali comunicazioni di attribuzione aggiuntive non possano essere interpretate come modifiche della Licenza.

Potete aggiungere il Vostro avviso di copyright alle Vostre modifiche e specificare termini e condizioni di licenza aggiuntivi o differenti per l'utilizzo, la riproduzione o la distribuzione delle Vostre modifiche, oppure per i Lavori derivati nel loro complesso, a condizione che l'utilizzo, la riproduzione e la distribuzione del Lavoro da parte Vostra rispettino le condizioni definite nella presente Licenza.

5. Presentazione dei Contributi.

Salvo esplicita dichiarazione in senso contrario, qualsiasi Contributo intenzionalmente presentato da Voi al Licenziatario affinché venga incluso nel Lavoro dovrà rispettare i termini e le condizioni della presente Licenza, senza termini o condizioni supplementari. Nonostante quanto sopra, nulla di quanto qui esposto potrà sostituire o modificare i termini di eventuali accordi di licenza separati tra Voi e il Licenziatario in relazione a tali Contributi.

6. Marchi.

La presente Licenza non concede l'autorizzazione a utilizzare i nomi commerciali, i marchi commerciali, i marchi di servizio o i nomi di prodotto del Licenziatario, fatta eccezione per quanto richiesto dall'uso ragionevole e abituale per descrivere l'origine del Lavoro e riprodurre il contenuto del file di COMUNICAZIONI.

7. Esclusione di garanzie.

Fatto salvo quanto richiesto dalla legislazione vigente o concordato per iscritto, il Licenziatario fornisce il Lavoro (e ogni Collaboratore fornisce i propri Contributi) "COSÌ COM'È", SENZA GARANZIA DI ALCUN TIPO, espressa o implicita, comprese, a titolo esemplificativo ma non esaustivo, tutte le garanzie o condizioni di TITOLARITÀ, NON VIOLAZIONE, COMMERCIALIZZABILITÀ o IDONEITÀ A UNO SCOPO PARTICOLARE. È Vostra responsabilità esclusiva determinare l'appropriatezza dell'utilizzo o della redistribuzione del Lavoro e assumervi gli eventuali rischi associati all'esercizio da parte Vostra delle autorizzazioni concesse dalla presente Licenza.

8. Limitazione di responsabilità.

In nessun caso e in base a nessuna teoria giuridica, per fatto illecito (negligenza inclusa), per contratto o altrimenti, salvo nei casi prescritti dalla legge applicabile (quali atti intenzionali e di evidente negligenza) o in caso di accordo per iscritto, qualsiasi Collaboratore sarà considerato responsabile nei Vostri confronti di danni, inclusi eventuali danni diretti, indiretti, speciali, accidentali o consequenziali, di qualsiasi natura, risultanti dalla presente Licenza o dall'utilizzo o impossibilità di utilizzare il Lavoro (inclusi, a titolo esemplificativo ma non esaustivo, i danni da perdita di avviamento, interruzione dell'attività lavorativa, errore o malfunzionamento dei sistemi informatici, così come

qualsiasi altro danno o perdita di natura commerciale), anche nel caso in cui il Collaboratore sia stato informato della possibilità di tali danni.

9. Accettazione della garanzia o di responsabilità aggiuntive.

Quando ridistribuite il Lavoro o i relativi Lavori derivati, avete la facoltà di offrire, a pagamento, l'accettazione di supporto, garanzia, indennità o altri vincoli di responsabilità e/o diritti coerenti con la presente Licenza. Tuttavia, nell'accettare tali vincoli, potete agire unicamente a titolo personale e sotto la Vostra esclusiva responsabilità, non per conto di qualsiasi altro Collaboratore, e soltanto se accettate di indennizzare, difendere e tutelare qualsiasi Collaboratore da eventuali responsabilità o rivendicazioni a suo carico derivanti dalla Vostra accettazione di tali garanzie o responsabilità aggiuntive.

FINE DEI TERMINI E DELLE CONDIZIONI

Come utilizzare questo documento

Stili del testo

Questo stile è utilizzato per il testo visualizzato sullo schermo.

Questo stile è utilizzato per il testo che l'utente deve digitare.

Questo stile è utilizzato per i collegamenti ipertestuali alle pagine web e i collegamenti interni ad altre pagine del manuale.

Questo stile è utilizzato per gli esempi di codice: codice XML, variabili ed espressioni regolari.

Simboli



Importante:
informazioni essenziali per il corretto funzionamento del software uniFLOW.



Ulteriori informazioni:
Rimando a ulteriori manuali, manuali di installazione, white paper o alla Knowledgebase NT-ware.



Funzione disponibile in un'area regionale specifica:
Indicatore per funzioni uniFLOW non disponibili in tutto il mondo.



Collegamento esterno:
Collegamento a una pagina web esterna.



Impostazioni:
Spiegazione dettagliata di impostazioni di configurazione o procedure operative.



Bussola:
Percorso del menu o della pagina di configurazione nel software.

Schermate e diagrammi

Questo manuale contiene schermate del software, diagrammi esplicativi e immagini di prodotti. Anche se tutti gli elementi visivi sono aggiornati al momento della redazione del manuale, possono subire delle modifiche successivamente.

Lingua e traduzioni

La versione originale di questo documento è stata scritta in lingua inglese. Le traduzioni di questo documento sono basate sull'originale inglese. Alcuni diagrammi, schermate e immagini incluse in questo documento potrebbero non essere tradotte e apparire solo in lingua inglese.

Invia commento

Qualora si riscontrassero errori particolari oppure se si desidera inviare dei suggerimenti, contattare documentation@nt-ware.com o utilizzare il pulsante *Invia commento* della Guida in linea di uniFLOW.

Informazioni su questo documento

Il presente documento fa parte della dotazione del dispositivo/software fornito da NT-ware. Leggere attentamente il documento prima di utilizzare il dispositivo/software e conservarlo (o conservare un collegamento a una versione online del documento) per farvi riferimento in futuro. È importante che il documento sia letto da tutte le persone che utilizzeranno il dispositivo/software. Osservare tutte le istruzioni fornite nel documento. Le procedure di installazione, configurazione e manutenzione devono essere svolte da personale sufficientemente qualificato. La mancata osservanza delle istruzioni contenute in questo documento può rendere nulla la garanzia.

È stato profuso il massimo impegno per assicurare che il contenuto del manuale sia accurato. Ciononostante, NT-ware si riserva il diritto di apportare modifiche senza preavviso.

Sommaro

1	Introduzione generale	1
2	Introduzione.....	1
2.1	Architettura generale.....	1
2.2	Metodo di autenticazione	2
2.2.1	Metodo di autenticazione Locale	3
2.2.2	Metodo di autenticazione Dominio	3
2.2.3	Metodo Server uniFLOW	3
2.3	Tipi di login	4
2.3.1	Immagine Login o Immagine Login + PIN.....	4
2.3.2	Login Badge di prossimità o Login Badge di prossimità + PIN	4
2.3.3	Login con nome utente e password.....	5
3	Componenti.....	5
3.1	Applicazione	6
3.2	Usage Tracker (Rich Internet Application).....	6
4	Requisiti di sistema.....	7
4.1	Hardware e elementi opzionali.....	7
4.2	Requisiti software	7
4.2.1	Browser web	7
4.2.2	Driver di stampante e Modulo aggiuntivo driver di stampante AMS.....	8
4.2.3	Requisiti server per Active Directory	8
5	Installazione	8
5.1	Installazione tramite sistema di gestione dei contenuti	9
5.2	Installazione tramite sistema di gestione dei contenuti (interfaccia utente remota)	14
5.3	Installazione manuale mediante interfaccia utente remota	17
6	Disinstallazione	19
7	Configurazione	22
7.1	Accesso al tool di amministrazione.....	23
7.1.1	Attivazione	24
7.1.2	Pagina principale.....	25
7.2	Users	26
7.2.1	Home Folder	29
7.2.2	Impostazioni Home Folder.....	30
7.3	Profilo.....	32

7.4	Configurazione	33
7.4.1	Tipo di accesso	34
7.4.1.1	Immagine Login e Immagine Login + PIN	34
7.4.1.2	Badge di prossimità e Badge di prossimità + PIN	35
7.4.1.3	Nome utente/password	36
7.4.2	Metodo di autenticazione.....	36
7.4.2.1	Active Directory.....	38
7.4.3	Importa/Esporta	41
7.4.4	Impostazioni Amministratore di sistema.....	43
7.5	Ruoli	43
7.5.1	Mappatura ACL	44
7.5.2	Importazione e mappatura di gruppi da Active Directory	45
7.6	Personalizzare	47
7.6.1	Stringhe localizzate	50
7.7	Usage Tracker	53
7.7.1	Aggiunta di un dispositivo.....	56
7.7.1.1	Creazione di un certificato	57
7.7.2	Tabella costi	59
7.7.3	Creazione di un rapporto	59
7.7.4	Aspetti relativi alla sicurezza.....	62
8	Secure Print	64
9	Aggiornamento a uniFLOW Server	64
10	Come ottenere i file di registro	64
11	Appendice	65
11.1	Hardware	65
11.2	Elementi opzionali	66
11.2.1	USB Device Port	66
11.2.2	AMS - Access Management System.....	67
12	Index	69

1 Introduzione generale

Questo documento descrive i requisiti tecnici e le procedure di configurazione relative a Universal Login Manager. È indirizzato a product manager, service manager, tecnici, account manager, addetti all'assistenza, personale di showroom e partner Canon esterni che devono saper installare e configurare Universal Login Manager.

Definizioni e abbreviazioni utilizzate nel documento

ULM: Universal Login Manager

AD: Active Directory

CDS: Content Delivery System

RIA: Rich Internet Application

AMS: Access Management System

2 Introduzione

Universal Login Manager è un'applicazione MEAP per dispositivi imageRUNNER ADVANCE sviluppata da NT-ware per offrire una pratica soluzione server-less per l'autenticazione semplificata degli utenti, con il supporto per il login tramite immagine e tramite badge di prossimità. L'applicazione permette di personalizzare le funzionalità native di imageRUNNER ADVANCE e offre inoltre funzioni di base per la reportistica relativa a utilizzo e costi. Universal Login Manager inoltre utilizza Access Management System (AMS) per consentire un controllo granulare degli accessi dei singoli utenti.














Universal Login Manager può anche essere utilizzato come applicazione di login per uniFLOW. Gli utenti possono migrare facilmente a una soluzione uniFLOW senza sacrificare eventuali investimenti iniziali, ad esempio l'acquisto di lettori di badge MiCard PLUS.

2.1 Architettura generale

Universal Login Manager combina due concetti principali:

- **Fornitore di autenticazione:** il server sul quale l'utente si autentica. Questo server può essere configurato nell'impostazione **Metodo di autenticazione**.
- **Presentazione dell'autenticazione:** la modalità con la quale l'utente esegue il login su un dispositivo. Può essere configurata nell'impostazione **Tipo di login**.

Universal Login Manager è molto flessibile e supporta clienti di qualsiasi dimensione grazie alla combinazione di metodo di autenticazione e tipo di login.

Authentication Mode Login Type	Local Authentication 	Domain Authentication 	
Image Login 			
Proximity Card Login 			
User Name and Password Login 			

2.2 Metodo di autenticazione

È possibile selezionare tre tipi differenti di *Fornitore autenticazione*.

- Metodo di autenticazione Locale:**
 Un amministratore può definire un database di utenti localmente sul dispositivo e utilizzarlo come fornitore di autenticazione.
- Metodo di autenticazione Dominio:**
 Utilizza una Active Directory esistente su un server Windows come fornitore di autenticazione.
- Server uniFLOW:**
 È possibile selezionare un server uniFLOW come fornitore di autenticazione. Universal Login Manager può anche operare come applicazione di login per uniFLOW. In questo modo è possibile passare facilmente da una soluzione server-less alla soluzione uniFLOW. In questo caso, per il server uniFLOW è necessaria una licenza di accesso al dispositivo (Device Access License) a pagamento.



Metodo di autenticazione Locale e **Metodo di autenticazione Dominio** possono essere attivati **solo** se il dispositivo **non** è configurato come stampante in uniFLOW. In caso contrario, il **metodo di autenticazione** viene impostato automaticamente su **Server uniFLOW** non appena il server uniFLOW si connette al dispositivo.

2.2.1 Metodo di autenticazione Locale

Il Metodo di autenticazione Locale consente agli utenti di autenticarsi su un database locale presente sul dispositivo, che contiene tutti i dati di autenticazione. Questo database può essere esportato e importato tramite un'interfaccia web e distribuito manualmente ad altri dispositivi.

La configurazione di Universal Login Manager supporta la registrazione di un numero massimo di 1.000 utenti. Solo gli utenti associati al ruolo amministratore possono gestire gli utenti.

Il metodo di autenticazione Locale supporta le seguenti modalità di login:

- Immagine Login (fino a 48 utenti)
- Immagine Login + PIN (fino a 48 utenti)
- Login Badge di prossimità (fino a 1.000 utenti)
- Login Badge di prossimità + PIN (fino a 1.000 utenti)
- Nome utente & password (fino a 1.000 utenti)

È possibile selezionare il tipo di login nel menu *Installazione* di Universal Login Manager Administration Configuration.

2.2.2 Metodo di autenticazione Dominio

Il Metodo di autenticazione Dominio consente agli utenti di autenticarsi su una Active Directory presente su un server Windows presso la sede del cliente. È anche possibile assegnare informazioni di ruolo a ciascun gruppo di una Active Directory.

Sono disponibili le seguenti modalità di login:

- Login Badge di prossimità
- Login Badge di prossimità + PIN
- Nome utente & password

Quando l'utente inserisce il proprio nome utente e password per l'accesso alla rete oppure striscia il suo badge di prossimità collegato alle credenziali di rete, viene eseguita l'autenticazione dell'utente.

2.2.3 Metodo Server uniFLOW

Universal Login Manager può essere utilizzato come applicazione di login per la soluzione uniFLOW, riducendo così al minimo gli investimenti aggiuntivi richiesti in caso di upgrade a uniFLOW.

2.3 Tipi di login

Universal Login Manager supporta diversi tipi di login che sono descritti nei capitoli seguenti.



Il codice PIN utilizzato in alcuni tipi di login **non** è lo stesso codice PIN usato per la gestione dell'ID reparto della stampante. I codici PIN usati per gli ID reparto dei dispositivi dovrebbero essere impostati su 0 per evitare problemi.

2.3.1 Immagine Login o Immagine Login + PIN

Il metodo Immagine Login consente agli utenti di effettuare l'accesso premendo un pulsante sull'interfaccia del dispositivo con un'immagine che rappresenta l'account utente. Il login tramite immagine funziona solo nella modalità di autenticazione Locale.

È possibile registrare e caricare fino a 48 icone utente come immagini account tramite la configurazione ULM sull'interfaccia remota di Universal Login Manager. Si può selezionare il metodo *Immagine Login* o *Immagine + PIN*, nel qual caso per effettuare l'accesso è anche necessario inserire un codice PIN.

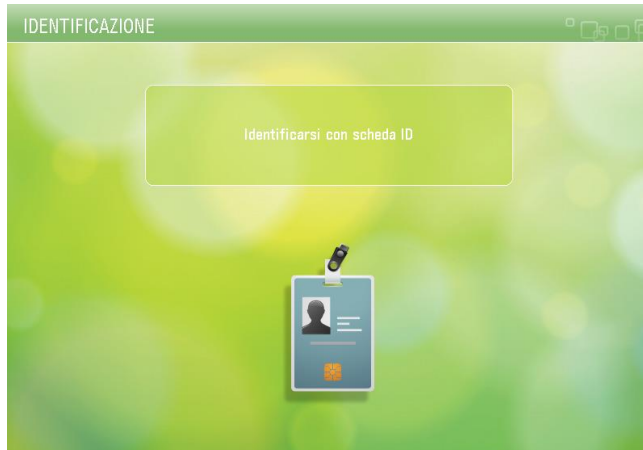


2.3.2 Login Badge di prossimità o Login Badge di prossimità + PIN

Il login Badge di prossimità permette agli utenti di autenticarsi utilizzando un badge di prossimità, ad esempio HID, Mifare o un altro tipo.

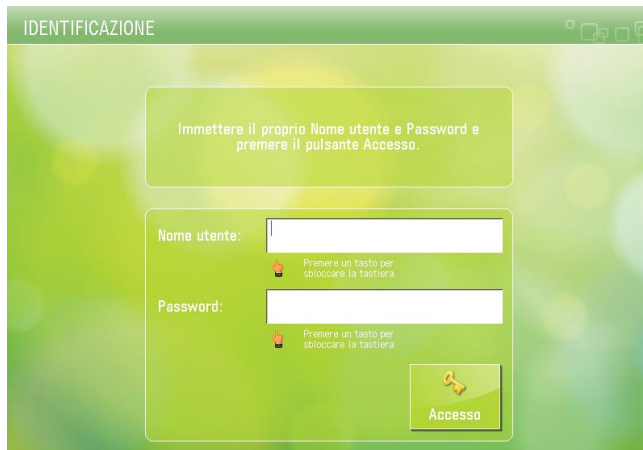
Il lettore di badge supportato deve essere collegato al dispositivo. Si consiglia l'uso dell'accessorio USB Device Port per conservare al sicuro il lettore di badge all'interno del dispositivo. Il login con badge di prossimità funziona in tutte le modalità di autenticazione (Locale, AD, uniFLOW). È anche possibile impostare un codice PIN per rafforzare la sicurezza in fase di login.

Il lettore di badge di prossimità supportato è il modello MiCard PLUS .



2.3.3 Login con nome utente e password

Analogamente alla modalità SSO-H, che è standard sui dispositivi abilitati per MEAP (iR e imageRUNNER ADVANCE), è possibile effettuare il login con un nome utente e una password registrati nel database utenti. Tutte le modalità di autenticazione (Locale, AD e uniFLOW) sono possibili.

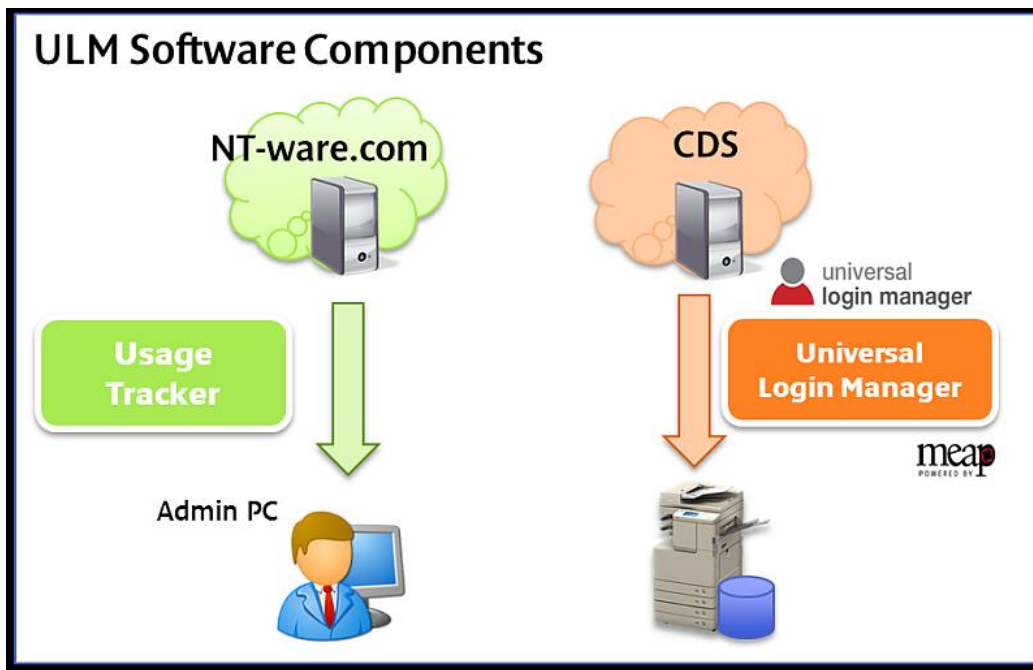


3 Componenti

Universal Login Manager consiste di due moduli software, descritti individualmente nelle sezioni che seguono.

- Universal Login Manager : Il pacchetto principale installato localmente sul dispositivo.

- ULM Usage Tracker: applicazione plug-in per browser web (RIA).



3.1 Applicazione

Universal Login Manager for MEAP

Universal Login Manager è sviluppato da NT-ware ed è basato su uniFLOW Login Manager. A differenza di uniFLOW Login Manager, può essere eseguito senza un server uniFLOW e ottimizza le funzionalità native dei dispositivi imageRUNNER ADVANCE (come Invia a me stesso, i pulsanti/flussi di lavoro personali e la funzione AMS), che dipendono tutte dall'autenticazione dell'utente sul dispositivo.

	Formato
Spazio file massimo	20.000 KB
Utilizzo massimo memoria	6.000 KB
Utilizzo massimo descrittore file	30 KB
Utilizzo massimo socket	8 KB
Utilizzo massimo thread	20 KB

3.2 Usage Tracker (Rich Internet Application)

ULM Usage Tracker è un'applicazione web che può essere scaricata come plug-in del browser tramite un collegamento disponibile nell'interfaccia remota di Universal Login

Manager. Una volta scaricata su un PC, viene eseguita nel browser web finché la cache non viene cancellata.

ULM Usage Tracker consente di raccogliere i dati del registro lavori di tutti i dispositivi registrati (fino a 10) e mostra le attività di stampa/copia/scansione suddivise per utente o per dispositivo, compresi i costi delle transazioni, inclusi in una tabella separata.

In Aspetti relativi alla sicurezza (a pag. [62](#)) è descritto in dettaglio il funzionamento di ULM Usage Tracker e viene spiegato perché è opportuno utilizzarlo.

4 Requisiti di sistema

4.1 Hardware e elementi opzionali

Nell'appendice (a pag. [65](#)) è riportato l'elenco dei dispositivi e delle versioni firmware supportate, nonché degli elementi opzionali.

4.2 Requisiti software

4.2.1 Browser web

È necessario un browser web per accedere alla configurazione ULM e a ULM Usage Tracker e per utilizzarli.

- Universal Login Manager supporta i browser seguenti:
 - Internet Explorer (versione 9 o successiva)
 - Chrome (21 o versioni successive)
 - Mozilla Firefox (15 o versioni successive)
 - Opera per Mac (12 o versioni successive)
 - Safari (5.1 o versioni successive)
- ULM Usage Tracker supporta i browser seguenti:
 - Internet Explorer (versione 9 o successiva).
 - Chrome (21 o versioni successive)
 - Mozilla Firefox (15 o versioni successive)
 - Opera per Mac (12 o versioni successive)
 - Safari (5.1 o versioni successive)



Le funzionalità di esportazione/importazione delle tabelle dei costi in ULM Usage Tracker impiegano Flash e funzionano esclusivamente su sistemi in cui è installato Adobe Flash Player versione 10.0 o successive.

A causa dei limiti di IE9, la funzionalità di importazione delle tabelle dei costi non è

supportata da questo browser in ULM fino alla versione 4.0.1. Da ULM V.4.0.2 in poi, questo browser è perfettamente supportato.

4.2.2 Driver di stampante e Modulo aggiuntivo driver di stampante AMS

Uno dei seguenti driver di stampante deve essere installato sul computer in anticipo.

- Driver di stampa UFR II V20.60 o successivo
- Driver di stampa PCL 6 V20.60 o successivo
- Driver di stampa PCL 5e/5c V20.60 o successivo
- Driver di stampa PS 3 V20.60 o successivo

Se gli utenti necessitano della funzionalità AMS, deve essere installato su tutti i PC della rete anche il Modulo aggiuntivo driver di stampante AMS (AMS Printer Driver Plugin).

4.2.3 Requisiti server per Active Directory

Server Windows supportato: Windows Server 2003/2008 o versioni successive.



Le relazioni di attendibilità tra i domini non sono attualmente supportate da Universal Login Manager.

5 Installazione



I modelli imageRUNNER ADVANCE di terza generazione vengono forniti con Universal Login Manager già installato. Pertanto, le procedure di installazione descritte in questo manuale possono essere ignorate, tranne nel caso in cui sia necessario procedere a una reinstallazione per qualsiasi motivo.

Questa sezione descrive la procedura da seguire per installare Universal Login Manager su un dispositivo MEAP.

Sono disponibili vari modi per installare l'applicazione Universal Login Manager:

- Content Delivery System - tramite un codice LAN (license access number)
 - Dall'interfaccia utente locale del dispositivo
 - Dall'interfaccia utente remota del dispositivo (installazione distribuita)
- Installazione manuale - File .jar e .lic richiesti
 - Da Service Management System (SMS)

Elementi richiesto Metodi di installazione	Password predefinita amministratore	Codice LAN (License Access Number)	File di applicazione e [.jar/.lic]	PC connesso in rete con browser web	Connessione Internet
CDS da interfaccia locale	vedere documentazione e Canon	Obbligatorio			Obbligatorio
CDS da interfaccia remota	vedere documentazione e Canon	Obbligatorio		Obbligatorio	Obbligatorio
Installazione manuale via SMS	vedere documentazione e Canon		Obbligatorio	Obbligatorio	

Il metodo di installazione consigliato è quello basato su CDS. Tuttavia, in determinate circostanze questa potrebbe non essere l'opzione più indicata. In questi casi, procurarsi il file .jar dell'applicazione MEAP e il file .lic dal Canon Software Download Center ed eseguire l'installazione tramite SMS.



Se si installa l'applicazione mediante SMS (Service Management Service), viene visualizzato il Contratto di licenza con l'utente finale (EULA) e viene richiesto di accettarne le condizioni. In caso contrario, l'installazione viene annullata.

5.1 Installazione tramite sistema di gestione dei contenuti

Per installare Universal Login Manager tramite CDS (Content Delivery System, sistema di gestione dei contenuti), è necessario un codice di accesso licenza (LAN, License Access Number) di sedici cifre:

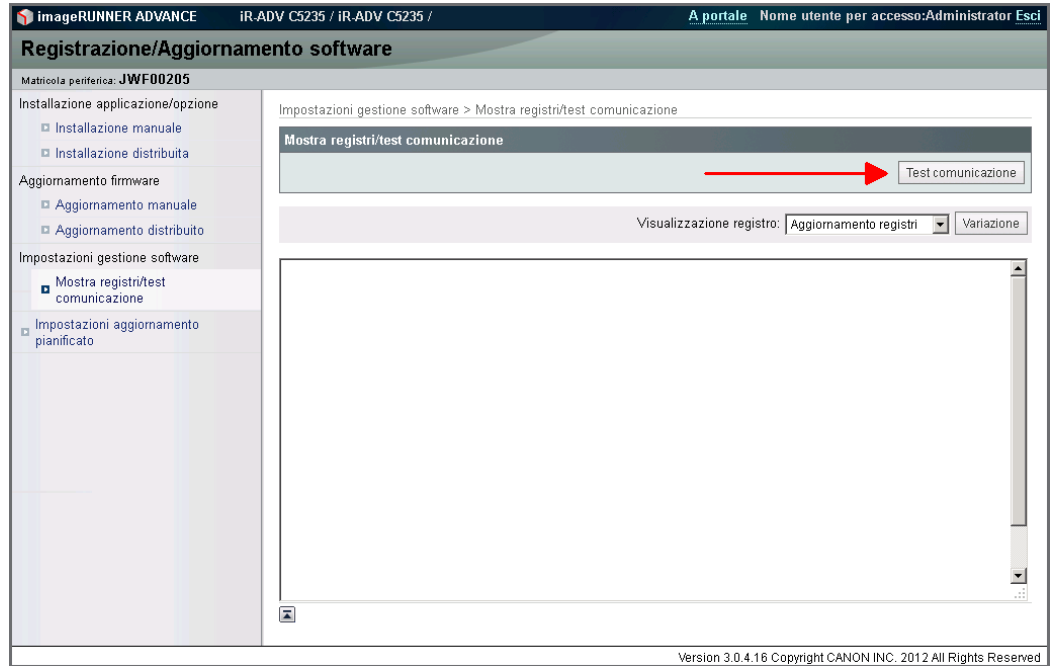
Individuare il numero LAN della propria versione di ULM qui (<http://link.nt-ware.net/id250>).

Per accedere al CDS, è possibile operare dall'interfaccia utente locale del dispositivo oppure da quella remota di un PC connesso in rete.

Prima di installare Universal Login Manager tramite CDS, assicurarsi che quest'ultimo riesca a comunicare con la rete. La funzione "test di comunicazione" permette di verificare le condizioni della rete.

Interfaccia utente remota

Settings & Registration > Liscense/Other > Register/Update Software > Display Logs/Communication Test



Interfaccia utente locale

Settings and Registration > Management Settings > License/Other > Register/Update Software > Software Setting Management > Test Communication



Installazione CDS dall'interfaccia locale

Procedere nel modo descritto di seguito:

- Dal pannello sensibile del dispositivo MFP, premere **Settings and Registration** e accedere come amministratore di sistema (se richiesto).

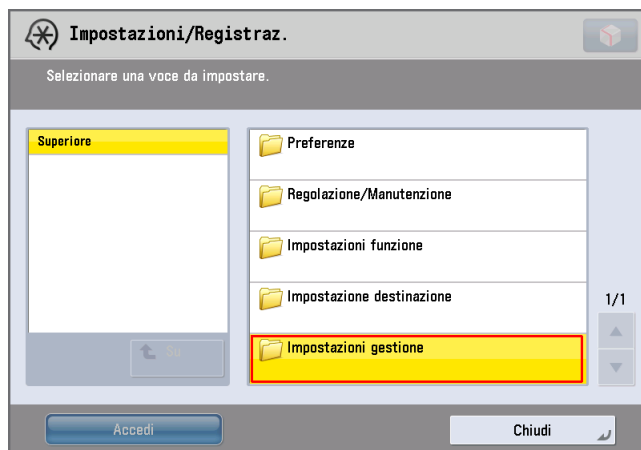


La combinazione predefinita di nome utente/password di imageRUNNER ADVANCE è la seguente:

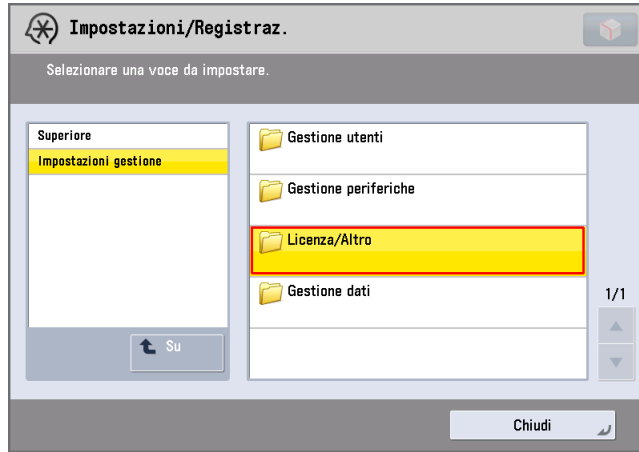
Nome utente: 7654321

PIN: 7654321

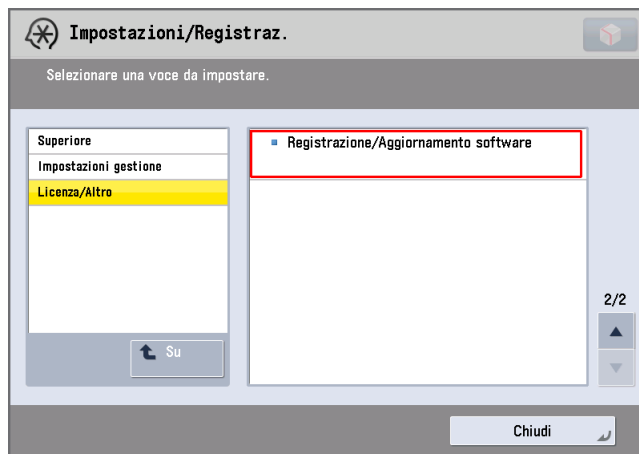
- Dal menu **Settings/Registration**, selezionare **Management Settings**.



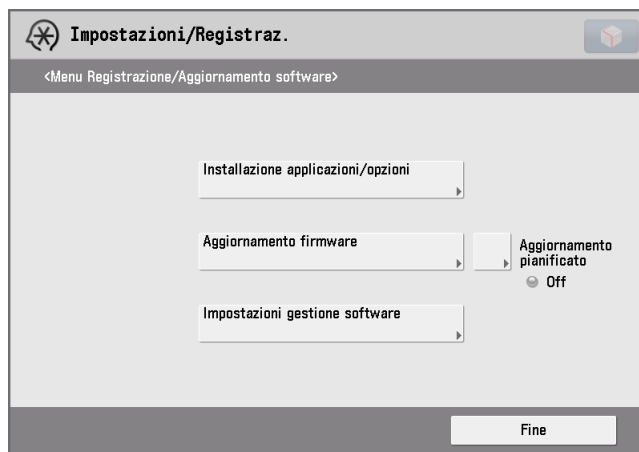
- Selezionare **License/Other**.



- Selezionare **Register/Update Software**.



- Fare clic su **Install Applications/Options**.

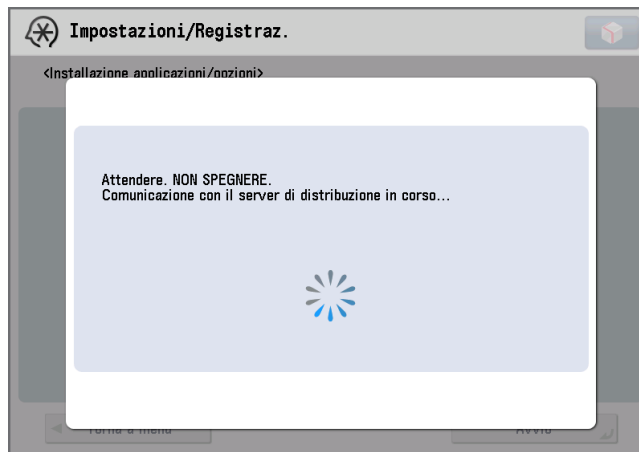


- Inserire il codice LAN di sedici cifre. Ogni gruppo di quattro cifre deve essere digitato separatamente:

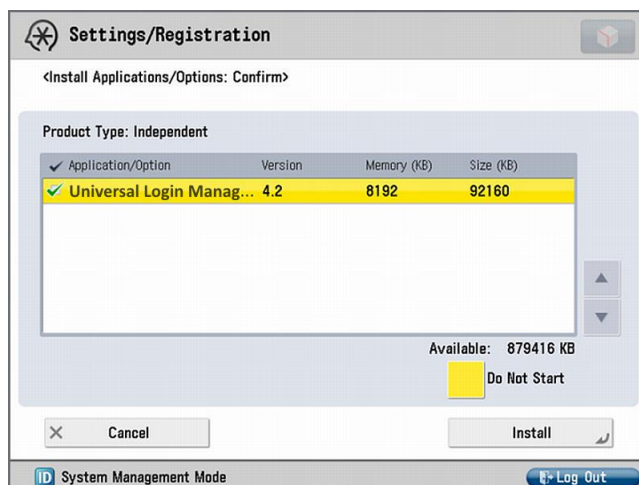
Individuare il numero LAN della propria versione di ULM qui (<http://link.nt-ware.net/id250>).



- Fare clic su **Start** per avviare il processo di installazione.

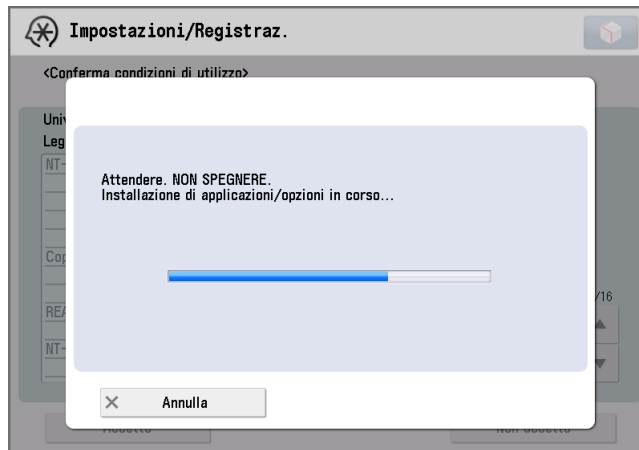


- Selezionare Universal Login Manager spuntando la casella nella prima colonna. Verificare che sia selezionato anche il pulsante **Do Not Start**.

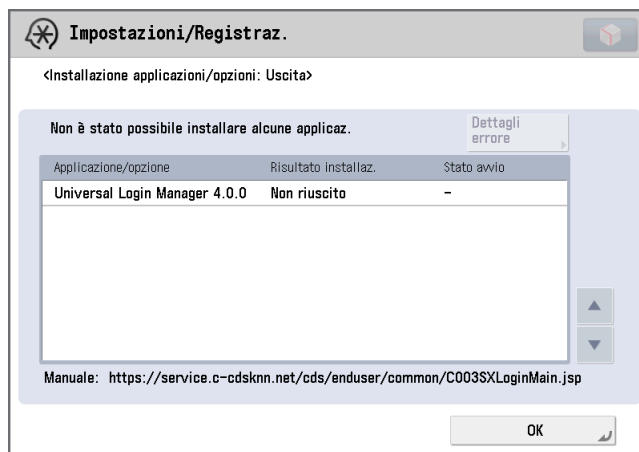


- Leggere e accettare il contratto di licenza. Se non si è in grado di soddisfare le condizioni del contratto di licenza, non procedere con l'installazione.

- L'applicazione verrà scaricata e installata.



- Al termine della procedura, viene visualizzata una nuova schermata che richiede di completare l'installazione. Fare clic sul pulsante **OK** per portare a termine l'installazione.



5.2 Installazione tramite sistema di gestione dei contenuti (interfaccia utente remota)

Procedere nel modo descritto di seguito:

- Aprire il browser web e accedere all'interfaccia remota digitando l'URL seguente:
http://<indirizzoIP>:8000
 dove <indirizzoIP> è l'indirizzo IP del dispositivo sul quale si desidera installare Universal Login Manager.
 - La combinazione predefinita di nome utente/password di imageRUNNER ADVANCE è la seguente:
 - Nome utente: 7654321

- PIN: 7654321

Canon Log In
iR-ADV C7065 / iR-ADV C7065 /

Department ID:

PIN:

Enter the Department ID and PIN and click [Log In].

Copyright CANON INC. 2010 All Rights Reserved

- Dal menu **Settings/Registration**, selezionare **Management Settings**.

imageRUNNER ADVANCE Nome periferica : iR-ADV C7065 Nome utente per accesso : Administrator Esci
Nome prodotto (Matricola) : iR-ADV C7065 (FNP00202) Posizione :

IU remota: Portale Language: Italian Invia a gestore sistema

Ultimo aggiornamento : 12/11 2012 16:01:54

Informazioni principali periferica

Stato periferica
Stampante : ● Ricontrato errore.
Scanner : ● Pronta per scansione.
Fax : ● Pronta per invio o ricezione fax.

Informazioni sull'errore
⚠ La carta è esaurita.
⚠ La carta è esaurita.
⚠ La carta è esaurita.
Dettagli errore (Totale: 3 errori)

Informazioni sui consumabili

Informazioni carta

Cassetto	Carta residua	Formato carta	Tipo di carta
Vassoio multiuso	Assente	Sconosciuto	Non definito

Strumenti di base
Accesso a file ricevuti/memorizzati
Rubrica
Quick Menu
Universal Login Manager

- Selezionare **License/Other**.

imageRUNNER ADVANCE iR-ADV C7065 / iR-ADV C7065 / **A portale** Nome utente per accesso : Administrator Esci

Impostazioni/Registrazione Invia a gestore sistema

Rilavio periferica

Impostazioni/Registrazione : Preferenze : Impostazioni carta

Preferenze : Impostazioni carta Ultimo aggiornamento : 12/11 2012 16:13:03

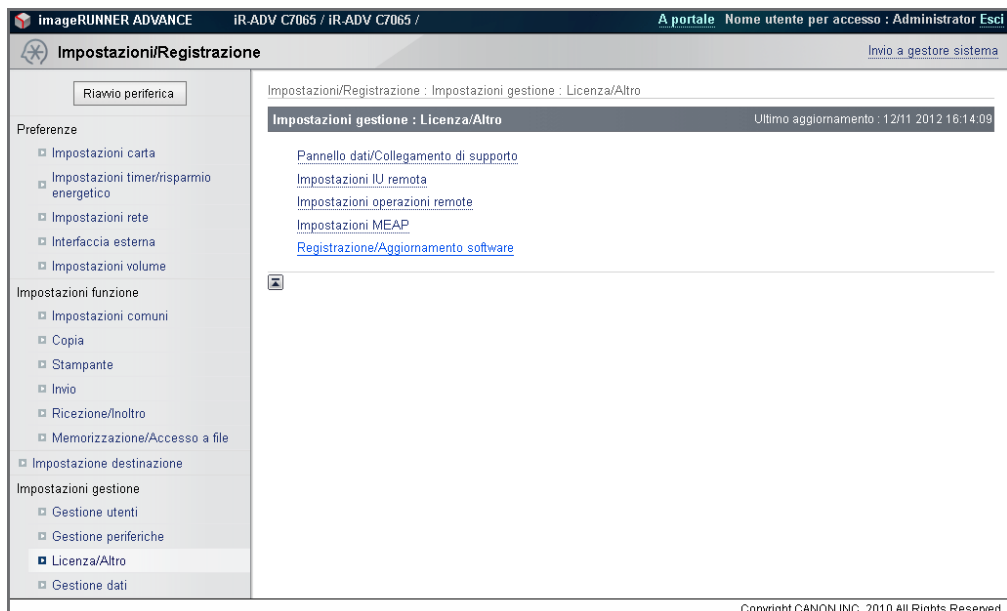
Impostazioni carta
Impostazioni gestione tipo di carta

Preferenze

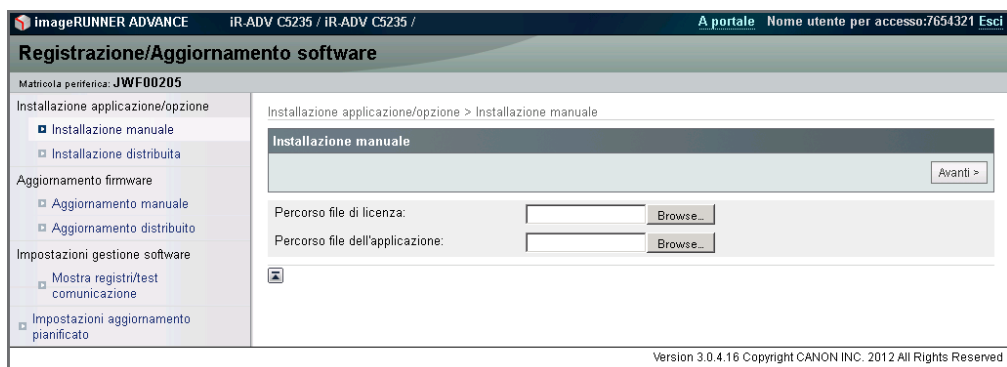
- ▣ Impostazioni carta
 - ▣ Impostazioni timer/risparmio energetico
 - ▣ Impostazioni rete
 - ▣ Interfaccia esterna
 - ▣ Impostazioni volume
- Impostazioni funzione
 - ▣ Impostazioni comuni
 - ▣ Copia
 - ▣ Stampante
 - ▣ Invio
 - ▣ Ricezione/Inoltro
 - ▣ Memorizzazione/Accesso a file
- ▣ Impostazione destinazione
- Impostazioni gestione
 - ▣ Gestione utenti
 - ▣ Gestione periferiche
 - ▣ Licenza/Altro
 - ▣ Gestione dati

Copyright CANON INC. 2010 All Rights Reserved

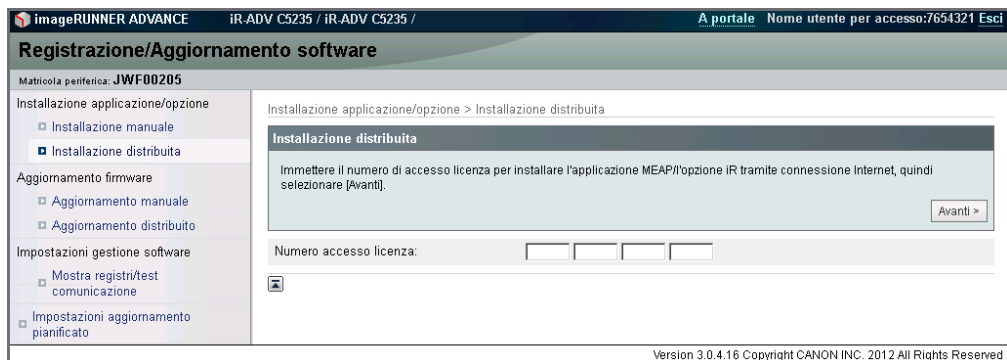
- Selezionare **Register/Update Software**.



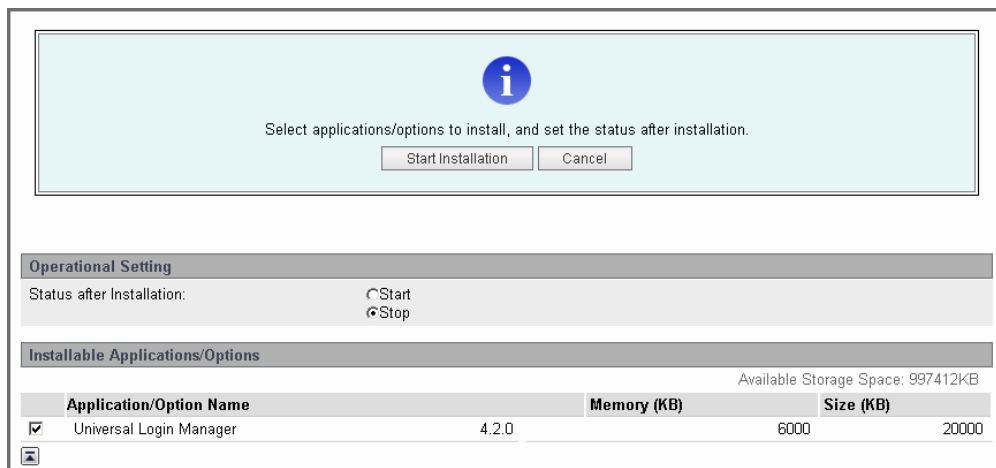
- Fare clic su **Install Applications/Options**.



- Inserire il codice LAN di sedici cifre. Ogni gruppo di quattro cifre deve essere digitato separatamente:
 Individuare il numero LAN della propria versione di ULM qui (<http://link.nt-ware.net/id250>).



- Selezionare Universal Login Manager spuntando la casella nella prima colonna. Assicurarsi inoltre che il pulsante di opzione **Interrompi** sia selezionato, se non si desidera avviare immediatamente Universal Login Manager (e riavviare il dispositivo). Fare clic su **Start** per avviare il processo di installazione.



- Leggere e accettare il contratto di licenza. Se non si è in grado di soddisfare le condizioni del contratto di licenza, non procedere con l'installazione.
- L'applicazione verrà scaricata e installata.

Al termine della procedura, viene visualizzata una nuova schermata che richiede di completare l'installazione. Fare clic sul pulsante **OK** per portare a termine l'installazione.

5.3 Installazione manuale mediante interfaccia utente remota

L'installazione manuale non richiede una connessione Internet per il dispositivo imageRUNNER ADVANCE. È possibile utilizzare il proprio PC connesso in rete per installare Universal Login Manager con un browser web.

SMS - Service Management Service

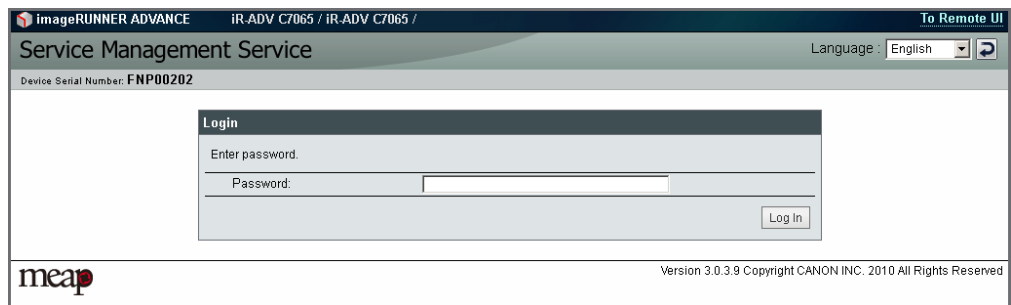
SMS (Service Management Service) è una servlet che permette di accedere ai dispositivi imageRUNNER ADVANCE tramite una rete da un browser web e installare o gestire le applicazioni MEAP. Per installare Universal Login Manager tramite SMS, è necessario avere il file dell'applicazione Universal Login Manager (.jar) e il file di licenza (.lic) su un file system accessibile dal PC.

È possibile scaricare il file .jar e il file .lic di Universal Login Manager dal Canon Software Download Center (<http://software.canon-europe.com/>).

Per l'installazione tramite SMS, procedere nel modo seguente:

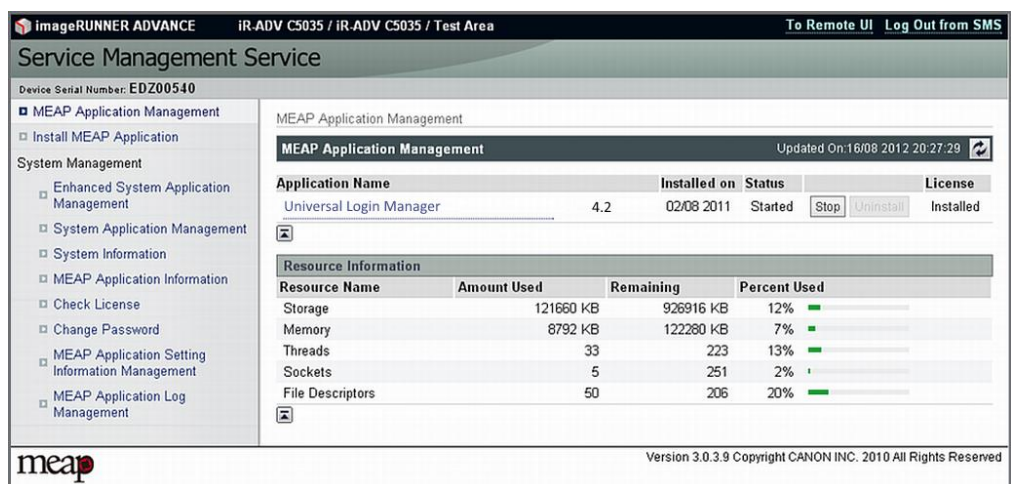
- Accedere a Service Management System (SMS).
Aprire il browser web e accedere a SMS digitando l'URL seguente:
`http://<indirizzo_IP>:8000/sms`

dove <indirizzo-IP> è l'indirizzo IP del dispositivo sul quale si desidera installare Universal Login Manager.

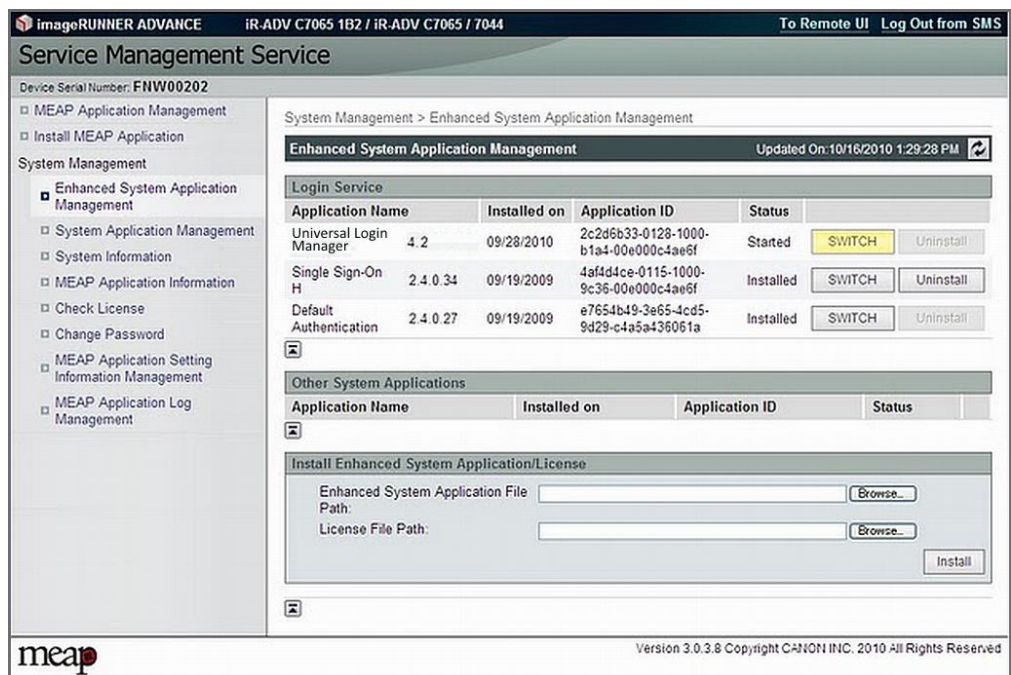


Digitare la password appropriata (rispettando maiuscole e minuscole) nel campo Password.

Fare clic sul pulsante **Login** per accedere a SMS.



- Selezionare **Enhanced System Application Management**.



Nella pagina di elenco **Enhanced System Application Management** sono visualizzati lo stato e altri dettagli delle applicazioni di sistema avanzate che risultano installate nella macchina. Da questa schermata è anche possibile aggiungere nuove applicazioni o arrestare l'esecuzione delle applicazioni.

- Individuare il file .jar.
Fare clic sul pulsante **Sfogli**a accanto al campo **Enhanced System Application File Path** per selezionare il file .jar di Universal Login Manager.
- Individuare il file .lic.
Per poter procedere con l'installazione, è necessario fornire un file di licenza. Fare clic sul pulsante **Sfogli**a accanto al campo **License File Path** per selezionare il file .lic di Universal Login Manager.
- Avviare l'installazione.
Dopo aver selezionato il percorso, fare clic su **Installa** per procedere.
Fare clic sul pulsante **SWITCH** per attivare Universal Login Manager subito dopo il successivo riavvio.

The screenshot shows the 'Service Management Service' interface for 'Enhanced System Application Management'. The main content area displays a table of installed applications:

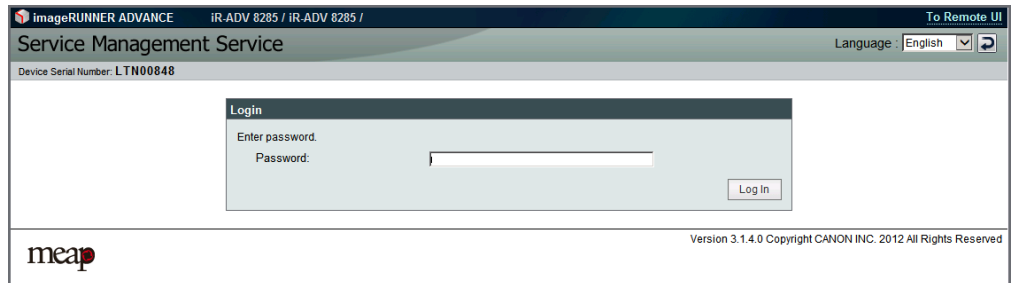
Application Name	Version	Installed on	Application ID	Status	Actions
Universal Login Manager	4.2	09/28/2010	2c2d6b33-0128-1000-b1a4-00e000c4ae6f	Started	[SWITCH] [Uninstall]
Single Sign-On H	2.4.0.34	09/19/2009	4af4d4ce-0115-1000-9c36-00e000c4ae6f	Installed	[SWITCH] [Uninstall]
Default Authentication	2.4.0.27	09/19/2009	e7654b49-3e65-4cd5-9d29-c4a5a436061a	Installed	[SWITCH] [Uninstall]

Below the table, there is an 'Install Enhanced System Application/License' section with two 'Browse...' buttons for 'Enhanced System Application File Path' and 'License File Path', and an 'Install' button.

6 Disinstallazione

Per disinstallare Universal Login Manager mediante Service Management System (SMS), procedere nel modo seguente:

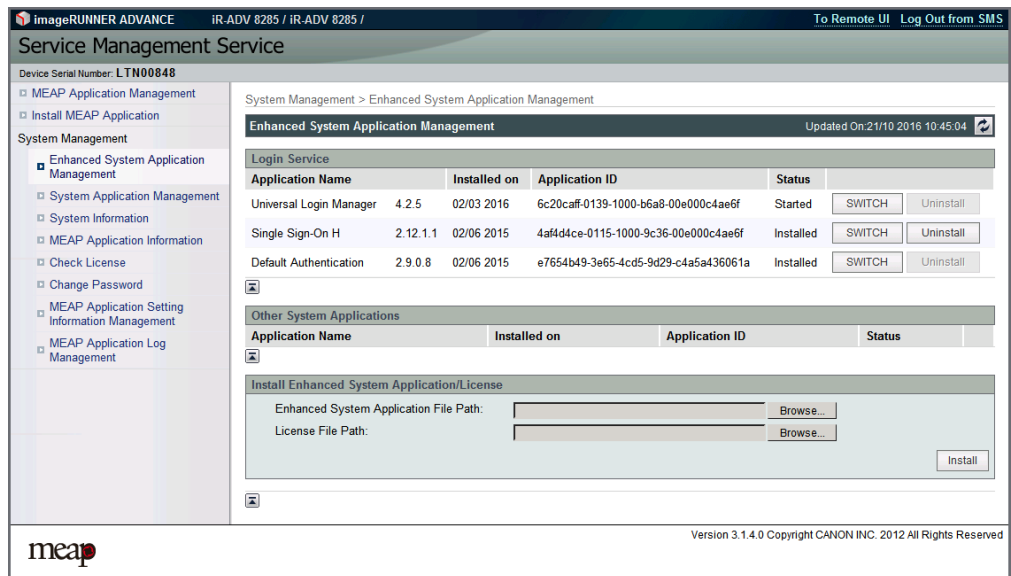
- Accedere a Service Management System (SMS).
 Aprire il browser web e accedere a SMS digitando l'URL seguente:
http://<indirizzo_IP>:8000/sms
 oppure, se SSL è configurato sul dispositivo:
https://<indirizzo_IP>:8443/sms
 dove <indirizzo_IP> è l'indirizzo IP del dispositivo sul quale si desidera disinstallare Universal Login Manager.



Digitare la password appropriata (rispettando maiuscole e minuscole) nel campo **Password**.

Fare clic sul pulsante **Login** per accedere a SMS.

- Selezionare **Enhanced System Application Management**.
 Nella pagina di elenco **Enhanced System Application Management** sono visualizzati lo stato e altri dettagli delle applicazioni di sistema avanzate che risultano installate nella macchina. Da questa schermata è anche possibile aggiungere nuove applicazioni o arrestare l'esecuzione delle applicazioni.



- Fare clic sul pulsante **SWITCH** accanto a **Default Authentication**.

Service Management Service

Device Serial Number: LTN00848

System Management > Enhanced System Application Management

Enhanced System Application Management Updated On: 21/10 2016 10:45:04

Login Service					
Application Name	Version	Installed on	Application ID	Status	
Universal Login Manager	4.2.5	02/03 2016	6c20caff-0139-1000-b6a8-00e000c4ae6f	Started	SWITCH Uninstall
Single Sign-On H	2.12.1.1	02/06 2015	4af4d4ce-0115-1000-9c36-00e000c4ae6f	Installed	SWITCH Uninstall
Default Authentication	2.9.0.8	02/06 2015	e7654b49-3e65-4cd5-9d29-c4a5a436061a	Installed	SWITCH Uninstall

Other System Applications

Application Name	Installed on	Application ID	Status

Install Enhanced System Application/License

Enhanced System Application File Path: Browse...

License File Path: Browse...

Install

meap Version 3.1.4.0 Copyright CANON INC. 2012 All Rights Reserved

- Lo stato di Universal Login Manager cambia in **Stop after Restart** e lo stato di **Default Authentication** cambia in **Start after Restart**.

Service Management Service

Device Serial Number: LTN00848

System Management > Enhanced System Application Management

Enhanced System Application Management Updated On: 21/10 2016 10:45:23

Login Service					
Application Name	Version	Installed on	Application ID	Status	
Universal Login Manager	4.2.5	02/03 2016	6c20caff-0139-1000-b6a8-00e000c4ae6f	Stop after Restart	SWITCH Uninstall
Single Sign-On H	2.12.1.1	02/06 2015	4af4d4ce-0115-1000-9c36-00e000c4ae6f	Installed	SWITCH Uninstall
Default Authentication	2.9.0.8	02/06 2015	e7654b49-3e65-4cd5-9d29-c4a5a436061a	Start after Restart	SWITCH Uninstall

Other System Applications

Application Name	Installed on	Application ID	Status

Install Enhanced System Application/License

Enhanced System Application File Path: Browse...

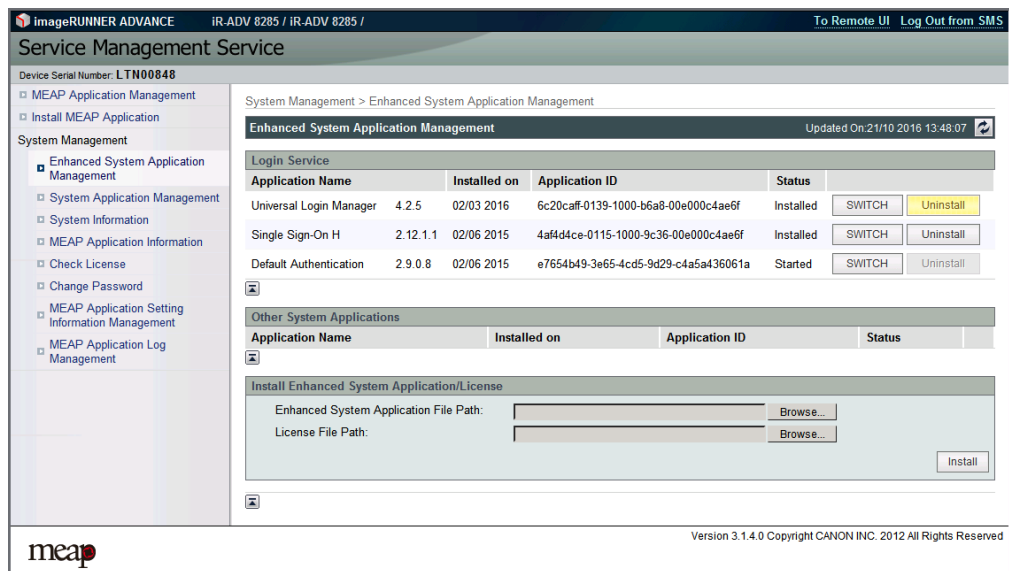
License File Path: Browse...

Install

meap Version 3.1.4.0 Copyright CANON INC. 2012 All Rights Reserved

- A questo punto, riavviare il dispositivo manualmente oppure tramite l'**interfaccia remota**.
- Accedere a Service Management System (SMS) e selezionare di nuovo **Enhanced System Application Management**.
 - Lo stato di **Default Authentication** è ora **Started** e lo stato di Universal Login Manager è **Installed**.

- Fare clic sul pulsante **Uninstall** accanto a **Universal Login Manager**.



- Accettare il messaggio di conferma.
- Universal Login Manager è stato disinstallato e la voce corrispondente è stata rimossa dall'elenco.

7 Configurazione

L'amministratore può configurare vari parametri e impostazioni dall'interfaccia utente remota di Universal Login Manager:

- Gli utenti e i loro profili, con le relative password, immagini o cartelle home.
- Fornitori di autenticazione quali **Active Directory**, **Locale** o **uniFLOW**
- Metodi di presentazione dell'autenticazione quali **Immagine Login** o **Nome utente/Password**.
- **Esportazione e importazione** del database locale.
- **Ruoli** e relativi diritti di accesso.
- Personalizzazione dell'interfaccia utente.



Impostazioni lingua

L'interfaccia remota di Universal Login Manager (RUI) è sempre visualizzata nella stessa lingua dell'interfaccia Universal Login Manager del dispositivo.

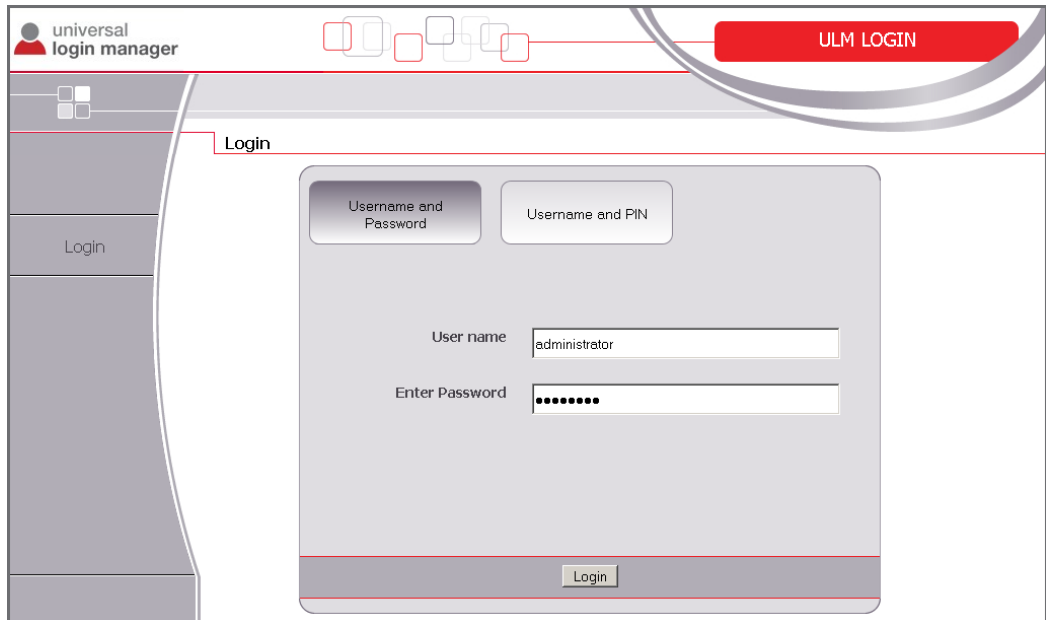
La lingua dell'interfaccia di Universal Login Manager sul dispositivo può essere cambiata modificando la lingua di visualizzazione del dispositivo.

7.1 Accesso al tool di amministrazione

Universal Login Manager ospita un proprio sito web. È possibile accedere direttamente a Universal Login Manager Administration Tool dal seguente indirizzo:

Dispositivi ULM for MEAP: *http://<indirizzoIP>:8000/ulm*

A questo indirizzo è possibile eseguire il login come amministratore, se in possesso della password appropriata. La password predefinita per l'amministratore è "password". Può essere modificata nella pagina Profilo di Universal Login Manager.



In alternativa, il sito web è accessibile dall'interfaccia remota dei dispositivi imageRUNNER ADVANCE, che può essere aperta nel browser web digitando l'URL seguente:

http://<indirizzo_IP>:8000

Una volta eseguito il login, è possibile accedere a Universal Login Manager da Strumenti di base, su lato destro dello schermo.

Nome periferica : iR-ADV C7065
 Nome prodotto(Matricola) : iR-ADV C7065 (FNP00202)
 Posizione :
 Nome utente per accesso : Administrator Esci

IU remota: Portale Language: Italian Invio a gestore sistema

Ultimo aggiornamento : 11/10 2012 15:52:58

Informazioni principali periferica

Stato periferica
 Stampante : ● Ricontrato errore.
 Scanner : ● Pronta per scansione.
 Fax : ● Pronta per invio o ricezione fax.

Informazioni sull'errore
 ! La carta è esaurita.
 ! La carta è esaurita.
 ! La carta è esaurita.
 Dettagli errore (Totale: 3 errori)

Informazioni sui consumabili

Informazioni carta

Cassetto	Carta residua	Formato carta	Tipo di carta
Vassoio multiuso	Assente	Sconosciuto	Non definito
Cassetto 1	Vuoto	A4	Comune 1 (64-90 g/m2)
Cassetto 2	Vuoto	A4	Comune 1 (64-90 g/m2)
Cassetto 3	Basso	A3	Comune 1 (64-90 g/m2)
Cassetto 4	Basso	A4R	Comune 1 (64-90 g/m2)
Cassetto 5	Vuoto	A4	Comune 1 (64-90 g/m2)

Strumenti di base:
 Monitoraggio stato/Annulla
 Impostazioni/Registrazione
 Accesso a file ricevuti/memorizzati
 Rubrica
 Quick Menu
 Universal Login Manager
 Strumenti di gestione:
 User Setting Information Management Service
 Service Management Service

7.1.1 Attivazione

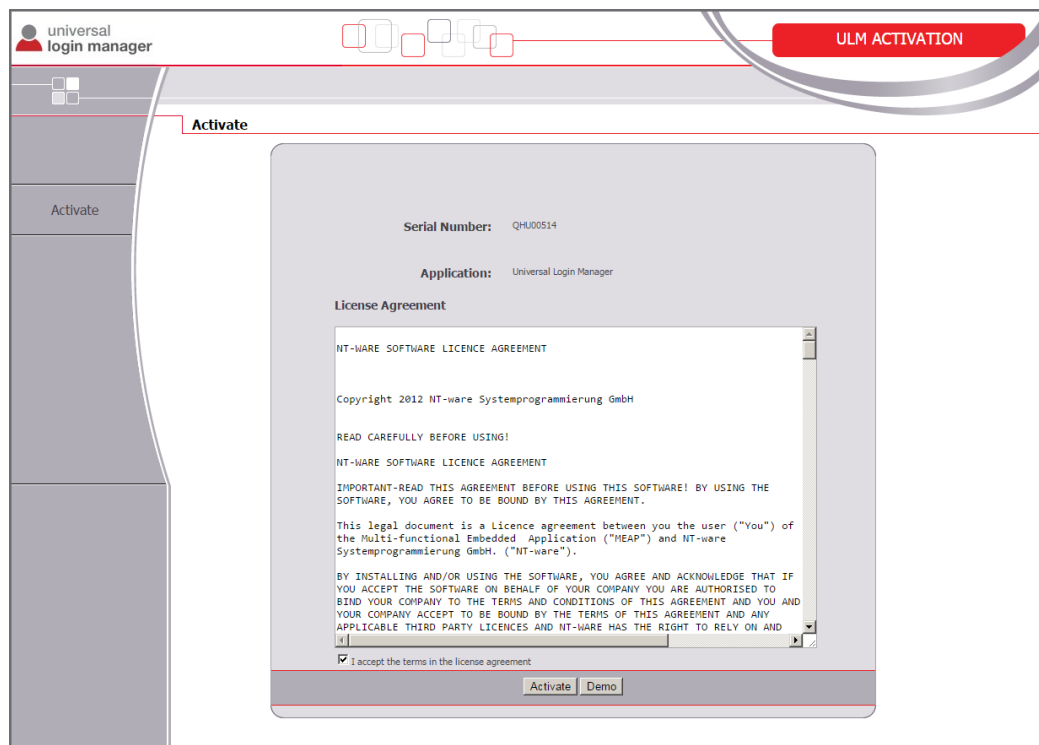


I modelli imageRUNNER ADVANCE di terza generazione vengono forniti con Universal Login Manager già installato. Pertanto, le procedure di installazione descritte in questo manuale possono essere ignorate, tranne nel caso in cui sia necessario procedere a una reinstallazione per qualsiasi motivo.

Se è la prima volta che si avvia Universal Login Manager, è necessario attivarlo. A questo scopo, il computer dal quale si accede al dispositivo deve essere connesso a Internet.

1. Selezionare *I accept the terms in the license agreement* (Accetto i termini del contratto di licenza).
2. Premere il pulsante **Attiva**.

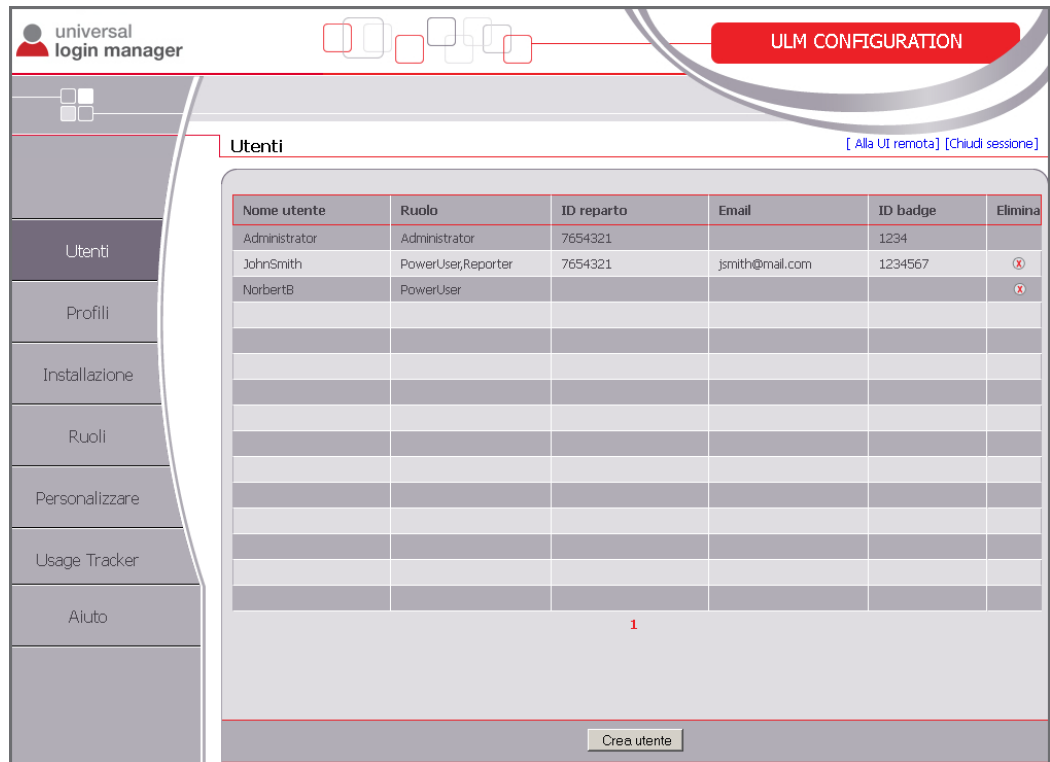
L'uso del pulsante **Demo**, che attiva Universal Login Manager solo fino al riavvio del dispositivo, è riservato alle attività di testing.



7.1.2 Pagina principale

Quando si accede a Universal Login Manager, viene visualizzato il menu principale, che comprende le voci seguenti:

• Users	Solo per il metodo di autenticazione Locale.
• Profilo	Dati utente dell'utente connesso.
• Configurazione	Metodo di autenticazione, Tipo di login, Importa/Esporta.
• Ruoli	Per le impostazioni della funzione AMS.
• Personalizzare	Personalizzazione della schermata di interfaccia.
• Usage Tracker	Collegamento al tool ULM Usage Tracker.
• Aiuto	Collegamento alla Guida in linea.



I sottomenu sono descritti nei capitoli seguenti.

7.2 Users

Nella schermata **Utenti** è riportato l'elenco degli utenti attualmente registrati sul dispositivo. In questa schermata è possibile creare, rimuovere o modificare gli utenti.

Per visualizzare le proprietà di un utente, fare clic sul pulsante **Crea utente** oppure su un utente esistente.





Login name	Role	Department ID	Email	Card ID	Delete
Administrator	Administrator	0			
NorbertB	PowerUser				
PaulS	PowerUser				

Create User
✕

- Reporter
- FunctionLevelLogin
- Administrator
- Guest

List of ID images
 Here you can choose your ID image or you can upload new images. The recommended width and height is: 75x75 pixels. The allowed image formats are: JPEG, PNG and GIF.

Available images

La tabella seguente specifica i campi che si possono modificare qui:

Campo	Descrizione	Condizioni per l'impostazione
Nome utente	Nome di login dell'account	Nome univoco con una lunghezza massima 32 caratteri esclusi i seguenti: SPAZIO (\ / : * ? < > [] ; , = + @ ") . Per il nome utente non viene fatta distinzione tra maiuscole e minuscole.
Immettere PIN / Conferma PIN	Il codice PIN utilizzato per il login tramite ID semplice (con o senza immagini) o tramite ID con badge di prossimità. Deve essere confermata nel secondo campo.	Può essere vuoto oppure un numero di sette cifre al massimo. Se si inseriscono meno di sette cifre, vengono automaticamente inseriti degli zeri iniziali.
Home Folder	La cartella iniziale dell'utente. Non supportato dai dispositivi imageRUNNER ADVANCE di prima generazione.	Percorso completo nella notazione UNC.

Campo	Descrizione	Condizioni per l'impostazione
Password / Conferma password	La password utilizzata per l'autenticazione con il metodo "nome utente/password". Deve essere confermata nel secondo campo.	
ID badge	Il numero di badge registrato per il badge dell'utente.	Il formato dipende dal tipo di badge.
ID reparto	L'ID reparto dell'utente	Dipende dal dispositivo.
E-mail	Indirizzo e-mail dell'utente.	Qualsiasi indirizzo e-mail valido.
Usa indice di visualizzazione	Utilizzato per ordinare le immagini ID sulla schermata di accesso. Le immagini vengono ordinate in modo decrescente, affinché l'utente con il numero di indice più alto venga visualizzato per primo nell'elenco.	Qualsiasi numero intero.
Ruolo	I ruoli assegnati all'utente.	Sono possibili più selezioni.
Lista ID immagini	Rappresentazione grafica dell'utente	Le immagini possono essere caricate e devono avere una dimensione di 75x75 pixel. I formati accettati sono JPG, GIF e PNG. Le immagini più grandi vengono ridotte.



- Quando si configurano gli ID reparto, tenere presente che in Universal Login Manager è possibile configurare solo un ID reparto ma non la relativa password. Per questo motivo, in questo caso non è necessario impostare a zero la password degli ID reparto sui dispositivi.
- Se si selezionano i ruoli Administrator, Reporter, NetworkAdmin, DeviceAdmin, il campo "ID reparto" risulterà disabilitato e al suo interno verrà visualizzato "Amministratore di sistema". Per questi ruoli, all'utente verrà assegnato l'ID reparto dell'amministratore di sistema.
- Le immagini ID non devono superare i 500 KB. Le immagini più grandi possono rallentare sensibilmente l'interfaccia utente.
- Gli utenti con nomi che consistono solo di numeri non possono avere un'immagine personalizzata come immagine ID. È comunque possibile caricare un'immagine, ma sarà visualizzata solo l'immagine ID standard.

7.2.1 Home Folder

La funzionalità Home Folder è disponibile solo su dispositivi imageRUNNER ADVANCE di seconda generazione. Se una cartella valida viene specificata come **Home Folder** nel profilo utente, le relative impostazioni di **Scan and Send** sul dispositivo vengono compilate automaticamente.

A seconda del fornitore e del metodo di autenticazione, le impostazioni sul dispositivo sono leggermente diverse.

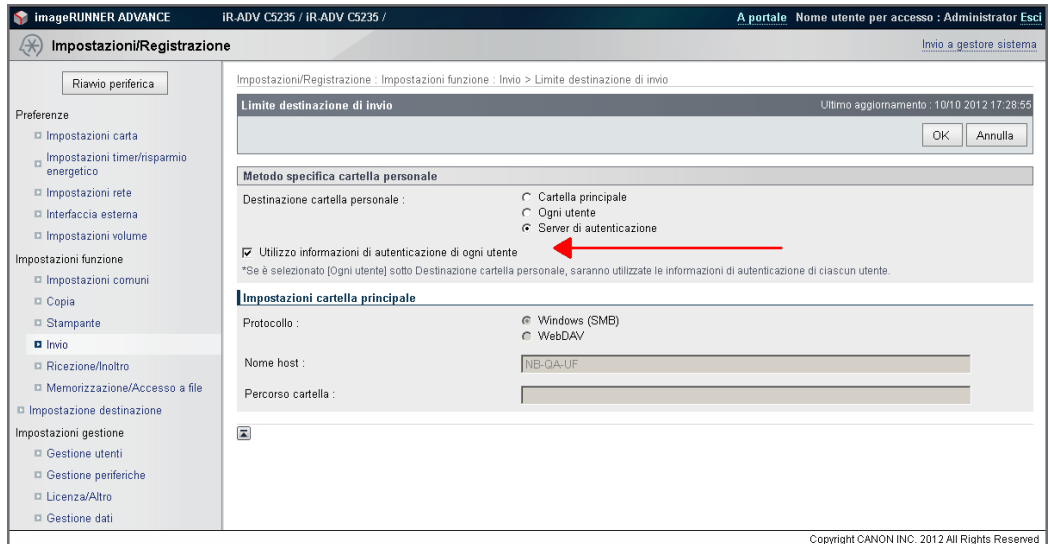
Se il fornitore di autenticazione è **Active Directory con il tipo di login Nome utente/password**, le credenziali utente vengono compilate automaticamente ogni volta che la funzione viene utilizzata.

- Eseguire il login sul dispositivo come amministratore di sistema e accedere a **Impostazioni/Registrazione : Function Settings : Send > Limit Send Destination**. Nella sezione **Personal Folder Specification Method** selezionare **Login Server**.
- L'impostazione **Use Authentication Information of each User** determina come vengono gestite le credenziali:
 - Se è **attiva**, le credenziali devono essere immesse manualmente al primo utilizzo e successivamente rimangono memorizzate in modo permanente sul dispositivo. La volta seguente, verranno quindi compilate automaticamente.
 - Se è **inattiva**, le credenziali vengono compilate automaticamente da Universal Login Manager.

Se il fornitore di autenticazione utilizzato è **Active Directory senza tipo di login Nome utente/password** oppure **Database locale**, le credenziali utente devono essere immesse al primo utilizzo ma possono essere memorizzate sul dispositivo in modo permanente. Vedere la sezione **Impostazioni Home Folder sul dispositivo** di seguito.

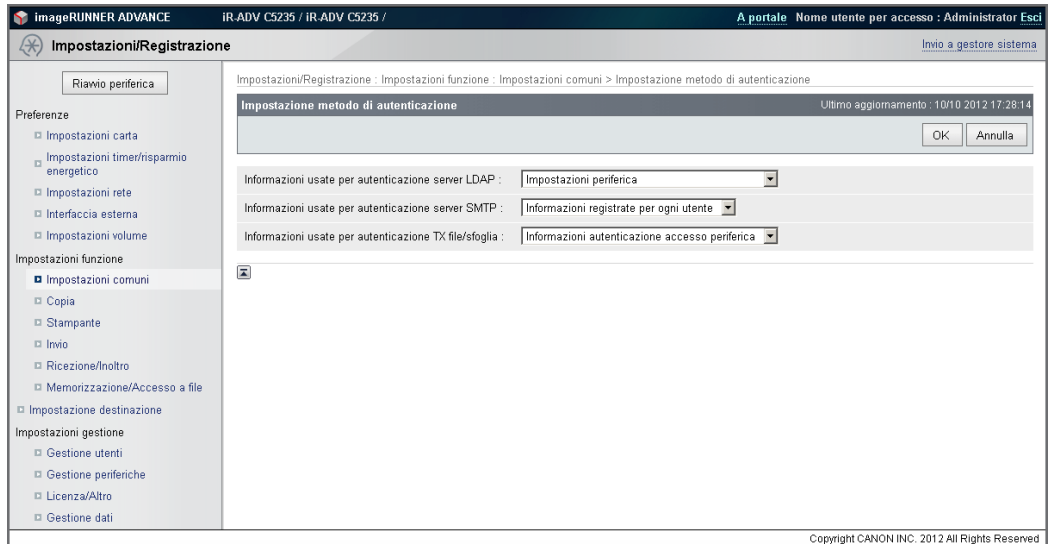
- Eseguire il login sul dispositivo come amministratore di sistema e accedere a **Impostazioni/Registrazione : Function Settings : Send > Limit Send Destination**. Nella sezione **Personal Folder Specification Method** selezionare **Login Server**.
- L'impostazione **Use Authentication Information of each User** determina come vengono gestite le credenziali:
 - Se è **attiva**, le credenziali devono essere immesse manualmente solo al primo utilizzo e successivamente rimangono memorizzate in modo permanente sul dispositivo. La volta seguente, verranno quindi compilate automaticamente.
 - Se è **inattiva**, le credenziali non vengono mai compilate da Universal Login Manager. Devono essere digitate manualmente a ogni utilizzo.

Premere **OK**. A questo punto la funzionalità Home Folder è pronta per l'uso.



Quindi, aprire la pagina seguente: **Settings/Registration : Function Settings : Common Settings > Set Authentication Method**

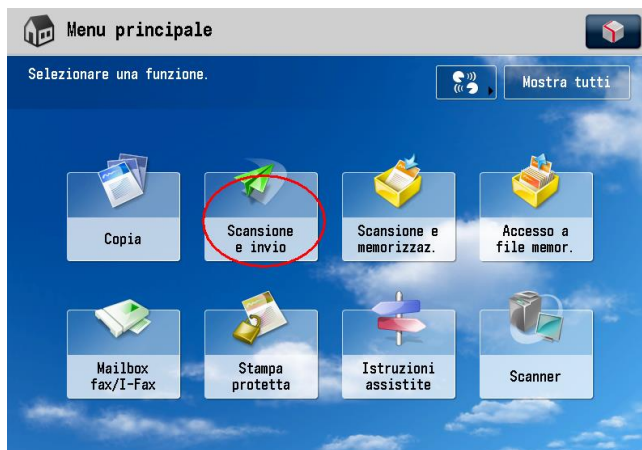
Dal menu a discesa **Information Used for File TX/Browsing Authentication**, selezionare **Device Login Authentication Information**.



7.2.2 Impostazioni Home Folder

Se il fornitore di autenticazione è **Database locale**, gli utenti devono eseguire la procedura seguente una volta su ogni dispositivo che intendono utilizzare con il proprio account.

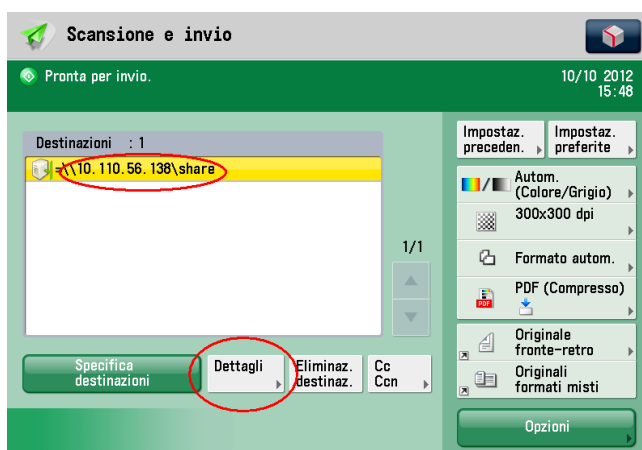
- Dopo il login, l'utente apre *Scan and Send*.



- Qui l'utente apre le impostazioni *Cartella personale*.



- Dovrebbe essere indicata la cartella home delle impostazioni ULM, come illustrato nella schermata seguente.



- Selezionare **Dettagli** per visualizzare le impostazioni dettagliate. **Nome host** e **Percorso Hotfolder** dovrebbero essere preimpostati. L'utente deve compilare i campi **Nome utente** e **Password**, quindi selezionare **Store Password** e infine fare clic su **OK**. Da questo momento in poi le impostazioni sono salvate nel dispositivo e pronte all'uso.



7.3 Profilo

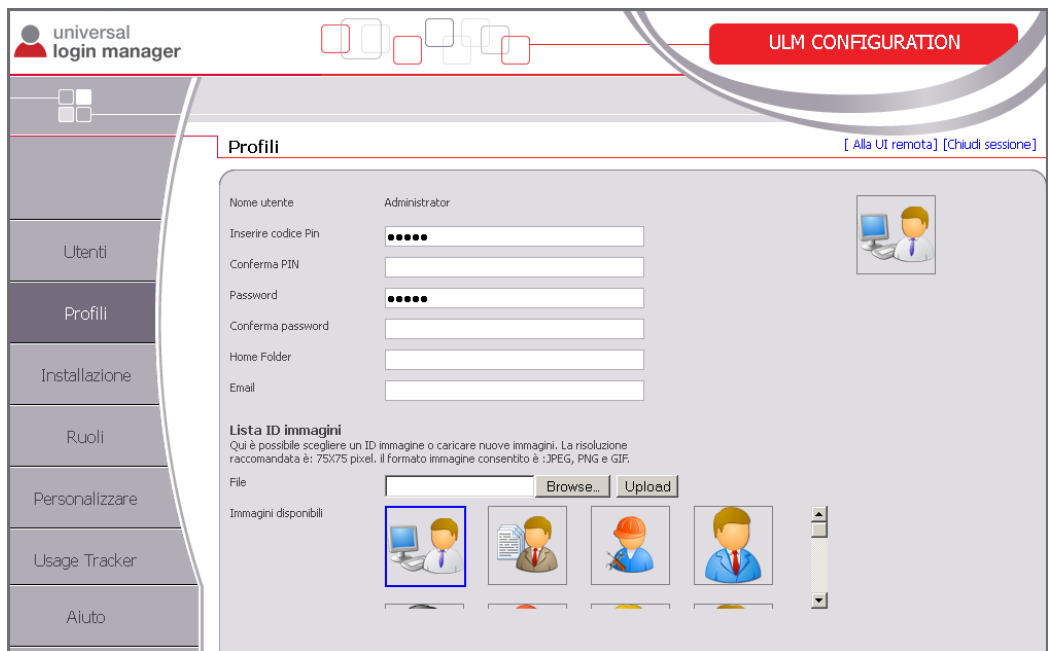
Nella schermata **Profilo** gli utenti finali possono modificare alcune delle proprie proprietà utente:

- PIN
- Password
- Home Folder
- E-mail
- Immagine ID



Questa funzione non è disponibile se è attivata l'autenticazione Active Directory.

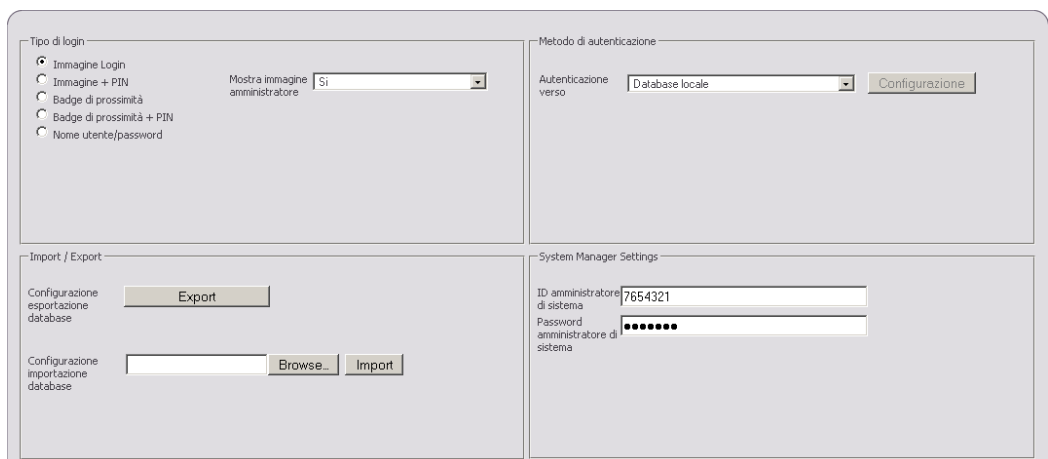
L'utente deve eseguire il login sull'interfaccia remota del dispositivo e quindi aprire la pagina **Profilo**. Per ulteriori informazioni, vedere il capitolo Utenti (vedere "[Users](#)" a pag. [26](#)).



7.4 Configurazione

La pagina *Installazione* offre all'amministratore un modo semplice per configurare le funzioni seguenti:

- **Login Type** (vedere "[Tipo di accesso](#)" a pag. 34)
- **Metodo di autenticazione** (a pag. 36)
- **Esportazione e importazione** (vedere "[Importa/Esporta](#)" a pag. 41) del database degli utenti
- **Impostazioni Amministratore di sistema** (a pag. 43)



7.4.1 Tipo di accesso

In questa sezione è possibile selezionare il tipo di presentazione dell'autenticazione. Sono disponibili i tipi seguenti:

- Immagine Login
- Immagine Login + PIN
- Badge di prossimità
- Badge di prossimità + PIN
- Nome utente/password

7.4.1.1 Immagine Login e Immagine Login + PIN

Immagine Login

L'opzione *Immagine Login* fornisce all'utente un metodo semplice per effettuare il login. È infatti sufficiente toccare l'icona associata all'utente sulla schermata del dispositivo. In questo caso non è possibile eseguire alcuna autenticazione oltre a quella del nome utente assegnato all'immagine ID. Non viene eseguito alcun controllo di sicurezza e chiunque possa accedere fisicamente alla stampante può eseguire il login con qualsiasi identità.



Questo metodo di login è indicato solo per i piccoli uffici dove non si verificano problemi di sicurezza e non è necessario registrare i dati di utilizzo.

Immagine Login + PIN

Il metodo *Immagine Login* può anche essere abbinato all'inserimento di un codice PIN. Questo codice è definito nella configurazione Utente/Profilo e può contenere fino a sette cifre. Poiché questa configurazione prevede un controllo di sicurezza, è indicata per i piccoli uffici in cui sono necessarie funzionalità di registrazione dei dati di utilizzo e/o di controllo degli accessi.

Per entrambi i tipi di login è possibile configurare fino a 48 account. Questo metodo di login funziona unicamente con l'impostazione *Autenticazione verso Database locale*.

Mostra immagine amministratore

È possibile escludere l'amministratore dal login mediante immagine. Così facendo, nessun utente potrà eseguire il login con diritti amministrativi utilizzando questo metodo. A questo scopo, impostare l'opzione *Mostra immagine amministratore* su *No*.

Mostra nomi di login

Se questa opzione è impostata su **Si**, i nomi utente vengono visualizzati sotto l'immagine ID sulla schermata di accesso ULM. Altrimenti vengono visualizzate solo le immagini ID.

7.4.1.2 Badge di prossimità e Badge di prossimità + PIN

I tipi di login **Badge di prossimità** e **Badge di prossimità + PIN** offrono una modalità di login semplice con un livello di sicurezza elevato. Gli utenti devono semplicemente strisciare il proprio badge e (se l'opzione è stata attivata) inserire il codice PIN corrispondente per una maggiore sicurezza.



Per questo tipo di login è richiesto l'uso di un lettore MiCard PLUS. Questo lettore supporta i badge di prossimità HID e i badge MIFARE in modo automatico, ma può anche essere personalizzato per supportare oltre 35 tipi di badge differenti.

Questi tipi di login possono essere configurati anche per Active Directory. Con un processo di auto-registrazione è molto semplice registrare il badge con un fornitore di autenticazione quale un server Active Directory. Il numero del badge viene registrato durante il primo login insieme al nuovo badge, in modo che l'amministratore debba inserire manualmente solo il nome utente e la password. Per questo tipo di login è necessaria la seguente configurazione:

- **Metodo istruzione badge**
 - **Nessuno:**
Indica che il badge deve essere registrato manualmente dall'amministratore.
 - **Nome utente/password:**
Il badge viene registrato nel momento in cui l'utente si autentica con il proprio nome utente e password.
- **Registrazione Codice PIN** (visibile solo per **Badge di prossimità + PIN**):
Questo parametro determina se l'utente può anche inserire un nuovo codice PIN durante la registrazione del badge. Se impostato su **No**, l'amministratore dovrà inserire manualmente i codici PIN per gli utenti, mentre se impostato su **Si**, gli utenti potranno inserire autonomamente i propri codici PIN.

- **Metodo di login alternativo:**
Per entrambi i tipi di **Login Badge di prossimità** è disponibile un metodo di autenticazione alternativo, che può essere **Nessuno** o **Nome utente/Password**. Nel secondo caso, l'utente ha l'alternativa di effettuare il login senza badge.

Come registrare un nuovo badge

1. L'utente striscia il nuovo badge.
2. L'utente digita nome utente e password per l'autenticazione.
3. Se la configurazione lo prevede, l'utente inserisce il nuovo codice PIN.
4. Il numero di badge viene così associato all'utente e memorizzato nel database.

Sono supportate le modalità di autenticazione Locale e Dominio. Con il tipo di login **Badge di prossimità** non esiste alcun limite per il numero di utenti. Poiché anche uniFLOW supporta il lettore MiCard PLUS, l'eventuale migrazione a una soluzione uniFLOW risulterà semplificata.



Per memorizzare automaticamente il nuovo numero di badge in una Active Directory, gli utenti necessitano dell'accesso in scrittura al loro profilo Active Directory. Se tale accesso non è disponibile, la registrazione automatica non è possibile e il numero di badge deve essere memorizzato manualmente dall'amministratore.

7.4.1.3 Nome utente/password

Con questo metodo, l'utente deve specificare il proprio nome utente e la propria password per eseguire il login sul dispositivo. Si tratta di un metodo sicuro e facile da configurare, ma non altrettanto pratico quanto i metodi descritti in precedenza.

Funziona con tutti i fornitori di autenticazione.

7.4.2 Metodo di autenticazione

Nella sezione **Metodo di autenticazione**, l'amministratore può configurare come vengono gestiti i dati utente e se il dispositivo è connesso a un server uniFLOW locale o al servizio cloud uniFLOW Online.

Se il dispositivo è connesso a un server uniFLOW locale, l'interfaccia utente e i comportamenti vengono caricati da tale server uniFLOW.

Se il dispositivo è connesso a uniFLOW Online, l'interfaccia utente e i comportamenti vengono caricati dal servizio cloud uniFLOW Online. In tal caso, l'impostazione **Autenticazione verso** è irrilevante.

- **Autenticazione verso:**

Le modifiche apportate in **Autenticazione verso** vengono salvate automaticamente dopo la selezione di un fornitore di autenticazione. Non è necessario fare clic su **Salva**.

Questo parametro è irrilevante se si usa uniFLOW Online.

- **Active Directory:**

Viene eseguita la connessione a un server Active Directory. Vedere il capitolo Active Directory (a pag. [38](#)) per ulteriori dettagli.



Tenere presente che i server LDAP diversi da Microsoft Active Directory non sono supportati. Se occorre impiegare un sistema LDAP differente (ad es. OpenLDAP), utilizzare uniFLOW.

- **Database locale:**

Viene utilizzato un database di utenti locale presente sul dispositivo.

- **uniFLOW:**

Questa impostazione può essere utilizzata solo se il dispositivo viene configurato da un server uniFLOW. Viene impostata automaticamente dopo il riavvio del dispositivo quando la configurazione uniFLOW è stata completata.

Connessione con uniFLOW Online



Le impostazioni seguenti sono visibili solo se si accede a Universal Login Manager tramite una connessione SSL (HTTPS). La connessione deve essere configurata nelle impostazioni dispositivo (vedere di seguito).

Le impostazioni seguenti hanno valore solo se il dispositivo è connesso a uniFLOW Online.

- **URL di uniFLOW Online:**

Immettere l'URL di uniFLOW Online. Tenere presente che il prefisso *https://* è obbligatorio per la connessione a uniFLOW Online.

- **Impostazioni proxy:**

In questa sezione è possibile configurare un proxy di rete, se necessario, per la connessione a Internet. Inserire l'indirizzo IP o FQDN e la porta. La connessione a uniFLOW Online non è possibile senza accesso a Internet.



Per ulteriori informazioni sulla connessione di dispositivi a uniFLOW Online, consultare la Guida in linea di uniFLOW Online, sezione Device Registration (Registrazione dei dispositivi).



Abilitazione di SSL per MEAP

Se SSL non è già abilitato per le applicazioni MEAP della stampante imageRUNNER ADVANCE, procedere nel modo seguente:

1. Aprire l'*interfaccia utente remota*:
http://<indirizzo_IP_dispositivo>
2. Aprire *Settings/Registration* (Impostazioni/Registrazione).
3. In *Management Settings* (Impostazioni di gestione), aprire *License/Other* (Licenza/Altro).
4. Aprire *MEAP Settings* (Impostazioni MEAP).
5. Selezionare *Use SSL* (Usa SSL).
6. Fare clic su *OK*.
7. Riavviare la stampante.

La volta successiva che si accede a Universal Login Manager, è possibile utilizzare l'URL seguente:

https://<indirizzo_IP_dispositivo>:8443/ulm

7.4.2.1 Active Directory

Se *Autenticazione verso* è impostato su *Active Directory*, è possibile selezionare il pulsante *Configura* per impostare tutti i parametri necessari per la connessione.

Le schermate seguenti mostrano i passaggi da seguire per stabilire la connessione:

- Immettere i dati del server.

Fornitore autenticazione LDAP ✕

Generale

Nome Server/DNS

Porta

- Inserire i dati di autenticazione per un utente con diritti di lettura sulla Active Directory, in modo da poter consultare la struttura di directory. L'accesso in scrittura non è necessario in questo caso. Per **Metodo di autenticazione** è possibile selezionare le seguenti modalità: **NTLM**, **Kerberos** e **Active Directory**. I passaggi descritti di seguito sono identici per tutte le modalità.

The screenshot shows a dialog box titled "Fornitore autenticazione LDAP" with a close button (X) in the top right corner. The "Autenticazione" section contains the following fields:

- Metodo di autenticazione:** A dropdown menu with "NTLM" selected. Below it is the example text "e.g. user@domain".
- Nome utente:** A text input field containing "michaelr@lab".
- Password:** A password input field with masked characters "*****".

A "Prossimo" button is located at the bottom center of the dialog box.

- Selezionare la modalità di consultazione della struttura di directory. Selezionare **Tutti gli utenti**.

The screenshot shows the same dialog box "Fornitore autenticazione LDAP" but with the "Sfoggia directory" section active. It contains:

- Sfoggia utenti:** A dropdown menu with "Tutti gli utenti" selected.

A "Prossimo" button is located at the bottom center of the dialog box.

- A questo punto è possibile semplicemente mappare gli attributi esistenti al profilo dell'utente. Premere **Salva + Chiudi** per completare la procedura.

Fornitore autenticazione LDAP

Sorgente mappatura campo

Nome login: Administrator Attributi di ricerca

Numero badge: - Nessuno -

ID reparto: Casella Postale

Cognome: - Nessuno -

Importazione database

- Nessuno -
- Cognome
- Città
- Stato/Provincia
- Titolo lavoro
- Nome visualizzato
- Nome
- Descrizione (Built-in account for administering the computer/domain)
- CAP
- Casella Postale
- Telefono
- Telefono
- Fax
- Iniziali

- In alternativa, selezionare **Specifica utente** in uno dei passaggi precedenti per abilitare la consultazione dettagliata della struttura di directory.

Fornitore autenticazione LDAP

Sfoggia directory

Sfoggia utenti: Tutti gli utenti

Specificamente utente

Prossimo

- Consultare le directory e selezionare quella desiderata.

Fornitore autenticazione LDAP

Sfoggia directory

Sfoggia utenti: Specifica utente

Base DN: CN=Administrator,CN=Users,DC=lab,DC=n

Filtro espressione LDAP: (objectclass=user)

Prossimo

- Selezionare la mappatura dei campi.

Una volta visualizzate e compilate tutte le schermate di configurazione, la connessione è pronta per l'uso.



- Per l'accesso Active Directory sono necessari solo i diritti di lettura, tranne nel caso di modifiche apportate dagli utenti ai propri profili. In questo caso, gli utenti necessitano dell'accesso in scrittura ai propri profili Active Directory.
- Questo è importante anche per l'istruzione dei badge, per consentire agli utenti di cambiare i propri numeri di badge salvati associando i badge ai propri profili mediante l'inserimento delle relative credenziali.

7.4.3 Importa/Esporta

L'amministratore può esportare e importare la configurazione di Universal Login Manager insieme alle impostazioni utente. Questa operazione può essere eseguita nella schermata *Installazione* (vedere "[Configurazione](#)" a pag. 33). Verranno salvati tutti i dati di sistema, comprese le immagini di sfondo, le icone, i dati utente, ecc. Questa operazione funziona con tutti i tipi di database.

I dati esportati possono poi essere importati facilmente in un altro dispositivo imageRUNNER ADVANCE.

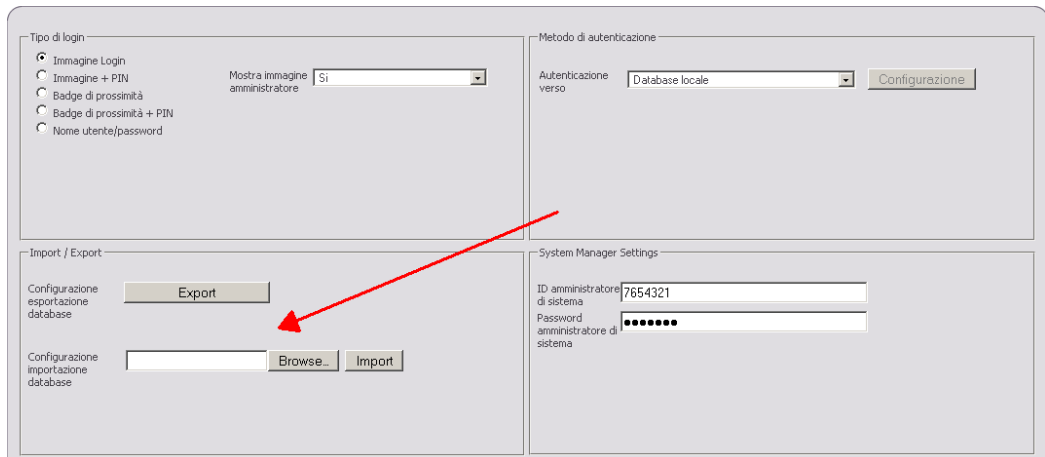
Per le operazioni di importazione ed esportazione sono disponibili varie opzioni.

- **Configurazione esportazione database:**
Questa opzione consente di esportare l'intero database di Universal Login Manager, compresi i dati utente e i dati di configurazione di Universal Login Manager, in un file *ulmConfig.ucf*. Questo file .ucf può quindi essere importato su

altri dispositivi per applicare ad essi la medesima configurazione ULM e gli stessi dati utente.

- **Configurazione importazione database:**

Con questa opzione è possibile importare un file *ulmConfig.ucf* per trasferire le impostazioni di configurazione e i dati utente da un dispositivo differente senza dover configurare manualmente il dispositivo. Sono supportati solo i file *ulmConfig.ucf* esportati da dispositivi Universal Login Manager mediante l'opzione **Configurazione esportazione database**.



- **Importa dati utente da CSV:**

Questa opzione consente di importare dati utente da un file di testo separato da virgole (CSV). Il file .csv deve essere costituito da un'intestazione di colonna contenente tutte o solo alcune delle seguenti parole chiave:

loginname, mail, cardid, homefolder, pincodex, password, deptid, roles, displayindex



Devono essere soddisfatti i seguenti requisiti:

- La parola chiave **loginname** è obbligatoria.
- Come delimitatore è possibile utilizzare "," o ";" (senza le virgolette).
- Se delimitatori del tipo "," o ";" fanno parte del valore di un campo, tale valore deve essere inserito tra virgolette doppie.
Esempio: *10,4* deve essere espresso come *"10,4"*
- Se le virgolette fanno parte di un valore, le virgolette devono essere raddoppiate e l'intero valore inserito tra virgolette doppie.
Esempio: Il valore *Stringa ("A")* deve essere espresso come *"Stringa (""A"")"*.
- Le barre rovesciate all'interno di un valore devono essere raddoppiate e l'intero valore inserito tra virgolette doppie.
Esempio: [\\server\homefolder](#) deve essere espresso come *"\\\\server\\homefolder"*



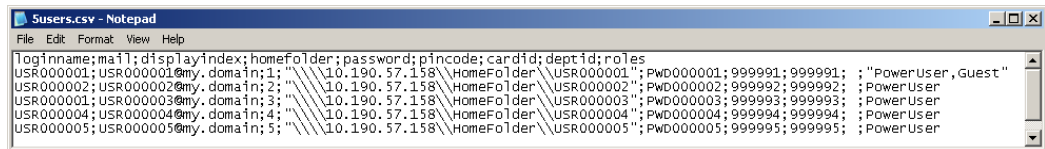
Si tenga presente che i dati verranno uniti. I dati esistenti saranno sovrascritti dai dati importati.

Esempio

Utente A e Utente B esistono nel database. Viene importato un file CSV con i dati di Utente B e Utente C. Al termine, Utente A rimane inalterato e Utente C viene

importato dal file CSV, mentre i dati esistenti di Utente B vengono sovrascritti con quelli del file CSV.

Vedere l'esempio seguente. Si noti l'uso delle virgolette nell'ultima colonna del primo utente, dove il campo contiene una virgola.



```

Loginname;mail;displayindex;homefolder;password;pincode;cardid;deptid;roles
USR000001;USR000001@my.domain;1;"";10.190.57.158\HomeFolder\USR000001";PWD000001;999991;999991;";"PowerUser,Guest"
USR000002;USR000002@my.domain;2;"";10.190.57.158\HomeFolder\USR000002";PWD000002;999992;999992;";PowerUser
USR000003;USR000003@my.domain;3;"";10.190.57.158\HomeFolder\USR000003";PWD000003;999993;999993;";PowerUser
USR000004;USR000004@my.domain;4;"";10.190.57.158\HomeFolder\USR000004";PWD000004;999994;999994;";PowerUser
USR000005;USR000005@my.domain;5;"";10.190.57.158\HomeFolder\USR000005";PWD000005;999995;999995;";PowerUser

```

7.4.4 Impostazioni Amministratore di sistema

Qui è possibile modificare l'ID e la password dell'amministratore di sistema.

7.5 Ruoli

Un ruolo è un gruppo di diritti di accesso alle funzioni del dispositivo (ad es. l'autorizzazione all'uso della stampa fronte/retro o a colori). I diritti di accesso sono controllati dal kit AMS, che deve quindi essere presente nel dispositivo. La schermata **Ruoli** permette agli amministratori di definire ruoli differenti con diritti di accesso specifici. Ciascun utente ha almeno un ruolo, che viene assegnato dall'amministratore. L'assegnazione dei ruoli viene eseguita nel menu **Utente** (vedere "[Users](#)" a pag. 26).

Sono disponibili tipi di ruoli differenti: preconfigurati e personalizzati.

Ruoli preconfigurati

Per la maggior parte, i nomi dei ruoli preconfigurati esistono anche sul dispositivo e sono stati implementati in Universal Login Manager per motivi di uniformità. I ruoli **Administrator**, **NetworkAdmin** e **DeviceAdmin** utilizzano tutti l'ID amministratore di sistema come ID reparto e hanno pertanto accesso a ULM Usage Tracker. Anche il ruolo **Reporter** ha accesso a ULM Usage Tracker. Questo ruolo è stato creato specificamente per consentire a un utente non amministrativo di accedere a ULM Usage Tracker se necessario. I ruoli **PowerUser**, **GeneralUser**, **LimitedUser** e **Guest** sono preconfigurati con varie autorizzazioni limitate. Per maggiori dettagli, consultare la configurazione delle autorizzazioni specifiche di ciascun ruolo, visualizzata sul lato destro del menu **Ruoli**.



I ruoli preconfigurati non possono essere modificati.

Ruoli personalizzati

Un ruolo personalizzato può essere creato facendo clic sul pulsante **Crea** e immettendo un nome per il nuovo ruolo. I ruoli personalizzati già esistenti possono essere modificati facendo clic sul nome del ruolo desiderato nell'elenco dei ruoli. È quindi

possibile configurare ogni funzione supportata da AMS per il ruolo selezionato, ad esempio l'autorizzazione per la stampa a colori o la stampa fronte/retro.

7.5.1 Mappatura ACL

Nella sezione **Controllo accessi** nella parte inferiore sinistra è possibile specificare se il controllo degli accessi avviene a livello di dispositivo o di funzione.

- **Livello login dispositivo** - Se questo pulsante di opzione è selezionato, il dispositivo risulta bloccato quando nessun utente è connesso. Non appena un utente si autentica, il dispositivo si sblocca e l'utente ha accesso a tutte le funzioni assegnate al proprio ruolo individuale.
- **Funzione login dispositivo** - Se questo pulsante di opzione è selezionato, alcune funzioni particolari del dispositivo possono essere utilizzate senza autenticazione dell'utente. Le funzioni utilizzabili senza autenticazione possono essere configurate nelle impostazioni **Autorizza/Rifiuta** del ruolo **FunctionLevelLogin**. Per questo ruolo, solo le funzionalità principali possono essere autorizzate o negate, ad esempio la stampa ma non più specificamente la stampa a colori o in bianco e nero. Quando un utente sceglie una funzione che non è disponibile nel ruolo **FunctionLevelLogin**, viene richiesta l'autenticazione. In tal caso, la disponibilità o meno della funzione richiesta per l'utente specifico dipende dalle impostazioni del ruolo associato a tale utente.
 - In **Applet limitate** è possibile limitare ciascuna MEAP applet installata.

Feature	Setting
Print Category	Permit
Copy Category	Permit
Color Copy	Color
Scan Category	Permit
Mailbox Category	Permit
Send Category	Permit
Browser Category	Permit
Utility Category	Permit
Default (MEAP) Category	Permit
Restricted Applets	-None- Copy ConvenienceCo



Se **Department ID Management** (Gestione ID reparto) è attivato sul dispositivo, la funzione login dispositivo funziona esclusivamente se l'ID reparto 9 è stato creato manualmente senza inserire anticipatamente una password.

Nella sezione **Controllo accessi** è possibile autorizzare o negare l'uso delle funzioni generali. Le funzioni selezionabili in questo caso sono **Scansione remota**, **Copia remota** e **Stampa remota**. Se autorizzate, queste funzioni possono essere utilizzate in modalità remota, altrimenti non sono disponibili.

Il campo **AMS Printer Driver Plugin** specifica se l'uso di questo plugin è obbligatorio o meno per l'uso delle funzioni controllate da AMS.

Una volta completata la configurazione, selezionare il pulsante **Salva** per salvare le impostazioni.

The screenshot shows the configuration interface for the 'PowerUser' role. It is divided into three main sections:

- Ruoli (Roles):** A list of roles including PowerUser (selected), Reporter, FunctionLevelLogin, Administrator, Guest, NetworkAdmin, DeviceAdmin, GeneralUser, and LimitedUser. There are 'Create' and 'Delete' buttons.
- Controllo accessi (Access Control):** Contains radio buttons for 'Livello login dispositivo' (selected) and 'Funzione login dispositivo'. Below are dropdown menus for 'Scansione remota', 'Copia remota', 'Stampa remota', and 'AMS Printer Driver Plugin' (set to 'Opzionale').
- PowerUser (Role Settings):** A table with 'Feature' and 'Setting' columns.

Feature	Setting
Print Category	Permit
Color print	Color
Simplex Print	Permit
Mailbox Print	Permit
Copy Category	Permit
Color Copy	Color
Simplex Copy	Permit
1 Page Per Sheet (no NUP)	1
Scan Category	Permit
Color Scan	Color
Mailbox Category	Permit
Color Print	Color
Simplex Print	Permit
1 Page Per Sheet (no NUP)	1

7.5.2 Importazione e mappatura di gruppi da Active Directory

Se è configurata una connessione a una Active Directory (AD), è possibile importare gruppi da AD e mapparli ai ruoli di Universal Login Manager.

Per importare un gruppo AD, premere il pulsante **Import AD Groups** (Importa gruppi AD). Viene visualizzato l'elenco dei gruppi AD, dal quale è possibile selezionare uno o più gruppi. Quando si preme **Salva**, i gruppi vengono importati come ruoli con lo stesso nome e appaiono nella sezione **Ruoli** insieme ai ruoli già esistenti.

Ruoli

- PowerUser
- Reporter
- FunctionLevelLogin
- Administrator
- Guest
- NetworkAdmin
- DeviceAdmin
- GeneralUser
- LimitedUser
- Users

Buttons: Create, Delete, Import AD Groups, Map groups to roles

Controllo accessi

Livello login dispositivo
 Funzione login dispositivo

Scansione remota:
 Copia remota:
 Stampa remota:
 AMS Printer Driver Plugin:

PowerUser

Feature	Setting
Print Category	Permit
Color print	Color
Simplex Print	Permit
Mailbox Print	Permit
Copy Category	Permit
Color Copy	Color
Simplex Copy	Permit
1 Page Per Sheet (no NUP)	1
Scan Category	Permit
Color Scan	Color
Mailbox Category	Permit
Color Print	Color
Simplex Print	Permit
1 Page Per Sheet (no NUP)	1

Save

Importazione gruppi

Prego selezionare il gruppo da importare.

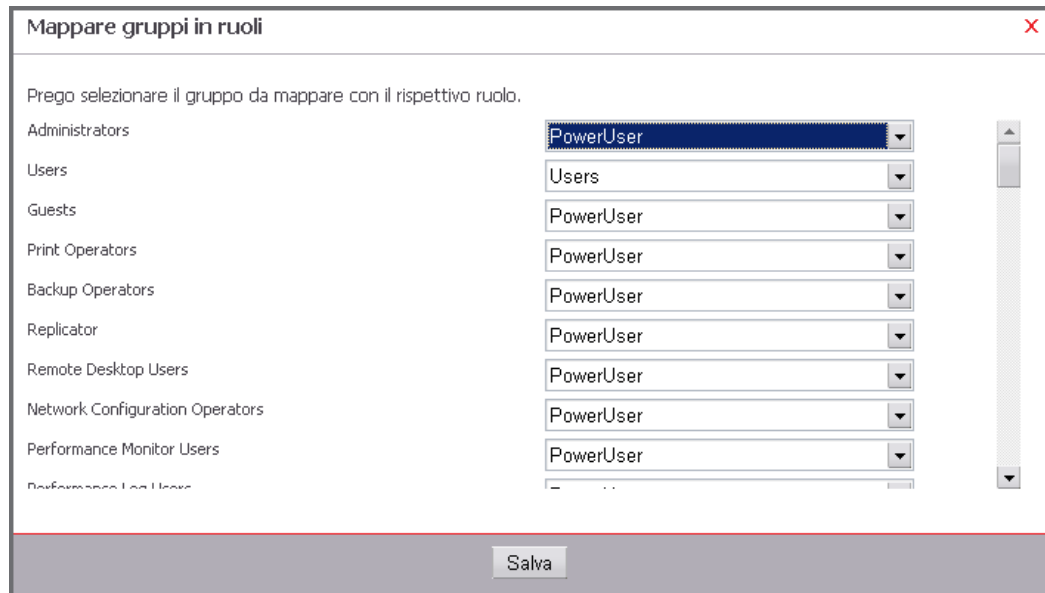
- Administrators
- Users
- Guests
- Print Operators
- Backup Operators
- Replicator
- Remote Desktop Users
- Network Configuration Operators
- Performance Monitor Users
- Performance Log Users
- Distributed COM Users
- IIS_IUSRS

Creare una mappatura implicita di gruppi in ruoli. Se si deselecta questa casella, sarà necessario creare la mappatura manualmente facendo clic sul pulsante "mappare gruppi in ruoli".

Salva

Se è selezionata l'opzione **Creare una mappatura implicita di gruppi in ruoli**, i gruppi importati vengono mappati automaticamente ai nuovi ruoli creati con lo stesso nome. In caso contrario, la mappatura deve essere eseguita manualmente.

Per mappare manualmente i gruppi, premere il pulsante **Mappare gruppi in ruoli**. Viene visualizzata una nuova finestra con i gruppi sulla sinistra e i ruoli selezionabili da un elenco a discesa sulla destra. Se è stata selezionata l'opzione **Creare una mappatura implicita di gruppi in ruoli** nel primo passaggio, il gruppo e il ruolo con lo stesso nome vengono mappati automaticamente (come nel caso di "users" nella schermata raffigurata). In caso contrario, la mappatura non viene eseguita e dovrà essere selezionata manualmente dall'amministratore. Premere **Salva** per completare la mappatura.



7.6 Personalizzare

In questa schermata è possibile personalizzare l'interfaccia utente. Questa operazione può essere eseguita selezionando un tema esistente oppure creandone uno nuovo dalla sezione **Sfondi**. Sul lato destro è possibile immettere un nome per il nuovo tema (non è invece possibile rinominare i temi esistenti) e specificare varie impostazioni quali **Dimensione font** e altre relative ai colori. Inoltre, è possibile caricare un'immagine di sfondo e impostare la posizione della maschera di login e del testo informativo. I formati di immagine accettati sono JPG, PNG e GIF.

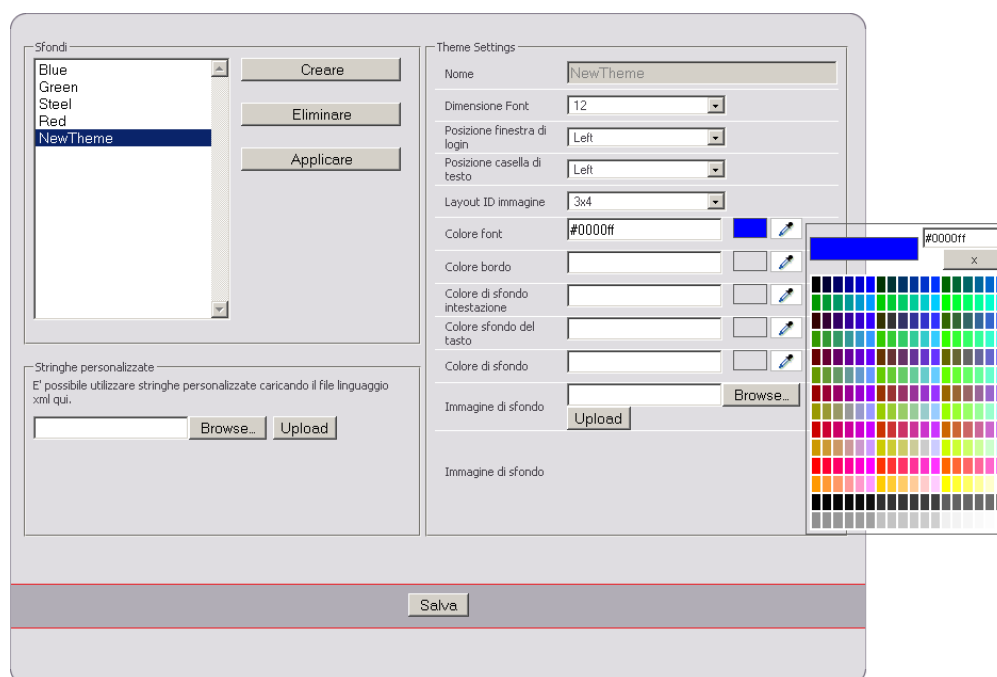
Sono disponibili le **Impostazioni tema** seguenti:

- **Nome** - Il nome del tema. Non può più essere modificato dopo che un tema è stato creato.
- **Dimensione font** - Dimensione font dei testi visualizzati.
- **Posizione finestra di login** - La posizione della finestra di login. Può essere **Sinistra**, **Centro**, **Destra** o **Nascosto**. Se viene selezionato **Nascosto**, non viene visualizzato alcun simbolo di badge per i tipi di login Badge di prossimità e Badge di prossimità con PIN.
- **Posizione casella di testo** - La posizione della casella di testo. Può essere **Sinistra**, **Centro** o **Destra**.

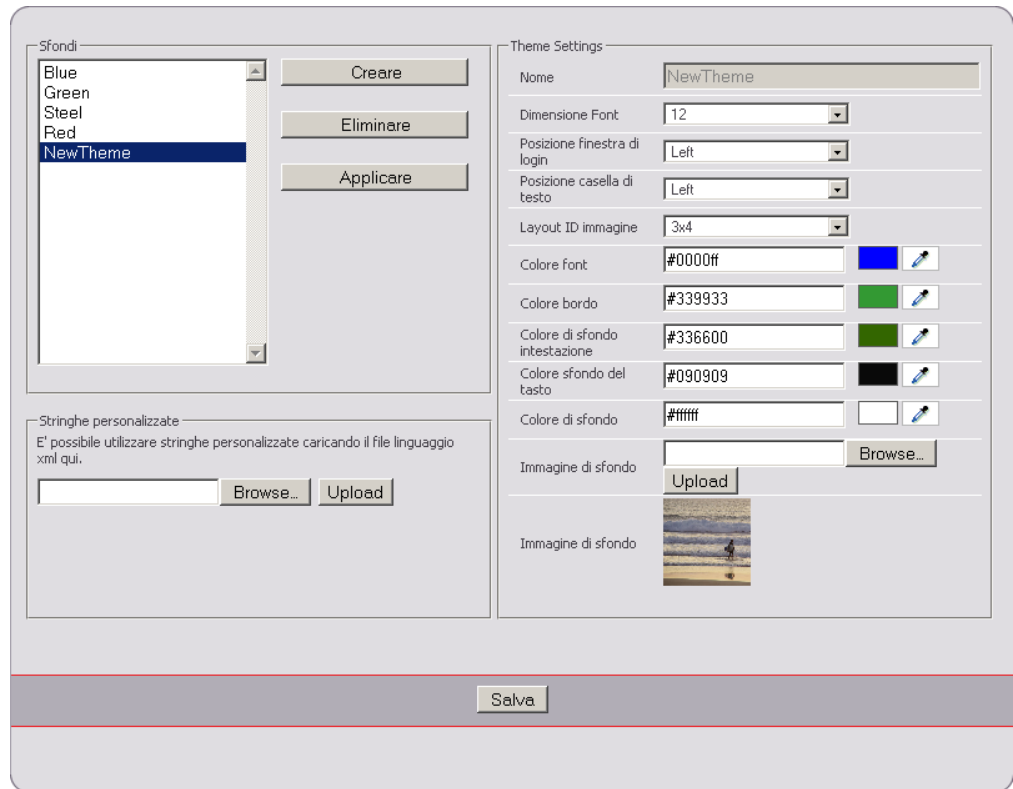
- **Layout ID immagine** - Determina quale matrice viene utilizzata per l'allineamento delle immagini ID sull'interfaccia del dispositivo. È possibile visualizzare 2x4 o 3x4 immagini su una sola schermata.
- **Colore font** - Il colore dei font.
- **Colore bordo** - Il colore del bordo intorno alle caselle.
- **Colore di sfondo intestazione** - Il colore di sfondo della barra del titolo.
- **Colore sfondo del tasto** - Il colore di sfondo del pulsante di login.
- **Colore di sfondo** - Il colore di sfondo della finestra principale.
- **Immagine di sfondo** - Miniatura dell'immagine caricata.

Esempio

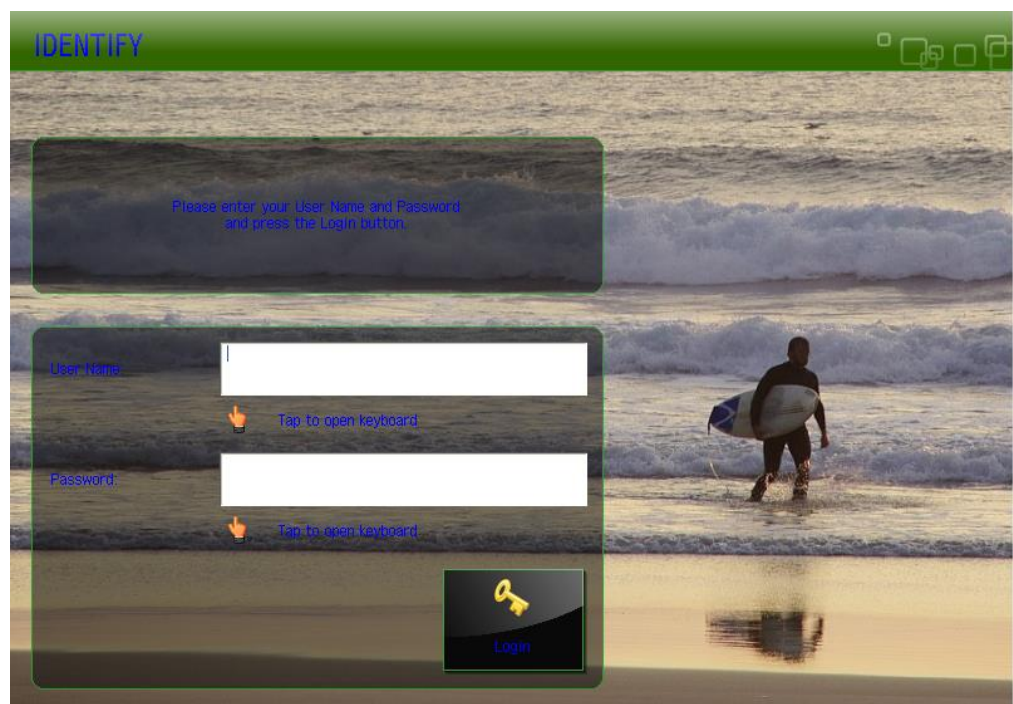
- Premere il pulsante **Crea** e immettere un nome. Scegliere la dimensione font desiderata e specificare la posizione della finestra di login e della casella di testo delle informazioni. Quindi, usare il selettore per ciascuno dei campi di selezione del colore.



- Scegliere un colore per il font e, se necessario, un colore per il bordo, il titolo, il pulsante e lo sfondo generale.



- È anche possibile selezionare e caricare un'immagine di sfondo per il dispositivo. Fare clic su **Salva** per applicare le impostazioni. Le impostazioni diventano attive e l'interfaccia di Login Manager viene personalizzata in base alle preferenze specificate.



7.6.1 Stringhe localizzate



- La lingua di visualizzazione di Universal Login Manager dipende dalla lingua di visualizzazione del dispositivo.
- Per cambiare la lingua dell'interfaccia di Universal Login Manager, è necessario cambiare la lingua di visualizzazione del dispositivo. Ad esempio, se si seleziona lo spagnolo come lingua di visualizzazione del dispositivo, anche l'interfaccia utente di Universal Login Manager sarà visualizzata in spagnolo.
- Non è possibile impostare tutte le lingue installate sul dispositivo. Pertanto, prima di cambiare la lingua occorre assicurarsi che il language pack della lingua che si desidera impostare sia disponibile sul dispositivo.

Il programma di installazione di Universal Login Manager include le stringhe tradotte in tutte le lingue che erano disponibili nel portale delle stringhe (NT-ware String Portal) nel momento in cui il programma è stato creato. Queste stringhe sono contenute in un file chiamato *MomLang.xml*. Una volta installato Universal Login Manager, è possibile cambiare la lingua dell'interfaccia utente di Universal Login Manager scegliendo una di queste lingue. NT-ware fornisce le stringhe tradotte solo nelle lingue EFIGS (inglese, francese, italiano, tedesco e spagnolo). Per questo può accadere che le stringhe (o alcune di esse) non siano disponibili nella lingua locale anche se tale lingua è inclusa in *MomLang.xml*. Per risolvere questa situazione, è possibile scaricare *MomLang.xml* con le stringhe di Universal Login Manager, aggiungere le traduzioni mancanti e quindi caricare il file tradotto sul dispositivo in questione (vedere di seguito). Se la propria lingua non è ancora inclusa in *MomLang.xml*, occorre prima aggiungerla a *MomLang.xml* e quindi tradurre le stringhe corrispondenti. Per eseguire questa operazione è necessaria una certa conoscenza del linguaggio XML.

Lingue disponibili

Attualmente sono disponibili le lingue seguenti:



Per i codici lingua viene fatta distinzione tra lettere maiuscole e minuscole. Usare solo caratteri maiuscoli.

Lingua	Codice lingua
Arabo	AR
Bahasa Melayu	MS
Portoghese brasiliano	BRA
Inglese britannico	GB
Catalano	CA
Cinese	CN
Croato	HR

Lingua	Codice lingua
Ceco	CZ
Danese	DK
Olandese	NL
Inglese	EN
Estone	EE
Finlandese	FI
Francese	FR
Tedesco	DE
Ebraico	HE
Ungherese	HU
Islandese	IS
Italiano	IT
Giapponese	JP
Coreano	KO
Lettone	LVA
Lituano	LT
Norvegese	NO
Polacco	PL
Portoghese	PT
Russo	RU
Sloveno	SL
Spagnolo	ES
Svedese	SE
Thai	TH
Cinese tradizionale	TW
Turco	TR

File in lingua personalizzato (MomLang.xml)

Se si desidera utilizzare un file in lingua personalizzato, procedere nel modo seguente.

1. Estrarre le stringhe richieste dal portale delle stringhe NT-ware facendo clic sul collegamento seguente: Esportazione stringhe per Universal Login Manager (<http://ntwlabib.dnsalias.com/Stringtable/MomLang.xml?from=40000&to=40999>)

2. Salvare localmente il file MomLang.xml scaricato. Assegnare al file un nome indicativo del contenuto, ad esempio aggiungere il codice della lingua al nome in modo da distinguerlo facilmente dal file MomLang.xml predefinito del programma di installazione.
3. Aprire il file in un editor XML, individuare la lingua desiderata o creare le stringhe localizzate nella propria lingua, se non esistono ancora. Se occorre aggiungere al file le stringhe tradotte nella propria lingua, utilizzare il codice ISO-639-1 della lingua da aggiungere.
4. Al termine, caricare il file modificato nel **menu Personalizza** alla voce **Stringhe personalizzate**. Specificare il file facendo clic sul pulsante **Sfoglia** e caricarlo con il pulsante **Carica**. In seguito, se necessario, è possibile eliminarlo facendo clic su **Rimuovi**. In questo modo viene riattivato il file MomLang.xml predefinito del programma di installazione.



Oltre alla propria lingua locale, le stringhe in inglese devono sempre essere presenti nel file XML personalizzato. In caso contrario, l'importazione delle stringhe personalizzate non riuscirà.



I file in lingua sono archiviati localmente sul dispositivo. Se si hanno più dispositivi, è necessario ripetere l'importazione per ciascuno di essi.

Modifica di stringhe per l'interfaccia utente MEAP

È inoltre possibile modificare le stringhe visualizzate sul display MEAP. Premere **Modifica stringhe** nella pagina **Personalizza**. Selezionare la stringa da modificare inserendo un segno di spunta nella relativa casella di controllo. Selezionare **Salva** per finire.

Personalizza Stringhe ✕

Spuntare la casella di controllo per ogni stringa che si vuole personalizzare.

Identificarsi con scheda ID	<input type="checkbox"/>
Immettere il proprio Nome utente e Password e premere il pulsante Accesso.	<input type="checkbox"/>
Identificarsi con il proprio PIN personale e premere il pulsante Accesso.	<input type="checkbox"/>
Prego inserire il Codice Pin da associare al proprio badge	<input type="checkbox"/>
Accesso in corso. Attendere un momento.	<input type="checkbox"/>
Immettere il proprio nome utente e password e premere il pulsante Accesso.	<input type="checkbox"/>
Scheda ID sconosciuta. Eseguire l'accesso utilizzando il proprio nome utente e password per registrare la scheda ID.	<input type="checkbox"/>
Riprovare immettendo i propri dati completi.	<input type="checkbox"/>



Per ripristinare i valori dei singoli campi, deselezionare la casella di controllo. La stringa verrà reimpostata sul valore predefinito.

7.7 Usage Tracker

Universal Login Manager/embedded Universal Login Manager offre la possibilità di scaricare un'applicazione Rich Internet per il monitoraggio dell'uso dei dispositivi: Universal Login Manager Usage Tracker. Questa applicazione viene eseguita in un browser locale sul computer dell'utente e permette di gestire un elenco di dispositivi registrati (fino a 10) e recuperare dati di report da tali dispositivi.



Limite dati di rapporto

Tenere presente che la quantità di dati di rapporto recuperabili dipende dalla capacità di archiviazione del registro CPCA sul dispositivo. La capacità di archiviazione è solitamente limitata a 5.000 voci, ma può variare a seconda del dispositivo. Per informazioni dettagliate, fare riferimento al manuale utente del dispositivo in uso.

Il collegamento a ULM Usage Tracker è disponibile nella scheda **Usage Tracker** di Universal Login Manager/embedded Universal Login Manager Administration Tool.

ULM Usage Tracker offre tre sottomenu:

ULM Usage Tracker

In questa pagina è possibile aggiungere fino a 10 stampanti e creare rapporti per un periodo di tempo specifico.

The screenshot shows the 'Usage Tracker' page in the Universal Login Manager interface. It features a sidebar with 'Usage Tracker' selected, a main content area with login fields, a table for adding devices, and a table for selecting report types.

Select	Device Model	Device IP Address	Serial Number	Earliest Date	Neighbors	Delete	Availability
There are no configured devices.							

Report Name	Report Description	Generate Report
User Details	Will show a report of all the jobs which were performed between the given dates, grouped per user.	
Device Details	Will show a report of all the jobs which were performed between the given dates, grouped per device.	
User Summary	Will show a summary report for each user which has executed a job on one of the selected devices between the given dates.	
Device Summary	Will show a summary report for the selected devices, for the jobs executed on them between the given dates.	

Tabella costi

In questa pagina è possibile specificare i prezzi di ogni prodotto, ordinati per supporti e servizio, ad es. per **Stampa A4 a colori**. Il valore viene immesso semplicemente come numero, senza specificare la valuta.



I prezzi possono essere specificati con due decimali.

universal login manager ULM Usage Tracker

Cost Table

	Print	Copy	Scan	Fax
A3 B/W	8.00	7.00	1.00	0.00
Small B/W	2.00	5.00	0.00	0.00
A4 B/W	3.00	6.00	0.00	0.00
A5 B/W	2.00	4.00	0.00	0.00
SRA3 B/W	0.00	0.00	0.00	0.00
Letter B/W	0.00	0.00	0.00	0.00
Legal B/W	0.00	0.00	0.00	0.00
Tabloid B/W	0.00	0.00	0.00	0.00
Half Letter B/W	0.00	0.00	0.00	0.00
A3 Color	0.00	0.00	0.00	
Small Color	0.00	0.00	0.00	
A4 Color	5.00	8.00	1.00	
A5 Color	3.00	5.00	1.00	
SRA3 Color	0.00	0.00	0.00	
Letter Color	0.00	0.00	0.00	
Legal Color	0.00	0.00	0.00	
Tabloid Color	0.00	0.00	0.00	
Half Letter Color	0.00	0.00	0.00	
Staple	0.00			
Hole Punch	0.00			

Save



Tutti i dati quali i prezzi o le stampanti aggiunte vengono memorizzati solo nella cache locale del browser e controllati mediante cookie. Se la cache e i cookie vengono cancellati, tutti i dati configurati vengono persi. Per salvare i dati, utilizzare le funzioni di importazione ed esportazione nei casi in cui sono disponibili.

Impostazioni

Qui è possibile modificare due parametri per l'esportazione dei rapporti in formato CSV e delle **Tablelle costi**.

- Delimitatore decimale:**
 Il delimitatore decimale può essere un punto (.) o una virgola (,).
- Delimitatore colonna CSV:**
 È possibile selezionare il punto e virgola (;), la virgola (,) o il carattere di tabulazione (TAB).

universal login manager ULM Usage Tracker

Settings

Decimals delimiter: Dot (.)

CSV columns delimiter: Semicolon (;)

7.7.1 Aggiunta di un dispositivo

Per aggiungere un dispositivo per il quale si desidera creare un rapporto, aprire la pagina di ULM Usage Tracker e premere il pulsante **Aggiungi dispositivo**. Si apre una riga nella quale si può aggiungere un nuovo dispositivo. Immettere l'indirizzo IP e premere il pulsante **Aggiungi**. Se è stata selezionata l'opzione **Cerca nei paraggi**, ULM Usage Tracker tenta di trovare altri dispositivi nella stessa sottorete. I nuovi dispositivi vengono quindi visualizzati nell'elenco dei dispositivi. I nomi vengono compilati automaticamente. Al termine della procedura di registrazione, premere il pulsante **Fatto**. La riga "Aggiungi dispositivo" si chiude.

L'elenco dei dispositivi comprende le seguenti colonne:

- **La colonna di selezione (prima colonna):**
Consente di selezionare il dispositivo per il report facendo clic sulla rispettiva casella di controllo. Selezionando la casella di controllo nell'intestazione della colonna, vengono selezionati tutti i dispositivi disponibili. Deselezionando la casella di controllo, tutti i dispositivi vengono deselezionati.
- **Modello di dispositivo:**
Questo nome viene recuperato automaticamente nel momento in cui viene immesso l'indirizzo IP del dispositivo.
- **Indirizzo IP dispositivo:**
L'indirizzo IP del dispositivo.
- **Serial Number (Numero di serie):**
Numero di serie del dispositivo.
- **Data più vicina:**
Se si fa clic su **Verifica**, ULM Usage Tracker tenta di determinare la data della voce più vecchia nell'elenco lavori del dispositivo. Questa operazione funziona solo se sono stati immessi un nome utente e una password validi.
- **Vicini:**
Se si fa clic su **Trova**, ULM Usage Tracker tenta di trovare altri dispositivi nella stessa sottorete.
- **Delete:**
Premere l'icona Elimina se si desidera rimuovere il dispositivo dall'elenco.

- **Disponibilità:**
Se il dispositivo è disponibile, l'icona visualizzata qui è verde, altrimenti è rossa.

The screenshot shows the 'Usage Tracker' interface in the Universal Login Manager. It includes a sidebar with navigation options like 'Usage Tracker', 'Cost Table', 'Settings', and 'Help'. The main content area has a form for logging in as 'administrator' with a password field, and date selection for 'Start Date' (01-05-2012) and 'End Date' (30-04-2013). Below the form is a table of devices with columns for Device Model, Device IP Address, Serial Number, Earliest Date, Neighbors, Delete, and Availability. The 'Availability' column shows green checkmarks for available devices and red minus signs for unavailable ones. At the bottom, there is a 'Generate Report' section with a table of report types and descriptions.

Device Model	Device IP Address	Serial Number	Earliest Date	Neighbors	Delete	Availability
<input type="checkbox"/> IR-ADV C5030/5035	10.129.51.86	GNM01678	27-01-2010	[Find]	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> IR-ADV C2020/2030i		EZU00213	[Check]	[Find]	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> IR-ADV C2220/2230	10.129.51.235	LYB00212	13-09-2012	[Find]	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Miskin	192.168.38.100	VDE00000	[Check]	[Find]	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> IR-ADV C2020/2030i	10.129.50.98	EZU00213	[Check]	[Find]	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> IR-ADV C7055/7065	10.129.50.21	FNP00202	[Check]	[Find]	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> IR-ADV 400/500	10.129.51.92	PYL00205	[Check]	[Find]	<input type="checkbox"/>	<input type="checkbox"/>

Report Name	Report Description	Generate Report
User Details	Will show a report of all the jobs which were performed between the given dates, grouped per user.	
Device Details	Will show a report of all the jobs which were performed between the given dates, grouped per device.	
User Summary	Will show a summary report for each user which has executed a job on one of the selected devices between the given dates.	
Device Summary	Will show a summary report for the selected devices, for the jobs executed on them between the given dates.	

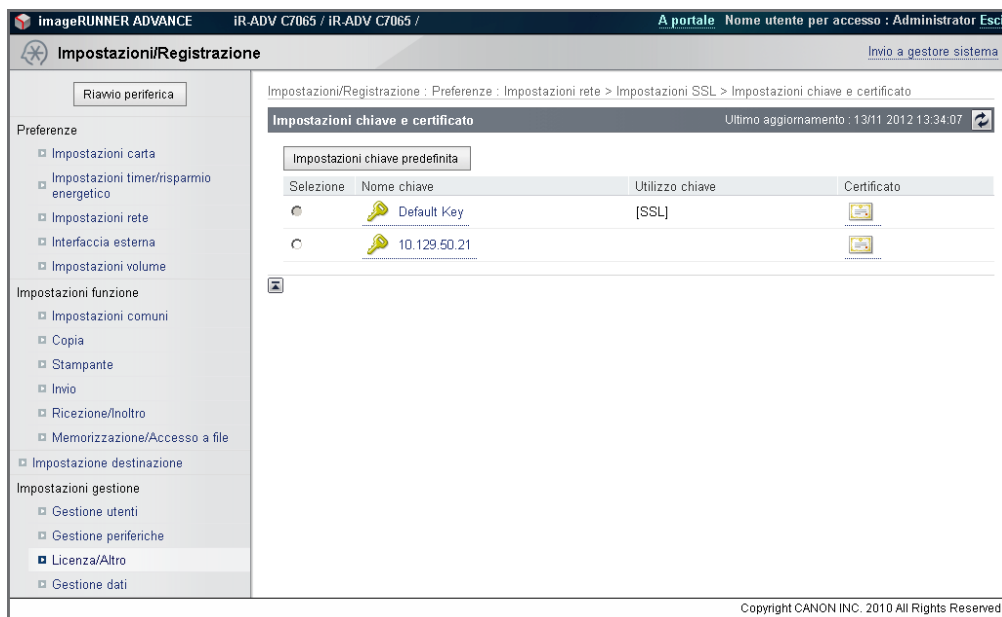
7.7.1.1 Creazione di un certificato

È possibile che il browser non sia in grado di recuperare informazioni dal dispositivo a causa di problemi con il certificato quando si usa una connessione SSL. In tal caso, la stampante figura come non disponibile nell'elenco dei dispositivi.

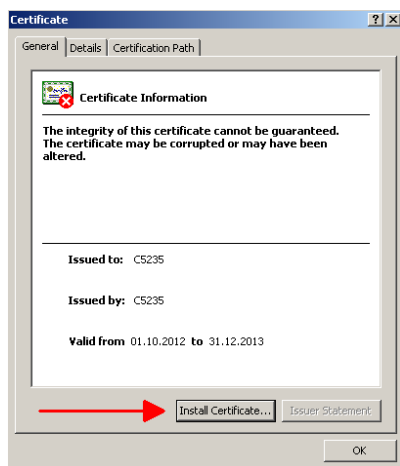
Per risolvere questo problema, è necessario creare un nuovo certificato sul dispositivo includendone l'indirizzo IP. A questo scopo, procedere nel modo seguente:

- Aprire l'interfaccia remota del dispositivo in un browser e accedere con le credenziali di amministratore di sistema.
- Aprire **Settings/Registration : Management Settings : License/Other > MEAP Settings** e deselezionare **Use SSL**.
- Fare clic su **OK** e riavviare il dispositivo.
- Accedere di nuovo e aprire **Settings/Registration : Preferences : Network Settings > SSL Settings > Key and Certificate Settings**.
- Se in precedenza veniva utilizzata una chiave diversa dalla **chiave predefinita**, selezionare il pulsante di opzione davanti a **Default Key** e fare clic su **Default Key Settings** per impostare la chiave predefinita come chiave SSL standard. Riavviare il dispositivo.
- Eseguire di nuovo l'accesso. In **Settings/Registration : Management Settings : Device Management > Key and Certificate Settings**, fare clic su **Generate Key**, quindi aprire **Network Communication**.

- Digitare l'indirizzo IP nel campo **Common Name**, specificare le impostazioni **Certificate Settings** e fare clic su **OK**.
- Aprire **Settings/Registration : Preferences : Network Settings > SSL Settings > Key and Certificate Settings**.
- Selezionare la nuova chiave e fare clic su **Default Key Settings**. Ora **[SSL]** indica questa chiave come chiave SSL attiva.



- Aprire **Settings/Registration : Management Settings : License/Other > MEAP Settings** e selezionare **Use SSL**.
- Fare clic su **OK** e riavviare il dispositivo.
- A questo punto aprire di nuovo l'interfaccia remota del dispositivo dal browser e salvare il certificato SSL nel file system. L'operazione esatta da eseguire dipende dal browser in uso.
- Aprire Esplora risorse di Windows e fare doppio clic sul certificato salvato.



- Avviare la procedura Importazione guidata certificati facendo clic su **Installa certificato** e seguire le istruzioni visualizzate.
- Al termine della procedura guidata, avviare ULM Usage Tracker. A questo punto la stampante figura come disponibile nell'elenco dei dispositivi.



Il certificato deve essere installato su ogni PC che esegue ULM Usage Tracker.

7.7.2 Tabella costi

In questa pagina è possibile specificare i prezzi dei supporti e dei servizi. Ad esempio, è possibile impostare prezzi differenti per i servizi Fax o Stampa A4.

	Print	Copy	Scan	Fax
A3 B/W	8.00	7.00	1.00	0.00
Small B/W	2.00	5.00	0.00	0.00
A4 B/W	3.00	6.00	0.00	0.00
A5 B/W	2.00	4.00	0.00	0.00
SRA3 B/W	0.00	0.00	0.00	0.00
Letter B/W	0.00	0.00	0.00	0.00
Legal B/W	0.00	0.00	0.00	0.00
Tabloid B/W	0.00	0.00	0.00	0.00
Half Letter B/W	0.00	0.00	0.00	0.00
A3 Color	0.00	0.00	0.00	
Small Color	0.00	0.00	0.00	
A4 Color	5.00	8.00	1.00	
A5 Color	3.00	5.00	1.00	
SRA3 Color	0.00	0.00	0.00	
Letter Color	0.00	0.00	0.00	
Legal Color	0.00	0.00	0.00	
Tabloid Color	0.00	0.00	0.00	
Half Letter Color	0.00	0.00	0.00	
Staple	0.00			
Hole Punch	0.00			

La **Tabella costi** può essere esportata e importata utilizzando gli appositi pulsanti disponibili nell'angolo superiore destro della schermata.

7.7.3 Creazione di un rapporto

Per creare un rapporto, procedere nel modo seguente:

- Immettere un nome utente e una password validi.
- Specificare l'intervallo di date nei campi **Data inizio** e **Data fine**.
- Nell'elenco dei dispositivi, selezionare le caselle di controllo dei dispositivi da includere nei rapporti oppure la casella di controllo nell'intestazione della colonna per includere tutti i dispositivi. È possibile selezionare solo i dispositivi indicati come disponibili.

- Selezionare un rapporto facendo clic sull'icona corrispondente nella colonna **Generare report**. Il rapporto viene generato e quindi visualizzato. A seconda dell'intervallo di date e del numero di dispositivi, l'operazione può durare vari minuti.



- Se si selezionano più dispositivi, assicurarsi che l'utente che ha generato il rapporto sia associato al ruolo Administrator o Reporter per tutti i dispositivi selezionati e che nome e password siano uguali su tutti i dispositivi.
- I registri fax possono essere letti solo da dispositivi che eseguono Universal Login Manager V4.1 o versioni successive.

User name:

Password:

Start Date:

End Date:

Here you can add or edit the devices for which you would like to create a report. You can add a maximum of 10 devices. After you have finished editing the list, please indicate which device you would like to be included in your report, by selecting the checkboxes.

<input checked="" type="checkbox"/>	Device Model	Device IP Address	Serial Number	Earliest Date	Neighbors	Delete	Availability
<input checked="" type="checkbox"/>	IR-ADV C5030/5035	10.129.51.86	GNM01678	27-01-2010	[Find]		
<input type="checkbox"/>	IR-ADV C2020i/2030i		EZU00213	[Check]	[Find]		
<input checked="" type="checkbox"/>	IR-ADV C2220/2230	10.128.51.235	LYB00212	13-09-2012	[Find]		
<input type="checkbox"/>	Miskin	192.168.38.100	VDE00000	[Check]	[Find]		
<input type="checkbox"/>	IR-ADV C2020i/2030i	10.129.50.98	EZU00213	[Check]	[Find]		
<input type="checkbox"/>	IR-ADV C7055/7065	10.129.50.21	FNP00202	[Check]	[Find]		
<input type="checkbox"/>	IR-ADV 400/500	10.129.51.92	PYL00205	[Check]	[Find]		

Please choose the type of statistic data that should be generated.

Report Name	Report Description	Generate Report
User Details	Will show a report of all the jobs which were performed between the given dates, grouped per user.	
Device Details	Will show a report of all the jobs which were performed between the given dates, grouped per device.	
User Summary	Will show a summary report for each user which has executed a job on one of the selected devices between the given dates.	
Device Summary	Will show a summary report for the selected devices, for the jobs executed on them between the given dates.	

Dopo la lettura dei dati dai dispositivi, il rapporto selezionato viene visualizzato. È possibile cambiare tipo di rapporto senza ripetere la lettura dei dati semplicemente facendo clic sui nomi dei rapporti nell'angolo superiore sinistro. Dalla scheda della vista non impaginata, il rapporto selezionato si apre in una finestra pop-up che permette all'utente di stampare la pagina html visualizzata. Per chiudere la finestra pop-up, fare clic sulla X rossa nell'angolo in alto a destra.



Se per un lavoro di stampa vengono contabilizzati articoli diversi, per alcuni tipi di rapporto viene indicata per il lavoro la quantità complessiva di articoli, seguita dagli articoli stessi raggruppati per tipo.

Esempio

Un lavoro comprende 5 pagine A4 a colori, 6 pagine A4 in bianco e nero e 5 pagine in fronte/retro. In totale fanno 16 articoli. Nella tabella, il totale indicato per il lavoro di stampa è 16 e i tipi di lavoro sono elencati separatamente con i relativi totali parziali.

I rapporti possono essere esportati come file *.csv per elaborarli ulteriormente in un'applicazione di fogli di calcolo. A questo scopo, fare clic sull'icona di esportazione nell'angolo superiore destro della schermata.



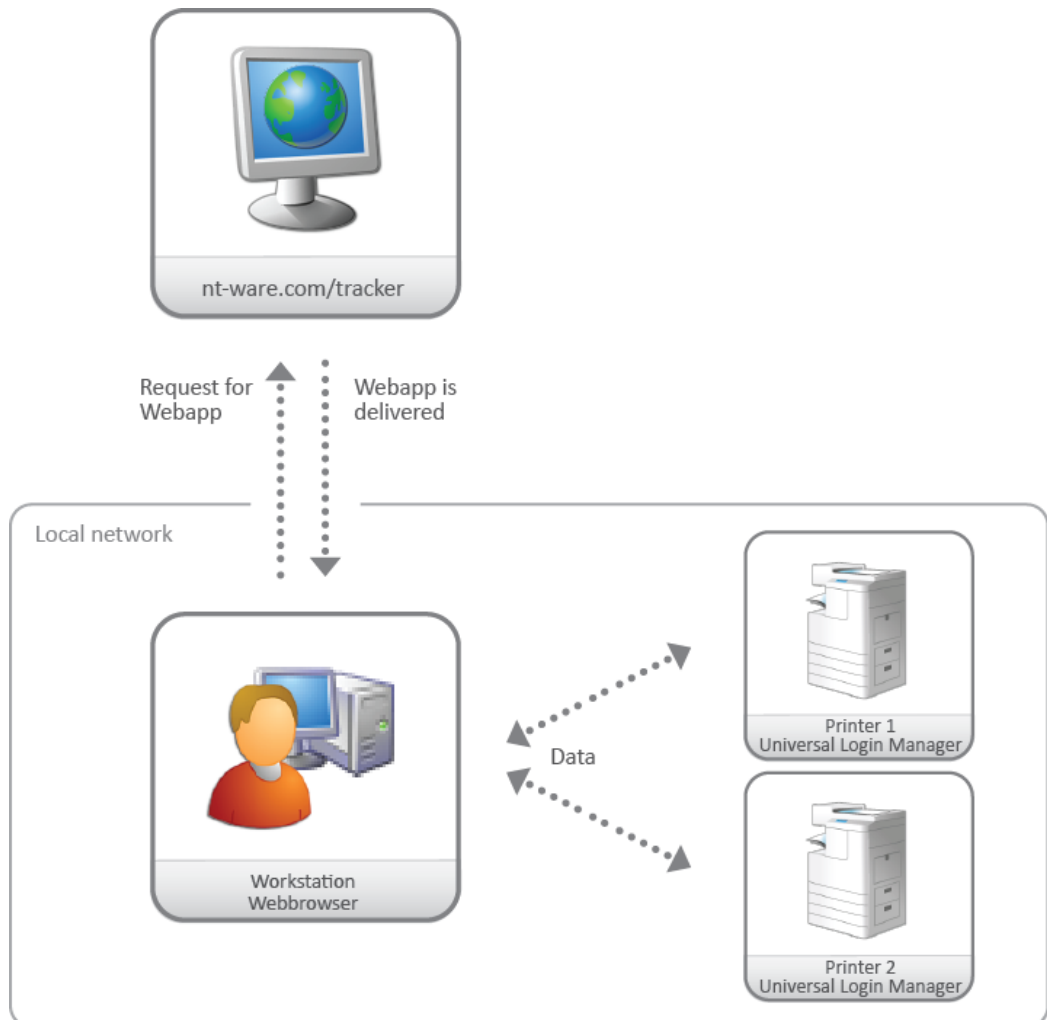
Il file *.csv esportato usa i delimitatori configurati in *Impostazioni*.

7.7.4 Aspetti relativi alla sicurezza

ULM Usage Tracker è un'app web che viene eseguita localmente nel browser. Quando l'utente apre ULM Usage Tracker dall'interfaccia utente, il browser web richiede il pacchetto dell'app web al sito web NT-ware. Il pacchetto include tutti gli script e i file necessari per eseguire ULM Usage Tracker (JS, Flash, HTML, immagini, CSS). Una volta ricevuto il pacchetto, il browser avvia l'app web localmente. L'app viene eseguita unicamente nel browser e conserva i propri dati nella cache o nei cookie del browser, a seconda del tipo di dati (vedere di seguito per ulteriori dettagli).



Nessun dato viene condiviso al di fuori della rete locale e nessun dato lascia la rete locale. La comunicazione con le stampanti avviene in modo criptato mediante il protocollo HTTPS.



Dettaglio delle comunicazioni di ULM Usage Tracker

- Tutti gli script eseguiti nell'ambiente di ULM Usage Tracker vengono scaricati a livello locale e conservati nella cache del browser. Sono coinvolte le seguenti tecnologie:
 - **JavaScript + HTML:**
Applicazione generica.
Importazione dei prezzi, tranne che per IE8/9.
 - **Adobe Flash:**
Tutti i browser: esportazione di rapporti e prezzi.
Solo IE8/9: importazione di prezzi
- Il browser invia delle richieste ai dispositivi tramite il protocollo HTTP(S), utilizzando chiamate JavaScript AJAX. La risposta viene restituita nel formato JSON e analizzata a livello locale dal codice JavaScript eseguito nel browser.
- Il trasferimento dei dati tra la workstation e la stampante avviene via HTTPS. Solo se il protocollo HTTPS non è disponibile per qualsiasi motivo (configurazione di rete, certificati, ecc.), il sistema utilizza HTTP in alternativa.
- Nome utente e password, IP stampante e impostazioni nonché tabelle prezzi vengono memorizzati all'interno dei cookie.
- I dati ricevuti dalle stampanti vengono conservati nella memoria della workstation.
- A causa delle diverse tecnologie impiegate in Internet Explorer (solo versione 8/9), le comunicazioni avvengono nel formato JSON-P. Se si usa il protocollo HTTPS, viene visualizzato un messaggio che segnala che il certificato è sconosciuto. Per ovviare a questo problema, è possibile installare il certificato a livello locale. Vedere il capitolo Creazione di un certificato sul dispositivo (vedere "[Creazione di un certificato](#)" a pag. [57](#)).

8 Secure Print

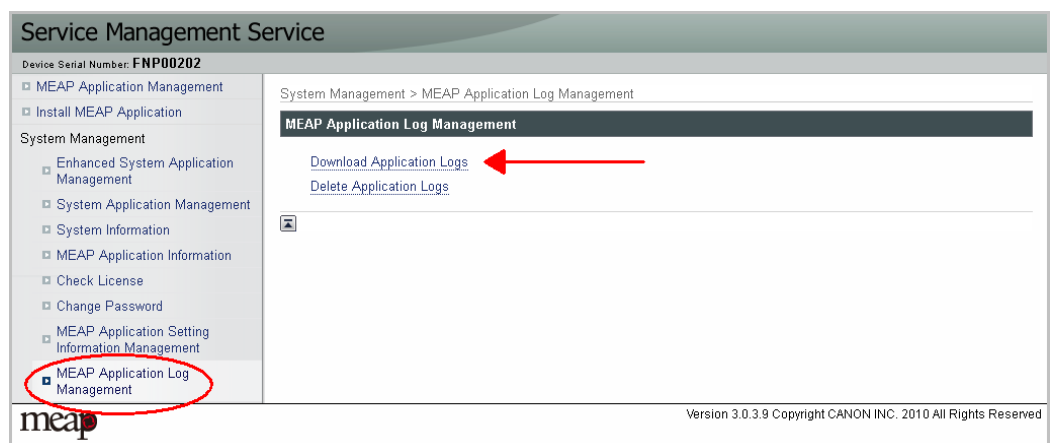
Per configurare la funzione Stampa protetta della stampante, consultare il portale *Canon Prodotti di office imaging Manuali utente* (http://ug.oipsrv.net/portal-eu-af-me-ru/frame_htmls/home.html) e cercare il modello specifico della propria stampante.

9 Aggiornamento a uniFLOW Server

Universal Login Manager può anche essere connesso a un server uniFLOW o RPS. In questo caso, funzionerà automaticamente in modalità "Client uniFLOW", nella quale Universal Login Manager è controllato dal server uniFLOW come un'istanza di uniFLOW Login Manager standard.

10 Come ottenere i file di registro

Universal Login Manager registra le proprie attività e scrive i relativi dati nei registri dispositivo, ai quali è possibile accedere dalla pagina Service Management Service.



11 Appendice

11.1 Hardware

Di seguito è riportato l'elenco dei dispositivi e delle versioni firmware supportate.

Nome dispositivo	Vers. firmware	AMS	Nota
imageRUNNER ADVANCE C9280 PRO	v10.23	STD	*1
imageRUNNER ADVANCE C7280i/C7270i/ C7260i	v10.23	STD	
imageRUNNER ADVANCE C5255/C5255i/C5250/C5250i/C5240i/ C5235i	v06.01	STD	
imageRUNNER ADVANCE C2230i/C2225i/C2220i	v06.01	STD	
imageRUNNER ADVANCE C2220L	v10.23	STD	
imageRUNNER ADVANCE 8205 PRO/8295 PRO/8285 PRO	v02.01	STD	
imageRUNNER ADVANCE 6275i/6265i/ 6255i	v02.01	STD	
imageRUNNER ADVANCE 4251i/4245i/4235i/4225i	v10.20	STD	
imageRUNNER ADVANCE C9070 PRO /C9060 PRO	v69.03	Opzione	*1
imageRUNNER ADVANCE C7065i /C7055i	v69.03	Opzione	
imageRUNNER ADVANCE C5051/ C5051i /C5045/C5045i/C5035/C5035i/C5030/C5030i	v69.03	Opzione	
imageRUNNER ADVANCE C2030L/C2020L	v32.01	Opzione	*2
imageRUNNER ADVANCE C2030i/C2025i/C2020i	v32.01	Opzione	
imageRUNNER ADVANCE 8105 PRO /8095 PRO/8085 PRO	v44.03	Opzione	
imageRUNNER ADVANCE 6075/6075i/6065/6065i/6055/	v44.03	Opzione	

Nome dispositivo	Vers. firmware	AMS	Nota
6055i			
imageRUNNER ADVANCE 4051i/4045i/4035i/4025i	v17.02	Opzione	
imageRUNNER ADVANCE 500i/400i	v1.02	STD	
imageRUNNER ADVANCE C351iF/C350i/C250i/C350P	v17.01	STD	
imagePRESS C700/800	v05.02	STD	
imageRUNNER ADVANCE C33xx	v3.15	STD	
imageRUNNER ADVANCE 8405/8495/8485			
imageRUNNER ADVANCE 8505/8505P/8595/8585			
imageRUNNER ADVANCE 6575i/6565i/6555i			
imageRUNNER ADVANCE C5560i/5550i/5540i/5535i/5535			
imagePRESS C850/C750/C650/C65			
imageRUNNER ADVANCE C255/C355			
imageRUNNER ADVANCE C3530/C3525/C3520			
imageRUNNER ADVANCE 4551/4545/4535/4525			
imageRUNNER ADVANCE C256/356			

*1 AMS per la funzione di stampa non supportato in modalità locale/AD

*2 Funzione Secure Print/stampa protetta (stato lavori personali) non supportata

11.2 Elementi opzionali

11.2.1 USB Device Port

Si consiglia l'uso dell'accessorio USB Device Port per conservare al sicuro il lettore di badge. Questo accessorio fornisce due ulteriori porte USB e la possibilità di installare e alloggiare facilmente un lettore MiCard PLUS. I dispositivi A4 ADVANCE non

dispongono dell'accessorio device port opzionale. Per alloggiare un lettore MiCard PLUS in modo sicuro, utilizzare il lettore IC Card opzionale.



Codice articolo	Prodotti	Dispositivi supportati
5594B004AA	USB Device Port-E4	imageRUNNER ADVANCE C50xx/C52xx/C22xx/42xx/33xx
5594B003AA	USB Device Port-E3	imageRUNNER ADVANCE 4251i/4245i/4235i/4225i C50xx/C52xx/C22xx
5594B002AA	USB Device Port-E1	imageRUNNER ADVANCE C5255/C5255i/C5250/C5250i/C5240i/C5235i/ C5051/C5051i/C5045/C5045i/C5035/C5035i/C5030/C5030i/ C2230i/C2225i/C2220i/ C2220L
3720B001AA	USB Device Port-B1	imageRUNNER ADVANCE C5051/C5051i/C5045/C5045i/C5035/C5035i/C5030/C5030i
4790B001AA	USB Device Port-C1	imageRUNNER ADVANCE C2030i/C2030L/C2025i/C2020i/C2020L
5010B001AA	USB Device Port-D1	imageRUNNER ADVANCE 4051i/4045i/4035i/4025i
6866B001AA	Lettore IC Card Alloggiamento-A1	imageRUNNER ADVANCE 500i/400i C351iF/C350i/C250i

USB Device Port fa parte della dotazione standard dei dispositivi imageRUNNER ADVANCE 6xxx/8xxx PRO, C7xxx/C9xxxPRO.

11.2.2 AMS - Access Management System

Kit AMS

Per impostare il controllo degli accessi basato su utenti/gruppi, è necessario utilizzare un kit AMS. Access Management System è presente nella configurazione standard delle serie imageRUNNER ADVANCE C92xx/C72xx/C52xx/C22xx/C351iF/C350i/C350P/C33xx/C250i/82xx/62xx/42xx/500i/400i. Per altri modelli imageRUNNER ADVANCE, fare riferimento alla tabella seguente per conoscere gli elementi opzionali richiesti da ordinare.

1642B011AA	Kit AMS-B1	iR ADV C9070 PRO/C9060 PRO/ C7065/C7055/C5051/C5051i/C5045/C5045i/C5035/C5035i/C5030/C5030i/C2030L/C2020L/C2030i/C2025i/C2020i/8105 PRO/8095 PRO/8085 PRO/6075/6075i/6065/6065i/6055/6055i/4051i/4045i/4035i/4025i
------------	------------	---

Modulo aggiuntivo driver di stampante AMS

Per impostare il controllo degli accessi per i lavori di stampa da un PC Windows, è necessario installare il modulo aggiuntivo driver di stampante AMS (AMS Printer Driver Add-in Module) nel driver di stampa Canon (UFR II/PCL/PS). Il modulo aggiuntivo driver di stampante AMS è scaricabile dal Software Download Center (<http://software.canon-europe.com/>).

Versione supportata: Modulo aggiuntivo driver di stampante AMS vers. 3.1.0 o successiva.

Index

A

Access Management System 8

Active Directory 8, 38, 45

Aggiunta di un dispositivo 56

Attivazione 24

Autenticazione

 Modalità 36

B

Browser web 7

C

Certificato 57

Componenti 5

Configurazione 22, 33

Creazione di un rapporto 59

D

Declinazione di responsabilità 3

E

Elementi opzionali 66

F

File di registro 64

H

Home Folder 29, 30

I

ID reparto 44

Immagine Login 4, 34

 Immagine Login e Immagine Login + PIN 34

Importa 45

Installazione 8, 17

M

Mappatura ACL 44

MEAP 6

Metodo di autenticazione Dominio 3

Metodo di autenticazione Locale 3

P

Personalizzare 47, 50

Profilo vedere Utente 32

Proximity Card

 Login Badge di prossimità e Badge di
 prossimità + PIN 35

R

Requisiti 7

Rich Internet Application 6

Ruoli

 Preconfigurato 43

S

Sicurezza 62

Stampa protetta 64

Stringhe in lingua vedere Personalizzazione .. 50

System Manager

 ID e Password 33

 Impostazioni 43

T

Tabella costi 59

Tipi di login 4, 34

Tool di amministrazione23

U

uniFLOW

Upgrade64

Usage Tracker6, 53

Utente 26

Crea..... 26

Login con nome utente e password5, 36

Profilo 32

